Perceived Security and Usage of a Mobile Payment Application

vorgelegt von
M.A.
Hanul Sieger
geb. in Recklinghausen

von der Fakultät IV – Elektrotechnik und Informatik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
– Dr.-Ing. –

genehmigte Dissertation

Promotionsausschuss:

Vorsitzender:	Prof. Dr. Stephan Kreutzer
Gutachter:	Prof. Dr.-Ing. Sebastian Möller
	Prof. Dr. Matthew Smith (Universität Bonn)
	Prof. Dr. Yuval Elovici (Ben-Gurion University of the Negev, Israel)

Tag der wissenschaftlichen Aussprache: 16. Oktober 2015

Berlin 2015

Contents

Chapter 1

Introduction

Security, privacy, and trust are buzzwords in the computer industry today – and because nearly everyone uses a computer these topics touch everybody. Facebook has currently more than a billion frequent users, WhatsApp half a billion, and Twitter around 250 million, Apple's iTunes counts more than 800 million customers, Amazon 200 million, it is obvious that "being online" – communicating and buying – is part of a lot of people's life.[1]

Additionally, smartphones are everywhere nowadays as they surpassed traditional feature phones in market sales in 2013 (Gartner Inc., 2014). Capable all-purpose computers are in everyone's pockets and purses. Smartphones are used for a wide variety of tasks, among them gaming, navigation, listening to music, watching movies, surfing the web. Available applications for the predominant platforms, Android and iOS, are counting in the millions.

One interesting genre of applications emerged recently: mobile payment apps. While the idea and implementation of using mobile phones for payment transactions is certainly not radically new: SMS-based transactions are in use for several years now, the textbook examples being the introduction of *M-Pesa* in Kenya by mobile network operators Safaricom and Vodafone in 2007; NFC-based mobile wallets for public transport and payment services are common in Japan with the introduction of *Mobile Suica* by mobile network operators NTT DoCoMo and au in 2006 (now also offered by SoftBank Mobile and Willcomin). These apps are among the first wave of using mobile phones and smartphones as generic payment devices for general-purpose payment transactions. Besides ordering online through websites and apps – more and more via mobile devices, like smartphones and tablets –, in the last few years a new kind of financial application came up, that transforms smartphones into digital equivalents of payment cards at the point-of-sale, for example in retail stores, restaurants, and at vending machines. These payment apps are considered to be on the verge of wide-spread use, and insights into how they are perceived by the user are an advantage for further development.

Think about your wallet or your purse. For example, the wallet of the author contains the following items: ID card, emergency certificate, driver's license, health insurance card, two debit cards, one credit card, several membership

[1] WhatsApp Blog, April 22, 2014 – blog.whatsapp.com/613/500000000; Twitter Company Profile, Nov 5, 2014 – about.twitter.com/company; Apple Inc. 2nd fiscal quarter of 2014 conference call – www.macrumors.com/2014/04/23/q2-2014-apple-earnings/.

cards (gym etc.), and cash. There are also some phone numbers and family photos. The wallet is not secured against theft or misuse, if lost. One has to call up several places to get all the cards deactivated, while the cash and data like personal and contact data, and the photos are totally unsecured. Concerning mobile phones, this author's phone has the following data and applications: complete list of contacts, several hundred photos, several thousands songs, a dozen videos, a browser with history, notes and voice memos, access to e-mails, access to an on-line store for music, videos, and applications, and access to personal data in cloud-based storage. The default setup for this phone is to secure access to the cellular network via a 4-digit PIN for the SIM card. All other data is open by default.

Wallets and phones are carried almost all the time by people. Both are very personal belongings. Sometimes, they are given to children, the spouse, a friend, or relatives. And in both cases, you do not want them to flip through all of what it is in them. Other than the wallet, it is relatively easy to implement additional security measures on a smartphone. One can build a wallet out of steel and secure it with a lock, but this approach would be apparently very inconvenient in daily use. The questions are, whether it is possible to offer additional or alternative security methods on mobile phones that are both secure and usable, and how those offerings might alter the security perecption of potential users.

Security and privacy issues are currently topics discussed from scientific community to mainstream media, e.g. TIME Magazine's cover story on Facebook privacy (Fletcher, 2010). Mobile phones – especially smartphones – offer ever increasing internet connection and social network applications, and how to handle security (and privacy) is an ongoing debate.

All these new mobile ways to pay for goods offline and online are also under "attack" from different sources, which are currently extensively covered in the media. Just to name a few high-profile cases of the last few years: the NSA scandal is a direct assault on privacy including personal financial data; the turmoils involving the crypto-currency Bitcoin touches on the topic of financial stability, in the case that all transactions becoming purely virtualized (cash at least uses a physical token); the security breach of Sony's Playstation Network shows that payment data can be compromized; and a security software failure like "Heartbleed" exemplifies the vulnerability of authentication methods. Users are constantly pointed towards computer security, to think about secure authentication and to encrypt personal data and communications. One of the seminal books on the practice computer security, "Hacking Exposed", dedicates more than 70 pages in its current 7th edition on the subject of "Mobile Hacking" alone. (McCLure et al., 2012)

In this environment, several questions about security, privacy, and trust arise almost naturally: What kind of security methods are *perceived* as secure? How can they be implemented? Will the user refrain from added security due to those methods also adding inconvenience, in other words because their usability is low? What can be done to support hardware and software developers to build devices, applications, and – in the special area of this research – mobile payment apps, which address the important security issues of financial transactions?

For several years, the question how security features of computers are perceived and how they can be made usable, is at the center of research of usability and security (sometimes referred to as usable security).

Those questions touch everyday life. Business observers expect smartphones to be the mobile digital wallets replacing the physical ones, and the change will happen in the near future. Only made possible with current technology, a mobile wallet combines all the credit and debit cards, vouchers, coupons, membership cards, event and mass transit tickets, and keys to homes and cars. What is not possible in a physical wallet with a stack of plastic cards, cash and paper coupons, can be done in a wallet app: interaction between features. On the other hand, the technological advancements of smartphones make it also possible to use a mobile payment app without user interaction.

In an emerging market like mobile payment – fragmented and with no clear predominant platform or standard at the time of this writing – the service often "wins" economically, which offers the best user experience, cost-benefit ratio, or – sometimes – a perceived "coolness" factor. It is therefore of great importance to address the key features of an app in the right way as soon as possible to appeal to as many customers as possible. One of the key features of a mobile payment app found in surveys (prior to the availability of mobile payment) is how the user perceives its securiy (Ben-Asher et al., 2011). This is well-established in several studies as in Dahlberg et al. (2008) and Sieger et al. (2012).

Getting security of a payment app right in the way that it is *perceived* as secure can be an advantage in competing within the market. Thus, it is both academically and economically interesting to find key factors, which influence the perceived security of mobile payment. Academically, because it alters the way how people pay and this affects everybody's daily lives, and it may make people more traceable without the anonymity of cash, which also touches the perception of security and privacy. Economically, because the payment industry is a multi-billion US dollar business and getting a stake in it can be very profitable.

1.1 Definition of mobile payment

The aforementioned broad usage scenarios also show, that there is currently no clear definition what counts as mobile payment. In the broadest sense, mobile payment happens whenever a payment transaction occurs using a mobile device. Examples for these use cases are: paying for goods in an online shop using a laptop computer, receiving payments using a credit card reader dongle attached to a tablet computer, paying in a small supermarket using an SMS-based closed-loop payment system.

In this thesis mobile payment is used for the task of making generic point-of-sale-based payments using a smartphone. A point of sale, short POS, is a physical location for payment transaction such as a cash register. The app may contain other features not directly related to payment, or the payment feature may allow to make other forms of payments like closed-loop (e.g. cantinas), peer-to-peer, or online. But the feature being focused on is basically the use of an app as a substitute for cash or card-based payments in retail stores.

Payment devices other than cash like checks, cards, and apps were always tied to a security method, being it a signature, an ID card, or a PIN. All these methods have been compromized, and users have their own perceptions of those methods' security, whether this is influenced by personality, experience, media, or immediate context of the payment task. This thesis' focus is on possible influences of personality traits, experience, and environmental context.

1.2 Security concepts of mobile phones

Smartphones are not a new device category built from scratch, but rather follow a long evolutionary path, rooted in software and hardware concepts going back to the early days of personal computers.

This section tries to establish a point of view on the "historical causes" for the recent state of smartphone security, the developer's "mind-set" and the user's security perceptions of the implemented security features. This can be viewed as being more of an interpretation (in terms of reasoning) of the historical facts, than executing a "proof". Computer science can now look back at several decades of existence, and thus, it is possible to highlight certain patterns, which evolved in theory and practice.

Most historical views of computer security focus either on the timeline of security concepts and methods or on the "hacking" of the implementation of those concepts (see Computer Security Laboratory of the Computer Science Department at the University of California (1998)), but not necessarily what *leads* to certain implementations of security methods. The following sections present a view on the historically available security methods on (mobile) computers until today's smartphones. What is new in this presentation is that it combines a perspective on the developer's mindset, which lead to the implementation of security methods with the hardware and software available at the time. The developer mindset is drawn from available interviews, manifests, and "philosophies" and is of course not a given hard fact like the date of a first-time implementation of a certain security method. But adding this into the picture enhances the understanding of the current set of security features available on smartphones.

There is an evolutionary path from interactions with a computers which are very close to how the machine itself works (e.g. programming bit for bit using flip switches) to increasingly more human-like interactions (e.g. speech recognition). Also, especially in personal computers, the devices became increasingly smaller, forbidding "traditional" interaction using a keyboard (with or without a pointing device for graphical user interfaces) and a display.

The big-picture development can be described as going from desktop computers to mobile ones with form factors getting smaller (laptops/notebooks, PDAs, mobile phones, smartphones) and further to wearables and ambient computers (embedded into every-day objects). The interaction evolves from specialized human-computer interaction to more human-like interaction (arguably still in its infancy) with speech-recognition applications like Apple's Siri, Google's Google Now, and Microsoft's Cortana. "Visible" security methods like PINs and passwords fade into the background, replaced by more "natural" ones like fingerprint or voice recognition.

The application used in the experiments of this work is a prototype mobile payment system installed as an application on an Android-based smartphone. A large part of the user's reaction to the payment application might be influenced by the overall perception of security of such devices. Today's smartphones combine two lines of heritage, mobile phones and personal computers. To set the historical context, in which some of the parameters for the user's perception are set, a short outline of the history of security on smartphones is useful.

The security features of mobile computing devices are rooted in their development as derivatives of desktop operating systems and in hardware constraints due to their size. Additionally, some users view the smartphone as an extension of the mobile feature-phone whereas technically it is a miniaturization of a desktop computer. Younger users may not know any other mobile phone concepts other than smartphones.

Due to these roots and the traditional lack of security on mobile feature-phones most smartphones do not implement features recommended by security experts, among them strong (biometric) authentication mechanisms and encryption by default. The state of desktop computer security is about to be extended to smartphones.

Three areas can be identified, which are each responsible for the lack of strong security mechanisms on smartphones (and mobile computing devices in general): 1. The user's lack of awareness for security issues and inappropriate behavior (sometimes called "lazy" or "uneducated" by security experts). 2. It makes no economic sense for the user to follow all security recommendations. 3. During the historical evolution of mobile computing devices to the currently available smartphones, developers and users could not develop a "mindset" for special security on mobile devices.

The first point seems to be a common understanding (up to being a textbook cliché) of security experts (Cranor and Garfinkel, 2005; Young and Simon, 2006; Collins, 2010), the second point was brought up by Herley (2009), and the third is presented in the following section.

1.2.1 Evolution of smartphones

Mobile computing devices exist for more than 30 years, if you think of the Osborne 1 as the first truly portable general-purpose computer, first offered in 1981. While it could not be operated without plugging it into an AC outlet, the computer was designed to be lugged around by a single person. It ran Digital Research's CP/M operating system (OS) offering no security mechanisms. As it had not any built-in storage device other than floppy disk drives, data could be seen as secure as long as the floppy disks were stored separately from the machine. A lot of the early home and special-purpose computers of the 1970s and 1980s could be seen as portable in the sense of weight and dimensions (for example, Apple sold special carrying bags for the first Macintosh systems), but they were either desktop machines requiring further equipment to operate, or only provided special functions like word processors, calculators etc.

It took several more years until the design standard of the modern laptop computer was established with the advent of the Apple PowerBook 100 in 1991 emerging from designs found in its predecessor, the Macintosh Portable, and similar early portable computers like the Atari STacy (both released in 1989), and Datavue Spark (1987). In contrast to earlier systems like the Osborne 1, Compaq Portable (1983), Commodore SX64 (1984), Apple IIc (1984, with optional LCD), Hewlett-Packard HP-110 (1984), and Toshiba T1100 (1985), these devices had built-in batteries, a recessed keyboard, a pointing device, and an LCD with backlight and resolutions similar to desktop computers, allowing truly mobile computing (Freiberger and Swaine, 2000; Hertzfeld, 2004; Laing, 2004; Bagnall, 2006).

Shortly after the breakthrough of the laptop computer concept, a new class of so-called personal digital assistants (PDA) emerged in the form of the Apple Newton (1993) and Palm Pilot (1996). While there were certainly numerous "pocket computer" systems available before, which were capable of providing the same functions in a similar small package (e.g. Sharp PC-1210 (1981), Cambridge Computers Z88 (1988)), the new PDAs emphasized screen real estate and pen-based, hand-written input.

One could easily view modern smartphones (mobile phones with a general-purpose operating system allowing the installation of additional and third-party software, the IBM Simon being the first such device coming to market in 1994) as an evolution from the PDA class. While there certainly were and are types of smartphones which followed this path (e.g. Palm Treo, Nokia 9000 and N series), it will be shown, that today's major players in the smartphone market evolved from the laptop concept and thus are direct descendants of the desktop computer.

Except for variants of the UNIX operating system, the main actors of the emerging home and office computer markets of the 1970s (Apple, Atari, Commodore, IBM, Compaq on the hardware side, and Apple, Microsoft and, to a lesser extent, Digital Research on the software side) had no security built into the hardware and software of the their machines. Digital Research's CP/M, Microsoft's MS-DOS, Apple's Pro-DOS and Mac OS did not have any password protection, encryption, or any other security measure at all. Many of the machines sold in this era (1976-1989) did not have anything, what is considered an operating system as many of them just booted into a BASIC interpreter, which offered commands to interact with the I/O of the computer. IBM's foray into the micro-computer market established MS-DOS as the predominant operating system, first for business use and later also for home use. The second big player in this field were Apple's ProDOS and Mac OS. Portable devices running CP/M, Atari's TOS, and several BASIC Interpreters can be neglected as they were limited to a niche market with very little devices and did not last for a long time. Also, they had no impact on the design of portable computers and operating systems. The same goes for other popular operating systems of the 1980s and early 1990s, as there were virtually no portable devices running them, namely AmigaOS, OS/2, BeOS, and UNIX.

In the 1990s the predominant operating systems used on mobile computing devices were MS-DOS with Windows 3 to 98, and on the business variant Windows NT (using a new kernel and providing some security features). The emerging market for so-called personal digital assistants (PDA) had offerings by Apple, Palm, Psion and others using little security features, if any, usually PINs and passwords. Some specialized UNIX offerings on the market (portable RISC-based workstations featuring proprietary UNIX variants like SunOS/Solaris or HP-UX) and the rise of Linux and some BSD UNIX variants left no discernible mark in this decade to develop a consciousness for extra security on mobile devices.

A compressed version of the intertwining paths of software, hardware, security concepts, and security methods is depicted in Figure 1.1. While far from being complete, it shows that concepts from different fields were adapted as computers got smaller and mobile.

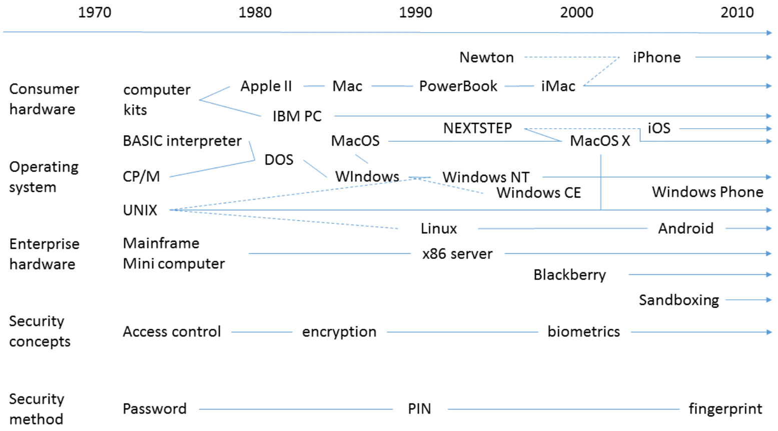


Figure 1.1: Evolution of selected hardware, software, and security methods leading to current smartphone designs

A pattern how computer security was handled emerged from the UNIX philosophy (Gancarz, 2003), its successor in the open source movement (Raymond, 1999), and up to Google's former approach of "Don't be evil" in addition to its rapid development cycle of trial and error (or of "perpetual beta").

Mobile computing devices have additional security risks opposed to desktop computers, as they can be more easily lost, stolen, or accessed by "attackers". Attack vectors are multiplied by the use of mobile devices in open, public, and crowded places from shoulder surfing to network interception.

On the other hand, they were (and are) built to provide the same work as a desktop machine and are thus bound to what the operating system has to offer, the main purpose being a "desktop" computer able to travel with. The operating systems used on mobile devices were the same used on desktop computers and no security features were offered that could strengthen mobile computers against the added risks. As the predominant operating systems, Microsoft Windows and Apple Mac OS, were build to be operated by a single user (in contrast to UNIX and UNIX-like operating systems, which were multi-user), no strong security mechanisms were at hand (if at all). But the UNIX concepts evolved in the 1960s and UNIX's modular *everything-is-a-file*-concept was vulnerable. For example, a machine's user password file was in a known location at `/etc/passwd` and unencrypted. It could be read and manipulated directly using a text editor. Security advancements of such a system are often "bolted on". If the password file would be encrypted, it would still be in a known location and attackable by brute force methods. If the password file was moved around, hidden or randomized, it would defy the design philosophy.

The last 25 years (counting the 1980s as an era of trial and error) of mobile computing (laptop computers, PDAs, and cell phones) can be traced back to be rooted in hardware and software not suited to provide security features. At least the years (1980s to 1990s) until the advent of Mac OS X and Windows XP in 2001 saw no operating system for personal computers in widespread use, which could provide any reasonable security feature. And only recently the hardware is strong enough to provide on-the-fly encryption of storage devices without severely affecting the user interaction (although there is still a performance penalty, see Collins (2010)). Still, the existence of "forks" or enhancements with a special (and advertized) focus on security like OpenBSD and SELinux (see Shabtai et al. (2010) for an Android implementation) underline the notion of the "commonly used" or standard operating systems to be vulnerable.

The same mechanism can be seen going on in the smartphone area, were the current operating systems are often derivatives of either UNIX-like OS (Google's Android and Apple's iOS) or Microsoft Windows (Windows CE, Windows Mobile, Windows Phone). Early operating systems created solely for the purpose of driving mobile computing devices (usually PDAs) like Palm OS, Symbian, and Blackberry OS are platforms already abandoned or in decline.

Even an operating system like Google's Android is (as a Linux derivative) firmly rooted in the desktop computer area. It is not suggested that desktop OS derivatives developed for PDAs and smartphones are the same in the way the OS used on mobile computers are identical to their desktop counterparts. Operating systems on smartphones and desktop computers share the same architecture including how the OS is structured and how data is organized and manipulated. Although the user interface is heavily adapted to the different screen size and (often) lack of keyboard, they try to be as similar as possible for a familiar look and feel through identical icons, derivatives of popular applications and so on.

There is also a common code base and APIs to ease software development, although smartphone operating systems are nonetheless stand-alone systems with no binary or full source-code compatibility to the desktop OS they were derived from. A technical example for the heritage from a desktop OS can be identified by looking at iOS as being a direct descendant of NEXTSTEP (the predecessor of OS X), which was conceived in the mid-1980s as a desktop operating system for general purpose workstations aimed at the academic market (Young and Simon, 2006) and itself is heavily influenced by BSD UNIX. Many of the API calls of iOS still have the same "NS" prefix found in NEXTSTEP, e.g. "NSBundle" (Garfinkel and Mahoney, 1993; NeXT Computer, 1994; Davidson and Apple Computer, 2002).

Further proof for the heritage of iOS from its desktop counterpart OS X can be found in the fact, that both are intertwined in the Mac OS X and iOS reference libraries with iOS treated as a subset of OS X. Especially concerning security concepts, it shows that little additional security methods are introduced, which may cater to special needs of mobile devices (Apple Inc., 2014a,b).

Google Inc.'s Android (and other Linux-based smartphone OS like Nokia's and Intel's MeeGo, and Palm/HP's abandonded WebOS) can also be added to the list of operating systems for smartphones derived from a desktop OS. Google's initial business model is aimed at the desktop (or at least relied on reasonable screen size) by providing advertisements next to web search results. The choice of Linux as the underlying platform is also deeply rooted in desktop computing.

This strongly supports the paradigm of smartphones as miniaturized desktop computers, inheriting those security frameworks. Major smartphone vendors extended they initial business model from desktop to laptop computers and then to smartphones. Along the way, their main interest was to appeal to existing customers and developers, thus creating a known desktop-derived environment for their respective mobile platforms.

1.2.2 Developer issues

It can also be argued that the main developers and their “philosophy” have a strong influence on the security aspects of an operating system. The philosophy behind UNIX and UNIX-like operating systems has its root in the late 1960s’ academia and counter-culture, which emphasized trust, sharing, open communication, and collaboration, thus de-emphasizing security (Levy, 2001; Gancarz, 2003; Turner, 2006). It has to be emphasized that these initial developers were both users *and* developers, building tools for their own work or amusement. An influential part was the UNIX variant distributed as the *Berkeley Software Distribution*, which originated at the University of California, Berkeley and is still part of many UNIX flavors including Mac OS X (and hence iOS) as the forked *FreeBSD*. The Linux and open source movement now prevalent (as Google’s Android) have its origins in the same spirit (Torvalds and Diamond, 2001).

Thus, the developer’s mindset is still rooted in desktop computing (or even way back to time-sharing systems). For example, both iOS and Windows Mobile/Windows Phone support this mindset by providing the same integrated development environment, programming language, and similar APIs and structural concepts as the desktop OS counterparts (Apple Inc., 2014b). Microsoft states on its website, that Windows-based mobile devices share much in common with “desktop Windows”, although, of course, there are also some differences in the user interface (Microsoft Corporation, 2014).

Notable exceptions from this desktop computing derived path are foremost Blackberry Inc., which primarily addresses the business market with its Blackberry devices, and start-ups like Blackphone, which uses a security and privacy enhanced version of Android. Evolved from a single-purpose device to deliver mobile e-mail to corporate users, Blackberry devices are now full-featured smartphones. Security features include PINs, strong password authentication, and encryption, mainly driven by business demands. But as of 2014 the platform is commercially in steep decline.

Makers of smartphones and their operating systems try to appeal to their large base of existing developers for general computing operating systems, and thus, cater to their mutual desire of a flat learning curve in developing for a smartphone OS. Despite this lack of security, the probability of a threat for smartphone users is very small at the moment (Herley, 2009; IC3 Internet Crime Complaint Center, 2010), but will likely increase in the future, if projected from desktop computing’s security history and the growing capabilities of smartphones, especially multitasking. It may be interpreted as a sign of an economic rationale to not implement recommended security features as long as the numbers of successful attacks on smartphones are low.

Of course, the aspects of security and privacy are addressed, but rather than making the operating system inherently secure, Android and iOS are foremost made more secure by restricting how applications can be installed. The most effort in securing the devices is essentially a manual service done by Google and Apple: curating what is avalaible on the app stores. Further, running every application in its own “sandbox” with limited access to the file system and restricting ressource usage to APIs enhances security. This design decisions still allows, for example, unencrypted messaging or plain password transmission. It is not enforced on developers to program for security.

While nearly all smartphones shipped world-wide run an operating system developed by companies with a strong background in desktop computing, the user gets his or her smartphone as a replacement for a mobile feature phone, not to substitute a mobile or desktop computer (although this differentiation my vanish over time as more and more first-time users already start with a smartphone). The development approach (and the user's view) of smartphones combines two historically evolved traces of how security is handled on mobile computing devices (as a legacy of desktop computers and mobile phones, which both did not see a need for additional security). Desktop computers do not face the extra risks of mobile computing devices and mobile phones usually have nothing valuable to protect (besides the cost of the device itself and access to the carrier network, which is sufficiently secured by the SIM PIN).

Taking the state of security on desktop and laptop computing as a sign of how developers (and users) act on the growing security threat, it can be safely assumed that this will not change with smartphones. Despite viruses, e-mail scams, credit card fraud, rip-offs at online shops, auctions, classified ads, and governmental surveillance, people still use computers for these tasks. There is no reason to believe this attitude to security will change while using smartphones and mobile payment apps installed on them.

There are and were hundreds of mobile payment apps planned, launched, and already cancelled in the past few years. Some prominent examples in the United States are: Google Wallet, Apple Pay, MCX CurrentC, Square Wallet, Dwolla, Clinkle, and LevelUp. In Europe: Deutsche Telekom MyWallet, O_2 Wallet, BASE Wallet, Vodafone Wallet, Cityzi, Turkcell Cep-T Cüzdan, PayPal, and Yapital. In Asia: Sony-developed Osaifu-Keitai/FeliCa (the *de-facto* standard in Japan supported by several mobile network operators), and SK Telecom Smart Wallet. A mobile payment application is not a niché product anymore, but gaining increasing attention. Thus, any application's (weak) security being compromized once mobile payment is mainstream will probably be scandalized by the media like any other security breach involving privacy issues. A usable and strong security method will be an important feature to choose and implement during development.

1.3 Security perceptions and usable security

Computer security in general describes features of computer systems which secure the confidentiality, availability, and integrity of processed and stored data. Among these features are procedures to authenticate and identify users (e.g. login passwords, biometric authentication), methods to encrypt communications and data (e.g. e-mail cryptography, Secure HTTP, hard disk encryption, firewalls), or software to fend of unauthorized access (e.g. anti-virus software). All these features may also be capable to defend the user's privacy by providing her or him full control over the data.

This research focuses on the user's perception of security (features) of computer systems, e.g. graphical user interfaces, or biometric sensors, in the context of the use case "mobile payment". A mobile payment system touches several aspects of this work's aim: It covers (mobile) computers and it incorporates payment as a task sensitive to the user's security concerns (and also privacy and trust). Surveys done prior to the experiments by this author in collaboration with N. Ben-Asher et al. (Ben-Asher et al., 2011) showed that "Making eWallet payments" lead by a wide margin as considered a very sensitive function to use on a mobile phone.

The user's perception of computer security varies along many parameters, among them knowledge, experience, exposure to media coverage, influence of colleagues, friends, and family, changes in hardware, software, and device categories, introduction of new use cases and concepts, and vanishing of once common things. All this cumulates into a mental model, "folk models" according to Wash (2010), which may change over time.

It may also be the psychological aspect of the mobile phone's all-day use and proximity (it is usually carried and used very close to the body), which makes it a "close companion" and leads the user to overestimate trust and security (West, 2008). There are a number of studies on user perception and preferences regarding security on mobile and smartphones. Recent focus group discussions and web surveys showed little demand for additional security features, with most users leaning towards fingerprint recognition as an alternative authentication mechanism and the ability to further restrict access to certain applications (e.g. e-mail, text messages, see Furnell and Clarke (2005); West (2008); Dörflinger et al. (2010)). Chin et al. (2012) found that people are less willing to access their bank accounts on a smartphone ("mobile banking") than on a laptop. The main fears were physical theft, data loss, malware, and wireless network attacks.

At this point of using a mobile payment app, the two mental models (or mind-sets) of user and developer meet, although they necessarily do not have to overlap. Mobile payment apps build upon the infrastructure provided by hardware and software vendors, whose historical development was described in the previous sections. User perceptions are influenced among others by personality, knowledge, experience (their own, and others), social norms, and media exposure, but all are set within the historically developed context of computer security.

When thinking of usability of computer systems, often ergonomic aspects come to mind: user interface guidelines, keyboard layout, hardware design of input devices. Here, the focus is on the area of user experience, which involves the perceptive experience of use and some hedonic aspects of it (also called "joy of use"). The main research topic of this work is the user perception of security using a mobile payment system. Since the interaction with a mobile payment system is often aimed to be as short as possible, "traditional" tools to track user interaction like keyboard input, eye movement, and time keeping cannot be used. These *micro-interactions* are carried out almost instantaneously. In its extreme form a mobile payment application does not require any user interaction. The app "checks the customer in" based on location-tracking or via radio-based information send by the store (e.g. using Bluetooth Low Energy beacons), and the customer is recognized by a photo. Example applications are PayPal and Dwolla (see also Dodson and Lam (2012) for a proposed NFC-based class of small exchanges between devices).

How do users react to these offerings? Do they find it to be a convenient way of making a purchase? How do they perceive the security of their financial transactions using a smartphone and a wireless transaction route? What do they think about privacy issues? Can predictive modeling of those perceptions be done to develop better software? Is there an added value besides exchanging a plastic card or cash with a phone? Which problems are solved by shifting the payment method onto an app?

A possible user reaction could be “I like the convenience of paying with my smartphone, but I feel really bad about my data security”. In this case, the overall experience of using the device as a payment system is diminished, even though the usability of the payment application is perfectly fine. So, how do user perceptions of security influence the use of the device as a payment system? And what factors influence the user to perceive security as he or she does? What models can be derived from empirical data? Those questions will guide the theoretical and empirical parts of this work.

The idea of securing computer systems and in doing so making the process or method usable for the user is a relative young field in academic research. The seminal textbook by Lorrie Faith Cranor and Simson Garfinkel “Security and Usability: Designing Secure Systems That People Can Use” (Cranor and Garfinkel, 2005) classifies three papers from the late 1990 as “classics”. Each topic for itself, security and usability, is something hardware and software designers, programmers, computer scientists and specialists work on – and users struggle with – since the late 1960s. Combining both approaches into “usable security” could be seen as trying to achieve the impossible, because intuitively securing a system (e.g. asking for authentication, validation, and encryption) involves additional effort for the user, which is the opposite of what usability aims for (Cranor and Garfinkel, 2005).

Scientific research focusing on usable security now spans 15 years. The main body of published work centers on authentication and encryption, but moved on to a broader vision in recent years, especially user perception.

Usable security in its broadest sense encompasses all interactions by humans with a computer system, which involves any kind of security mechanism ranging from authentication to encryption. In this sense, “usable” refers not only to the concepts of usability, but also to the more general notion of user experience. (Hartson and Pyla, 2012).

The requirements for security and privacy of computer systems have increased significantly in the past years, often due to the development in mobile devices, internet-based services and social networks. Next to the purely technical aspects of security issues the lack of appropriate user behavior is the main cause for experiencing attacks, phishing, malware etc. (Fischer-Hübner et al., 2010; McCLure et al., 2012) whereas “cause” is not meant to be deprecatory. Some reasons assumed by experts to be responsible for reducing security awareness are the improper use by the uninformed layperson (Adams and Sasse, 1999), the low level of usability of computer systems (Tognazzini, 2005), and the low cost-benefit-ratio of the assumed risk compared to the increase in effort of raising security (Herley, 2009).

There are numerous cases of data breaches involving smartphones and with more and more data added to cloud-connected smartphones, pure statistical probability will eventually lead to growing attacks. The vicious cycle is the user’s and developer’s historically evolved view on security, the psychological effect of feeling safer than statistics advises, and the relatively new emergence of smartphones as a mass market. The main focus of research in the area of security on smartphones and mobile phones is on authentication mechanisms, especially biometrics, and usability, although, as can be argued, this somehow contradicts the development roots of smartphones. This may explain why so little progress is seen in this area. Security experts should be aware not only of the user's view, usability aspects, and security threats, but also hardware constraints and development history.

In order to address security and privacy of computer systems it is helpful to analyze and formalize user behavior and to identify relevant parameters (or influencing factors). These parameters should be considered during the design of a system or a software application. One goal is to provide a tool for the system designer to anticipate and then eliminate (or at least minimize) design flaws in terms of usability. This would make it easier to reach a good balance between the often conflicting aspects of usability and security.

1.4 Application and infrastructure

The hardware and operating system are the ground-work upon which applications are built. It is of course possible to extend both hardware and software, but this is limited to fundamental components like CPU, RAM, and I/O. For example, it is possible to extend the memory of a (now vintage) 8-bit system beyond 64kB of RAM through bank-switching, but the systems is still only capable of using a (theoretical) maximum of 64kB at once.

In this sense the evolution of the hardware and its operating system leading to the smartphone of today is also the limitation of its applications. Especially the development of smartphone apps is restricted by principles governed by the platform vendors. Implemented security methods have to obey these rules. For example, the fingerprint sensor introduced with the Apple iPhone 5s could not be used by third-party applications prior to iOS 8. Thus, any third-party mobile payment developer had to stick to the available security methods, meaning in this case essentially PIN and password.

Mobile payment application are also under close scrutiny of fincancial regulatory bodies, both public and private. They are also under close scrutiny of any (possible) user. Financial transaction are very closely observed, if they obey security and privacy rules. Any doubts about the security (or even a real security breach) of the underlying device, its operating system, and the application itself would deprive it from its required certifications and would be perceived by customers (and others) as untrustworthy.

Any developer of a mobile payment application (especially third-party developers e.g. a bank, a mobile network operator, a retail company) is limited by the evolution of the smartphone and its current state, and by any further restrictions of the hardware manufacturer and software provider to access the security interfaces and methods.

The available methods influence the perception of security of those devices and their applications. This is underlined by several studies presented in Chapters 2 and 3, among them papers co-authored by this author.

It would be helpful for developers to have a guideline what to choose from the available methods. For example, whether PIN, password, fingerprint, or iris recognition should be used as the application's default security method.

The main focus of this research is to find relevant factors which influence the security perception of users interacting with a mobile payment app. To test the area where – according to the taxonomy presented later on – influencing connections should occur, a prototype mobile payment system from Deutsche Telekom was used.

Empirical studies on usability and security of mobile payment have to conform to several constraints. Beyond the usual budget constraints within research projects the main reason to conduct laboratory-based experiments was that there was no significant infrastructure usable for a field test at the time of conducting the experiments (from mid-2010 to mid-2013).

At the time, when the experiments were started, no mobile wallet using the existing payment network was on the market. Of the then-four German mobile network operators, the first wallet system was launched by Telefonica Deutschland under their O_2 brand as the O_2 Wallet in early 2013. But this product was not advertised and had to be actively requested by its customers (underscoring this, was the exclusion of the product's website from Google search via its robot.txt). This was followed by Vodafone Deutschland at the end of 2013. MyWallet by Deutsche Telekom, the commercial successor based in part on the prototype used in the experiments, was launched in May 2014. E-Plus Mobilfunk (merged with Telefonica Deutschland in October 2014) launched their mobile wallet products BASE Wallet in July 2014. The fact had to be taken seriously that most people (not having experienced any comparable systems) do not have preconceptions about new technology prior to exposure.

It was essentially attempted to measure two outcomes to collect data: How many goods a participant bought using the mobile payment app, and how she or he rated the perceived security of this payment method. These are the dependent variables. The hypotheses assumed that there are dependencies on a number of factors, among them personal traits like risk perception and technical affinity. These were the independent variables.

There are several technologies to introduce smartphone-based payment. The one used for the experiments described here is an extension of the contactless payment card and is based on Near Field Communication (NFC) and a SIM-card-based secure element to store card data.

Other offerings use Quick Response (QR) codes, either scanned by the POS system or by the smartphone app. Also, systems using transaction authentication numbers (TAN) and face recognition are on the market. These variants can be divided in the following thre categories:

- Closed-loop systems, where the connected payer (e.g. customers) and payee (e.g. retail or online shops) transfer money primarily within the payment system (e.g. PayPal, Starbucks, cantinas with prepaid cards). Getting access to money from outside the closed-loop system requires a second step (e.g. transferring to or from a bank account).

- Cash or card substitutes, where money is transferred directly from the payer's bank account to the payee's bank account, but without using an existing (card-based) payment network (e.g. CurrentC)

- Cash or card substitutes, where the existing payment system is used (e.g. NFC-SIM-based mobile wallets).

In this thesis an NFC-based mobile payment system of the last type is used. There are multiple reasons for choosing this system for research over alternative mobile payment systems. It is an evolutionary extension of an established payment system. It is backed by international standardization bodies, among them Groupe Speciale Mobile Association (GSMA), European Telecommunications Standards Institute (ETSI), and EMVCo (American Express, Discover, JCB, MasterCard, UnionPay, and Visa coordinating the EMV specification for worldwide interoperability and acceptance of secure payment transactions), and it is not tied to a singluar vendor, e.g. Google, PayPal or Starbucks. It can be used world-wide at retailers using already implemented systems. At the time, when this research was started, several mobile network operators in Europe, Asia, and in the United States were in the prototype and test phase of NFC-based mobile payment system. These systems were considered to be the most promising form of mobile payment. As mentioned, some of these systems were brought to market in 2013 and 2014.

In its current implementation, these solutions transfer the payment card paradigm essentially 1:1 to a smartphone app. The payment card is visually virtualized – instead of a plastic card, the user sees a virtual representation of a plastic card. Basically, it is a simple rendering of a personalized plastic payment card.

The card paradigm is the nearest to the existing payment card system. The user can easily understand the connection between the widely used plastic card and its transformation into its virtual form within a payment app.

1.4.1 Ecosystem of card-based payment systems

To understand why the experiments were done in a lab environment, an overview of the required infrastructure of a mobile payment system is helpful.

The mobile payment system used here is in its core an extension of the card-based payment system that has been installed for decades with a variety of credit and debit cards, which itself evolved from cash-based and cheque-based (including debt notes) transactions. Mobile payment is basically an EMV-chip based plastic payment card transferred into another form factor using the same logic and processing infrastructure.

The difference between credit and debit card is how the bills are paid by the customer and user of the card. Credit cards usually grant a line of credit to the customer. All accumulated purchases using the credit card are then partly (revolving credit) or in total (deferred debit) billed to the customer in a given timeframe (usually monthly). A debit card purchase will be deducted individually and immediately from the customer's bank account. There is no line of credit on the card itself (but there could be one on the account associated with the debit card).

A card-based transaction usually involves either a so-called point of sale (POS) terminal connected to a payment processing network via telephone line (landline or mobile) or through an IP-based network. Alternatively, the transaction is done by person via telephone or over the internet. Depending on the presence of a cashier or sales-person at the point of sale, the transactions are divided as being "card-present" (the cashier sees the physical card and bearer) or "card-not-present" (the sales-person cannot see the card, e.g. via telephone or internet order). There are different methods how a transaction is processed. It may be batch-processed, when the (cash) register is closed, e.g. when a shops closes in the evening. Or it may be processed in real-time.

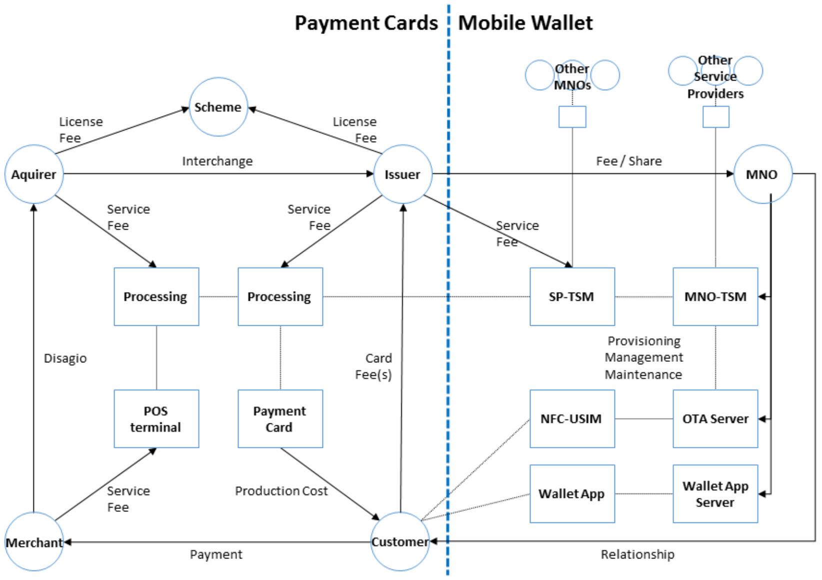


Figure 1.2: Eco-system of NFC-based mobile payment[2]

A credit card payment system is controlled by a payment processor, who regulates how financial transactions involving the credit cards have to be processed. Those rules include technical specifications of how the payment is processed as well as other issues like fees, card appearance, acceptance and branding. Payment processors operating world-wide include the aforementioned EMVCo members, who dominate world-wide credit card processing and standardize technical specifications. Those specifications regulate card size, magnet stripe, chip, operating system, data size, data content, and encryption. They also regulate POS terminals, data transfer, and data processing. Further, all involved hardware and software has to be certified by the payment processor. For data processing, data centers have to obey a set of security rules (PCI Security Standards Council, LLC, 2013).

The technical specification for mobile payment extends the existing electronic contactless chip-based credit and debit card transaction. Prior to chip-based cards magnetic stripes stored the customer's payment information. Magnetic stripes are still in use in parallel to chips, but are in the process of being phased out due to the ease of manipulation. Then, chip-based card transactions were extended to use so-called contactless readers, which rely on Near Field Communication (NFC).

There are a number of country-specific implementations in Germany, mainly the use of a national payment processing scheme called "girocard" (formerly known as "Electronic Cash", or short "EC"), which is incompatible with other payment systems used around the world. For this reason most girocards are co-badged with payment schemes available world-wide, namely Mastercard's debit card scheme "Maestro" or Visa's "Vpay".

[2] Adapted from invited talk by the author at "4. Unisys Client Exchange", Essen, November 11th, 2013.

Mobile payment applications including the prototype used for the experiments require certain infrastructure elements. Figure 1.2 shows the typical four-party model used for most credit card payment schemes where the customer buys at a *merchant's* shop (online or offline), the shop's payment terminal is connected to the *aquirer* (who may or may not be the payment network provider) and in turn to the customer's bank, which *issues* the payment card, while the whole transaction process itself is conducted via the payment *scheme* provider (e.g. Mastercard).

These payment systems are divided economically into four separate parties: card issuer, merchant acquirer, customer, and (retail) merchant. The issuer issues the payment card to the customer. Usually, the customer has a payment account with the issuer. The retailer is contracted to the acquirer and has a business account there. Issuer and acquirer have to be regulated financial institutions with a bank license (American Express is an exception by being both issuer and acquirer).

The card issuer garantuees the payment made by the customer to the retailer. Any possible default by the customer is a risk of the issuing bank. The service (and the risk) is paid by the retailer through a so-called disagio. This is a percentage or a fixed fee, but most often a combination of both, of every payment transaction handled for the retailer by the acquirer, payment network, and the issuer. The disagio paid by the merchant – which is of course part of the price paid by the customer – to the acquirer is composed of several fees, which are split between acquirer, payment network, and issuer.

1.4.2 Payment system components

The technical components involve the payment card with its chip and operating system. The personalized card data is encrypted and allocated in the chip's memory. The POS terminal reads the card data and usually checks with the payment network, whether the transaction can be authorized or not. As a fallback option, the transaction can be done offline, but then it is more at risk for fraud. The acquirer usually reserves the authorized payment with the customer account at the issuing bank. Actual settlement of the payment may be batch-processed within a few days. Acquirer, payment network, and issuer all use interconnected data centers, which have to obey the rules of the payment network.

The indvidual processing tasks of acquirer, payment network, and issuer can all be delegated to third-party service providers. The production of the payment card itself also involves several steps. The physical plastic card containing the chip is designed with custom brand designs and personalized with the customer name and card data. Data personalization and encryption is often done by specialized entities, which get the raw data from the issuer.

Modern contactless cards contain a chip, a magnet stripe, and an NFC antenna. POS terminals equipped with an NFC-reader are able to read both chip and magnet stripe with the built-in contact reader as well as reading the chip via the NFC antenna (the "contactless" reader). The different methods are due to different preferences in usage: In the United States "swipe and sign" using the magnet stripe is still commom, while Europe switched to the more secure "chip and PIN" method.

NFC-based contactless payment cards still utilize the same involved parties as non-NFC cards, only the POS terminal is enhanced with an NFC reader and the plastic card equipped with an NFC ability (both in magnet stripe and EMV chip form, depending on geography). The picture gets different, when the contactless card (of the EMV type) is virtualized for use with an NFC-equipped smartphone. This virtualization step requires two more parties to join the four-party model of issuer and customer, acquirer and merchant. The new parties are the mobile network operator and the so-called Trusted Service Manager. Again, these services can be partially outsourced to third party providers.

The mobile network operator (MNO) owns the Universal Integrated Circuit Card (UICC), which runs the subscriber identity module (SIM) application used in mobile phones to connect to the network in GSM (Global System for Mobile Communications) and the universal subscriber identity module (USIM) application for UMTS (Universal Mobile Telecommunications System) networks. Additionally, it contains data for the international mobile subscriber identity (IMSI) and each card has a unique serial number, the integrated circuit card identifier (ICCID). Security authentication and encryption information in the form of an 128-bit key for network connection are also stored. One or two personal identification numbers (PIN) and one or two PIN unlock keys (PUK) are stored on the UICC. Besides this data, the UICC has a ROM with the operating system, RAM, EEPROMs, and I/O connectors.

The NFC-enabled UICC connects through Single Wire Protocol (SWP) to the NFC module within the handset and can exchange data this way. The specifications (see GSMA NFC UICC Requirements Specification Version 4.0) require the data to be stored in a Secure Element (SE), which can contain several applets for use with NFC. Most commonly, the SE is part of the UICC, but it can also be stored on an special removable SD card, or built into the handset on a separate module.

The applet for mobile payment emulates a contactless payment card. The data could be copied to the UICC during the production process, but in this case, UICCs would be delivered like personalized payment cards. Usually, UICCs given to customers are stock cards, without any personalization. This way, they can be "sold" directly, and without additional time for delivery. In order to personalize the NFC UICCs with data for the emulated payment card, the delivery channel is "over-the-air" (OTA). This enables the MNO to deploy services to the customer's UICC without re-issuing the card. Examples using this channel are, for example, updating configuration data in SIM cards and sending settings for services such as MMS.

The payment card applet send to the secure element on the UICC is in the form of a Java applet. It uses several silent SMS to transport several kilobytes of binary data used for the applet to the UICC.

The data itself contains the personalized card data and is sent from the card issuer to the MNO via a Trusted Service Manager (TSM). The most common use is a split TSM, where the service provider TSM (SP-TSM) on the issuer side sends the data to the TSM at the mobile network provider premises (MNO-TSM), which forwards it via the OTA server to the UICC. The TSM is responsible for the authentication and security of the data. TSMs can also exchange information on the status of the data and the UICC (e.g. active or suspended) and act on this information according to rules set up between service provider and mobile network operator.

Figure 1.2 shows an overview of all involved parties for a typical mobile payment system. The right side shows the extension of the card-based system with the added parties, mainly mobile network operator and Trusted Service Manager provider.

On economic terms the four-party model of card-based payment is extended to include one to three additional parties: the MNO and the provider(s) of the TSM. The fixed fees have to be split up within an extended group.

1.4.3 Smartphone and application requirements

The specification of contactless payment cards were adapted for use on NFC-equipped mobile phones, where the payment information is now stored on a so-called "secure element", which is either a separate chip incorporated into the handset, or more commonly installed on the special NFC-enabled SIM cards with a secure element. Access to these secure elements is controlled by the owner of the SIM card, usually the mobile network operator.

Near Field Communication is a wireless and contactless communication protocol, which is used in various implementations. Technically, NFC is a specialized variant of radio-frequency identification (RFID) acting on 13.56 MHz with rates up to 424 kbit/s (see ISO 18000-2, -3; 22536). NFC implements device handshake and secure communication between devices and NFC works both active-active and active-passive. The typical distance between devices is up to 10cm.

An NFC-equipped handset requires a medium to securely store any payment card information. The medium can either be on the handset or "in the cloud". If stored on the handset, the payment processor usually demands a so-called "secure element", where the payment card information is encrypted on special hardware. Secure elements can consist of a built-in secure element or be on removable storage like SIM cards or Micro SD cards. All secure elements have in common, that they operate independently from the handset's operating system. For example, a SIM card hosts its own operating system and storage facilities, and can perform computations on its own bypassing the smartphone's CPU. Thus, it is possible to perform an NFC-based payment transaction even with the handset turned off. The NFC reader will induce enough current to obtain the required information through the NFC antenna, the NFC controller and the connected NFC SIM card (via Single Wire Protocol, SWP).

The security concepts implemented in mobile payment applications use the security methods available on smartphones. As the app has to work on several handsets of different vendors, the common denominator is using a PIN. This is in line with the findings presented in the previous sections on security concepts of mobile phones.

1.5 Research questions

Why is research into the field of user perceptions of security necessary, if expert advice on how to handle security on smartphones is already available, and could be incorporated into security methods for smartphones and their use cases and applications? Expert advice and user perceptions are sometimes very different views on the same subject (Wash, 2010). In this sense, the guiding research questions related to usable security of computer systems in general are (Cranor and Garfinkel, 2005; McCLure et al., 2012)

- How can user behavior in the context of security of computer systems be described?
- How does readiness to assume risk, cost-benefit ratio and feeling threatened affect user behavior?
- What is required to integrate aforementioned factors into a simulation of the behavior model?
- Are any predictions on usability and subjective perceived security made by such a simulation useful for developers?

This work aims to advance solutions to some of the aforementioned problems within a small and exemplary subset of computer-related security – a smartphone-based mobile payment system. In order to reach the research goals, the following steps are taken:

- Analyzing the evolution of hardware and software to the current state of smartphone-related security concepts.
- Establishing a taxonomy of (usable) security to extract suitable parameters for the field of research.
- Developing test methods and conducting experiments using a prototype mobile payment system.
- Analyzing user behavior and generating a user behavior model for perceived security and usage of a mobile payment system.
- Evaluating the implementation of the results into simulation software.

A mobile payment application is a piece of software on a smartphone offering a new payment method. The customer's choice to use such a new method is shaped – among other factors – by personal attributes, social influences, and cultural norms. What is the effect of *personal* attributes like personality traits, risk behavior, and technical affinity on the user's choice of a new payment method compared to existing ones? How are these factors modified by the application, device, security method, environment, and threat?

1.6 Thesis structure and research goals

The thesis presents research done over the past five years by the author at the Quality and Usability Lab, Telekom Innovation Laboratories, Technical University Berlin. Some content herein has been previously published as conference papers and posters, but was notably broadened with new data and insights. Joint work and co-authors are of course mentioned appropriately. The collaboration with Niklas Kirschnick should be especially noted, with whom the author jointly coordinated and conducted the experiments. Early results were published in several papers with shared authorship of which five are cited herein.

In this thesis, all data preparation, analysis, computation, model development, and software enhancement were done by this author.

Security design and methods are influenced by developers' culture and philosophy as well as by hardware and software available to implement those security concepts at the time. Security perception is also influenced by media attention of current topics, layman's to power user's point of views, and arbitrary hardware and software choices. The structure of this work tries to establish a path, where it starts with the historical context described above. The evolutionary path from the previous sections can be visualized, which can be seen as a kind of pre-study to the taxonomy developed in Chapter 2. A taxonomy of (perceived) security is established and adapted to the area of mobile phones. It allows the identification of influencing factors to address the research questions and to build experiments around them deliver data for a user behavior model of security perception.

By focusing on the mobile phone and security method parts of the taxonomy, the question arises, how these might influence a user's perceptions of using security-sensitive applications on smartphones. The main goal of this work was to find the impact of personal attributes and security methods on usage and perceived security of users interacting with a mobile payment system. To test the area where – according to the taxonomy – influencing connections should occur, an NFC-based prototype system was used in the experiments described in Chapter 3. This chapter deals with the test methods used in the experiments, and presents the empirical data. Questionnaires and experimental setup were chosen to approach the user perceptions of security using the mobile payment system and to link them to the then-hypothetical influencing factors derived from the taxonomy.

Chapter 4 evaluates models built from the empirical data and discusses and compares the methodical approach used for building the model. It also describes the simulation software MeMo and implementation of the models. Enhancement modules were written to run the models derived in the beginning of the chapter as a proof-of-concept. This groundwork for a predictive simulation using the MeMo workbench expands the model into a possible design aid for software development. These simulation modules are the basis for further development and future work.

The last chapter concludes this thesis with a discussion of the achieved results, the state of mobile payment as of end of 2014, and future work.

1.7 Summary

Smartphone-based apps as a mobile payment system are an emerging class of applications using a variety of technical solutions. This class is filled with applications from dozens of start-ups and established players, and is considered to become a multi-billion dollar industry. TIME magazine proclaimed "The End of Cash" in its January 9th, 2012 issue (van Dyk, 2012). This raises questions of security, privacy, and trust, due to the possibilites of financial fraud, loss of anonymity, and increasing insights into user finances from additional entitites.

The introduction of new mobile payment apps is still on-going. Several mobile payment systems are currently competing, the widely-known contenders are Google Wallet and Apple Pay. But paying with mobile phones is still not common use in most parts of the world. This work evaluates mobile payment regarding user perception of security and usage, as research in this area is still scarce (Dahlberg et al., 2008; Sieger et al., 2012).

The historical roots of the current state of smartphone security show that the majority of operating systems for smartphones, iOS, Windows Phone, and Android, evolved from desktop-oriented operating systems inheriting the developer's mindset for security on those platforms, which was heavily influenced by the openness and hacker culture of late 1960's academia. This focus on openness and less on security and privacy is still prevalent in "Silicon Valley" as shown in both success and critique of social networks, social media and the upcoming sharing economy (Turner, 2014). The security shortcomings dragged along the past decades of computer history haunt today's users with the need for everchanging passwords, malware like viruses and trojans, phishing emails, surveillance and loss of privacy. The mobile payment application developer has to choose a security method which a potential user perceives as secure and which leads to frequent use of the app (or at least does not prevent it). In this way, it would be useful to know perceived security and personal factors influencing the security perceptions to suit a product to those user perceptions – or even influence them by the product itself. Products, where security is paramount – and financial products are certainly among them –, can gain a market adavantage, if they are perceived as being secure. In contrast to the focus on current method, exploits, and security holes, this work argues that the historical roots are largely responsible for today's lack of consistent computer security.

Additionally, the user is not aware of the smartphone being a miniaturized desktop computer, and still carries the mindset for mobile phone security. Only in the corporate and government environment could a mindset for slightly stronger security be established by specifically targeting this market with a operating system without desktop legacy. Advice for stronger security measures on mobile and smartphones should keep in mind (in addition to the user's view and probabilities for real threats) that many smartphone OS carry the legacy of a desktop OS, and should be addressed accordingly.

The definition of mobile payment is broad and encompassed both offline and online payment. This research concentrates on mobile payment systems, that can be used at the point-of-sale at stores. The technical solution used in this case is based on NFC for communicating the transaction, and uses the UICC Secure Element for storing payment card data. This solution is backed by standard bodies, payment networks, and mobile network operators, and does not rely on a single party.

This research tries essentially to measure two outcomes: How many items a participant bought using the mobile wallet prototype, and how she or he perceived the security of this payment method. The presented hypothesis assumes that there is a dependence on a number of factors, among them personal traits like risk perception, technical affinity, as well as trust in service providers and store environments.

Throughout this thesis several results are presented which are new to the field of research: A taxonomy of influencing factors of security-related user behavior; the first experiments to link and quantify the effects of specific security methods on perceived security and usage of mobile payment; and regression models and classifiers which are based on experimental data rather than survey data. These models are then used for a conceptual implementation of a simulation tool.

Chapter 2

Taxonomy

Developer mindset and user perception, which were covered extensively in the previous chapter, meet in the use of the smartphone hardware, its operating system and the installed applications, in this case a mobile payment application.

The user perceptions of security of such an application does not necessarily have to be consistent with those of the developer and can vary widely among users. Perceived computer security by (untrained) users are subjective and can be utterly wrong from an expert's point of view. Important aspects were laid out in Wash (2010) and Herley (2009). Wash describes "folk models" of security threats, and how they differ from expert advice. He identifies different conceptualizations of "viruses" and "hackers" for users of home computer systems. In this regard, viruses can be seen by users as just "buggy software" or being catched like a (computer) cold. Herley shows what may drive users to disregard advice from security experts: the cost-benefit-ratio calculated by users favors the ommission of security precautions, following security advice is too inconvenient. As was shown in Chapter 1 for the evolution of smartphones from desktop computer systems, these conceptualizations can be transferred to mobile systems including smartphones.

The focus of this work is not on such conceptualizations itself, but rather how those concepts, mental models, and underlying perceptions are formed by various factors and how they influence user behavior. These influencing factors and their interdependencies are the main part of the following taxonomy of security perception and user behavior in (mobile) computer-related security. A taxonomy helps to collect, sort, and visualize connections, dependencies, and relationships of the field of research. It can also support software development by making developers aware of users' mental concepts, perceptions, concepts, and influences on behavior as well as acceptance of a specific type of application.

In the area of computer and information technology the aim of any user activity is usually not security itself, but the task at hand. Security is merely an incidental and supporting aspect. For example, transferring money via online banking is the main activity, not to secure the computer against malware or thinking about phishing attacks. The cognitive effort, time, and possibly monetary costs for security software are added to the ones of the main goal of the activity as shown by research on the cognitive load of authentication methods (Weir et al., 2009). As an analogy, the same applies for the decision for or against sometimes costly security locks for a bike, where cycling is the main purpose and security plays only a secondary role (see Heckhausen and Heckhausen (2006)).

Starting points to find key factors and relevant taxonomical terms were several focus groups and surveys on the topic of possible security features on mobile phones. There, participants were asked about security perceptions concerning mobile phones. These studies were part of this research work and delivered input for user preferences on different authentication methods and security levels. They give an overview of the subjective perceptions of the presented security features (Dörflinger et al., 2010; Sieger and Möller, 2012). Focus groups, interviews, and surveys generate good qualitative insight into what people prefer or think to prefer.

Prior relevant studies were conducted by Furnell and Clarke (2005) and Imperva Application Defense Center (2010). Other examples include Ben-Asher et al. (2011), who interviewed users to characterize types and their different actions regarding computer security aspects (e.g. surfing the web, malware). Recent surveys include BITKOM (2014).

The focus groups tried to get an insight into what people think about possible future mobile phones with alternative or additional (biometric) authentication methods. Offering more authentication methods may attract those users who are for whatever reason appalled by the standard method of using a PIN. Possible users include elderly people or technophiles among others.

The main questions were: Which authentication methods are preferred? What influences the preference? Are preferences consistent with security perceptions of those methods?

The results from these focus group discussions and web surveys on the perceived security and possible usage of different authentication methods show a preference for biometric authentication, especially fingerprint recognition. These authentication methods were perceived as both secure and convenient, because they do not interrupt touch-based smartphone usage (for further results see also Section 2.1.2).

Additionally, the focus groups and surveys asked for the need of additional security layers to secure applications and content data, an approach called "graded security". Put another way, what types of application and data require a more secure method than others. The subjective perception of security aside, the data also revealed what users consider sensitive areas on their phones.

The taxonomical terms compiled by the focus groups and web-based surveys cover the areas of sensitive data and perceived security of authentication methods. In short, what should be secured and how it should be preferably secured. Combined with the aforementioned studies by Firesmith (2005), Wash (2010), and Herley (2009), connections to possible influencing factors can be drawn.

2.1 Taxonomical terms

A *taxonomy* provides a classification of a subject matter and the connections, dependencies, and associations, among others, of the different subjects it classifies. A paragon of the method of taxonomy can be found in biological classification.

In computer science an *ontology* is also often associated with taxonomical ranking (Gruber, 1993). But as Blanco et al. (2011) have shown recently, an ontology covering computer security, let alone usable security, is still missing. An interesting similarity to concepts of safety can be found in Firesmith (2005).

The taxonomy focuses on producing a (visual) overview on influencing–mainly personal–factors on user perception and behavior concerning mobile payment. It considers the key factors user, system, environment, task, and threat.

There are several topical keywords fitting a taxonomy of security-related user behavior: benevolence, goodwill, confidence, credibility, predictability, perceived competence, and perceived security. Not all of these are used in the taxonomy presented here as the focus is on perceived security. These keywords can be called *user-centered* as most other keywords center on device-related or software-related topics like reliability, protocol, methods, policy, risk, measurement, and attack. Blanco et al. (2011) "observed that the majority of the identified works focus in specific domains, thus signifying that the scientific community has not accomplished an integrated security ontology, although this has been identified as a branch of research."

Some literature examines mobile payment prior to the breakthrough of the touch-based, app-driven smartphone model in 2007, for example Zmijewska and Lawrence (2006). While these surveys are relevant for general questions concerning the implementation and acceptance of mobile payment (e.g. payment scenarios and involved players), the examined payment models and applications are mostly obsolete now. Among them are premium SMS, mobile carrier billing (a niche product now), and mobile network operator-centric payment systems.

Therefore, the general area of interest here has to rely on a "ready-made" ontology to circle relevant terms for a taxonomy of user perception of smartphone-related security, and user behavior at smartphone-specific, and smartphone-supported or smartphone-aided tasks.

This taxonomy categorizes influencing factors of security perceptions within the field of research and allows to derive test variables for the experiments presented in Chapter 3. The generation of this overview and its possible visualization is an iterative process, which in this case uses surveys, focus groups, preliminary test, and previous work done on a software simulation of security-related user behavior. It also takes a taxonomy of safety into account.

The taxonomy covers the following areas:

- *user-related factors*: willingness to take on risks, privacy concerns, trust in the computer system and associated "institutions" and persons, self-assessment of computer knowledge, experience with attacks on computer security, understanding the effectiveness of security systems, individual perception of risks, personality traits;

- *aim of the interaction*: type of primary task, motivation of the user, expected cost-benefit ratio of taking security measures;

- *(mobile) computer system/smartphone*: general usability of the system, arrangement of the interaction elements, type and time of the presentation of possible risks, security method;

- *environment*: news reports on attacks on and weaknesses of computer security, potential educational campaigns on computer security, individual surroundings, current usage activity, context of activity;

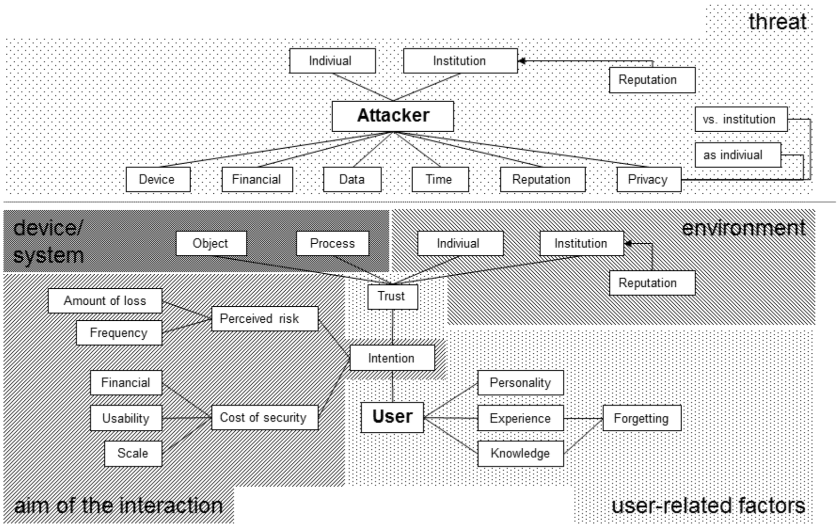


Figure 2.1: Taxonomy of security-related factors influencing user and attacker, modfied from Sieger et al. (2011)

- *threat*: type of attacker, type of attack, aim of threat, probability of threat;

A published version of a taxonomy of security-related user behavior concerning the parameters above can be found in (Sieger et al., 2011). The main interest in this work is to find personal attributes, which potentially influence the behavior shown in the security-related part of smartphone interaction. Such parameters may indicate possible changes in the motivation concerning the user's aims. These factors were collected, and then combined from original research (as mentioned in the previous section) and other studies.

The taxonomy is not constructed as a model like the well-known extended unified theory of acceptance and use of technology (UTAUT2) (Venkatesh et al., 2012), an extension of UTAUT which itself is built on the Technology Acceptance Model (TAM) (Venkatesh and Davis, 2000). UTAUT2 is specifically aimed at the consumer technology use context. The reason to divert from these widely used models is the difficulty to include threat, security method, and security perception. The taxonomy presents threat as an individual or organizational antagonist to the user, a concept not incorporated in other models. Further, the focus is not only on behavior, but also on perception. UTAUT2 describes performance expectancy, effort expectancy, social influence, hedonic motivation, price value, habit, and facilitating conditions as critical factors predicting behaviorial intention and use behavior of consumer technology. These factors are moderated by age, gender, and experience. Social influence and habit have to be both measured in longitudinal field studies to be valuable data as these cannot be observed in a short lab test or via surveys where participants would have to rate those long-term external factors via questionnaires. As some factors could not be gained by lab experiments, and (security) perception is not part of UTAUT2, another suitable concept had to be developed. The taxonomy presented here takes the same approach as UTAUT2 by building 2-dimensional relationships between factors assumed to influence perception and behavior. They can essentially be computed using correlations and the performance of any derived model can be calculated by the explained variance of the dataset.

In contrast to UTAUT2, social influence would be incorporated into the taxonomy by establishing an additional 2-dimensional plane, where environmental factors would be extended to include factors like culture, norms, and regional differences which then would relate to personal and device-related factors on both user and attacker. Relevant data had to be collected through field tests and is part of future work.

As opposed to models of mobile payment usage (see Section 4.1 for an extensive discussion), the taxonomy is open to *include* alternative devices, applications, (existing) payment methods, environmental settings, an extensive set of relationships to possible threats, and a broad set of personal attributes. It deliberately *excludes* socio-cultural influences in its first iteration. The intention to base the experiments on the taxonomy limits its center on direct personal attributes influencing the security perception and usage of mobile payment. Additonal data for socio-cultural factors can only be collected in a meaningful way by longitudinal studies (see also Section on future work in Chapter 5), but requires an established mobile payment infrastructure.

In the following sections the taxonomical terms are defined and their relations, dependencies and influences explained.

2.1.1 User – security perception

Not too few publications depict the state of computer security as something lost or won at the user's front. For example, Lampson (2009) comments, that "[t]he root cause of the problem is economics: the costs of either getting security or or not is not known, so users quite rationally don't care much about it. Therefore, vendors have no incentive to make security usable". How can vendors (and the developers making the product) shape the user perceptions of their offerings and their security-related features? "In addition to overestimating benefits, advice almost always ignores the cost of user effort. The incremental cost of forcing users to choose an 8-character strong password, as opposed to allowing a 6-digit PIN, is hard to measure, but is certainly not zero. And ignoring it leads to failure to understand the rational and predictable nature of user response" (Herley, 2009).

Schierz et al. found six key factors influencing the acceptance of mobile payment: Perceived compatibility, individual mobility, subjective norm, perceived usefulness, perceived security, and perceived ease of use (Schierz et al., 2010). This work focuses mainly on perceived security, but will also take perceived usefulness, and perceived ease of use into account. Socio-cultural factors like perceived compatibility, individual mobility, and subjective norm are too broad to fit into the intended lab experiments as they can only be examined via field tests (for example using a diary method).

The terms itself, *security perception* as the mental concept or *perceived security* as the actual rating of the perception, can be described in this context as the user's impression, ad-hoc judgement, gut feeling, or mental model concerning (mobile) computer security (see also Chapter 1), all shaped by several influencing factors.

Users are rarely computer experts, but as stated by Herley (2009) "[t]hey are offered long, complex and growing sets of advice, mandates, policy updates and tips" . Wash (2010) adds "[c]omputer security experts have been providing security advice to home computer users for many years now. [...] However, many home computer users still do not follow this advice."

Users build different mental models of computer security and they follow security advice according to their models. For example, if they perceive a computer virus merely as some kind of "buggy software" they tend to see the advice to use anti-virus software as not necessary to follow (Wash, 2010). All four classes of mental models concerning computer security are (*ib.*):

- Attacks and malicious software are generally bad and spread like an infectious disease.
- They are like faulty software (buggy), but must be executed manually.
- They are disseminated by Internet "troublemakers" but do not cause "real" damage.
- They are used by criminals to spy for information saved in the computer system itself but do no harm itself.

Along with self-assessment a user's insight into the effectiveness of computer security is also an important factor for his behavior. Previous studies already emphasized that users tend to circumvent safety rules or make them ineffective for a lack of knowledge of their effectiveness or usefulness paired with discomfort using security methods (Adams & Sasse, 1999).

The main result from these considerations is that there are two sides. There is the computer system (or device) itself to protect, containing data, financial, and personal information, which may affect privacy and reputation; and there is a threat, an attack, a virus, a trojan, or a phishing mail against which to take security measures (or protective means). Therefore, the taxonomy is built as a confrontation of two antagonists, the "user" and the "attacker" (see also Kainda et al. (2010) for a security-usability threat model). While the user is in the end always an individual computer user, the attacker is less clearly defined. It, too, can be an individual, but it can also be a group, an institution, or even a state ("cyber-warfare"). As the research interest is on the user's security perception, the attacker might be a vague "threat" in the user's point of view as is emphasized by the description of some users, that there are "bad" parts of the internet, where a computer can be infected by a virus (Wash, 2010).

The user perception is influenced by his or her personality, by experience, and by knowledge. The latter are both prone to forgetting. If an experience happened a long time ago, its influence may vanish (but it does not have to, for example in the case of a traumatic experience). If knowledge has not been accessed for a long time, it may be lost for immediate use. These influencing factors are assumed to be a common ground in psychological research.

The general psychological factors – subsumed here under the taxonomical term "personality" – include personal risk behavior and confidence in institutions and individuals, as well as concern for privacy (Gerrig and Zimbardo, 2008). This behavior can be used to characterize a person, but behavior is not always consistent all the time and thus observations in one area of life are not directly transferable to another. Individuals can invest in risky adventures in one area while behaving risk-averse in another area being very careful and safety/security-aware. Someone might protect his house by a plethora of safeguards against intrusion, but disclose very personal information on social networks (see also Weber and Milliman (1997)). Nevertheless, at least a statistical probability can be derived from personal risk behavior concerning the behavior in the area of computer security – as is done in similar areas (Zuckerman and Kuhlman, 2000). The same is true for user concerns about privacy and trust in institutions, companies, and individuals (RISEPTIS, 2008).

2.1.2 Interaction – cost of security

The user has an intended task to do, which requires a computer. In the research presented here, the task is to pay for goods at the point-of-sale using a smartphone-based mobile payment system.

In line with the findings from Lampson (2009) and Herley (2009), every security measure is associated with costs. For a mobile payment system the smartphone's hardware and software is the application platform; and the security measures are tied to the smartphone's hardware security systems, its operating system, and the payment app itself. The evolution to the current state has been laid out in Chapter 1.

Tognazzini (2005) observers that "[b]alance is the key to all security efforts.[...] Unless you stand over them with a loaded gun, users will disable, evade, or avoid any security system that proves to be too burdensome or bothersome." It may not seem to be too exaggerated as a recent study on password security by Imperva Application Defense Center (2010) has shown: Roughly 1% of the analyzed 32 million passwords used for a web service were simply '123456', and "almost all of the 5000 most popular passwords, that are used by a share of 20% of the users, were just that – names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on)."

The usability of the computer system has also a big impact on user behavior. For example, the arrangement of the elements of a user interface (e.g. graphical arrangement of elements on a web page) and the sequence of interaction steps are crucial to the successful use of the security features of a computer system. As mentioned above, the cognitive burden of using certain security methods should be minimized in order to avoid an unfavorable cost-benefit ratio compared to the user's actual goals. Otherwise it can undermine for what the security feature aims (Adams and Sasse, 1999). A broader meaning of usability includes the general proficiency in using the system and its inherent rules (e.g. password policies). Inglesant and Sasse (2010) have examined the cost of bad password rules. They come to the conclusion that password rules should aim not only at the security of selected passwords and the rule how frequently they have to be changed. Rather, principles of human-machine interaction should be applied so that users choose a password that is "good enough" based on the context.

In an actual use situation, the user implicitly checks her or his personal cost-benefit ratio, the desired target and the required action – i.e. from her or his individual perspective and existing computer literacy (resulting in a mental model). Here, many users tend to look at the expenses required for the provision of security and privacy as too high. The amount of a possible loss has to be in balance to the security effort: If the user sees the chances of a successful attack as too low, security systems are ignored or turned off. In addition, many known attack vectors cannot be avoided by computer security methods alone. This includes social engineering, which does not seek to overcome technical security barriers, but tries to con the user (Herley, 2009). Additionally, attacks on the server infrastructure bypass the end-user.

The device can contain different security measures, depending both on hardware and software implementations. In this regard, the device itself – as mentioned above – can be an influencing factor. How are different security methods and multiple security levels perceived by the user for the intended task? What can be extracted from the participants answers as influencing factors for the taxonomy?

In order to gain first insights into user preferences for different authentication methods and graded security on mobile phones, a two-fold approach with focus group discussions and a web survey to cross-validate the results was used.

Linck et. al asked participants in a survey about mobile payment "What would you require to feel secure about using mobile payments?". The Top 5 ranked resulting categories for the dimension subjective security were (in that order) confidentiality, encryption, stating "security", transparency and traceability, and authentication and authorization. (Linck et al., 2006). The focus in a survey done for this thesis is on the subjective view on possible implementations of security methods (Sieger et al., 2010).

Moderated discussions with a focus group deliver a deeper insight into a topic than an anonymous web survey. The moderators and participants can show devices, prototypes, methods etc. They can clarify questions and answers and generally discuss in more detail. This way of data collection is particularly suited for this research subject, as biometric authentication and graded security are uncommon and have to be explained and displayed before the user can provide a well-founded opinion.

A focus group discussion with a total of 19 participants was conducted at the Quality and Usability Lab facility in Berlin in November 2009 [1]. The participants were segmented into four groups: parents, students, business professionals and fully employed singles and couples.

During the focus group discussion the following knowledge-based and biometric authentication methods were demonstrated (through real hardware or "mock-ups") and discussed: fingerprint recognition with swipe sensor on a laptop computer; 2D gesture recognition using a touch-pad on a laptop computer using a prototype software; 3D gesture recognition explained in analogy to the Nintendo Wii's controller using a mock-up; iris scan or face recognition with a phone's camera using a mock-up; activity-based verification through keyboard typing patterns using a laptop computer's keyboard and prototype software; recognition-based authentication by electing points on a picture in a specific order using a mock-up; speaker recognition using a mock-up.

While knowledge-based and token-based authentication are used on a regular basis by many people around the world (think ATM cards (token, PIN) and

[1] The following in this subsection draws mostly from (Dörflinger et al., 2010) which this author supported in a minor role.

mobile phones (PIN)), biometric authentication methods are at least known to exist (fingerprint and iris recognition in movies etc.) by a part of the users. Biometric authentication methods are often seen as having advantages over other methods, because no password has to be remembered, no token or written-down note can be lost or stolen, which does not mean that biometric methods are necessarily harder to crack.

Token-based methods are not considered here, as the hardware constraints of mobile phones do not favor them at the moment. Tokens like USB dongles or smart cards require connectors or readers, which are not implemented yet while other methods can take advantage of functions that are already built into mobile phones. Currently available smartphones most commonly use the following security feature: a 4-digit PIN to secure access to the SIM card or to lock the device. A few devices introduced character-based passwords, two-dimensional patterns, or face recognition.

The participants valued the different methods according to the questions (among others) whether the method was perceived as secure, and whether the participants would use it, if available. The evaluations of the authentication methods and graded security levels were introduced with little scenarios for possible use, which were presented by the moderators or resulted from in-group discussions. The results show a significant lead for the fingerprint recognition method as being both secure and usable (see Table 1 and 2).

This leads to an interesting perception of the use of security methods for different levels of security, which was addressed in asking "How should they be combined with authentication methods?" Instead of assigning each security level an "appropriate" method (lower security levels match with less secure authentication methods) a "one size fits all" approach (fingerprint) was preferred. This result initiated the implementation of a (mock-up) fingerprint recognition method into the prototype used in the experiments.

"The idea of having a gradual security system with different authentication methods was favored most by parents because it allows sharing one smartphone among family members without having to bother about private data or cost-intensive applications." (Dörflinger et al., 2010)

Security method	
Iris recognition	100%
Fingerprint authentication	95%
Speaker recognition	68%
Face recognition	64%
Activity-based verification	63%
2D gestures	63%
3D gestures	42%
Recognition-based authentication	37%

Table 2.2: Focus groups – "I think this method is secure" (Dörflinger et al., 2010)

The perception of biometric methods and the user preferences for possible future use show a significant lead for the fingerprint method. Mobile phones are operated by using one or two fingers and fingerprint authentication fits this context of use. Speaker recognition would also fit, but is sometimes seen as

Security method	
Fingerprint authentication	95%
2D gestures	63%
Recognition-based authentication	47%
Activity-based verification	42%
3D gestures	37%
Speaker recognition	37%
Face recognition	27%
Iris recognition	26%

Table 2.3: Focus groups – "I would use this method" (Dörflinger et al., 2010)

awkward (especially in crowded places) as remarks in the focus groups revealed. An iris scan, for example, would interrupt the finger-driven flow. From the studies presented here, it can be concluded that authentication methods breaking the operating mode are considered as inconvenient. In this way, an "optimum" could be reached by combining a touch screen with an *integrated* fingerprint reader (such a product is not commercially available yet, although there are products with a separate fingerprint reader in close proximity to the screen, e.g. Apple iPhone 5s and 6). When the user tabs on an application icon, the phone could automatically authenticate the user – the experience would be seamless. In the same way, graded security is desired, but in a very low-key way. An additional layer of security to secure single applications or data would suffice for most participants in the study. The findings in the focus groups revealed, that if an authentication method was perceived as convenient and secure, the consensus was to use it throughout for all security levels.

The idea to combine low security levels with relatively less secure authentication methods was disregarded. It also has to be considered who is willing to pay for new and additional security methods on mobile phones. The device manufacturer probably has to implement additional hardware that is capable of e.g. biometric authentication. The operating system has to make use of this hardware, which means it has to be adapted, too. The same goes for application development. And in the end, the user must be willing to pay for these additional capabilities. There must be an urge for security and the added security has to be convincing to justify a higher price. The problem is, that hardware and operating system vendors, application developers, and users are all different parties, whose priorities not always align.

It was not asked for possible individual and social implications of a widespread use of biometrics. Although biometric methods are investigated here for the sole purpose of securing the phone or an app, they inherently touch privacy issues as very personal data is stored and processed. The participants of the focus groups did not reject biometrics *per se* and did not object to any specific method discussed here. On the other hand, the focus groups' hosts did not touch this subject as the main interest was the user's initial reaction to biometrics' general usability to secure mobile phones (Dörflinger et al., 2010; Ben-Asher et al., 2011). While both studies were not strictly representative, the trends found are of value for both the resulting taxonomy presented here and the experiments built upon the findings.

In the same time-frame as the focus group discussions took place a web survey was also conducted (in co-operation with Joachim Meyer and Noam Ben-Asher from the Ben-Gurion University of the Negev, Israel) with a similar set of questions to cross-validate the findings of the focus group discussions. The survey consisted of 64 questions with closed answers on a 6-point Likert scale. It generated 308 individual responses in its run-time of two weeks.

The results support the rankings found in the focus groups. Table 3 and 4 show the distributions of responses to the perception of security and possible future use of biometric authentication (Dörflinger et al., 2010). The results are also in line with earlier findings by Clarke et al. (2002), where fingerprint recognition got also the highest rating in a survey. PIN and speaker recognition, as well gesture recognition and IRIS recognition switched their respective position.

Security method	
Fingerprint recognition	75%
Face recognition	44%
Speaker recognition	30%
PIN	29%
Gesture recognition	14%
Iris recognition	6%

Table 2.4: Focus groups – "perceived as high level of security by method" (Dörflinger et al., 2010)

Security method	
Fingerprint recognition	49%
Face recognition	23%
PIN	35%
Speaker recognition	23%
Iris recognition	21%
Gesture recognition	16%

Table 2.5: Focus groups – "future use by method" (Dörflinger et al., 2010)

The findings of the focus groups and surveys indirectly were included in the taxonomy (Figure 2.1) in the area of the user's intention and the associated costs of security. User pereceptions of different security methods vary significantly over different types. Usability concerns are important: the usage flow should not be interrupted; using the security method should not be awkward (e.g. holding the phone's camera close to the eye for iris recognition) or embarrassing (e.g. speaker recognition in a subway full of commuters); and the method has to "scale", when used often (gesture recognition might be tiresome, if it had to be perfomed for longer periods of time). Some security methods like fingerprint recognition require additional hardware, making the device more expensive. Therefore, the factors "Financial" (as the direct cost of the security measure), "Usability", and "Scale" are connected to the cost of security.

As a "counterweight" to the cost of security acts the "perceived risk" as is evident in the folk models of home computer security (Wash, 2010). Users tend to follow expert advice as long as it is in line with their perceived risk of the threat. The possible amount of loss (financial, data, privacy) and its possible frequency (one-time, frequently) are influencing factors.

A third factor to the intended task is the user's trust in achieving the intended goal. In this case, it would be a good to purchase: What item to buy (object), how to buy it (process), where to buy it (institution), and who will process the payment (individual).

2.1.3 Device – security methods

To implement protective measures, demand by users and the appropriate mindset on the developer's side is needed, but it also requires specific hardware and additional space on the device, especially for biometric authentication: Keyboards, cameras, microphones, gyroscopes, fingerprint sensors, raw CPU power and fast storage media. Even non-biometric methods like strong passwords or data encryption might hit the limitations of the underlying hardware (Collins, 2010).

As cited above the key is to balance usability and security. As the study on passwords shows a significant amount of users either do not know the concept of secure passwords or do not care (Imperva Application Defense Center, 2010). Convenient passwords are easily attacked with brute force, but still offer some advantages over no passwords at all. A device, its data, or its application are secured against a "casual" attack from children, spouses, friends, co-workers etc. It can be assumed, that in the context of mobile phones users show a similar behavior, whereby the security mechanisms of a smartphone (and mobile phones in general) are to be considered even weaker than the security mechanisms of web services (or computers in general), because a 4-digit PIN is easier attacked or even guessed, than, for example, an 8-character password.

It can be argued, that as long as important data is not encrypted, even the best authentication mechanism can be bypassed, if the data transmission or storage media can be physically accessed, the latter being the case by unattended, lost or stolen devices. What is the use of e.g. strong password protection, if the memory card of a smartphone can be easily removed and be read on any other computer? The hardware (namely CPU) of the early mobile computing devices was not fast enough to provide on-the-fly encryption/decryption of data on storage media and in RAM, and this is mostly the case even today. Even desktop systems have noticable performance penalties when using data encryption on hard disk drives (Collins, 2010).

The focus groups and surveys asked for the perceived security of different security methods (for use as authentication methods see (Dörflinger et al., 2010; Ben-Asher et al., 2011)). How are those methods implemented in commercially available devices?

Many of the security methods aim at the authentication of the user. Mobile phones were and are usually solely secured by a 4-digit (SIM) PIN to authorize access to the carrier network. The first mobile phones with additional security features showed up at the end of the 1990s (Siemens SL 10 D with fingerprint sensor, 1999), but more than ten years later, mobile phones are still predominantly secured by a 4-digit PIN alone.

The number of mobile phones and smartphones, which implemented additional security features besides 4-digit PINs, is very small compared to the overall variety of models produced. Phones with built-in keyboards tend to offer alphanumerical passwords (Nokia 9000 series, Blackberry, Palm), and there are very few models with biometric authentication like fingerprint and face recognition, all of them released to limited markets (predominantly Japan). Example devices are: Sharp 904SH with face recognition released in 2006; Fujitsu FOMA F905i with fingerprint sensor, released in 2008; LG eXpo GW820, a Windows Mobile 6.5-based model incorporating a fingerprint swipe sensor, which can secure access to the phone and individual applications and data, released in 2009 (Sieger et al., 2010); Motorola Atrix 4G with fingerprint recognition released in 2011; Apple and Samsung released the iPhone 5s in 2013 and the Galaxy S5 in 2014 respectively, both containing a fingerprint sensor (subsequent models iPhone 6 and Galaxy S6 continued to offer fingerprint recognition). This is an interesting development as this touches this research of mobile payment directly. The use of fingerprint recognition for mobile payment is part of this work.

Consumer interest in stronger security is evidently low, otherwise the market should have already responded to those demands. The one exception already mentioned, Blackberry, was for a long time the sole provider of busines-oriented smartphones.

Since business is much more interested in data protection, encryption and strong authentication are on the wishlist, but are only partly fulfilled so far. This can lead to restrictions in the use of smartphones, if its lack of encryption of data and messages is seen as a weakness. Only very recently data encryption is available on smartphones (Apple Inc., 2014b; Research in Motion Ltd., 2006) or is planned to be integrated and turned on by default.

Furthermore, the user is not always able to secure the device. Programming bugs and certain types of attacks cannot be countermeasured by the user, because he cannot be aware of all of them (there is no way to notify him in every case) or, even if aware, there may not exist any measures to counter the attack (e.g. zero-day exploits, social engineering). The hardware constraints limit the design choices for security measures as mentioned above, and some restrictions on multitasking and application installation (e.g. Apple's app store) add some security of a smartphone. But the lack of "true" multitasking (iPhone OS up to version 3.2, Windows Phone 7) will probably vanish completely in the future (partly implemented from iOS 4 upwards), and therefore malware infiltration is more likely to happen. Third-party software (especially for discontinued Symbian and Windows Mobile) add security features like password protection, e-mail and SMS protection, and encryption, but these are commercial add-ons and not delivered as part of the operating system. The design is not secure per se, but has to be hardened by a knowledgeable user.

On the other hand, passwords are very well known for a lot of log-on processes, being it a personal computer or a web service. Passwords need a character-based input device, this probably prevented them to be widely used on mobile phones, which most commonly offer a keypad only. There were devices with full keyboards, for example, several devices from manufacturers like RIM (now Blackberry) and Nokia, among others. They allowed the use of passwords with 4 to 14 characters (and password rules).

Recognition- and recall-based "passwords" are now widespread. These non-character-based passwords were less common to be found in the past, and involve to draw a pattern, to select parts of a picture in a certain sequence, or to substitute PIN-numbers with pictures. As this method is now implemented in the Android operating system, it has seen a wide distribution. This security concept relies heavily on touch-based input devices for good usability. Something which could not be achieved on phones without touch-screens.

It can be assumed from former research, that users are interested in convenience (Cranor and Garfinkel, 2005). Every interaction, which "destroys" the work flow and/or takes up too much time, can be assumed as to be "too burdensome or bothersome". In this regard it is obvious, that biometric methods were not very well suited for mobile devices, if usability and for the most part hardware constraints are considered.

For example, palm-print, hand vascular, and hand or ear geometry recognition cannot be easily implemented due to size requirements. Gait recognition is implausible, because this would require to walk in a certain distance from one's own mobile phone to be captured by its camera (mobile phones are usually carried in pant pockets, jacket pockets or handbags, making gait recognition by motion sensor unsuitable). The same goes for any 3D object recognition as it either depends on considerable hardware or would be hard to use alone. Signature verification needs a relatively large input area, but this could be possible on today's smartphones.

This still leaves a lot of methods as potentially usable biometric authentication methods on mobile phones: fingerprint recognition, face recognition, iris recognition, speaker recognition, 2D and 3D gesture recognition, and continuous biometrics/activity-based verification (e.g. typing pattern).

There are some biometric methods already implemented on mobile phones. *Speech* recognition is already available on smartphones, but it is used as an interface, not as a security method as *speaker* recognition would do. Examples of (assistant) apps using speech recognition are Apple's Siri, Google's Now, and Microsoft's Cortana.

Graded security can be seen from two different perspectives: First, as a role-based hierarchical system to provide access to certain areas of the secured device, where access is defined by user-based roles (e.g. from guest-user to super-user). Second, graded security can be seen as a content-based system, where access to specific content is secured by access to this content alone. The user has to provide authentication to get access to content, but there is no overlap to other content. Each content has to be accessed individually. This is in contrast to the super-user, who can access everything on the system once authentication is passed.

Of course, both approaches to graded security can also be combined. Systems using a graded method of security to access defined areas are in common use, and it can be expected that users are accustomed to the concept. Especially in the area of computers, graded security has been in use for a long time (at least since the MULTICS operating system, a "predecessor" to UNIX built in the 1960s), even on consumer-oriented products (e.g. networked and mobile computers). For example, on a networked computer the user gains access by providing a password, for further access to network-based functions he may be prompted to provide another password (or the same again).

On mobile computers the user may need to provide a password or a fingerprint scan to start the device beyond the BIOS/EFI routine, and then provide further authentication when to log into his or her user account. If the computer connects to the Internet, users almost always require providing authentication to access certain web sites, being it an e-mail account, a web shop, or a banking account. Thus, it can be expected to a certain degree, that users are aware of the concepts of graded security.

Returning to the evolution of smartphones and "developers' mindset" lined out in Chapter 1 it can be seen, that development for mobile payment applications is restricted by what is available on smartphones. For example, if a security method requires special built-in hardware like a fingerprint reader, it relies on what smartphone vendors offer with their devices and whether they grant access to it or not. The same applies to software. Even if the hardware part is there, it does not necessarily has to be open for everyone. Examples are Apple's Touch ID, which as of 2014 was only recently opened to 3rd-party developers via an API. The new NFC and Secure Element capabilities of the iPhone 6 range are again closed and only accessible to Apple itself. Similar, the Secure Element found on NFC-SIM cards are only accessible through the mobile network operators and usually cannot be used by third parties.

Choosing a security method for a mobile payment application is not only limited by the evolution of smartphones and security concepts of mobile phones, but it is further regulated by national and international authorities and public and industry standard bodies. If the security method is available on the device and open to developers, it still has to apply to those regulations and standards to pass certification (Mastercard Inc., 2014; PCI Security Standards Council, LLC, 2013).

The chosen security method to secure a mobile payment app may "solve" the problems of (un)locking the app and securing authorization of a payment transaction, but the complex infrastructure of Figure 1.2 shows that there are many more possible vulnerabilities due to the numerous different systems involved.

2.1.4 Environment – types of stores, kinds of goods

Payments can be made at numerous varities of places. Just to name a few: retail stores and street vendors, restaurants and mobile food stands, public transport and public offices. It can be a big or a small store, it can be located in a hip or run-down part of the town, it can be brick and mortar or it can be a car. The point of sale can accept cash only or all kinds of payments methods. The customer can buy groceries at the supermarket or a hot dog in the street, expensive jewelry at Tiffany's or gas at a station. All of this might affect the decision what payment method to use in a particular environment.

Personal experience and exposure to media also play a role. Recent reportings about virus attacks, the daily flow of news via internet, press and television can lead to an increased awareness, which again can lead to a short-term change in behavior (Herley, 2009). The same goes for advice from personal environments, for example if colleagues from work, friends or relatives tell stories of security-related attacks on their computers (Wash, 2010). Furthermore, it can be assumed that educational campaigns, such as those used in other fields (e.g. health care: AIDS education) are somewhat effective. This can be done in the form of advertising, brochures, training, etc.

2.1.5 Threat – losing money

The main risk involving financial matters (using computers) is losing money by fraud. Another risk is to lose privacy and reputation, if financial information about worth or transactions are disclosed. The attacker can be an individual criminal or an institution like a domestic or foreign police or intelligence agency.

Fraudulent access to personal financial data is subsumed under the taxonomical term *threat*. The term *attack* is used to describe the threat being realized. Fraudulent access or use can be obtained by several means, usually described by “hacking”, a degoraty term which does not completely cover all types of computer security circumvention (see also Levy (2001)). This involves direct attacks by having physical access to the computer or remote access via network facilities. Among the techniques used to exploit computer systems are password cracking, spoofing, using known vulnerabilites, and malware like viruses, trojans, and keyloggers.

Then there are attacks via a wide variety of social engineering techniques, where the attacker tricks the user to reveal security information like passwords, e.g. by impersonating a supervisor or colleague. Studies on security threats of NFC-based mobile payment systems done by Gajda (2011) and Vermaas (2013) emphasized the high risks of theft and scams compared to attacks aimed directly at the hardware or software. Vermaas uses a model for expert-based risk assessment under uncertainty to gather information on the likelihoods of different attack scenarios. Gajda argues that smartphone-based mobile payment is an extension to other proximity-based payment methods like NFC-equipped credit cards and as such has the same risks. Additional risks due to new technological attacks could be mitigated by additional security measures (e.g. sending location information during payments).

A third category of fraud is not restricted to computers, but merely extends techniques used prior to the introduction of personal computers to the now thriving computer and internet-enabled economy. This includes spam e-mails, scams at online stores and auctions like overcharging or false delivery, bounced financial transactions, using false or stolen financial data, and theft of devices containing personal data like mobile computers and smartphones.

2.2 Similarities between safety and security

The main difference between safety and security is that the former tries to prevent physical harm, and the latter tries to limit access. But simply spoken, a fence around a site containing toxical waste does both. Also, when dealing with computer security, the two fields do overlap. A security bug in the firewall of a system controlling a power plant may have fatal consequences. In this way, implementing, for example, state-of-the-art network elements equally fulfills requirements of both safety and security.

Thus, it is useful to take a look at already existing taxonomies of safety. Firesmith did an extensive study on a taxonomy of security-related requirements, were he derived the taxonomy in analogy to safety. Four types of security requirements were presented. The interesting point of view is to define safety, security, and survivability as a subtype of defensibility (Firesmith, 2005). Those requirements are specification of what a system is required to have or to do in order to provide security against denial of service, data loss, data theft, and corruption of hardware, software, and people, and so on. This is done in a hierarchical order.

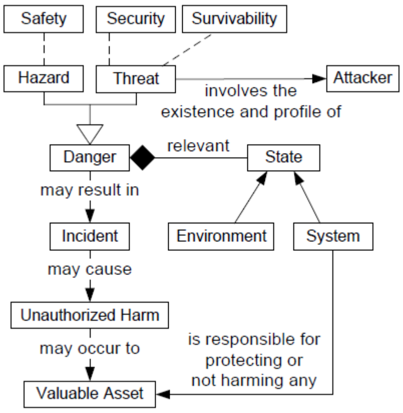


Figure 2.6: Safety Hazards vs. Security Threats (Firesmith, 2005)

While those *requirements* apply to the abilities of security systems, the main question here is how the security of those systems is perceived by the user. Especially useful for the taxonomy presented here is Firesmith's distinctions between safety harzards vs. security threats. Figure 2.6 shows the dependecies between the several aspects of safety hazards vs security threats.

Some terms can be transferred: The user's perception of the class "threat" (of the top type security), which is performed by the attacker. The "incident" divides the attacker from the user, because both have different perceptions of and intentions on acting and reacting to the incident. Plainly spoken, the incident is when the threats "happens".

All these actions rely on influencing factors delivered by the environment (institution, financial assets, reputation), the system (devices and processes), and the user (traits, experience, perception). One of the differences between Firesmith's taxonomy and the one presented here is, that Firesmith's is procedural (how to comply to security requirements?), while this research centers on dependencies (what influences security perceptions?).

2.3 Taxonomy-derived experiments

Figure 2.1 shows the user and possible influencing factors. As described, the taxonomy was derived from previous user tests and surveys, literature, and general considerations. After collecting and sorting the influencing factors, some of those factors are used to build and illustrate several hypotheses about security perception of users of a mobile payment system. Later on the results will be used to built experiments and to feed the experimental results into a user behavior model. An iterative circle is then started by using the behavior model for further tests in future work, gaining more insights into the influencing factors and then to refine the taxonomy (see also Sieger et al. (2011))

A series of experiments can be derived from the taxonomy, the main goal being an understanding of what influences the security perception of a mobile payment system.

The taxonomy shows influences on the user, which were outlined above: user-related, interaction-related, and device-related factors. In this regard, the experiments should deliver results in the following areas:

- Information on the user's personality, and his or her experience and knowledge of computer systems and smartphones;
- The intended task of buying goods is preset, but the individual user's view on the cost of security should be determined: choice and frequency of use, and perceived security of a mobile payment app;
- Perceived risk of the intended task;
- Influences of object, process, institution, and indiviual, on the choice of payment systems and its security perception;
- Additionally, further usability issues of the mobile payment app can be gathered;
- A formalized "threat" to influence the user's perception of the whole system, and to trigger especially the factor of cost of security.

The experiments described in the next chapter are built upon these requirements. The experimental results show the strength of the taxonomical relationships.

2.4 Summary

In this chapter a taxonomy of influencing factors of security-related user behavior was presented. It contains relevant taxonomical terms determined from the author's research and current literature. The taxonomy divides the area into two antagonist, user and attacker. As this research centers on the user's personal attributes, it segments the influencing factors on the user's side into three partitions: user-related, interaction-related, and device-related factors. All factors will be explored in a series of experiments using a mobile payment prototype application.

Is the taxonomy complete? Certainly not. First, it is an iterative process, refined through results from experiments based on the current version of the taxonomy. Second, there can always be *more* factors, or a re-arrangement of the dependencies is required. As happens all the time in the already mentioned analogy of taxonomies in biology: There are new species found every day. Is it complete enough? Certainly, if it helps to achieve the goal – in this case to find the influence of personal attributes and security methods on perceived security and usage of mobile payment.

The formalized taxonomy delivers a (visualized) overview of the field of research, its main actors and their influencing factors. Some assumptions and hypotheses are easily drawn. For example, risk averse users are assumed to avoid using mobile payment more often, because the app is unknown to them. Technophiles will use the application more often, just because it is a new thing. Linck et al. (2006) states that "[a]t merchants with no good reputation consumers have always been concerned about using debit or credit cards." A "shady" shop will see less frequent use of mobile payment as people might think their devices will get compromised. Less "usable" security methods will see less frequent use.

The hypotheses for the relationships between taxonomical factors are:

- H1: There is a positive relationship between personality, experience and knowledge (of computers) and usage of (intention to use) mobile payment.
- H2: There is a negative relationship between cost of security (by implemented security methods) and usage of mobile payment.
- H3: There is a negative relationship between the perceived risk (concerning environments) and perceived security, and usage of mobile payment.
- H4: There is a positive relationship between application design (trust inferred by object) and security perception, and usage of mobile payment.
- H5: There is a negative relationship between (financial) threat and perceived security, and usage of mobile payment.
- H6: There is a positive relationship between an institutions reputation and usage of mobile payment.

The taxonomy extensively covers the areas "surrounding" the user while using a (mobile) device for financial transactions. The taxonomy is not too specific to be applicable only to mobile payment applications, but rather to be used for user-centered computer-related (financial) tasks and threats. The taxonomy is not intended to reveal latent variables, but rather to map already *established* personal factors to the research variables perceived security and usage of mobile payment.

Chapter 3

Experiments

The previous chapters unfurled the motivation and the theoretical background for one of the main goals of this research, which is to find *to what degree* taxonomical factors influence security perception and usage of users interacting with a mobile payment system in order to support developers finding suitable solutions. To gather data in all relevant areas where – according to the previously presented taxonomy – influencing relationships should occur, the experiments cover essential factors from all taxonomical areas in the test design.

The experiments had to conform to several limitations. Beyond the usual budget constraints within research projects, the main reason to run the tests in a laboratory was that at the time of conducting the experiments (from early 2010 to mid-2013) there was no usable infrastructure for a field test. At the time, when the experiments were started, no mobile wallet using the existing payment network was on the market. Of the four German mobile network operators, the first wallet system was launched by Telefonica Deutschland under their O_2 brand as the *O_2 Wallet* in early 2013. But this product was not advertised and had to be actively requested by its customers (underscoring this, was the exclusion of the product's website from Google search via its robot.txt from early 2014). This was followed by Vodafone Deutschland's *Vodafone Wallet* at the end of 2013. *MyWallet* by Deutsche Telekom, the commercial successor based in part on the prototype used in the experiments, was launched in May 2014. E-Plus Mobilfunk launched their mobile wallet product under their BASE brand as *BASE Wallet* in July 2014.

There are several other technologies required to introduce smartphone-based payment. The one used here is an extension of the contactless payment card which is based on Near Field Communication (NFC) and a (U)SIM-card-based secure element to store payment card data (which is stored on the visible "chip" of plastic payment cards common in Europe). This secure element is a special compartment on the card and stores encrypted payment card data based on a Java card applet, which can be accessed only via special channels with access to the required key. These applets are certified and provided by payment scheme owners like MasterCard or Visa. The type of mobile payment applications used by several mobile network operators can be accessed only "over-the-air" via network elements available to the carriers.

As already mentioned in Chapter 1, other offerings use QR codes, either scanned by the point-of-sale system or by the smartphone application. Also, systems using a transaction authentication number (TAN) and face recognition (done by the cashier) are on the market. The latter systems were not included as test devices and applications, because they are tied to specific commercial vendors and do not adhere to industry standards. Also, most of these applications were geographically limited to the USA.

As laid out in Chapter 1, NFC-based and payment-scheme-backed mobile payment involves several players and numerous network elements. Due to regulations of the financial sector from both governing bodies and the industry itself, a test using "fake" accounts or mock-ups involving real money is forbidden (e.g. anti money-laundering act, DIRECTIVE 2005/60/EC). Thus, using real accounts (and real money) would require the whole infrastructure already to be installed. Even if this had been the case, a field test would either have involved only "early adopters" or participants, who would have had to go through a lenghty registration process (including credit rating) only for participating in an experiment. Because most people do not have preconceptions about new technology prior to exposure, it can be doubted that this way the test would have included a wide sprectrum of participants *ad-hoc*. The only working alternative was to set up lab experiments.

The experiments tried essentially to measure as many taxonomical terms concerning personal factors as possible. The lab experiment had to gather the relevant data while depicting the use of a mobile payment system as accurately as possible. The results show how the taxonomical factors are weighted and connected. They are also used as the basis for the behavior model developed in Chapter 4.

3.1 Design and methods

The experiments were designed to gather data for the taxonomical factors. The taxonomy was derived from considerations about computers in general and is therefore basically generic for a user's security perception of using a computer. The practical focus in this work is on mobile devices and especially on using mobile payment applications.

Speaking in taxonomical terms, the intention of the user is to buy goods at a store. With the mobile payment application, there are now three main choices how to pay at a retail point-of-sale: cash, card, or app (a fourth option would be to pay with vouchers, which is more or less a cash equivalent). He or she perceives the store environment, other customers, the familiarity and convenience of the payment methods, and the perceived risks and costs of security using a specific method. The choice can be influenced by what method the customer just before in line is using, or what amount has to be paid. The user can even think about threats to each method, like shortchanging, credit card fraud, or a computer virus. Maybe one of the threats was mentioned in the news recently or there was a conversation about them among colleagues. Figure 3.1 shows which taxonomical areas have to be considered in the experiment's design.

The participants in a field test ideally would have a smartphone-based mobile payment system connected to their real bank accounts and they would use it in their daily shopping routines with their own money. The users would visit different shops on different occasions in different areas with different goods to buy. They whould be exposed to various environments, a steady stream of

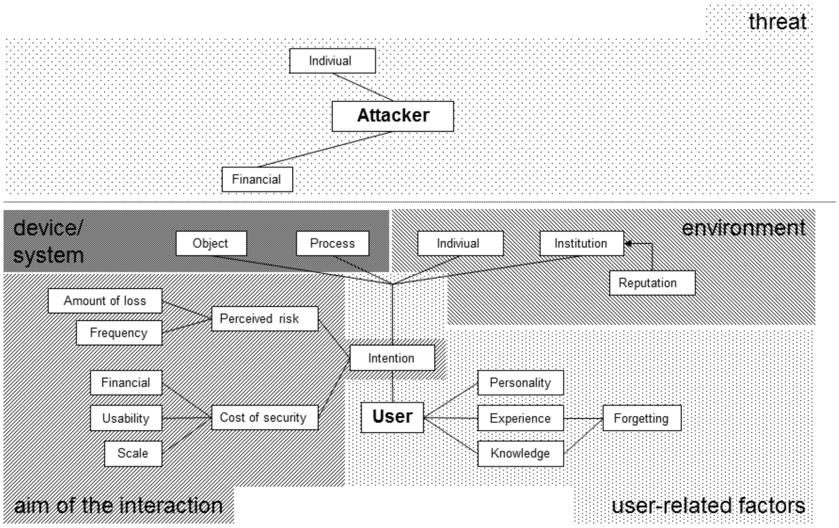


Figure 3.1: Taxonomical areas addressed in the experiments, modfied from Sieger et al. (2011)

friends, colleagues, strangers, the occasional threat, reactions, opinions, and news, which may or may not influence the participants' perception of the mobile payment system. A field test can also last longer than a lab experiment. While there are lab experiments that can go on for weeks and months, this would not suit an experiment were the participants' concern is about the choice of a payment method. The perceptions, opinions, reactions, and usage could be gathered via interviews or diaries, possibly by monitoring the behavior while paying in a store.

The experiment should ideally "emulate the field in a lab". One possible solution would have been to outfit *some* stores with a (closed-loop) payment system, which would use the mobile payment app as a front-end while having a back-end completely different from the NFC ecosystem, but which could emulate it. The difficulties are to infuse *real* money into the system and to have additional and separate point-of-sale systems at the stores. Such systems have also to conform to financial and tax regulations. Additionally, participants would have had to coordinate their finances on two separate streams – traditional cash and payment cards, and the new mobile payment app. This app would not be seemlessly incorporated into the participants' every day life, which would probably alter their perception of the new device.

These restrictions lead to the decision to conduct the experiment completely in a lab environment. This way, parameters could be controlled and variables altered in defined areas. The difficulty in this case is to compensate for the lack of reality or at least a realistic environment. The experimental setting did not completely disguise, that it was merely "playing shop". Because it did it so for all payment methods, the assumption is that while behavior might be affected by it, any bias would be balanced between these experimental conditions.

Some of the taxonomial factors are more or less "stable", for example a user's personality traits, others might change under certain circumstances, for example, the choice of a payment method, or how many items a participant bought using the mobile wallet, and how she or he perceived the security of this payment method. These are the *dependent variables.* The research hypotheses assumed that there are dependencies on a number of taxonomical factors. These were the *independent variables.* The five areas of the taxonomy were addressed as follows:

User-related factors: The data concerning these factors was collected using standard and self-developed questionnaires. The standard questionnaires consisted of "BIG Five" (Gerlitz and Schupp, 2005), which are the dimensions of human personality described by five factors – openness, conscientiousness, extraversion, agreeableness, and neuroticism. Risk perception and risk behavior was measured with "Domain-Specific Risk-Taking – DOSPERT-G" (Johnson et al., 2004). In order to detail technology-related personality traits the questionnaire "Technische Affinität Elektronische Geräte – TA-EG" (technical affinity – electronic devices) was used (Bruder et al., 2009). A self-developed questionnaire was used for demographical data and asked for knowledge and experience related to computers and smartphones. The focus lay on the *internal* (personal) factors rather than on *external* (social) influences: How *personal* is mobile payment?

Aim of the interaction: The aim of the "interaction" was to buy several goods in different stores. The goods were priced in different categories. The user had a choice of three payment methods: cash, payment card, or mobile payment app. Perceived security and perceived risk was measured using a short questionnaire (see Appendix).

Computer system: The perception of the usability of the mobile payment application was measured using "System Usability Scale SUS" (Brooke, 1996), and the user experience, especially hedonic and pragmatic qualitiy, using "AttrakDiff" (Hassenzahl and Monk, 2010).

Environment: The environment consisted of two to four different"stores" set up in the lab. The difference was used to vary the taxonomical "institutional" and "individual" impact on the customer. For example, an administrative office and a newspaper kiosk could have a different "reputation", which could possibly lead to different behavior. Data on further environmental factors addressed in the taxonomy like exposure to media was not collected as this would require a longitudinal study to gather relevant data.

Threat: A threat was realized by "attacking" the payment process in certain situations regardless of the chosen payment method. The customer was either shortchanged or presented with an overpriced receipt by the cashier. This represents the *individual attacker* of the taxonomy and also put an physical element into the threat, because the cashier and participant-customer were in the same store. The threat did not gather data on all taxonomical factors, but concentrated on "device" and "financial". The threat simulated conventional fraud (or a mere mistake by the cashier) and not an attack on the technological advancement of the mobile payment system, e.g. by simulating data theft or the sometimes stated fear of "drive-by" fraud by utilizing the NFC capabilities. As all payment method were attacked, the threat had to work on all of them in the same way to trigger comparable reactions. In this regard, the threat might not be one of those users fear the most like physical theft of the device or wireless network attacks (Chin et al., 2012).

One problem was the question what should threaten mobile payment. Usually, a financial threat involves loss of money. As no real money could be used, the threat was also *not real*, because it did not attack the participant's own *real* money. On the other hand, there was no way to involve a real threat in the experiments, due to the risk that using real or even their own money would have made the participants reluctant to spend it *at all.* Using the participants' compensation also would have severely limited the difference in price categories to a maximum of 20 Euro. Additionally, the threat should not single out a specific payment method as being less secure, because that is not the case (at least it cannot be quantified yet, if there is any difference). Thus, the effect of the threat could be somewhat diminished. This is further discussed in the section on results.

Another limiting factor in the design of a financial threat is an ethical issue. Financial loss can be an emotional burden. Within the test environment the threat is restricted to the lab and its symbolic money. But in a field test, the participants either know that the threat is not real (and they would get their money back), or the threat could put a lot of stress on them. Waiting for a *real* attack to happen would probably take too long as these are statistically very rare (Herley, 2009), especially in the case of a closed-loop test implementation of a mobile payment system.

To formalize user behavior in dealing with computer systems, it must first be quantified. For this, a user must be placed in a realistic situation, taking into account the above-mentioned factors, in which the test subject shows realistic behavior; at the same time, however, the factors must be controlled and the behavior of interest must be present for a limited period of time with sufficient frequency in order to quantify it without too much measurement error.

In the tests two *predictor variables* were changed – risk perception of a threat through "attacks", and security perception (of protective means) through the implemented security method. The main results are "perceived security of the security method used" and "frequency of specific payment method used" by the participant.

The experiment setting had to compromise on the ability to collect data in a timely way. Also, to make the data points comparable, a strict sequence had to be specified. If the participants were allowed to shop freely, more participants and a longer shopping sequence would be required in order to sum over the different shopping habits and preferences. It would have been impossible to discriminate between item prices. This way, the shopping sequence comprised of a somewhat *sped-up* shopping experience, because one usually does not rush through several shops in quick succession to buy one or two items and than *return* to the same shops again after a short pause (in which the participants rated their security perception of using the mobile payment application).

One of the key guiding questions concerning methods is whether they are valid and reliable or not. The test design generally followed standardized (textbook) principles and guidelines (Möller et al., 2011). The experiments had a three-part design. The first part collects data on participants' personalities, the second part is reserved for the practical test of the mobile payment app, its use, and users' perceptions. The third part again consists of questionnaires, but this time focuses on the app itself.

3.2 Mobile payment system

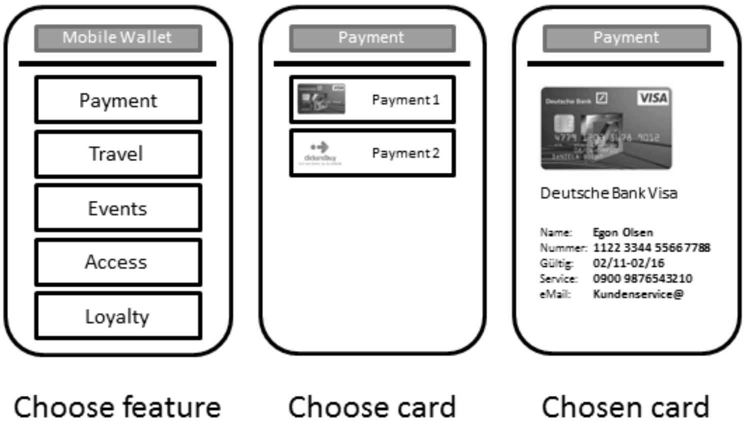
The mobile payment application was a prototype built by Deutsche Telekom. It had the advantage of coming with the source code and thus could be adapted for other security methods than the default PIN. The fingerprint mock-up used in test 5 was implemented by the author.

The prototype used in the experiments used some parts of the mobile payment infrastructure, but no real transactions using a payment network were done for regulatory and technical reasons. As is laid out in Chapter 1, the network elements provided by the mobile network operator are used to send the payment card data to the secure element on the NFC SIM card. Being a prototype mobile payment system, the existing parts of those network elements were the NFC SIM card to store card information, and a simple version of a trusted service manager, which usually transports the encrypted payment card data to the secure element via the over-the-air channel. For the experiments it was used as a web-server to download simple dummy card data and card images. No over-the-air provisioning was done. All data was pre-provisioned on the SIM card, and "hard-coded" into the Wallet application.

The Android versions used were 2.3 and 4.0. Over the course of the experiments, two different handsets were used, a HTC G2 Touch and an LG Nexus. The HTC device had a small external NFC tag taped to the back of the phone. The prototype system's modality was the standard Android-based smartphone touch-based GUI. The phones were locked using the default "slide to unlock" screen. The mobile payment application itself had no further security features other than PIN and the app remained the same except for test 5, where the security method was changed from using a PIN to a mock-up fingerprint recognition. The application did not generate any feedback, such as for successful usage (e.g. vibrations), warnings (alarm sounds), pop-up messages, or virtual receipts after successful payments.

The application itself was placed on the homescreen depicted by an icon showing a symbolized wallet and was named "mWallet" (renamed to "MyWallet" for commercial launch). Upon starting the application the first screen was seen by the user, allowing to choose one of the five features of the wallet application. The features were explained to the participants. "Payment" for storing contactless NFC-based payment cards; "Travel" for storing travel tickets (e.g. train, airplane); "Events" for storing event tickets (e.g. concerts); "Access" for storing keys (e.g. rental car, office); and "Loyalty" for storing loyalty cards. Participants were told, that the focus of the experiment would be payment. Upon tapping on the "Payment" button, a list of all stored payment cards was shown. The experiment's prototype showed two different payment cards, one issued by Deutsche Bank, another one by Click & Buy (a subsidiary of Deutsche Telekom). Another tap on one of the cards showed the card's details (see also Sieger et al. (2012)).

A user had to choose a payment card in order to start the payment process, then had to tap on a "Pay" button in the app and provide either no authentication, a PIN, or a fingerprint. To finally complete the transaction the handset



Name: Egon Olsen
Nummer: 1122 3344 5566 7788
Gültig: 02/11-02/16
Service: 0900 9876543210
eMail: Kundenservice@

Figure 3.2: Mobile Wallet prototype GUI screens

had to be tapped against the point-of-sale terminal. This user flow is equivalent to the *manual* mode implemented in mobile payment application like Deutsche Telekom's myWallet and other mobile network operator's products. The alternative *express* mode – often called "Tap & Go", a MasterCard trademark – defines a default payment card set by the user and initiates the payment without further user interaction with the app. The smartphone is just tapped against the payment terminal and the payment is done (as long as the threshold for authorizing of the payment is not met, usually 25 Euro or 20 US Dollar). A variant of this method is used in Apple Pay, where the user taps an iPhone against the terminal while simultaneously using fingerprint recognition on the device as authorization (Apple Pay is only available for iPhone version 6 as of end of 2014). Express mode was not used during the experiments.

Neither technical details were explained to the participants nor a comparison of other wallets to the prototype system were made, because there were no other systems available on the German market (and apps like Google Wallet just started in the US only). Some test users had heard or read about how mobile payment works, but had not seen any system in action.

The mock-up fingerprint recognition was designed to replace the PIN-based security method in the mobile payment prototype for test 5. It was chosen because of the high ratings it got in focus groups (Dörflinger et al., 2010) and surveys (Ben-Asher et al., 2011). The fingerprint recognition method was inserted into the provided source code of the prototype mWallet. It showed a symbolic fingerprint on the screen. Upon touching it, the mock-up generated an up-down "scanning mechanism" of the fingertip's surface. The mock-up randomly rejected one in ten attempts for a more realistic application behavior. The smartphone models used for the tests had no built-in fingerprint sensor – no such smartphone device was available at the time (see also Chapter 1). Instead, the fingerprint "recognition" was done by placing a thumb on the touch-screen. No explanation was given to the participants. It was up to the individual to believe, whether this was a working version of fingerprint recognition or not. At the time of the experiments, there was no commercially available mobile payment application using fingerprint recognition as a means of *payment authorization.*

3.3 Experiment setup

The basic test design is based on a retail store environment with several shops, where test users had to buy different goods and had to repeatedly buy them under varied conditions. The laboratory setting generated the security-related user behavior of interest in a temporally compressed form – i.e. more frequently than expected in reality –, which is necessary to collect reliable quantitative data in a limited test period. Nevertheless, the situation should appear realistic to the user (see also Sieger et al. (2012)).

The test was in general designed around three main parts: the questionnaires concerning BIG Five, technical affinity, and risk behavior and perception; the test of the payment app; and the questionnaires concerning use and perception of mobile payment and the app itself. The different test runs varied in several areas: modifications of the self-developed questionnaires; variation of the shop setup; different security methods (none, PIN, fingerprint recognition), and security threats ("attacks").

The following factors were collected: usability and security, level of threat, and risk perception and attitude of the users. Usability and security were varied by changes in the authentication process (different authentication methods by using PIN or fingerprint recognition, or no method). The extent of the threat was simulated by the amount of money at risk. This method was chosen because it seemed to be very unlikely to generate many security-related threats within an hour on the same target. The willingness to take risks is measured using a screening questionnaire.

For the collection of the described factors the following steps were done:

- Invitation of participants, classification of groups of subjects, recording of the test series;
- Collection of data with 88 participants (approx. 20 users per test);
- Formalization of all interaction and perception ratings for the subsequent behavior model;
- Execution of the tests, together with logging and the subsequent analysis (all manual annotation) and processing the obtained data;
- Lab test 1: mWallet, test with a fully fictionalized setting, the shopping sequence was interview-like;
- Lab test 2: mWallet, four shops, no security method and attacks;
- Lab test 3: mWallet, four shops, with an without PIN, with and without attacks, two participants per run;
- Lab test 4: mWallet, two shops, with PIN and attacks;
- Lab test 5: mWallet, two shops, with fingerprint recognition and attacks.

The first part of the experiment consisted of general questionnaires to collect data on user-related factors (duration of approx. 20 minutes): Demographic information; experience with computers, mobile phones and applications such as text messages, e-mail, and mobile internet; risk perception using mobile phones;

influencing factors for using an electronic system. These questionnaires were jointly developed by the author in collaboration with Niklas Kirschnick. For the questions in the first part the following established questionnaires were used: Big Five Inventory questionnaire (Gerlitz and Schupp, 2005); Technical affinity – electronic devices ("TA-EG") (Bruder et al., 2009); the Domain-specific Risk-taking Scale – German Version (DOSPERT-G) (Johnson et al., 2004). There was no intervention by the supervisor, but participants were able to ask for clarification.

The second part consisted of a sequence of shopping events to address the taxonomical aim of the interaction and the threat (duration of 20-30 minutes). The participants were handed out the mWallet prototype device, a symbolic debit card, some symbolic cash, and a symbolic ID card. From the second run of the experiments onwards they also got a shopping bag to carry the goods "bought" at the different shops. The shopping sequence was divided into four blocks. The first block consisted of 8 pre-defined transactions (3x Mobile Wallet, 3x debit card, 2x cash) and one access event by opening a door using a key or the Mobile Wallet. After each transaction a paper receipt was handed out. During the second block with 6 transactions the participants were free to choose their preferred method of payment and access. The third test block consisted again of 4 pre-defined transactions (1x Mobile Wallet, 2x debit card, 1x cash) and was used to simulate security threats by handing out incorrect receipts or short-changing the buyer (cash-only). The fourth block consisted of 7 free-choice transactions. The participants were now *biased* from the experience before. The four blocks generated 25 transactions for every participants, at least 4 using mWallet with one simulated security attack targeting the app. The participants rated mWallet for overall impression, usability, and security (using it like depicted in Fig. 3.2) after each block.

The third part consisted of questionnaires specific to the usage and usability of mobile payment and the perception of the different stores. This covered the taxonomical areas environment and system (duration approx. 15 minutes). The participants were asked how they perceived the features of the mobile payment application and to rate their impression regarding overall opinion, usage, security, and interaction. The questionnaires used were AttrakDiff mini (Hassenzahl and Monk, 2010), which is used to measure perceived product attractiveness (ATT), which is composed of pragmatic quality (PQ) and hedonic quality (HQ), and the System Usability Scale (SUS) (Brooke, 1996).

In the first test, participants sat at a table and used the mobile payment app (prototype "mWallet") in an interview-like situation, where the test supervisor would ask the participant to imagine several payment situations and to use the device accordingly. In the second and third experiment four more realistic stores were built for simulated shopping (administrative office, newspaper kiosk, supermarket, movie theater) to have different shopping environments from "formal" to "relaxed". The stores, office and cinema were fitted with several real goods like sweets, cigarettes, and beverages (different category price levels). Posters and similar accessories were used to enact an appropriate environment. For tests 4 and 5 the number of shops was reduced to two, a kiosk and a supermarket. In all experiments the participants used symbolic cash, a symbolic debit card, and mWallet. Each participant was tested individually, except for test 3, where two participants were tested simultaneously.

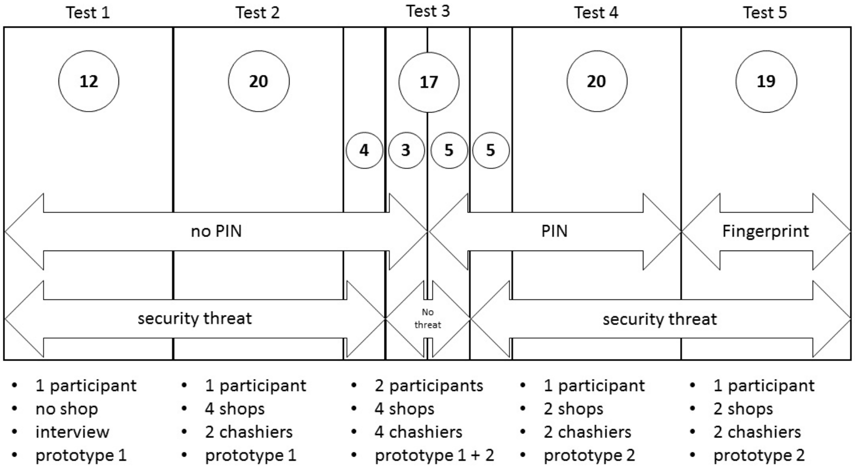


Figure 3.3: Test overview

To avoid bias in regard to security issues the participants were told that the experiment would be about mobile payment systems in general and not particularly about security perception.

The decision to use all payment methods in symbolic form was made to avoid any bias towards any of the three methods. If real cash or a real payment card had been used, it would have separated these methods from mWallet. The prototype was introduced as such, and would have stood out from the two other methods, if they were real.

Test 1 to 5 vary one or two variables, which are assumed to be orthogonal, from the following: presentation and number of shops, number of concurrent customers, security method used with the mobile payment app. Minor modifications were done on the questionnaires concerning demographics, and additional questions about possible future use of mobile payment.

Figure 3.3 shows the different test runs with the number of participants in circles. The security methods used are shown in the upper arrows, and whether a threat was made or not is shown in the lower arrows. The bullet points list the number of concurrent participants, the number of shops, the number of cashiers, and the prototype use (where prototype 1 is the smartphone made by HTC, and the prototype 2 is the smartphone made by LG). Except for test 3, the test supervisor was also one of the cashiers.

3.3.1 Test 1 - preliminary test

The first test had 12 participants. The age distribution was from 19 to 40. 50 percent were female, 50 percent male. The participants answered to flyers spread across the university campus at the Technical University Berlin. Each participant was tested individually. The compensation was 20 Euro.

The main goal of this test was to evaluate the test design itself. The duration for the three parts of the test were measured – questionnaires about personal traits, shopping with the mobile payment app, and the questionnaire about using the wallet. It was also checked how long it took to introduce the test and show and explain the mobile wallet prototype to the participants.

The concept of a mobile payment system and a mobile wallet was explained to the participants. The focus was on the payment part, but also an overview of all other use cases implemented in the prototype was given. Because the interaction for paying with the mobile wallet is very short, the explanation could be done in a few minutes. The procedures for installation, registration, provisioning, or how to change settings of the device or the mobile wallet were not covered. In this test, the mobile wallet had no security method (e.g. PIN).

The participants then sat down on a table for the questionnaires on personal traits. The test supervisor usually sat in the same room on a different table out of sight of the participants. In some instances the supervisor left the room for a few minutes. Filling out the questionnaires took on average 20 minutes per participant.

The introduction how to use the mobile wallet was repeated and the experimenter sat down on a table opposite of the participant. They were outfitted with the mobile wallet prototype, "cash" (printed pictures of Euro denominations), a substitue plastic payment card, and an substitute ID card (printed pictures of the German standard sample ID card).

In this preliminary test the practical part consisted of showing the participant printed pictures of several commercial goods, which the participants were about to buy. They were instructed to tell spontaneously what kind of payment method they would use to buy the shown item. The payment process was partly enacted, but not for every iteration of the sequence. The choice was registered on paper by the instructor. The sequence was segmented into the four aforementioned blocks. This part of the test took 20 minutes on average.

After finishing the shopping part, the participants answered the questionnaire about mWallet. The duration of this part was again 20 minutes on average. Overall the test was finished within an hour.

3.3.2 Test 2 - 4 shops, 1 customer

The second test had 20 participants. The age distribution was from 20 to 49. 40 percent were female, 60 percent male. The participants answered to flyers spread across the university campus. The compensation was 20 Euro.

The second test kept the questionnaires untouched, but altered the second part of the experiment from an abstract interview about what payment method the participants would use to a more realistic situation, where the mobile payment application was actually used, if the participants chose to do so.

The test design was altered to enhance the shop experience by setting up mock-up stores instead of the purely imaginary ones in the previous experiment. Four shops were set up in two rooms in a building of the Technical University of Berlin. Example photos can be found in the appendix section on the store concept. One room was usually used as an office and the other as a meeting room. One desk was decorated for each shop with different items and a point of sale with a contactless terminal. The terminal was an NFC-enabled PIN-pad and could also be used to insert payment cards. The receipts were pre-printed on paper and mimicked real receipts.

The main fear was, that participants may object the idea of "playing shop" as being too childish, thus undermining the concept, but none of the participants rejected the idea or was visibly offended by it.

The questionnaire parts at the beginning and at the end of the test remained in place. The shopping experience resembled a real shop within the limited setup. A lot of role-playing was certainly involved as each shop consisted mainly of all items being "bought" within one of the four shopping sequences. The main difference between the interview setup and the shop was, that participants had to actually walk to a store and go through the motions of buying things – pick up items, pull out a wallet or a purse or use the mWallet, pay, and put the goods into a bag.

Threatening the payment method through shortchanging and overpriced receipts was not immediately perceived as such by all participants. In this case the cashier made the participant aware of the fact. The threat was mainly done to inspire an awareness that each payment method has a (small) risk of financial loss.

3.3.3 Test 3 - 4 shops, 2 customers, 2 security methods

The third test had 17 participants. The age distribution was from 19 to 40. 65% were female, 35% male. The participants answered to flyers spread across the university campus. The compensation was 20 Euro.

The test design was changed to enhance the shop experience by having a cashier at every mock-up shop all the time. Additionaly, two participants were shopping at the same time to lessen the experience of being the lone customer. Also, some time a line formed, adding the experience of seeing what payment method was used by the other customer. With four cashiers and two participants the lab was sometimes feeling "crowded", but as the data revealed, these added touch of realism did not alter the behavior in a significant way.

The major deviation from all other tests was, that the attacks were waived for 8 of the participants. This was also the first test were a security method (preconfigured PIN "1234") was introduced. All previous tests were done without using a security setting for mWallet.

3.3.4 Test 4 - 2 shops, 1 customer

The test had 20 participants. The age distribution was from 20 to 36. 40% were female, 60 percent male. Again, the participants answered to flyers spread across the university campus. The compensation was 20 Euro.

The test design was altered again and the shop experience was reduced to two shops. Additionaly, the questionnaires during the shopping sequences was enhanced.

3.3.5 Test 5 - 2 shops, 1 customer, new security method

The fifth test was primarily reserved for introducing a new security method, fingerprint recognition, and to provide data for any predictive model (and possible simulation) for this security method.

The fifth test had 19 participants. The age distribution was from 20 to 48. 42 percent were female, 58 percent male. The participants answered to flyers spread across the university campus. The compensation was 10 Euro.

The test design was the same as in test 4, but another security method had been implemented into the prototype. This time a mock-up fingerprint reader was used, which was injected into the prototype's source code to replace the PIN. The fingerprint recognition replaced the PIN entirely. It was not intended that users could switch to PIN to authenticate.

The fingerprint mock-up filled the entire screen with a white grid on a black background. A fingerprint in real size was shown and the participant placed her or his thumb on the touchscreen. The mock-up simulated a authentication procedure by scrolling a line up and down for a second and provided authentication with a pre-defined failure rate of 10%.

3.4 Results

Five tests runs with several modifications and variations were done over the course of two years from mid 2011 to mid 2013. Overall 88 people participated. Using the laboratory situation a number of experiments were carried out with test persons of a mostly homogenous group – students. The subjects were classified using the previously described questionnaires so that their personal traits could be considered as influencing factors. These included personal attitude towards technology, personal experience with computers and smartphones, and different aspects of the usability of the mobile payment application. User behavior during the experiments was recorded on paper and later transferred to electronic form. In parallel, the subjects were asked after each of the four test sequences to provide subjective judgments ("gut feeling") of their perceived security.

Participants were between 19 and 49 years of age, with an average of 25.8 (SD = 6.48). 41 participants were female and 47 male. 83% were university students, 17% were employed. All participants rated themselves as (very) experienced using electronic devices. All ratings were at least 3 on a 5-point Likert scale ranging from 1 (little experience) to 5 (very experienced); computer and internet use have similar ratings, mobile phones slightly less. The average experience rating over all systems was 4.4 (SD = 0.8). While all considered themselves computer-literate, not all showed high ratings in technical affinity. All participants owned a mobile phone, 53.4% of those were smartphones and approx. 30% used the screen lock with a PIN.

The results aim at interpreting the taxonomical factors while also establishing a suitable (possibly predictive) user behavior and perception model for developers. The former requires statistically significant numbers, the latter results concerning appealing security methods and increased application usage. As was shown in the previous chapters considerations about how to improve perceived security lead to order all possible influencing factors in a taxonomy of security perception. 88 participants generated 32,680 usable data points, among them 1338 payment transactions in the free-choice sequences 2 and 4, and 429 ratings for security perceptions in sequences 1 to 4 as well as final overall ratings.

The associations within the taxonomical areas – user, interaction, device, enviroment, and threat – are mostly direct "dependencies". For example, a

Demographics – user-related		
Gender	Age	
Experience and Knowledge – user-related		
using computers	using the internet	using mobile phones
using a smartphone	using app stores	using mobile internet
Using security methods on mobile phones – user-related		
using a screen lock	trusting a PIN	restricting feature usage
Personality Traits – user-related		
Big Five		
neuroticism	extraversion	agreeableness
openness	conscientiousness	
Risk perception and behavior		
gambling	investment	[sum]
Technical affinity		
positive attitude	negative attitude	
competence	enthusiasm	
Device		
security method		
No method	PIN	Fingerprint recognition
Environment and Threat		
Threat	Store type	
Observations and results – aim of the interaction		
Security perceptions	[differences between sequences]	[sum]
Usage of mobile payment	[percentage of all payment methods]	[sum]
attractiveness	pragmatic quality	hedonic quality
SUS score		

Table 3.4: Variables used and extracted from experiments, with relation to taxonomical areas

user's personality, the system's cost of security, the device itself, the perceived risk, and the type of store should directly influence the dependent variables perceived security of using mobile payment and the frequency of use. In this regard, the taxonomy can be seen as a two-dimensional plane, where these *flat* dependencies can be computed as correlations between the various taxonomical factors collected during the experiments.

The correlation matrix in Figure 3.6 visually presents correlation levels of the main experimental results for participants using PIN as a security method as an example. One of the goals was to examine the relationships and hypotheses made in the taxonomy (see Chapter 2). The assumptions in designing the experiments were, that personality traits, security methods, and shop surroundings – among other factors – would influence security perceptions and choice of payment method according to the taxonomy. The color code shows the positively correlated items in blue, the negatively correlated items in red. Darker tones mean higher correlation. The matrix is mirrored at the diagonal from upper left to lower right. The items listed at the axis are agreeableness (from Big Five), positive attitude (from TA-EG), hedonic quality (from AttrakDiff), rated perceived security from sequences 1 to 4 and the overall rating, and observed usage of mobile payment (as percentage of methods used) during free-choice sequences 2 to 4 and their overall sum. Agreeableness is negatively correlated to security perception and usage. Positive attitude towards (consumer) technology is positively correlatec with security perception and usage. Perceived hedonic quality's correlation is comparably weaker.

All in all there are 38 variables related to the taxonomical terms presented in the following sections. An overview is shown in Table 3.4. 23 variables were computed from the results of the questionnaires (demographics, experience, Big Five, Technical Affinity – Electronic Devices, DOSPERT-G – risk perceptiona and behavior) in the first part of the experiments. Five variables – security method of the mobile payment app, threat, and store type – are part of the settings in the "hands-on" part of the experiments. Four variables are derived from the AttrakDiff and SUS questionnaires in part 3.

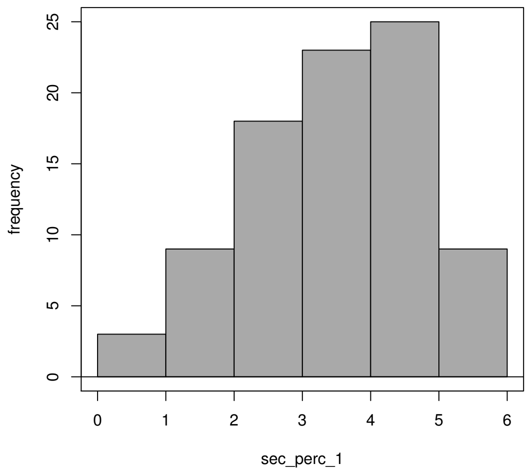


Figure 3.5: Exemplary skewed histogram showing perceived security for the first sequence.

Because some of the results are not normally distributed Spearman's rank correlation coefficients were computed for Figure 3.6 instead of the Pearson's for normal distributions. Figure 3.5 shows one of the skewed histograms as an example.

What can already be seen at a glance in the color-coded correlation matrix (Figure 3.6) – there are correlations between the assumed variables, but they are not particularly strong in every case. Computing the complete correlation matrix points to correlations not being directly relevant to the research goal itself, but nonetheless supporting the overall approach. Technical affinity

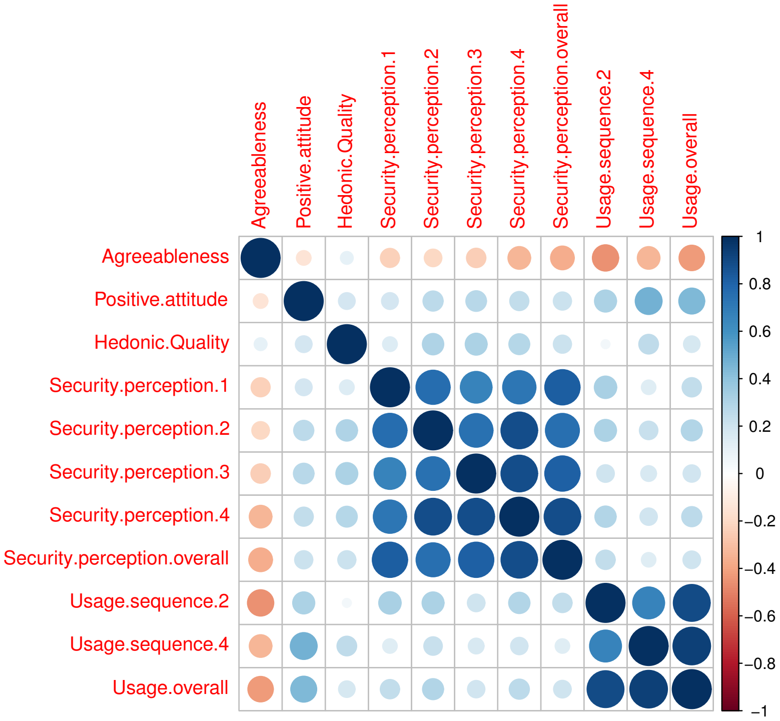


Figure 3.6: Correlation matrix for selected factors, results from participants using PIN as a security method. *Red* depicts negative correlation, *blue* depicts positive correlation, *darker* shade shows stronger correlation.

– enthusiam and self-described competence – correlates strongly with being a male participant. So does owning a smartphone and using an appstore. Second, the correlations of items belonging to the same questionnaires and observations show reliable measurement – which is what can be expected from widely used questionnaires and other research. Yang et al. (2012) found that "for potential adopters, behavioral beliefs, social influences (subjective norm and image), and personal trait (PIIT) are found to have significant and direct influence on adoption intention of mobile payment services".

There are some "visible" correlations of taxonomical factors, namely, using a PIN as security method for the mobile payment app and security perceptions are positively correlated. The same goes for using PIN and the frequency of use of mWallet as a payment method for more expensive goods. There are also correlations between positive attitude of technical affinity and security perception and use of mobile payment as a payment method for goods over all price categories, albeit relatively weak ones. A stronger correlation can be found between negative attitude of technical affinity and the willingness to use mobile payment for expensive goods. Interestingly, there is a similar negative correlation with risk behavior towards investments. Of the Big Five traits "Agreeablenes" shows the strongest (negative) correlations to security perception by far.

This supports the relationships in the taxonomy from usability, cost of security, and intention. Perceived security is “good enough” using the mobile payment systems compared to the alternatives cash and card. The usability scores are high (SUS and AttrakDiff). The influences of personality traits (including risk perception and technical affinity) and experience are there, too.

Of course, there are expected correlations (and the test design reflects this), which cannot be seen directly. The “threats” neither seem to significantly influence perceived security when using the ratings directly. But the threat had a notable effect, if the mean of changes from unthreatend sequence 2 to threatened sequence 3 is used. A difference in the security perception was expected after sequence 3 where the threats against each payment method was placed by shortchanging them or using pre-printed bills showing a higher sum than the item(s) the participants just bought. Additionally, the threats were placed on all three payment method, in order to not provoke a bias. The results of the individual taxonomical factors of Table 3.4 are presented and discussed below.

3.4.1 Gender and age

An observation concerning gender differences was published by this author in Sieger et al. (2012). The results were based on experiments 1 and 2 and analyzed differences in security perception and usage of mobile payment by gender. During the sequences where the participants could choose freely between the three payment methods, female test users used the mobile payment system significantly less than male test users. Female test users perceived the security of the system slightly (but still significant with $p = 0.04$) higher than male users.

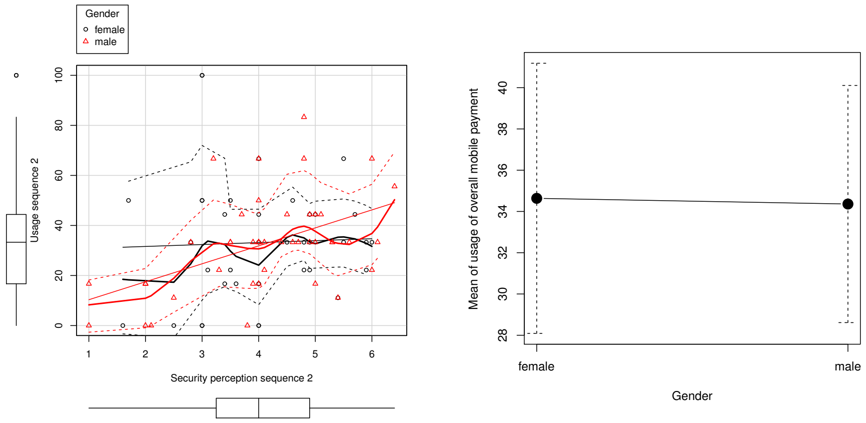


Figure 3.7: Gender. Boxplot shown an axis. *Left*: Gender and security perception. Black solid lines: smoothing curve and least-squares, men. Red solid lines: smoothing curve and least-squares, women. Confidence intervals (dotted). *Right*: Comparision of means of usage, female vs. male.

Although women had a higher perception of the mobile payment system’s security, they used it far less for purchase. Female participants accounted for only (adjusted) 40% of the purchases using the mobile payment system, while 60% were done by men. The usability scores (SUS and AttrakDiff mini) were

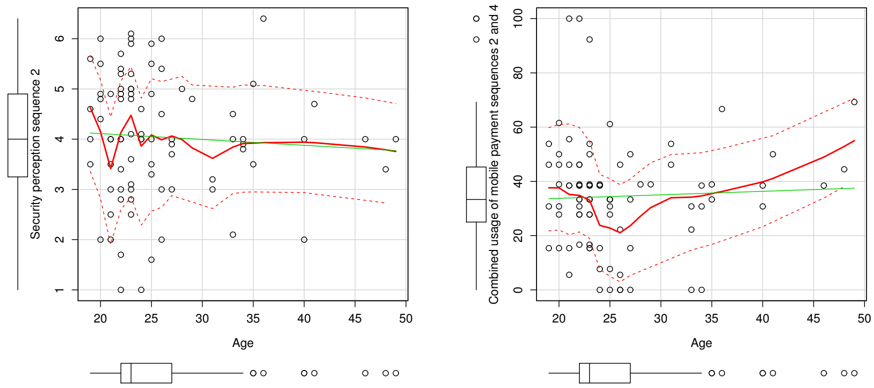


Figure 3.8: Age. *Left*: Age and security perception sequence 2. Green Line: least-squares. Red solid line: smoothing curve. *Right*: Age and usage. Red lines: smoothing curve and confidence interval.

nearly identical for male and female users, so this should not cause the difference. When asked for a possible future use of the mobile payment system, the answers are in line with the observed usage. On the same scale women answered with an average score of 3.43 vs. 3.61 for men.

There was a significant difference in the perception of security of mobile phones found in experiments *1 and 2*. In the surveys and focus groups women also tended to have a higher perception of the security of a particular system or method than men. They perceived biometric authentication methods and applications like mobile payment to be more secure (Dörflinger et al., 2010; Ben-Asher et al., 2011). The outcome is inconclusive. Women were far more willing to use alternative authentication methods, but showed reluctance to use a mobile payment system. One could attribute, that the former was just a statement, while the latter was actual usage of the system (albeit in lab test, experiments 1 and 2).

The differences were *not* preserved with the subsequent experiments. A Welch Two Sample t-test for security perception for sequence 2 by gender resulted in $p = 0.9615$. The calculation for overall use of mobile payment by gender is $p = 0.9493$. The diagrams in Figure 3.7 shows that there is no discernible difference both in security perception and usage.

Even if the differences would have been preserved, could any “design guidelines” be derived from the results? There should be some reluctance. The cliché “women’s phone” is often differentiated by manufacturers through color or fashion applications (both software and hardware). Any possible differences in security perception and usage could be erased after the introduction of mobile payment systems once the novelty factor wears off. But any differentiation of a mobile payment application through security features itself (the main differentiating factor) could not address gender differences. Nonetheless, a definitive answer whether gender produces significantly different outcomes requires further studies.

Calculating the influence of age on security perception and usage reveals no significant results as shown in Figure 3.8. The least-squares regression is nearly a flat line. This is a somewhat surprising outcome as the common assumption is that older participants would be more reluctant to use new technology. As all participants were under the age of 50 (with a median of 23), future tests should include older participants to study whether they differ in their perceived security and usage compared to younger users.

3.4.2 Personality traits

The questionnaires in the first block of every experiment asked for the personality traits of the participant concerning Big Five (openness, conscientiousness, extraversion, agreeableness, and neuroticism).

A user's personality traits are among the defined taxonomical terms and the hypothesis was, that they might have a strong influence on the perception and behavior shown in the security-related part of using mobile payment. A direct influence of a user's personality would be hinted at in any moderate to strong correlation between the individual personality traits and the perceived security and usage of the mobile payment app.

The overall calculations show no such relationship.

Security perception	N	E	O	A	C
sequence 1	-0.1557	0.0859	-0.0412	-0.0612	0.0994
sequence 2	-0.0275	-0.0155	-0.0263	-0.1500	0.1395
sequence 3	-0.0465	-0.1247	-0.1501	-0.2128	0.0721
sequence 4	0.0180	-0.09602	-0.0678	-0.2008	0.0590
overall	-0.1001	0.0878	-0.0067	-0.1260	0.0907
usage					
sequence 2	-0.1777	0.1144	-0.0302	-0.1426	0.1745
sequence 4	0.0362	0.0886	0.1038	-0.1161	0.0600
overal	-0.0717	0.1108	0.0441	-0.1398	0.1264

Table 3.9: Correlation coefficients of personality traits, security perception, and mWallet usage calculated over all experiments. N: Neurotiscism, E: Extraversion, O: Openness, A: Agreeableness, C: Conscientiousness

If restricted to those participants using no security method, *agreeableness* (being sympathetic and cooperative) has a significant moderate negative correlation (Pearson) with use of mobile payment with a coefficient of -0.4288, p = 0.01, for overall use of mobile payment, with -0.4511, p = 0.005, for sequence 2, and -0.3487, p = 0.04 for sequence 4 respectively. It also has a significant moderate negative correlation with the overall security perception with a coefficient of -0.3699, p-value = 0.03. All other coefficients are negligible. With the lack of any security method agreeable participants rated perceived security lower as others and seemed to be more reluctant to use mobile payment.

When controlled for those participants using PIN, *conscientiousness* has a moderate positive correlation (Pearson) with use of mobile payment with a coefficient of 0.2551 for overall use of mobile payment, with 0.3857 for sequence 2, and 0.02751 for sequence 4 respectively. All other coefficients are negligible. As conscientiousness is the personality trait of being thorough and careful, this fits with the result. A security method being present, the conscientious person uses mobile payment more in sequence 2, but as soon as the system is compromized is reluctant to continue using it. As all payment methods are compromized, mobile payment can be interpreted as the method where reversal of fraud seems to be the most difficult.

As the relevant data for the experiment introducing fingerprint recognition is not normally distributed (as opposed to the data of experiments 1 to 4), Spearman's rank correlation is used. Here, *openness* and overall use of mobile payment correlate significantly with cor = 0.4780 and $p = 0.04$. After the threat, ratings for security perception usually decrease from sequence 2 to 3 (see also subsection 3.4.7). This decrease shows a significant moderate correlation with *agreeableness* of -0.5271, $p = 0.02$. Participants could be "disappointed" by a security method which ranked highest for security perception in surveys (Ben-Asher et al., 2012). The result is in line with the findings above where no security method was used.

Of the five examined personality traits agreeableness, conscientiousness, and to a lesser extent openness are the most relevant for security perception and usage of mobile payment. Neuroticism and extraversion are insignificant in this regard. The type of security method functions as a modifier.

3.4.3 Experience, knowledge, and technical affinity

One of the hypotheses was that experience with and knowledge of computers in general, and smartphones in particular would influence a person's security perception and usage (pattern) of mobile payment.

Similar to the results above, the overall statistics for security perception and usage are inconclusive for factors concerning experience and knowledge (use of computers, internet, mobile phones, smartphone, app stores, mobile internet), if computed over all experiments. However, some expectedly consistent behavior is revealed within the examined area. Using mobile internet correlated highly with using an app store (cor 0.814, p <0.01). Also, using the internet correlated highly with using a computer (cor 0.792, p <0.01).

The results do not change, if the data is narrowed to those participants using no security method. There is no significant correlation between these factors of interest.

For those participants using mobile payment with a PIN during the experiments there is a significant moderate negative correlation (Spearman) between their overall security perception of the mobile payment app and their perception of PIN as a security method for mobile phones (i.e. higher ratings for "My mobile phone is in danger despite a PIN"). The correlation coefficient is -0.465 and $p = 0.02$. On the other hand, for those participants who used a screen lock with PIN the overall security perception correlates moderately with 0.392, p-value = 0.05.

The experiment using fingerprint recognition as a security method had one trending result where data using the screen lock with PIN correlates moderately negatively with security perception during sequence 2 (-0.339), but is insignificant with $p = 0.16$.

Technical affinity shows significant moderate correlations with both overall security perception and use of mobile payment. Spearman's rank correlation coefficient for positive attitude is 0.307 for the former (p = 0.004) and 0.233 (p = 0.03) for the latter.

For those participants using no security method positive attitude correlated even stronger with use of mobile payment with cor 0.443 (p = 0.01). If a PIN was used, this correlation vanished, but gained between positive attitude and overall security perception with cor 0.587 (p = 0.002). This is also the case for using fingerprint recognition with cor 0.489 (p = 0.03).

The results show that experience related to computers and mobile phones has little effect on the examined variables security perception and usage. Those who are sceptical about the security of PIN perceived the security of the mobile payment app significantly lower than others. In contrast, those who use a PIN to lock their phones rated security significantly higher. Of the four factors constituting technical affinity (enthusiasm, competence, positive and negative attitude), only positive attitude correlated significantly with use of mobile payment and security perception. Again, the type of security method is a modifier.

3.4.4 Risk perception and risk behavior

The assumption is that risk behavior and perception (especially those associated with financial activities) should be reflected in ratings for security perception and use of mobile payment.

Doing calculations on the overall data and for each security method individually do not reveal any significant correlations between the examined factors (overall) risk behavior and (overall) risk perception, and additionally focusing on sub-categories gambling and investment. A trend can be seen, if stretching the boundaries of significance a little bit, were risk perception of investments correlates with security perception after the first shopping sequence (were the interaction with mobile payment is "fresh"): cor 0.3267 with p = 0.055, using no security method.

The results for risk perception and risk behavior are too weak to indicate any meaningful relationship with security perceptions and use of mobile payment. It can be argued that the lab situation itself provided no "risky" environment at all (like a run-down store at night would probably do), and the threat was not specific enough to mobile payment that any personality traits for risky behavior or risk perception would exert an influence.

The overall effect of a threat can be shown (see below). This can be used in future studies to apply a more specific risky environment to mobile payment like theft of the device or an attack over the wireless network. The hypothesis is that differences in risk perception and risk behavior may then yield different results.

3.4.5 Environment

The environmental changes aim at the influencing factors of the taxonomical "institution", in this case the kind of store the participants had to shop at. Four separate types of stores were set up for the first three experiments: kiosk, supermarket, cinema, and public office. This was reduced to a kiosk and a supermarket in experiments 4 and 5 due to space constraints.

There are differences in the user behavior between paying at a kiosk and a public office for similar priced items. Participants had to shop for a pack of cigarettes for 5 Euro at the kiosk, and then immediately after it they had to request a copy of their birth certificate for the same price at the public office. In the former case, 41 out of 49 participants used cash (83.67%), 1 used a debit card and 7 mobile payment. In the latter case, this was reduced to 25 participants using cash (51.02%), while 9 used a debit card, and 15 used mobile payment. This change was highly significant with $p = 0.0002$. This was almost reversed in the following, when the participants had to shop for sweets at the supermarket in the same price range (3 Euro). 40 participants used cash (81.63%), while 3 used a debit card, and 6 used mobile payment. Again, this change was highly significant with $p = 0.0005$.

These numbers can be interpreted, that the experiment design of playing shop yields stable and thus realistic results. The participants did not randomly used the differents payment method just to play around with them, but rather used them in a consistent way (in line with expected use of payment methods (Wörlen et al., 2012)). It supports the applied design of the experiments, but no data is available for tests 4 an 5 as the store concept of public office was not pursued due to limited space.

3.4.6 Price

The participants “bought” several differents goods ranging from coffee-to-go to headphones covering a price range from 1 Euro to 250 Euro. The price is a good indicator of usage for either cash, card, or mobile payment. Goods are divided into three categories: cheap (1–9 Euro, 576 purchases over all experiments, free-choice sequences 2 and 4), medium (10–49 Euro, 430 purchases), and expensive (50 Euro and above, 332 purchases).

Payment method	cheap	medium	expensive
Cash	77.95	5.38	16.67
Card	24.42	28.14	47.44
Mobile	3.31	48.80	47.89

Table 3.10: Percentage of usage of specific payment method within price category

Overview				
Method	Count	Sum	Mean	Variance
Cash	565	5780.5	10.2310	626.3779
Card	314	30972.5	98.6385	7787.2388
Mobile Payment	459	30279.5	65.9684	6301.9155
ANOVA				
Degrees of freedom	F-ratio	p		
2	206.172	<0.001		

Table 3.11: Price and payment methods – ANOVA results

The threshold for dividing price categories might seem arbitrary. The background for this decision is how goods can be paid. Cheap goods can be paid using a reasonable amount of coins. As the highest denomination for Euro-coins is two Euro, the threshold for those “cheap” goods was set to 9 Euro (minimum of 5 coins, or 5 Euro note and 2 coins). The average amount of coins in one’s pocket is 5.90 Euro in Germany (Wörlen et al., 2012).

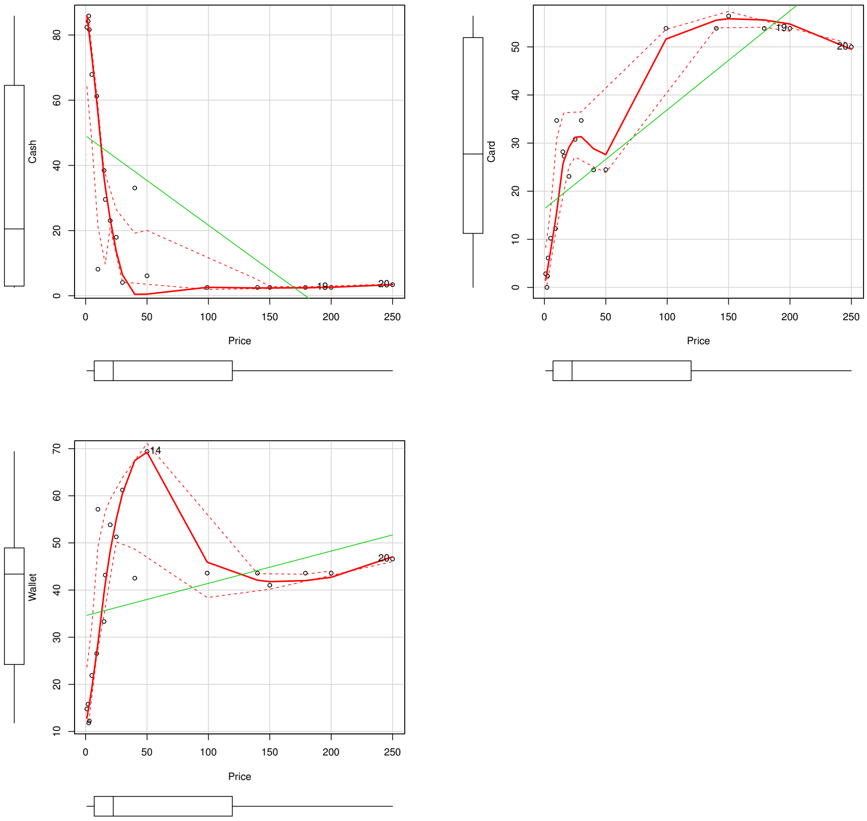


Figure 3.12: Distribution of price and usage of payment method. *Upper left*: Cash. *Upper right*: Card. *Lower left*: Mobile payment. Boxplot shown an axis. Red Line: Distribution’s smoothing curve (solid), Green line: Least-squares, confidence interval (dotted).

During the experiments the amount of symbolic cash was essentially limitless within the price of the goods to buy, which is not necessarily the case in reality, where the amount of cash one carries varies over time (the average amount of cash in one’s wallet is 103 Euro in Germany, *ib.*). For example, cash could be depleted after shopping in a store. This effect was prevented by using symbolic cash.

The use of the three different payment methods between the three price categories is significantly different as is shown in the three graphs in Figure 3.12. For each price category the percentage of usage of specific payment method is shown in Table 3.10. The shopping sequences gathered data on 20 different price points (in Euro): 1 (coffee-to-go, newspaper, public transport ticket, chocolate), 2 (soda), 2.5 (Post-It adhesive notes, paper clips), 3 (sweets), 5 (packet of cigarettes, birth certificate), 9 (bottle of vodka), 10 (video game), 15 (t-shirt), 16 (2 movie tickets), 20 (book), 25 (computer mouse), 30 (mobile phone prepaid card), 40 (another video game), 50 (passport), 99 (shoes), 140 (2 theater tickets), 150 (watch), 179 (smartphone), 200 (portable video game console), and 250 (headphones), which were summarized under the three payment methods. A Mann-Whitney test for two independent samples between two combinations each of cash, card, and mobile payment computed $p = 0.0$. Median for cash is 2.5 Euro, for card 50 Euro, and for mobile payment 30 Euro. A one-way ANOVA yields the same result, p <0.01 (see Table 3.11).

The pattern (visualized by smoothing curves) for usage of cash and card follows the expected usage pattern found in Germany (Wörlen et al., 2012). The new method mobile payment falls between these two existing methods, where it has its peak usage for the medium price category.[1] It is also used more for expensive items (in the range of card usage) than cash, and is also used more for cheap items than card.

3.4.7 Threat

One of the main factors presented in the taxonomy is the threat (or attack) on the task, the computer system, and/or the user. During the experiments the factor threat itself was changed once to having no threat at all during the shopping sequences. This was done in test 3. The threat is also subject to changes in the environment and the security method used for the mobile payment system. The perception of the threat may also be influenced by user's personality and his or her experiences.

The experiments were designed to catch the influence of threats through the user ratings of their perceived security in the third sequence. The assumption was that perceived security would drop in the third sequence and then recover during the fourth. Because the threat was executed in a role-play of playing shop without affecting the participant's own money, the effect was expected to be small.

The first examination is aimed at detecting an overall influence of threat versus no threat. 80 participants took part in both conditions, which were altered during the experiment in the third shopping sequence. A control group of 8 participants had no change of conditions and shopped without threat in the third sequence.

The assumption was that participants exposed to threat would alter their security perceptions of the mobile payment system compared to the perceptions in the two sequences before. The control group should show no change in their ratings. The dependent-means t-test results show a significant change in ratings with $p = 0.0381$ for the participants exposed to threats, while the control group shows no significant alteration in security perception ($p = 0.3499$). This is for the consecutive sequences 2 and 3. The average change (mean) from sequence 2 to 3 for participants exposed to threats was -0.308 (with a standard deviation

[1] The findings of the experiments concerning price are supported by the usage patterns of customers using a German MNO mobile wallet. Unfortunately the numbers are not published.

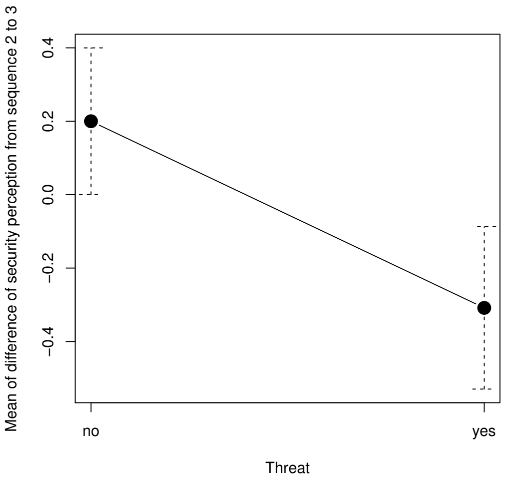


Figure 3.13: Means of differences in security perceptions from sequence 2 to 3, with and without threat, showing 95% confidence interval.

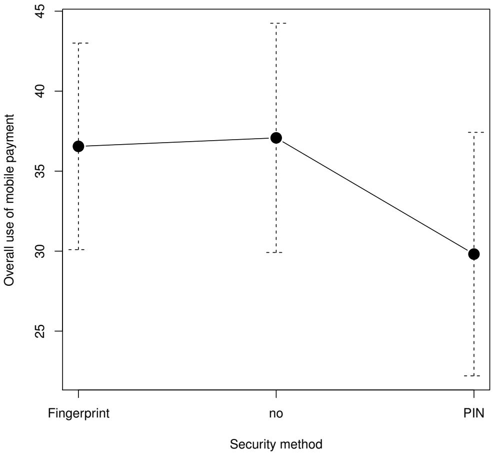


Figure 3.14: Means of usage of mobile payment split by security method showing 95% confidence interval.

of 0.99), while in the control group the change was +0.20 (with a standard deviation of 0.23). A Welch Two Sample independent t-test for the two groups (threat vs. no threat) calculated $p = 0.0007$.

Sequences 1 and 2 should see no significant changes in both groups as no threat had happened so far. This is indeed the case with the value of $p = 0.0953$ and 0.4441 respectively. There is also neither an immediate "recovery" once the threat is gone, nor a further decline in ratings of security perception – from sequence 3 to 4 no significant change is found ($p = 0.1284$ and 0.4257 resp.).

The change from sequence 3 to 4 was +0.2 for threat (with a standard deviation of 0.66) and -0.1 (with a standard deviation of 0.44) without.

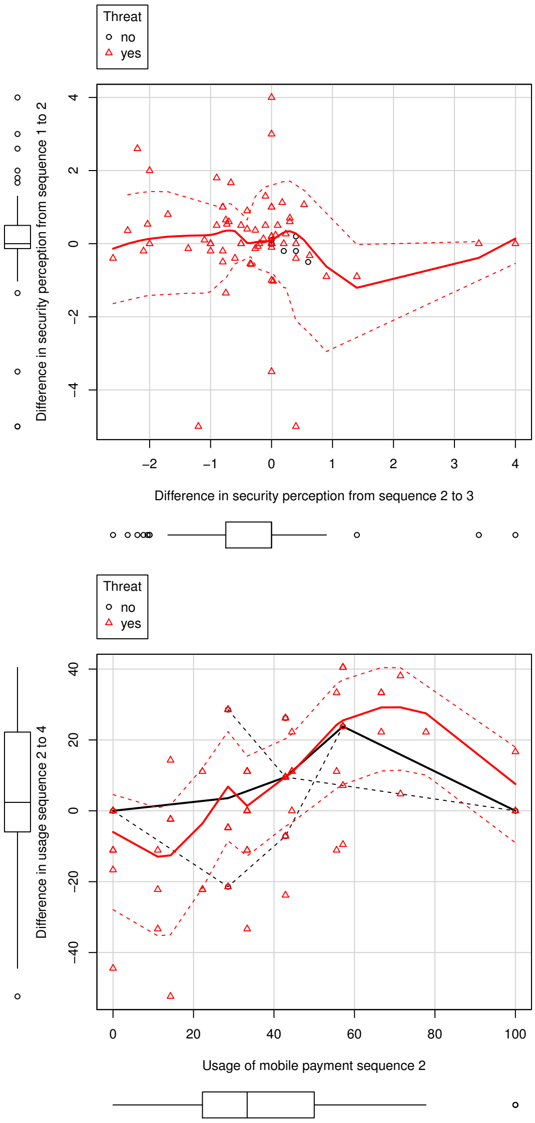


Figure 3.15: *Upper*: Change of security perception from sequence 1 to 2 versus change from sequence 2 to 3 *Lower*: Usage of mobile payment depending on threat. Boxplot shown an axis. Red Line: smoothing curve for threat (solid), confidence interval (dotted). Black line: smoothing curve for no threat (solid), confidence interval (dotted).

The result is shown in Figure 3.13. It depicts the mean and confidence interval of the participants' change of security perception from sequence 2 to 3. It shows the small but significant effect on the mean. The main result is the threat moves in the expected directions: lower ratings (change <0) by those participants exposed to threat and slightly higher ratings by those without exposure (change >0).

Another visualization is shown in the upper diagram of Figure 3.15 which depicts the distribution of differences in perceived security between threats ("attacks") and no threats. The main distinction is the cluster for no threats (black circles) clustering to the right of the zero point. Unthreatened participants rated their security perception slightly higher than during the previous block, which is the opposite to the threatened participants. This is in line with expected behavior. The small, but still significant difference might be caused by not using real money. All in all it can be said that the experimental "threat" – although done within the role-playing environment and without affecting the participants' own *real* money – "worked" in the assumed way of altering security perceptions.

This also leaves the taxonomical influence of "Forgetting" inconclusive yet. Probably the time-compressed format of the experiments did not actually allow the participants to forget the threating event.

The next question is whether the threat affected the choice of a payment method (it should not as all payment methods were threatened) or not. The interesting aspect is the individual participant's change in usage from free-choice sequence 2 to free-choice sequence 4 after the threat occured (or not). A Welch Two Sample independent t-test was computed for the difference between the sequences by threat. The mean for the difference in usage in the group without threat is 7.440 and the mean in the group with threat is 4.861. With $p = 0.709$ the difference is not significant. While the threat affected perceived security, it did not alter the usage of the mobile payment app significantly. As all payment methods were threatened, any resulting bias would probably do not favor any of the methods. This outcome for usage follows the experimental design. Nonetheless, the lower diagram in Figure 3.15 reveals an interesting trend, where participants who already used mobile payment comparably less often (<20%) would refrain from using it after the threat (participants with mobile payment usage on x-axis below 20% show mostly a negative difference between sequence 2 and 4 on y-axis indicating reduced usage in sequence 4). Participants who used mobile more often (>50%) would increase the usage even after the threat.

3.4.8 Security Method

One of the few areas where a vendor of a mobile payment applications can differentiate its product is the choice of a security method. While the user interface may differ, its main use is for initial registration and settings. During everyday use, many elements of the user interface itself are literally seldom touched, but the security method might be used for every payment (e.g. fingerprint recognition "Touch ID" for Apple Pay). In this regard, the choice of security method is important for the development of mobile payment applications.

Three different security methods were tested: no security method, PIN, and fingerprint recognition. The Levene Test is insignificant ($p = 0.3395$), so it can be assumed that the variances of the groups are homogenous. Table 3.16 shows the one-way ANOVA results for the third sequence with threat. There is a significant difference in how the three methods are perceived by the participants who experienced the threats.

The rating values for security perception of those participants who used the mobile payment app without a security method are significantly lower than using

Overview				
Method	Participants	Sum	Average	Variance
No method	36	120.7	3.3528	1.4631
PIN	25	101.7	4.068	1.4923
FP	19	78.5	4.1316	0.6101
ANOVA				
Degrees of freedom	F-ratio	p		
2	4.3073	0.017		

Table 3.16: Security method and threat – ANOVA results

the app with either PIN or fingerprint recognition. But there is no discernible difference between the ratings of perceived security for PIN and for fingerprint recognition.

But perceived security is not the only interesting outcome, but also usage of the different payment methods. Although PIN and fingerprint recognition got very similar ratings in perceived security, the usage was much higher with fingerprint recognition as the security method. The mobile payment app with PIN was used on average 29.4% for payment and the app with fingerprint recognition was used 36.8%. The means are significantly different with $p = 0.03$ during the first free-choice sequence. The difference in the second free-choice sequence (after the threat) is insignificant. In this regard, there is no direct correlation found between security perception and use of mobile payment. Only during the second sequence security perception correlates moderately ($R^2 = 0.19$) with use of mobile payment for high-priced items ($p = 0.002$).

In short: Having *a* security method increased perceived security over having no security method at all, while having *no* security method or a *novel* one increased usage over using a PIN.

3.4.9 Application Design

As mentioned above, the implemented security method was the only difference in the application design. Everything else remained the same. The design itself was rated by the participants using the AttrakDiff (Hassenzahl and Monk, 2010) und SUS (Brooke, 1996) questionnaires.

SUS ratings reached 81.25 of 100 (a rating between good and excellent). The overall impression and usability ratings were good, but security scored poor. The relatively high SUS score can be used for comparison with a variant of mobile payment app with implemented security features.

The users on average preferred mobile payment over using a debit card. The raw numbers of 1338 transactions (free choice sequences) were: 565 using cash (mostly cheap items up to 9 Euro), 314 using debit card, and 459 using mobile payment (mostly goods over 10). Participants would favor using a PIN upon starting mobile payment as an additional security feature. Using any feature without starting the app (compared to mobile payment running as a background process as in *express* mode) scored low (between 2.55 for access and 1.68 for payment). The ability to configure the security settings got the highest rating (4.73, SD = 0.75) (see also Sieger et al. (2012)).

Using AttrakDiff three main results were computed: overall attractiveness, pragmatic quality, and hedonic quality. The first two factors have no significantly different ratings across all security methods, but there is a significant association of the security method with hedonic quality.

The Wilcoxon rank sum test (with continuity correction) for using no security method or PIN shows a significant effect by the used method (or lack thereof) on perceived hedonic quality with $p = 0.004$ (W = 252.5). Hedonic quality for the mobile payment app with PIN was rated 4.16 (SD = 0.58), the mobile payment app without method was rated 3.65 (SD = 0.92), and fingerprint recognition was rated 4.46 (SD = 0.37). Similar significant findings were found for testing the overall perceived security by securiy method, which delivers $p = 0.0002$ (W = 198). A Wilcoxon rank sum test for PIN versus fingerprint recognition shows a significant difference in *using* the mobile payment system by method with $p = 0.046$ (W = 321.5). The average usage with PIN was overall 29.81% (SD = 20.04), while it was 36.55% (SD = 13.04) with fingerprint recognition.

This is an interesting result as one might expect the security *method* to be a *pragmatic* aspect of the mobile payment application. In order to increase the application's hedonic quality, a security method should be implemented. Of the examined methods, fingerprint recognition scored better results for usage than PIN.

3.5 Reliability

The experiments rely heavily on questionnaires to collect data. One of the key questions was about the participants' perceived security of the mobile payment application. These perceptions were rated after each of the four shopping sequences and an overall rating was given at the end.

	Alpha	Std.Alpha	r(item, total)
security perception 1	0.9541	0.9542	0.8399
security perception 2	0.9448	0.9454	0.8933
security perception 3	0.9584	0.9588	0.8108
security perception 4	0.9364	0.9367	0.9428
security perception sum	0.9410	0.9411	0.9181

Table 3.17: Reliability deleting each item in turn.

In order to examine the reliability of this questionnaire a factor analysis was computed on the results. The Alpha reliability is 0.9572 with a standardized alpha of 0.9575. All items asking for ratings of security perception after each shopping sequence load on the same factor as shown in Table 3.17.[2]

A Principal component analysis (PCA) was conducted on 10 items (security perceptions in sequences 1 to 4 plus overall, and observed usage of mobile payment in sequences 1 to 4 plus overall) with oblique rotation (oblimin). The Kayser-Meyer-Olkin measure verified the sampling adequacy for the analysis

[2] The reliability description in the following two paragraphs is adapted with the appropriate calculations from Field et al. (2012).

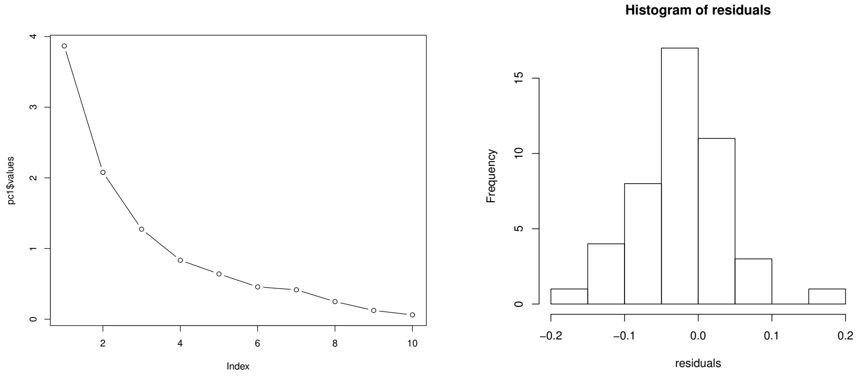


Figure 3.18: *Left*: Scree plot of PCA. *Right*: Histogram of residuals.

KMO = .75 ('good' according to Kaiser), and 9 out of 10 KMO values for individual items were >.56, which is above the aceptable limit of .5 Bartlett's test of sphericity, X^2 (45) = 354.8699, p < .001, indicated that correlations between items were sufficiently large for PCA. An initial analysis was run to obtain eigenvalues for each component in the data. Four components had eigenvalues over Kaiser's criterion of 1 and in combination explained 80.5% of the variance.

	item	TC1	TC2	TC3	TC4	h2	u2
security_perception_4	4	0.97				0.94	0.062
security_perception_2	2	0.93				0.89	0.111
security_perception_3	3	0.93				0.83	0.171
security_perception_1	1	0.87				0.86	0.144
SS loadings		3.67	1.97	1.24	1.17		
Proportion Var		0.37	0.20	0.12	0.12		
Cumulative Var		0.37	0.56	0.69	0.81		
Proportion Explained		0.46	0.24	0.15	0.15		
Cumulative Proportion		0.46	0.70	0.85	1.00		
TC1		1.00	0.17	0.13	0.04		
TC2		0.17	1.00	-0.05	0.14		
TC3		0.13	-0.05	1.00	-0.18		
TC4		0.04	0.14	-0.18	1.00		

Table 3.19: Principal Components Analysis, 4 factors, oblique rotation, standardized loadings based upon correlation matrix, and component correlations.

The scree plot (see Figure 3.18) showed no distinct inflexion point, but three components are above Kaiser's criterion of 1. Although the sample size is small, further analysis pointed to retain a fourth component, because the criterion for the residuals (see Figure 3.18) would have been otherwise to high. The histogram of residuals shows a seemingly normal distribution with no outliers. Table 3.19 shows the factor loadings after rotation. The items that cluster on the same component for "security perception" suggest that items 1 to 4 of the corresponding questionnaire are reliable. The test of the hypothesis that 4 components are sufficient shows the degrees of freedom for the null model are 45 and the objective function was 6.24. The degrees of freedom for the model are 11 and the objective function was 1.21. The total number of observations was 62 with MLE Chi Square = 65.69 with prob < 8E-10 Fit based upon off diagonal values = 0.97.

The reliability of the parts of the questionnaire with the items for security perception during the practical part used in the factor analysis shows the following: The value for Cronbach's α is excellent for factor 1 (security perception) with $\alpha = 0.957$.

3.6 Summary

This is the first study to link and quantify the effects of specific security methods on perceived security and usage of mobile payment. The mobile payment application was tested in a lab environment and used a prototype – the alternative being impossible to implement for various reasons: technical, practical, ethical, and legal.

The caveats are that the lab context could skew results, and the system – once readily available – could transform people's view of it through frequent exposure and use. The thorough analysis should have shown the reliability of the experiments, but of course it cannot predict future changes when mobile payment will be commonplace.

The experiments' data collection included almost all taxonomical factors on the user's side, and some factors of the attacker's side. The overall results support the first published iteration of the taxonomy. For example, a refinement could split some of the user-related factors into more details like placing technical affinity prominently, while de-emphasizing others like cost of security. The taxonomy assumes direct relationships and associations. If a factor's measured value or rating changes, all associated factors' values changes with it. The results show how strong, moderate, or weak those correlations are. The measure of "success" for the experiments is not that all associated factors are required to show *strong* correlations, but rather to discover how the empirical data unfolds for the assumed connections drawn in the taxonomy.

Of the 38 factors examined factors ten are found to be moderately influential. The user-related factors are agreeableness, conscientiousness, openness, and positive attitude (technical affinity). The experience and knowledge-related factor is the perceived risk of PIN as security method. The factors related to device and application are hedonic quality and security method. The threat showed a significant influence of the store type and price as environmental factors.

The hypotheses stated in the taxonomy can be addressed with the results:

- H1: There is a relationship between personality traits agreeableness, conscientiousness, and to a lesser extent openness and security perception and usage of mobile payment, but no relationship was found regarding experience and knowledge.

- H2: There is a negative relationship between cost of security and usage of mobile payment concerning using PIN as a security method, but there was no difference in usage between using no method at all and using fingerprint recognition (although in its tested implementation it required more effort by the user than using no method).

- H3: There was no relationship found between the risk perception and risk behavior and security perception, and usage of mobile payment.
- H4: There is a positive relationship between the perceived hedonic quality of the mobile payment application's design (by means of implemented security method)) and security perception, and usage of mobile payment (by absolute count over payment card).
- H5: There is a negative relationship between (financial) threat and security perception, but usage of mobile payment was not affected.
- H6: There is a positive relationship between an institution's reputation (public office versus retail stores) and usage of mobile payment.

Of the 6 hypotheses, H3 has to be rejected. H1, H2, H5 have to be modified to exclude either effects on security perception or usage of mobile payment. H4 and H6 are found to be supported.

The five areas covered by the taxonomy focus on the user and the given task, in this case using a mobile payment system (and rating the perceived security of it). The results show how much influence can be "explained" with the taxonomical factors. It also hints at the limitation of any predictive model based on the experimental results. Although being consistent with the taxonomy the findings also reveal where it can be extended. The dependencies and associations explain only part of the picture of what influences the security perception and especially the user's choice of the payment method. But the already taxonomically established connections can be used to form a model of security perception and usage of a mobile payment system. To support further development of mobile payment apps, the taxonomical factors can be modeled to compute interesting (commercial) implications: security perception and especially frequency of use of such applications. Developers of a mobile payment app might be interested to boost usage by choosing the "right" security method – all within the given and previously detailed historical context and development framework.

Further (more informal) findings from comments voiced during the experiments or in written in the comment section of the last questionnaire for the prototype of the mobile payment app are: A mobile wallet appears to be a good debit and credit card replacement, the overall impression is high. Most of the users linked the card paradigm to a real debit card ("EC card", officially *girocard* now), and the familiarity of the concept seemed to build trust (a concept examined in this thesis only indirectly by designing different store types as "reputation of the institution"). The participants using the app without a security method often mentioned security issues, which are also reflected in their respectively low ratings. They often mentioned that adding a PIN would satisfy their security needs, which points to the impression that PIN is the most widely known security method. No other security method was mentioned, not even the gesture-based screen un-lock known from Android (see also Sieger et al. (2012)). The different security methods have different ratings in surveys and the experimental results are somewhat inconsistent with the hypothesis derived from Ben-Asher et al. (2011) for mobile phones, and also Kim et al. (2010b) for e-payments.

While the experimental results do not allow to compute the outcome variables of perceived security and usage of mobile payment *completely* as expected, the taxonomy is shown to be *consistent*. The taxonomical factors are influential to a degree, but to paint a complete picture the taxonomy has to be expanded.

The questionnaires asking for personality characteristics, technical affinity, and risk-taking are set within a societal context. The questions and the resulting classifications are along a cultural consensus of what counts as neurotic, technical affine or risky, e.g. to be nervous, to read computer magazines or to go skydiving. The experiments were focused on the *personal* aspects of the participants. It was assumed this would be responsible for at least the majority of the "effects" on security perception and usage. This is clearly not the case. But rather than to overturn the taxonomy it also shows it to be consistent. The factors have a low or moderate correlation, therefore something is missing. This could be caused either by the granularity of the collected data or by missing taxonomical areas.

Because the personal-psychological aspects and user-related factors were already extensively covered, additional details would probably not uncover new factors. The aim of the interaction would remain the same: buy some goods, choose a payment method, and rate the security perception. The device aspects could be broadened to other mobile payment applications using other payment methods or other technology (e.g. QR, barcode), but this would retain the same "input" variables on the participant's side adding nothing to the existing results. The same goes for the environment. Even if the experiments were reduced to one type of store (which can be done on the existing dataset), the input variables would not compute the outcome. The threat is already a controlled variable as the computation can be executed on the pre-threat sequences only.

These considerations point to the aforementioned socio-cultural influences which affects the dependent variables of security perception and usage. The missing data points cannot be purely personal-psychological aspects, because otherwise the effect would be seen (as these are already covered by the questionnaires). The effect cannot reside within the other areas, because computations on these parts of the dataset should reveal it. The factor has to influence the personal decision of the participants, but without being part of their personality traits. This leaves a socio-cultural influence as the auspicious contender. Table manners could serve as an analogy for such influences. They differ between regions and can also differ between "classes" in the same region. Personality traits certainly influence the overall demeanor at the table, but not the fact that using cutlery is prevalent in some regions. Independent of personality traits, both shy and outgoing people will use forks and knives. In the same way, using a specific payment method is probably influenced by cultural norms and habits.

The taxonomy is essentially a two-dimensional plane connecting taxonomical factors. Any socio-cultural *background* would elevate this taxonomy plane into the third dimension, where socio-cultural factors would then connect to the different factors. Such a socio-cultural influence can be seen in the patterns of payment behaviour in Germany. For example, Germans usually decide to buy using cash depending on the amount of cash in the wallet (68%) and on the price of the good (59%). It is a spontaneous decision only for 13% of those asked in the survey (Wörlen et al., 2012).

The factors relevant to an expandend taxonomy including socio-cultural factors can neither be observed in a lab test nor collected using a questionnaire. Aggregated data as in Wörlen et al. (2012) cannot be used, because it cannot be linked to the individual behavior being examined in the experiments. Among those factors are frequency of use of different existing payment methods depending on price, store, and perceived threat. A person usually cannot remember *precisely* where and how often he or she uses a specific payment method under certain circumstances. To collect this data, a field test using a diary would be appropriate. As already mentioned, a field test could not be done as no mobile payment application was available at the time of this research. Even now, the mobile payment applications available on the German market have a very small user base (see also Chapter 5).

The main argument against lab experiments can also be brought up here. The results shown herein – while being overall consistent – may lack a proper view on realistic behavior in two ways. The user probably has no prior experience (and with it probably no associations or thoughts) of the tested mobile payment system. The user might also lack the proper anchor to compare the system and participants possibly do not have stable expectations during the experiments (Möller (2010), p. 155). The reliability of the questionnaire on perceived security and thus the validity of the data could be shown. Because using smartphone-based mobile payment applications for contactless payment at the POS is only in its infant state, it cannot be stated with certainty how its technology will evolve. In this case, the predictive model is limited to the type of technology its data relies on.

One of the major achievements is that this research can demonstrate a clear path leading straightforward from the taxonomy over the choice of taxonomical factors and a suitable experimental design to the collection of robust data for a predictive model. The experiments also delivered the first quantified data of usage of payment methods at the retail point-of-sale distributed over price categories and store types.

Chapter 4

Model

One of the goals of the research presented in this thesis is to both understand the influence of personal attributes on the choice of mobile payment and to support the further development of mobile payment applications. A (predictive) model is constructed based on the taxonomy and the empirical data to describe user behavior and security perceptions of a mobile payment application (see also Sieger et al. (2011)). While the (descriptive) statistics shown in the previous chapter deliver interesting results on their own, a robust model is required to deliver predictions of user behavior and perception, and to possibly use it for an implementation into a simulation model.

The analysis of the experiments' data set revealed a set of factors significantly correlated with usage of mobile payment and security perception. But as already hinted in the previous chapter, this is not entirely the case. There is no latent or hidden variable within the data (and was not assumed) and there was no need to classify (previously unknown) variables.

The last decade of research in usable security has often shown that programming a system to be both secure and usable is a rare occasion. This is caused by a number of factors, most notably

- disalignment between user goals and expectations, and security features (Cranor and Garfinkel, 2005);
- security rules enforcement and missing user understanding due to lack of communication and education (Clarke et al., 2002);
- users' rejection of security advice (Dörflinger et al., 2010);
- current operating systems' continued use of legacy concepts not being programmed with security in mind (see Chapter 1).

Other than in e.g. general GUI interaction, which in most times is an ongoing task as long as the user sits at the computer, security features and alerts are usually encountered rarely. Giving login credentials and maybe seeing a spam filter or web certificate alert is often all of security-related interaction during work.

To aid the software architect and programmer to build usable security right from the start, a user behavior model, which can be simulated to test security features during development, would be useful. The work done towards building such a user behavior model is presented in this chapter. It shows the steps taken to build a model, giving an overview of the iterative process from analyzing relevant factors. The key is to decide which model is statistically sound, and then to implement it into a computer simulation.

Due to the scarce interaction with security features (and the interaction itself often being one tap only), "life-like" user tests or even field tests are too time-consuming to gather enough usable data without enormous efforts.

The goal was to find key factors influencing the user behavior in security-related mobile computer interaction. Some of these factors were gathered graphically in the taxonomy (see figure 2.1) by sorting and counting influencing key relations and factors.

As with a general question in psychology and sociology "What drives people to form decisions and act on them?", it had to be answered in the special situation of people interacting with the payment system.

Focus groups and surveys cannot answer the question in quantitative terms how people actually react, when they have to make a decision on computer security.

Some of those questions are: How often is a mobile payment app used depending on the security method? Do threats change the perceived security and usage? How attractive is the application?

To gather quantitative data in terms of probabilities usable for the behavior model and its simulation, lab tests were inevitable. A behavior model not only requires rigorous statistics on user preferences, but data on decision timings, security perception, reactions to the environment and the context of the task.

Another approach to get data concerning user behavior is to set up a "microworld". This is a computer-based scenario, where the user is confronted with an "abstraction" of the real world in order to limit the variables. It delivers good quantitative results and generates lots of data in a very short time, being valuable input towards a user behavior model as was described in (Ben-Asher et al., 2009).

4.1 Model selection

Studies on *POS-based* mobile payment are scarce, mainly because the infrastructure and applications are still in their early stage of implementation worldwide. Only Kenya and Japan have a sizable number of mobile payment users with Japan being the only one with a POS-capable solution. For example, the market-share of NFC-ready POS terminals in Germany is still under 10% as of end of 2014. Hence, most studies developing (behavior) models have a broader definition of mobile payment including (and focusing on) *online* payments using mobile devices and almost all studies rely on survey data. The results presented in this thesis are among the first to use data collected through observations in an experiment.

Shin (2009) built a predictive model of consumer acceptance of a mobile wallet based on the unified theory of acceptance and use of technology (UTAUT) using structural equation modeling. The data is purely based on questionnaires and confirmed the influence of factors like technology acceptance, perceived security, and trust. An extended model was proposed, but not tested.

Kim et al. (2010a) constructed a model based on the extended technology acceptance model (TAM) also using structural equation modeling, but did not incorporate environment, security methods, and threat. Personal attributes were not as granular and consisted of personal innovativeness and mobile payment knowledge. The other factors were related to the mobile payment service and device: compatibility with user needs and lifestyles, convenience, ability to access services ubiquitously, and reachability (to be contacted anywhere, anytime). The resulting strong predictors were perceived ease of use and perceived usefulness. The model did use survey data collected in South Korea, but not actual usage behavior. This is in line with one of the earlier findings of Schierz et al. (2010) who identified perceived compatibility (contributing the largest effect by far), individual mobility, and subjective norm as effects determining consumer acceptance of mobile payment services. The model is also based on TAM and uses data gathered via online surveys in Germany. This model claims an R^2 of 0.84. It was shown in this work, that survey data on hypothetical devices and applications is not necessarily consistent with actual perception during use, for example in the case of security perception of PIN and fingerprint recognition.

Zhou (2010) studied factors with an effect on continuous usage of mobile payment using the information system success model and flow theory. Using structural equation modeling the determining factors to be found for continous usage were trust and satisfaction.

Yang et al. (2012) tried to rectify those prior model's deficiencies caused by TAM's and UTAUT's focus on organizational settings by proposing a model drawing from the studies on innovation adoption and consumer decision behavior. The model consists of three sets of factors influencing the intention to adopt and continue using mobile payment: behavioral beliefs (relative benefit of adopting mobile payment and compatibility through convenience, efficiency and ubiquity as two positive factors; perceived risk and perceived fee as two negative factors), social influences (perceived pressures from social networks on adoption of mobile payment), and personal traits (personal innovativeness). The data was collected from Alipay users (one of China's biggest online payment services) using an online survey. Again, the granularity of personal traits is low, and the definition of social influence is very narrow. Nonetheless, the model claims to explain 75% of the variance.

Amoroso and Magnier-Watanabe (2012) constructed an integrated research framework of mobile wallet adoption for the case of Japanese contactless payment technology. The hypothetical integrated model is based on a review of other proposed models and retains eleven constructs, which are also partly based on UTAUT or TAM. It includes the factors perceived security/privacy, perceived risk, trust, perceived usefulness, perceived ease of use, perceived value, social influence, attractiveness of alternatives, and facilitating conditions which influence attitude toward using, behaviorial intention to use, and actual use. The model remains hypothetical as no data was used to compute any results. The taxonomy already maps trust, perceived security, perceived security into the same plane, but omits the inclusion of social influence.

The key to the success of these models (high explanation of data variance in Kim et al. (2010a) of 84% and Yang et al. (2012) of 75%) is their sole focus on mobile payment without any comparison to existing payment methods like cash and credit cards. The models also omit external factors like device and application variants, store environment, and possible threats. The questionnaires used for the surveys are aimed at mobile payment. If the only possible answer is to rate a (hypothetical) usage of mobile payment, the only relationships of the influencing factors are of course directed towards mobile payment while alternatives are missing from the picture (and the constructed model). For example, Yang et al. (2012) asks only two questions concerning the intention to use mobile payment: "Assuming I have access to the mobile payment system, I intend to use it." and "Given that I have access to the mobile payment system, I predict that I would use it." The ratings are then set in relations to the aforementioned factors to construct the model. The taxonomy presented here is open to alternatives and uses a broader set of personal attributes to avoid this closed-loop scenario. The experiments are more realistic by offering the user a choice of existing payment methods in addition to mobile payment.

It has to be stressed again, that the taxonomy is *not* a model. The taxonomical terms may be used for modeling, but the terms are mapped as a taxonomical hierarchy. For example, the term *Cost of security* subsumes the terms *Financial* (cost of implementing security measures), *Usability* (of app, device, or method), and *Scale* (how often does this apply), but *Usability* is not meant to "bypass" *Cost of security* and indirectly influence another term, for example *Perceived risk* (of intention to use mobile payment). The experiments were designed to measure these direct relationships. Structural equation modeling, which was used in several of the discussed models above, makes use of direct *and* indirect (latent) relationships. The rejection of this approach is mainly due to the taxonomy having only direct and no indirect relationships between factors. No structural chain of equations is required, where one result is to be fed into the following equation.

The complete dataset of the experiments has 32,680 data points. This might seem to be the ideal set for data mining, pattern recognition or machine learning. But this is not the case here. Most of the data is part of established questionnaires, which boils down to representations of different personality traits. Other data is also plain: security method, threat, type of shop, price. Then there are the results from the participants' ratings of their perceived security, and their shopping behavior resulting in a choice of payment method. Among the many different methods for data exploration and analysis it is important to justify the choice of the method used in this case. The main question to answer here is: What type of problem has to be solved?

Factor analysis was used to compute the reliability of the questionnaire on security perception. It (and closely related principal component analysis) is a good starting point to find relevant clusters of correlated variables (factors), which could be associated with different variables. This also revealed that the factor loadings are all on the already established variables. There is no need to introduce new (formerly hidden) constructs. The trend is already visible, when the correlation matrix of the variables is partitioned into hierarchical clusters. The result of a factor analysis on all relevant variables shows no significant results.

Concerning the experiments' results itself doing a complete factor analysis gives no useful results. First, the taxonomy does not incorporate *latent variables*, the relationships are direct. Second, the dataset is generated using predominantly established (valid and reliable) questionnaires. The advantage is to know that these questionnaires cannot reveal "hidden variables". They were tested to measure for what they were designed. The aim of the experiments was

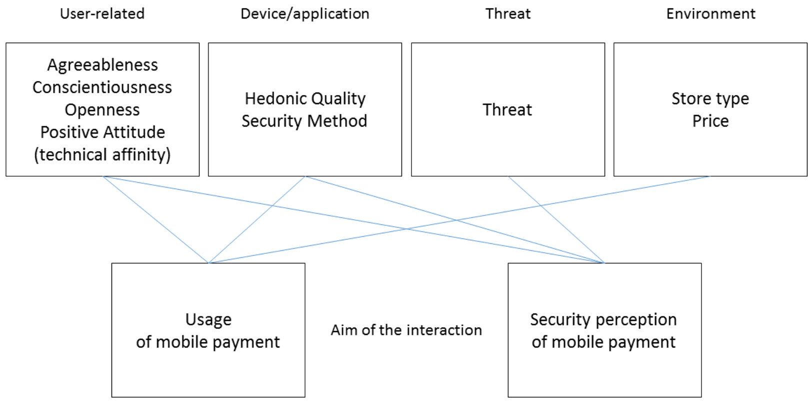


Figure 4.1: Model for security perception and usage of mobile payment derived from taxonomy and experimental results.

to get results for the strengths of the connections established in the taxonomy. The experiments were designed to get these results directly, because the *flat design* of the taxonomical connections assume a direct association between the factors. The resulting dataset was not designed to explore unknown variables and such an attempt would not generate useful results. The factor analysis to test the reliability of the security perception ratings proved this as a by-product. This also rules out data mining techniques used to discover unknown properties within the dataset. This applies to any method building on these assumptions to construct latent variables.

There is another argument against hidden or latent variables in the dataset. Any applied method has to either transform or recombine existing data vectors. In analogy to physics the “units of measurement” would mix up: personality traits, store types, price points etc. While this is entirely mathematically possible, it would make no sense in *this* dataset. The experimental results follow the *what-you-see-is-what-you-get* principle.

Because the shopping sequences are a time series, it might seem appropriate to model them as a Markov decision process (extension of Markov Chains). At each step in the shopping sequence the participant has to choose a payment method, where the choice may be modified by the relevant factors such as personality traits, store, price, and threat (but not by the choice beforehand). All these factors would stay the same for all steps and all participants, because the sequence remained unchanged for store, price, and threat, and was not randomized for every participant during the experiments. Sequences 2 and 4 were *extended* for experiments 4 and 5, but were still the same for every participant. The outcome of the process would be dependent only on the personality traits input, which does not alter from one state to the next – and the correlation between personality traits and the choice of payment method has already been computed. Hence, computing the Markov decision process would not deliver meaningful results in this case. Of course, in future tests, the sequence could be randomized regarding store, price, and threat, and the questionnaires could be extended to ask for usability of the app and security method, and trustworthiness of the shop after each single payment event.

Another approach could be to use machine learning (pattern recognition) algorithms like Linear Discriminant analysis (LDA) or Support Vector Machines (SVM) to build a model based on the dataset, although this is primarily not a classification problem as the results presented in the previous chapter show. The outcome variables (choice of mobile payment and security perception ratings) are continuous. But there were two groups which can be discriminated (see Section 3.4.8): with-security-method versus without-security-method showed significant differences in perceived security; and using no method or fingerprint recognition versus using PIN showed significant differences in usage.

This arguments support the chosen initial approach of using predominantly multiple regression models and is in line with the presented results in the previous chapter. It is also the recommended method for this kind of data (see Field et al. (2012)). It showed that the taxonomy covers all personal factors, but not those belonging to any socio-cultural background. Those factors are not latent variables in the dataset, because they are part of another set of influencing factors and cannot be computed using the collected dataset.

4.2 Predictors and models

The models presented here serve several purposes. They will be used in a conceptual implementation of a simulation tool, but, more importantely, are used to support further interpretations of the results from the experiments. The focus is less on predictions, but more on the ability to draw further conclusions. Thus, the models are computed using all data and are not trained and tested using splitted data.

4.2.1 Regression models

Figure 4.1 shows the predictor selection derived from the taxonomy and the results from the experiments as a possible multiple regression model. The selection is based on the effects found in Chapter 3 and are introduced into the model(s) in hierarchical order. This includes similar predictors found in other models, e.g. such as positive attitude (technical affinity), which roughly translates to personal innovativeness used in Kim et al. (2010a) and Yang et al. (2012). Based on these data the following predictors showing significant correlation with security perception and usage of mobile payment are contenders for incorporation into the model: agreeableness, conscientiousness, openness, and positive attitude (technical affinity) as user-related factors; hedonic quality and security method as device and application-related factors; threat; store type and price as environmental factors.

Security methods and threat act as a modifier for security perception and usage of mobile payment. Not all predictors shown in Figure 4.1 can be integrated into *one* model in a meaningful way. The recommended maximum number of predictors for the sample size used in the lab tests is 2 (see Field et al. (2012)). Security perception and usage are modeled using the three security methods. The other possible predictors were not chosen for different reasons: The main goal of modeling the empirical data is to find the influence of personal attributes in comparison to external, possibly socio-cultural factors.

	Estimate	Std. Error	t value	Pr(> $\|t\|$)	Signif.
(Intercept)	20.248	32.274	0.627	0.5344	
Agreeableness	-7.899	3.560	-2.218	0.0329	*
Positive attitude	16.218	6.241	2.599	0.0135	*
Residual std. error	19.32	36 DF			
F-statistic	6.86				

Table 4.2: Mobile payment application without security method: Coefficients for 2-factor model of usage of mobile payment using agreeableness and positive attitude (technical affinity), Signif. codes: '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1.

	Estimate	Std. Error	t value	Pr(> $\|t\|$)	Signif.
(Intercept)	-0.4649	1.8182	-0.256	0.7997	
Agreeableness	-0.1757	0.1608	-1.093	0.28183	
SUS rating	1.7437	0.5530	3.153	0.003	**
Residual std. error	0.8745	36 DF			
F-statistic	6.164				

Table 4.3: Mobile payment application without security method: Coefficients for 2-factor model of security perception using agreeableness and positive attitude (technical affinity), Signif. codes: '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1.

Another purpose of the model is a conceptual implementation as a simulation. The model will be incomplete due to the fact that data collection using field tests was and still is not possible (see Chapter 5), and many environmental and social influences habe to be omitted. The focus is less on the models' *general* predictive power, but more on the *share* of personal traits and security methods of the models' predictive ability.

Price is not selected as predictor (the models could target price categories) as it is limited to a maximum of 250 Euro. The lab test had to set a reasonable maximum price for the goods available, but in reality, much higher prices appear. Threat, though showing significant influence, is not selected as threat was no specific attack to the security method and the significant influence is calculated on the *change* of ratings rather than *absolute* ratings. Other types or more specific threats probably show other changes. Store type is not used as predictor, because it was not available to all security methods. All other factors used in the 2-factor models are chosen for best fit using both stepwise and all-subsets methods.

The overall usage for the mobile payment application without a security method is modeled using the factors agreeableness and positive attitude (technical affinity). The correlation values of the predictors represent a medium effect of around ±0.3 (see also Fischer-Hübner et al. (2010)). The results for this 2-factor model are shown in Table 4.2. Multiple $R^2 = 0.28$ and adjusted $R^2 = 0.24$ with $p = 0.003$. The two predictors explain around 24% of the variance. The *Estimate* column displays the model coefficients for the factors

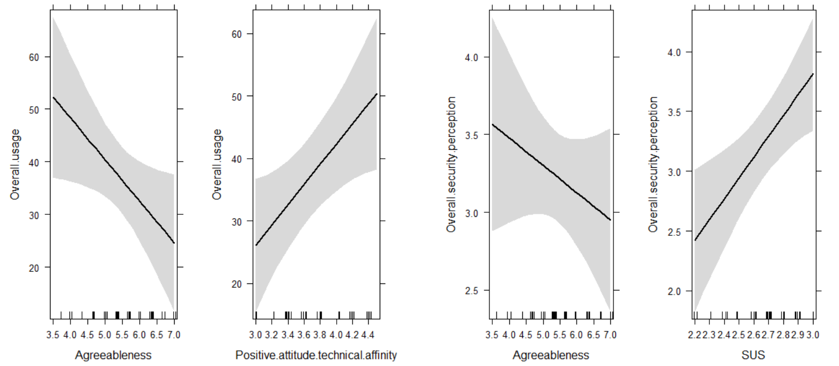


Figure 4.4: Mobile payment application without security method: Effect plots. *Left*: Linear regression model of agreeableness and technical affinity–positive attitude predicting usage of mobile payment. *Right*: Linear regression model of agreeableness and technical affinity–positive attitude predicting security perception

agreeableness and positive attitude, *Intercept* would be the z-axis interception (if the factors could be rated 0).

When using again agreeableness combined with SUS rating as predictors for the outcome of how security is perceived (as shown in Table 4.3) it results in multiple $R^2 = 0.2551$ and adjusted $R^2 = 0.2137$, with $p = 0.005$. In this case the model explains only around 21% of the variance.

Figure 4.4 shows the effect plots of these models. The plots present the linear regression of the predictors and their effect on the model.

The overall usage for the mobile payment application with security method PIN is modeled using the factors pragmatic quality and risk behavior concerning investments. The results for this 2-factor model are shown in Table 4.5. Multiple $R^2 = 0.2085$ and adjusted $R^2 = 0.1499$ with $p = 0.04$. The two predictors explain around 15% of the variance, which is rather low. The model is ill-fitting with a borderline p-value. The predictors also showed only very low correlations to perceived security and usage (see Chapter 3). This case requires more data.

Security perception of the mobile payment application using PIN is modeled using the following predictors: positive attitude (technical affinity) and hedonic quality. As shown in table 4.6 it results in multiple $R^2 = 0.415$ and adjusted $R^2 = 0.3618$, with $p = 0.003$. The model explains approx. 31% of the variance. Again, Figure 4.7 shows the effect plots of these models.

The overall usage for the mobile payment application with fingerprint recognition as security method is modeled using the factors agreeableness and conscientiousness. The results for this 2-factor model are shown in Table 4.8. Multiple $R^2 = 0.43$ and adjusted $R^2 = 0.36$ with $p = 0.01$. The two predictors explain around 36% of the variance.

Security perception of the mobile payment application using fingerprint recognition is modeled using the following predictors: conscientiousness and positive attitude (technical affinity) as shown in Table 4.9. It results in multiple $R^2 = 0.3816$ and adjusted $R^2 = 0.3043$, with $p = 0.02$. The model explains

	Estimate	Std. Error	t value	Pr(> $\|t\|$)	Signif.
(Intercept)	83.1645	20.3027	4.096	0.000343	***
Pragmatic quality	-10.5755	4.4795	-2.361	0.025709	*
Risk behavior	-1.7244	0.9895	-1.743	0.092766	.
Residual std. error	18.79	27 DF			
F-statistic	3.557				

Table 4.5: Mobile payment application with PIN: Coefficients for 2-factor model for of usage using conscientiousness and hedonic quality, Signif. codes: '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1.

	Estimate	Std. Error	t value	Pr(> $\|t\|$)	Signif.
(Intercept)	-1.8732	1.6648	-1.125	0.27264	
Positive attitude	0.9941	0.3354	2.964	0.00716	**
Hedonic Quality	0.5881	0.3413	1.723	0.09889	.
Residual std. error	0.9844	22 DF			
F-statistic	7.803				

Table 4.6: Mobile payment application with PIN: Coefficients for 2-factor model for of security percption using positive attitude (technical affinity) and hedonic quality, Signif. codes: '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1.

approx. 30% of the variance. Effect plots of these models are shown in Figure 4.10.

The models require some assumption concerning variable types, distribution and variance of the data.

The histogram on the upper-left of Figure 4.11 shows exemplarily the studentized residuals for the 2-factor model for usage of mobile payment without security method using agreeableness and positive attitude (technical affinity). The histogram shows a good fit to a normal distribution. But there is a hint at some possible outliers in the rightmost column. There are cases with large (studentized and standardized) residuals greater than 2. There are 6 cases, where participants did not use the mobile payment system at all, and an additional 2 cases, where it was used all the time. One possible assumption is that those participants did not act as they would have in real life, but were rather biased by the experimental settings (e.g. novelty factor, role-playing). If those cases are analyzed, only two can be found, which lie above the value of 2. This is below the recommended 5% rule for large residuals. Further, those cases' values for Cook's distance, leverage and covariance ratio are almost all within the recommended limits of 1, 0.154, and 0.77–1.23 respectively. Case 27 has a covariance ratio of 0.3584 which is below the limit, but Cook's distance allows to retain it, because it is no influential case. This is true for all presented models here.

The plot in the upper-right of Figure 4.11 shows the Q-Q plot of theoretical values against observed residuals for the 2-factor model using agreeableness and positive attitude (technical affinity). The plot shows the fit of the model data to the empirical data.

The lower-left plot in Figure 4.11 shows the scatterplot of fitted values against studentized residuals for the model. The plot shows no signs of a funnel or a curved shape, so the assumptions on linearity and homoscedasticity are met. This is the case for all presented models.

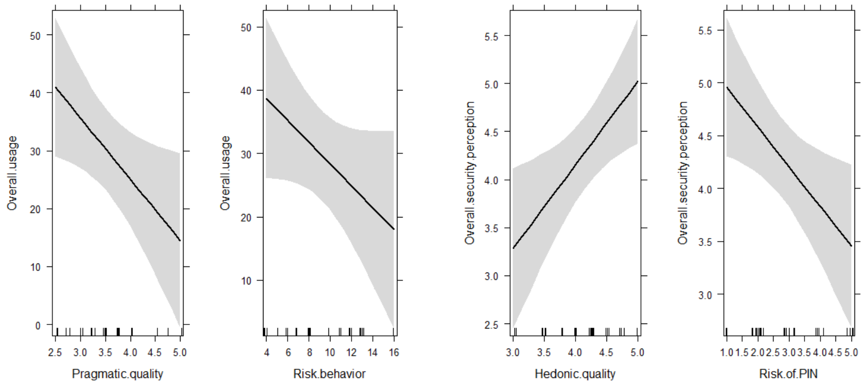


Figure 4.7: Mobile payment application with PIN: Effect plots. *Left*: Linear regression model of conscientiousness and hedonic quality predicting usage of mobile payment. *Right*: Linear regression model of perceived risk of PIN and positive (attitude technical affinity) predicting security perception

	Estimate	Std. Error	t value	Pr(> $\|t\|$)	Signif.
(Intercept)	30.781	10.200	3.018	0.00817	**
Agreeableness	-12.727	4.668	-2.726	0.01494	*
Conscientiousness	14.571	4.295	3.393	0.003721	**
Residual std. error	10.71				
F-statistic	6.064				

Table 4.8: Mobile payment application with fingerprint recognition: Coefficients for 2-factor model for of usage of mobile payment using agreeableness and conscientiousness, Signif. codes: '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1.

The two model formulas for usage of mobile payment and security perception are shown in Equations 4.1 and 4.2 with: NO: no security method; Ag: agreeableness; PA: positive attitude (technical affinity); RB: Risk Behavior concerning investments; PQ: pragmatic quality; HQ: hedonic quality; v is the value of the respective ratings.

$$usage = \begin{cases} NO: 20.248 - 7.899 \times v_{Ag} + 16.218 \times v_{PA} \\ PIN: 83.1645 - 10.5755 \times v_{PQ} - 1.7244 \times v_{RB} \\ FP: 30.781 - 12.727 \times v_{Ag} + 14.571 \times v_{Co} \end{cases} \tag{4.1}$$

$$perception = \begin{cases} NO: -0.4649 - 0.1757 \times v_{Ag} + 1.7437 \times v_{SUS} \\ PIN: -1.8732 + 0.9941 \times v_{PA} + 0.5881 \times v_{HQ} \\ FP: -1.4098 + 0.2675 \times v_{Co} + 0.9957 \times v_{HQ} \end{cases} \tag{4.2}$$

The models show the intented focus on personality traits, with positive attitude towards technology having the largest effect. Other influential traits are agreeableness, conscientiousness, and to a lesser extent risk behavior. The application's hedonic and pragmatic qualities play also a role as an influential

	Estimate	Std. Error	t value	Pr(> $\|t\|$)	Signif.
(Intercept)	-1.4098	1.9458	-0.725	0.4792	
Conscientiousness	0.2675	0.1185	2.258	0.0383	*
Hedonic quality	0.9957	0.4329	2.300	0.0353	*
Residual std. error	0.6832	16 DF			
F-statistic	5.965				

Table 4.9: Mobile payment application with fingerprint recognition: Coefficients for 2-factor model for of security percption using conscientiousness and hedonic quality, Signif. codes: '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1.

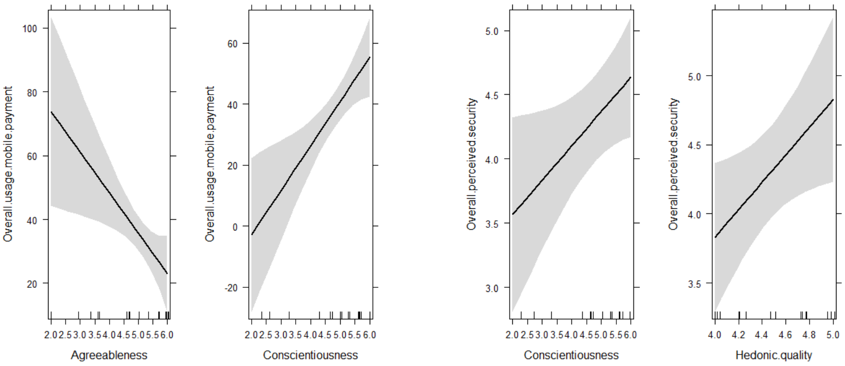


Figure 4.10: Mobile payment application with fingerprint recognition: Effect plots. *Left*: Linear regression model of agreeableness and conscientiousness predicting usage of mobile payment. *Right*: Linear regression model of conscientiousness and positive (attitude technical affinity) predicting security perception.

factor. Multiple regression models for usage and perceived security can be constructed for granular or dichotomous variables representing security methods (usage only). Personality traits (user), app design, and security method (chosen by the developer) explain approximately one third of the variance. As user personality was examined in detail the hypothesis for future work is that social influences, cultural norms, and possibly brand awareness (of the mobile payment provider) play a larger role in the adoption of mobile payment than indiviual personality, technical specifications concerning security, and an appealing application.

4.2.2 Classification

The models can be even more simplified, if some of the granularity concerning security methods is omitted. If the only difference is between having no security method and having *a* method, the model can be reduced to using a categorial variable for method (*0* for having no method and *1* for having either PIN or fingerprint recognition) and the factor positive attitude from technical affinity. The resulting formula is shown in Equation 4.3. The regression models factors are both highly significant (p <0.001 and p = 0.002). Adjusted $R^2 = 0.2827$ is slightly lower, but not by a wide margin.

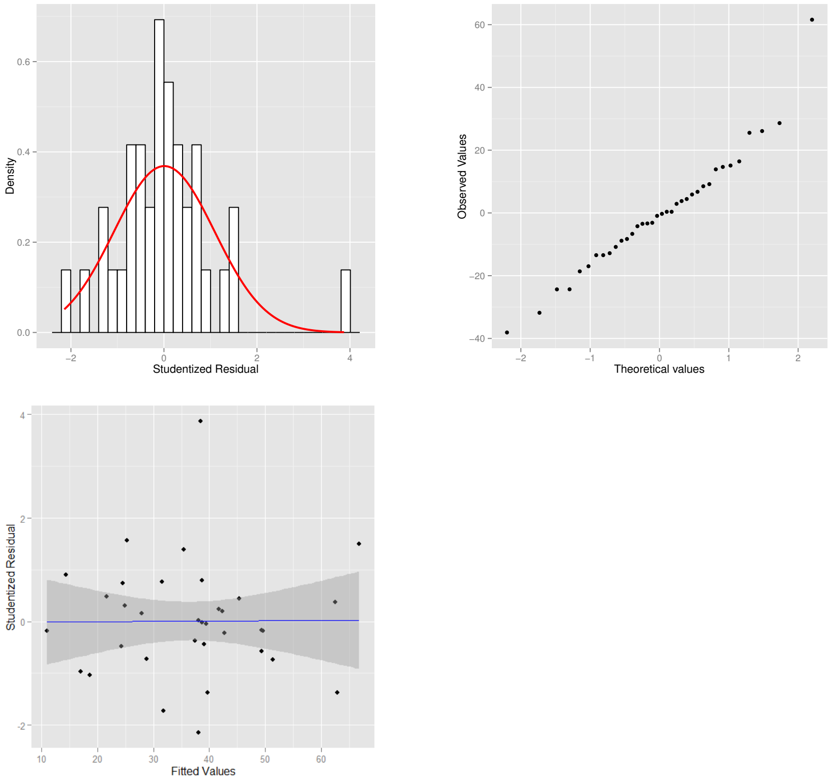


Figure 4.11: 2-factor model using agreeableness and positive attitude (technical affinity). *Upper left*: Histogram of studentized residuals. *Upper right*: Q-Q plot of theoretical values against observed residuals. *Lower left*: Scatterplot of fitted values against studentized residuals.

As was shown in Chapter 3 the usage scenario was split along PIN versus no method or fingerprint recognition. The same approach as above to simplification does not yield a similar result for usage of mobile payment. The adjusted R^2 is a rather low 0.07644 (with $p = 0.01268$). While such a split *per se* may seem awkward at first, it allows for another view on usage. Using no method obviously requires no additional user action on the task of paying. Fingerprint recognition adds one step to the process of authorizing the payment transaction (touching the thump to the mock-up fingerprint reader), but PIN adds five steps (4-digit PIN plus pressing OK). It can be assumed that the latter is less *convenient* than the former due to adding more motion and mental load (remembering the PIN).

$$perception = 1.1813 + 1.0474 \times v_{method} + 0.5567 \times v_{PA} \tag{4.3}$$

The simpler equations act similar to a basic *classifier*. To build upon this idea, two classifiers were constructed using Support Vector Machines (SVM). One classifier with factors perceived security and positive attitude (technical affinity) separates the mobile payment apps with security methods from the app without a method. The SVM uses C-classification with a radial kernel (cost = 10, gamma = 1). The other classifier with factors usage and positive

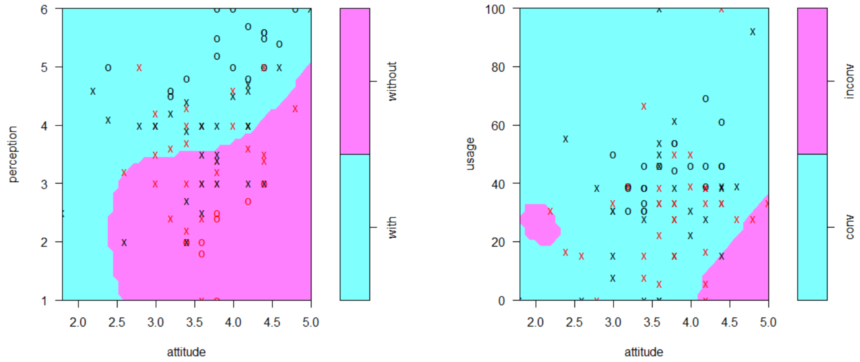


Figure 4.12: SVM scatterplots. x = data points used as support vectors. Data points colored in respective colors. *Left*: Perceived security and positive attitude, app with and without security method. *Right*: Usage and positive attitude, convenient and inconvenient security method.

attitude separates inconvenient method from the convenient ones. Again, the SVM uses C-classification with a radial kernel (cost = 10, gamma = 0.1). The accuracy of the classifications is 0.72 (approx. one out of three classification attempts fails). Class separation is assumed to improve with more data from field studies. The results are plotted in Figure 4.12. The main focus is to show that any security method discriminates against having no security method by increasing perceived security (left plot), and convenient methods discriminate against inconvenient ones by increasing usage (right plot). Both findings support the fundamentals of usable security: Using *any* security method is more likely to be perceived as more secure than using *none*; any security method *adding* substantial costs (e.g. time, money, mental load, motion) is less likely to be used (Cranor and Garfinkel, 2005). A method like fingerprint recognition increases in both perception *and* usage against other examined methods (as it adds no mental load and minimal extra motion) and could therefore be classified as being usable *and* secure. Classifiers such as the ones presented here can be used to optimize for usable security.

4.3 Towards simulation

The models compute useful results for the interpretation of influencing factors and their share of explaining the data variance. Their predictive strengths is untested as it was not the focus of building the models.

The models still inform about the behavior of a specific (target) population and how a mobile payment application should be designed, especially how any implemented security method(s) appeal to the user and lead to usage of the application. Thus, it is highly interesting to incorporate such a model into a simulation tool. This would have the advantage of adapting the model to different areas of interest. For example, to segment the population into smaller groups with shared attributs like age, gender, psychological traits, incapabilities etc. In this case the simulation would generate the user's perceived security and its accompanying behavior faster than doing the calculations “by hand”. It has the added benefit of being able to simulate “extreme” situations where user perceptions and behavior rarely seen in the experiments (or even in the field) could be made visible. For the formal description of user behavior, the previously identified factors and the theoretical models can be transferred into executable models. A more complete model would be able to generate user behavior on the basis of a description of the computer system (interaction sequence), the user (in terms of the previously identified and quantified relevant attributes), the interaction target and the context of use. As prototypical users do not always accurately show the same behavior on every day the model is able to generate different behavior variations in expected frequencies as well as extreme patterns of behavior. It is permissible that the model generates such rarely observable behavior, if it benefits to find edge cases of user behavior. As the model presented here is inevitably incomplete, the implementation in a simulation tool has to be seen as groundwork that will be extended using results from future work.

Besides the purely academic interest in this research, the implementation and results of such a simulation tool has to fullfil (among others) two requirements: useful predictions which provide at least trend expectations, and the possibilty to compare variations of the system in development to “optimize” it or at least get decision criteria.

4.3.1 Predictive model with heuristic substitution

This section on heuristic substitution and the following section on simulation propose two concepts which might be used to predict user behavior and perception on (security) methods not yet implemented in any application.

Simulating existing software with its user interface and security method, and compute resulting user behavior and perception works to fine-tune an application or to find usability failures. But a developer choosing a new security method for an application may not know how its implementation would influence the adoption of the app. This applies to all apps requiring a security method, not only mobile payment. With an established model, the interesting part is how good the model would fit by *substituting* one of its original variables with an untested one.

The main reason for this endeavor is to forego any new experiments, which would be too time-consuming and costly in fast-cycled software development. To avoid random trial and error, the predictive model should be able to substitute one variable with a similar (but not equal) one, with a coefficient derived from avaible information, i.e. literature, focus groups. Re-modeling on a new dataset may require too much effort, therefore substituting might be the only *economically* viable option. It is also quite possible that a new method is untested and only exists as a concept, or is treated as a trade secret, so tests are not an option. The possible user adoption can be examined via surveys (although not without caveats as was already shown, but possibly without alternatives). The method to be implemented could be the first of its kind and no comparision data is available. In this case a simulation has to rely on models derived from prior events and possible (historical) analogies and similarities (which is often used in business case modeling). The concept is to predict previously untested user behavior by relying on a very small set of new information.

As an example, the security method PIN is substitued with another (existing) security method fingerprint recognition. The coefficient is derived from the survey data presented in Chapter 2 instead of the real data as computed in Section 4.2. The main assumptions of this method is that users will react to the new security method in a similar way, but probably with other coefficient weights. These weights will be derived from other sources without doing further user tests.

The envisioned variable substitution would use already available data to replace one of the coefficients. This is done in analogy to the mathematical operation of substitution. But rather than changing the variables, and having the same equation (often a simpler one to compute), one variable is replaced with a *similar* (but not necessarily equal) factor with its approximated coefficient (derived from available data). Essentially, this technique is a *heuristic* applied to a predictive model. The resulting prediction is a *codified version of an educated guess.*

The variable substitution and the model implementation in a simulation tool is more efficient, if the heuristic derives changes easily. The heuristic approach is used with data collected from a survey. A coefficient is derived from Ben-Asher et al. (2011) for security perception of using a mobile payment system with predictors fingerprint recognition and technical affinity (positive attitude). The result from the survey puts fingerprint recognition ahead of PIN in terms of the *number* of users who (strongly) agree to fingerprint being secure. There are a number of users who think that both methods are secure. But with a fingerprint/PIN ratio of approximately 70:50, it can be assumed that the security perception would have a similar ratio. It can be also assumed, if a device or application uses fingerprint recognition, those users would rate their security perception of it accordingly. In this case, the substituted coefficient for fingerprint recognition can be computed as 1.4. Equation 4.4 is derived from Equation 4.2 by multiplying the *relevant* factors of the model for perceived security using PIN with the coefficient computed from survey data. The relevant factor here is hedonic quality, while positive attitude towards new technology is seen as a stable personality trait. The survey-derived coefficient is used with the equation's constant (for normalization) and hedonic quality.

$$perception_{FP} = -2.6225 + 0.9941 \times v_{PA} + 0.8233 \times v_{HQ} \tag{4.4}$$

Test 5 is used to cross-validate the predictive model with variable substition with real data. No data from test 5 was used in Equation 4.4 and thus did not have a share in the model. The predicted values in Figure 4.13 are plotted against actual data with both regression models (using 2D for clarity, ommitting factor positive attitude). A one-way ANOVA computes that the means are not significantly different ($p = 0.4$).

There is little reason to believe, that the biometric security method using fingerprint would lead to completely random ratings of perceived security by the user. It is reasonable to assume that users would rate it similar or better compared to PIN. At least this is what several of the surveys and focus groups got as a result. But the average rating value given to both methods is almost equal in the experiments and the heuristic method is (surprisingly) close to the model derived from actual data. According to the model for perceived security of fingerprint recognition derived in Section 4.2.1 the best fit uses factor

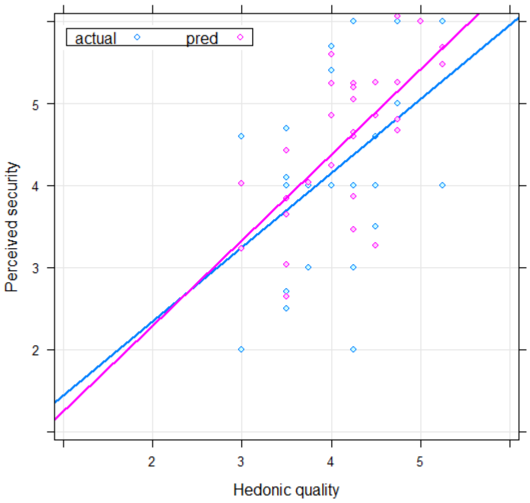


Figure 4.13: Scatterplot of heuristic prediction versus actual data with regression lines.

conscientiousness instead of positive attitude. It could be pure chance, that the heuristic substitution lead to a model so close to the model based on actual data. It was already stated that survey data and lab experiments sometimes differ in their results. Opinions expressed in surveys by un-experienced users (how do you *perceive* the level of security when *thinking* about fingerprint recognition as a security method? – Possibly without ever thinking about it before or even using it.) might not be identical when confronted with a lab experiment.

But all in all the concept of heuristic substitution in its first iteration provides a good fit which could be derived from the survey data directly. If any survey data is collected for use in a substitution model, it can be prepared accordingly and it might be possible to insert the data in a more sophisticated way (e.g. asking for known correlated factors, prepare values and factors for insertion). The approach looks promising and the concept has to be explored further in future work.

4.3.2 MeMo workbench

This section presents a conceptual implementation of the regression models into the simulation tool MeMo. At the current state the tool's output does not differ from direct computations using the models' formulas.

The MeMo workbench – short for mental model – is an analysis tool to support developers to evaluate software during various phases of development (Möller et al., 2006). As previously mentioned throughout this thesis developers face the challenge of inherited security concepts in both hardware and software. In the case of a mobile payment applications additional constraints by regulations and certifications apply. MeMo allows for a semi-automatic analysis of user behavior in interaction with a range of software including spoken-dialog systems (Engelbrecht et al., 2009) and graphical user interfaces (Schulz et al., 2012).

There are several reasons to choose MeMo over alternative concepts and implementations (among them PARADISE, CogTool, ACT-R, SOAR, CLARION, and EPIC): It was for example previously used to simulate user behavior in a modified version of the well-known game *Tetris* which extended it to combine financial profit or loss by balancing threat and security (Ben-Asher et al., 2009; Möller et al., 2011). Players could gain profit by completing rows and could be warned against upcoming threats on different levels. As the game was time-constrained and the warnings would interrupt the game, it could dimish the player's profit (no warnings to 100% warnings against threats, but with lots of false warnings). One of the results was how users changed the security level depending on the threats and warnings. Möller et al. (2011) state that based on the simulations, user behavior in security relevant situations can be predicted and user interfaces can be designed to guide intended behavior.

The behavior model derived from the Tetris test showed good results in predicting the overall trend of the user behavior: "The probabilistic and rule-based simulation approach [...] is apparently able to predict user behavior with respect to three security-relevant variables in a meaningful way. Overall, the frequencies and the range of values observed in the simulation match quite well the ones observed in the experiment" (Möller et al., 2011).

Another reason to prefer MeMo was that the source code and extensive "in-house" knowledge was readily available, because the simulation tool is still being developed at the Quality and Usability Lab at TU Berlin. But the major advantage is MeMo's flexible framework, which makes the software suitable for later combinations, variations, and implementations of security-related factors, tasks, and processes. Speech dialogue and GUI elements were already in place, tested, documented, and results published (Engelbrecht et al., 2009; Schulz et al., 2012). The modular approach allows it to add new modules and to use already implemented features like target user group selection.

MeMo does a rule-based analysis using a probabilistic user model. The model for use here is derived from the previous chapter. A model of the system and the user's tasks was also added. As its predictive power is still under-developed to be used for a guiding software analysis, the modules are implemented as a *proof-of-concept*. The theoretical and practical groundwork done in the previous chapters for the simulation enables to implement concepts to support tools for software development. The goal is to achieve better usability, usage, and improved security of the mobile payment application during development. A tool like MeMo makes it possible to efficiently evaluate security-related computer systems for usable security.

The predictive models generate two results: Which scale value a user appoints to perceived security of a card-paradigm-based mobile payment application. And how many items are "bought" using this payment application within a given determined set.

The simulation model is derived from theoretical considerations (see Chapter 2) and empirical studies (see Chapter 3) and then formalized and implemented as modules. The factors have been classified and analyzed in the previous chapters to cover all relevant aspects in empirical studies as well as in the subsequent modeling. One of interesting questions that arise is "What is the impact of the factors on the subjective security requirements and user behavior, if one tries to predict *something new* to the model?" Thus, user behavior concerning *new* security methods (think heuristic substitution) and features can already be

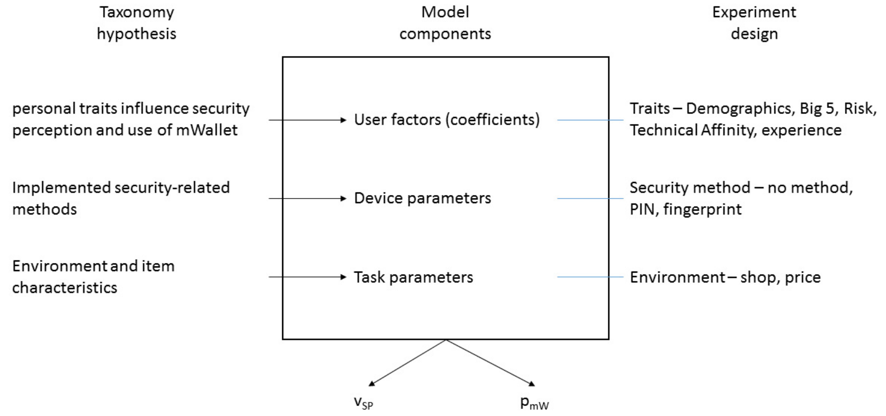

Taxonomy hypothesis
Model components
Experiment design
personal traits influence security perception and use of mWallet
User factors (coefficients)
Traits – Demographics, Big 5, Risk, Technical Affinity, experience
Implemented security-related methods
Device parameters
Security method – no method, PIN, fingerprint
Environment and item characteristics
Task parameters
Environment – shop, price
v_{SP}
p_{mW}

Figure 4.14: Model schematics used for MeMo

predicted during the development process of a new system. Such a prediction is – because it can be carried out during the on-going design process – more effective and more efficient than a subsequent test of the system after completion. Of course, empirical user testing can never be completely replaced by simulations.

Several factors influencing user behavior are already known. These include factors of the user (personal risk tolerance, concern for privacy, confidence in the computer system and associated institutions or persons, self-assessment of computer knowledge, experience with attacks on computer security, insight into the effectiveness of security systems, individual perceptions of risks, etc.), the interaction target (type of primary task motivation of the user, expected cost-benefit ratio in taking security measures, etc.), the computer system (general usability of the computer system, arrangement of interaction elements, type and date of presentation of the possible dangers, etc.) and use of the environment (daily reporting, potential educational campaigns, personal environment, current situation of use, etc.).

Since the observation of all the previously mentioned factors would be very extensive, a sub-model was designed (see Figure 4.14) to allow some limited simulation of user behavior. Several factors were empirically determined from this model. The factors were chosen so that they match the sample system, the mobile payment prototype mWallet. The current selection consists primarily of the significant factors related to usability and security as shown in the taxonomy (Figure 2.1). These factors were varied in the manner that primarily different (biometric) authentication methods were tested. A second selected factor is the nature or scope of the threat. The threat (case of misuse) can be varied, e.g. by the amount of money involved or the type of the environment it happened in. A third factor is the technical affinity (and to some degree risk perception) of the user.

Participants of the experiments were classified by a screening questionnaire. Those classification can be added to MeMo to the already existing groups (e.g. age, gender, disabilities). All added factors are related to the mobile payment prototype. The prototype authentication method could be switched off (by design, not the user), so the known trade-off between usability and security could be tested. Because it is a payment system, it was assumed that targeted attacks on the payment process would show an effect.

The model is represented as a set of states with certain transition probabilities and modifying rules to change the transition possibilities. The MeMo workbench is used to simulate the user model derived in chapter 4. In order to do so, an extension to MeMo was necessary:

- Define the model.
- Prepare the model for probabilities and rules to apply to security-related computer functions. This is done on the basis of the above-identified factors and coefficients, but is implemented as a static function due to missing state-altering informationn.
- Expand MeMo workbench with modules on payment method decision and security perception.
- Extend the existing interface of MeMo to the corresponding features for computer security.
- Test runs in restricted areas for review in each program step if meaningful results are produced in accordance with the empirical data.

The MeMo workbench generates user behavior on the basis of basic probabilities, which describe the general willingness to carry out a certain number of possible interaction steps, and modifying these basic probability rules. Basic probabilities and rules need to be redefined to use MeMo to simulate user behavior in the area of computer security. This is done on the basis of the above-identified and quantified factors as well as using the results of the experiments described in the chapters before. The MeMo workbench must also be expanded to include those behavioral factors. In contrast to an approach like PARADISE MeMo does not work purely statistically, but as a mixture of a rule-based and a statistical model. Furthermore, it can easily perform simulations of user behavior in order to identify any differences in this behavior.

Statements and forecasts about the expected subjective assessment of the usability and the perception of security are derived based on the simulated user behavior. For this purpose linear and muliple regression models and rule-based coefficients for variations were used for further refinements of the simulations. The state-based models are assumed to adjust better to local factors that influence user behavior (which arise from the current interaction step) than integrative models relying on linear regression only.

The result is an executable model of user behavior, which takes into account the previously identified relevant factors and simulates real, observable user behavior (carried out in accordance with the developed test method) with sufficient accuracy. Moreover, the model estimates assessments of usability and perception of security when dealing with mobile payment applications on the basis of simulated interactions and the factors influencing them.

Because the participants tasks of rating their perceived security and deciding which one of three given payment methods to use cannot be divided into subtasks, there is no sequential change of states to work on. The scale value of security perception and the choice of payment method are two ad-hoc decisions by the user. Because the shopping sequences were not randomized, probabilities

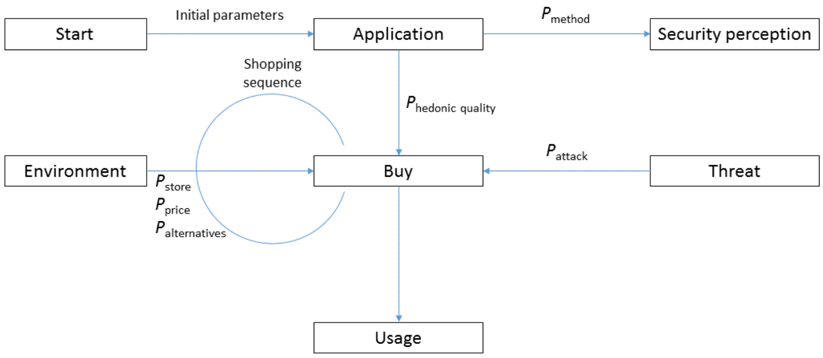


Figure 4.15: State chart model of mobile payment.

for state changes concerning sequential usage of different payment method can not be computed yet.

The model formulas derived in Chapter 4 were used. The author added three modules to MeMo in order to extend MeMo to mobile payment applications (see Figure 4.14 for the design concept). The modules expand MeMo with security-related models concerning mobile payment systems.

- The Payment Decision Module collects all possible payment options and computes current payment probabilities. It extracts relevant user attribute and calculates probabilities for all available payment methods depending on user attributes. Finally the module makes a decision for a specific payment method using Equation 4.1.
- The Payment Processing Module evaluates the different payment methods and checks if the current system state contains a payment decision dialogue, otherwise another module takes over (Device Knowledge Processing Module) to decide for a user interaction.
- The Payment Utility Module connects any perceived user interface elements with the current state of the Payment Decision.

One of the many useful aspects of MeMo is the ability to iterate over many steps. This enables any probabilistic effect to reach “extreme” values. In every data collection these values would be outliers. But in terms of usability outliers can provide valuable data. For example, failures to successfully use a device or application, because the simulated user needs a very long time to end a specific task. MeMo supports the developer in revealing those extremes. The developer would be then able to put preventive measures into the device or application. Because the current information for state change probabilities is missing (as no randomized shopping sequences were used) the output does not alter from one state to another. Effectively, there is only one state which could also be computed directly using Equations 4.1 and 4.2.

Figure 4.15 shows a state chart model for mobile payment as envisioned for implementation in MeMo using the three mobile payment-related modules (without probabilities for state changes). The model displays the flow within the simulation. It starts with setting initial parameters (e.g. personality traits, age, and gender), and sets an application design including a security method. This computes perceived security and sets a value for perceived hedonic quality. The shopping sequence iterates the user behavior influenced by environment, price, and available alternatives. An effect by threat may be added. The loop generates mobile payment usage. The program flow is:

- Start with user characteristics (existing MeMo module) and add application attributes security method (P_{method}) and design ($P_{hedonic\ quality}$) using the Payment Utility Module,
- buy using the Payment Decision Module and Payment Processing Module (loop through threat (P_{attack}), price (P_{price}), environment (P_{store}), and sequential changes ($P_{alternatives}$),
- produce output payment method and perceived security.

The probabilites for the user actions were derived from the experimental results and compute the different outcomes (perceived security and usage of mobile payment) depending on the settings. The probabilities are based on rules which follow an if-then-condition. For example: "If the user is technical affine and the security method is fingerprint recognition, then the probability for the user to use mobile payment is higher". These rules are implemented using the appropriate model of user behavior (Equation 4.1) and perception (Equation 4.2) derived in the previous chapters which includes the taxonomical factors in the model formulas. The simulation tool should be flexible enough to both implement the model into an executable simulation of user interactions with system (including its environment and context). The goal is to predict the target population's subjective perceptions of security and usability of the system on the basis of simulated interactions.

The missing data for the altered probability of future use based on prior use of mobile payment prevents to fully implement the function into the MeMo modules. A placeholder constant k is used instead until a proper function can be derived from new data. Of course, there is still the possibility that such a function does not exist. The function would alter the probability of using any payment method based on the payment method used in the step before (but would "forget" any step before the previous one). In the current implementation the function is set to the value of 0, so it does not change the next step of the iteration.

4.4 Summary

The regression models using two factors explain approximately one third of the variance of the data. These show the effects of *personal* attributes like personality traits, risk behavior, and technical affinity on the user's choice of a new payment method compared to existing ones like cash and payment cards. These factors are modified by the factors concerning application design, device, security method, environment, and threat based on suitable statistics for the data. Classifiers are able to separate convenient from inconvenient security methods, and methods perceived as secure from using no method at all. Still, accuracy needs to be improved.

More data is needed to expand the model to include additional factors. This cannot be observed via lab tests or surveys, but requires field tests using a commercially established platform. These platforms are starting to emerge now, but still have a very small user base to make the selection of representative participants difficult as of end of 2014.

The relatively low explanation of the data variance by the models and the low accuracy of the classification can point to several possible causes:

- the choice of a payment method is an “ad-hoc” (random) process like throwing dice and cannot be predicted well;
- the data has an unusual distribution, which will be rectified by collecting more data of the same type;
- the data is incomplete and several factors are missing, most of which can only be collected via field tests – this will be the hypothesis guiding future work.

The full implementation into the simulation software MeMo has to wait until further data for other factors – assumed social and cultural norms influencing the user – is available. The empirical data is not yet able to deliver probabilities for changes in the sequence of payments methods. A relationship could be expected between the prior use of mobile payment and any subsequent use. Prior use would alter the probability of using mobile payment for future purchases. Such a term could be included in the model and would be especially useful for inclusion into MeMo. But the data did not confirm the assumption so far. The proposed heuristic substitution, although promising, has to wait for more data to be further evaluated – or to be rejected.

Chapter 5

Conclusion

There are several *new insights* presented in this research work which cover several areas. This is the first study building upon a newly developed open taxonomy using empirical data from controlled lab tests, and constructing a model to show the different influences of personal attributes and security methods. Most other studies rely on survey data or on systems not applicable to the German market (see also Amoroso and Magnier-Watanabe (2012)). This research work has a far more granular examination of personality traits and also incorporates factors which are difficult or impossible to obtain using questionnaires because they rely on ad-hoc perceptions and decisions of the user like well-known payment methods as alternatives, different security methods, price, store type, and threat.

The IT industry selling personal computers to the masses is four decades old now, the telecommunications industry for GSM-based mobile communication more than two. Both industries converged in the recent years from Apple's introduction of the modern smartphone *and* its accompanying app store in 2007 until the recent buy-outs of Nokia's handset division by Microsoft and of Google's Motorola division by Lenovo in 2014. The smartphone market has also strong players like Samsung, LG, and Sony, all consumer electronics companies. As laid out in Chapter 1, the operating systems driving these smartphone – Android, iOS, Windows Phone – have their conceptual and philosophical roots in the 1960s. The criticism directed at both users and vendors (including their developers) concerning security issues – e.g. weak passwords, carelessness, weak software design, missing encryption, exploitable holes – does not always account for the legacy even modern systems carry with them. The dilemma of users and developers is this legacy framework which limits security design choices. Because security has not been a priority for most of the time personal computer device have been sold, both users and developers have to think about security and privacy threats targeting their (mobile) devices and how to prevent them. Developers have also to consider the right design choice for any security concept and method implemented into an application that enters a market with app stores filled with millions of apps. The differentiating (and winning) factor could be an appealing security method, but any bad choice will turn away users.

Someone using a computer has to think about security issues because of attackers. Without attackers, security would not be an issue. The intented task is influenced by user-related factors. The taxonomy unfurls a relationship map for the individual user with an emphasis on related factors, which cover several areas – *user, interaction, device, environment, and threat* – related to computer-security drawn from literature and studies where the author was part of the research team. The taxonomy assumes that a user's accomplishment of a given task using a (mobile) computer (including smartphones) is influenced by his or her personality traits, risk perception, experience, environment, threat perception, security percpetion (of the computer), and application or system design.

The taxonomical factors and relationships were applied to the specific field of interest of mobile payment and transferred to the design of several lab experiments, which focused on the influencing personal factors for user behavior and perception in the context of payment-related security. The design of the experiments centered on a mobile payment prototype as it satisfied the requirements of being a newly introduced system, offering features of computer-related security, and touching a user's security perception. The system could not be field-tested because necessary components for mobile payment were not in place at the time, so a laboratory test environment was built. Additionally, regulations and ethical issues prevented a real-world installation. In the end – even if implemented – such a real-world test system would not differ enough from a lab test. Users would still not be able to install the application on their own smartphones and get they own payment card personalized. No real or the participants' own money could be spent on real goods in a real shop. So, the user involvement was bound to the lab environment and based on a fictional role. Three cornerstones shown in Figure 1.2 were missing and prevented a real-life environment: A payment card issuer with its Service Provider Trusted Service Manager, a mobile network operator with its own Trusted Service Manager with over-the-air provisioning, and an NFC-based contactless payment terminal at a retail shop.

Five different experiments varied the security method of the mobile payment application and the threat to the payment method. These experiments are a new contribution to the field of research. Surveys had revealed what people *think* of a variety of security methods from PIN to biometrics. The high ratings for fingerprint recognition (Ben-Asher et al., 2011) lead to the method being implemented as a mock-up. The empirical results found 10 out of 38 examined factors to be relevant: agreeableness, conscientiousness, openness, and positive attitude (technical affinity); risk of PIN as a security method; hedonic quality and security method; threat; store type and price. Five of the six hypothesis derived from the taxonomy could be retained and one had to be rejected: relationship between personality traits and security perception and usage of mobile payment; negative relationship between cost of security and usage of mobile payment concerning using PIN as a security method; positive relationship between the perceived hedonic quality of the mobile payment application's design and security perception, and usage of mobile payment; negative relationship between (financial) threat and security perception; positive relationship between an institution's reputation (e.g. public office versus retail stores) and usage of mobile payment.

The multiple regression models derived from the experiments explain around 20 to 35% of the variance using two personality traits factors and security method as moderator. This is in contrast to other models by Kim et al. (2010a), Schierz et al. (2010), and Yang et al. (2012) which have much higher adjusted

R^2 beyond 0.5. These theoretical models based on survey data are not supported by the empirical data presented here. The limitations are due to either a constricted focus on mobile payment without offering alternatives, or the ommission of ad-hoc perceptions, or the missing granularity of security methods. The models presented in this work rectify some of the problems of the survey-based models by using new and *more realistic* data.

It has been examined throughout this work how application development can be supported by showing the influential factors for mobile payment usage. It has to be stated that the developer's decision is still not an easy one. Apart from the hardware and software constraints, the user interface elements for any mobile payment app are limited. The use case is normally *not* to use any GUI elements. The security method must not interfer with the payment process. Choice is often limited to what the hardware offers. In this regard, the findings of the experiment show that the only examined method being usable and perceived as secure is fingerprint recognition.

5.1 Current state of mobile payment

As of end of 2014 the latest entry into the mobile payment market is "Apple Pay" by Apple Inc. Still, the numerous currently available mobile payment applications wait for critical mass. Apple Pay has recently gained an impressive one million users in its first three days (Wakabayashi, 2014), and is using fingerprint recognition ("Touch ID"), which this research showed translates into more usage, but not necessarily to higher ratings of perceived security. This also reinforces the dilemma of developers how to differentiate a product where user interaction is merely a micro-interaction, if at all. It also shows that brand recognition of any payment solution is very likely another important factor. Two very similar offerings to Apple Pay's NFC-based mobile payment, Google Wallet and Softcard, did not gain a large customer base in the USA, although being on the market for years. The differentiators are Touch ID and Apple's brand.

The complex infrastructure using NFC SIM cards (see Figure 1.2) is also challenged by new technology. *Tokenization* removes the need for the Trusted Service Manager (for payment card provisioning to the SIM card) and replaces it with a system directly integrated into the payment process. Security is added with the use of one-time tokens for every payment transaction instead of transmitting payment card information. *Host card emulation* (HCE) sidesteps the Secure Element on the NFC SIM card and emulates the card directly in software on the device CPU. The payment card credentials can even be cloud-based using this approach.

Figure 5.1 shows an overview of worldwide use of mobile payments in 2014. The overview uses a broader definition covering not only smartphone-based mobile payment at the point-of-sale, but also online payments and contactless payment cards.

All in all the market for mobile payment applications is currently very fragmented and not mature. Only two countries, Kenya and Japan, have enough mobile payment users, that mobile payment can be called to be in wide-spread use. The service providers can be divided into two divisions. The ones using the existing payment networks as described in Chapter 1, and the others

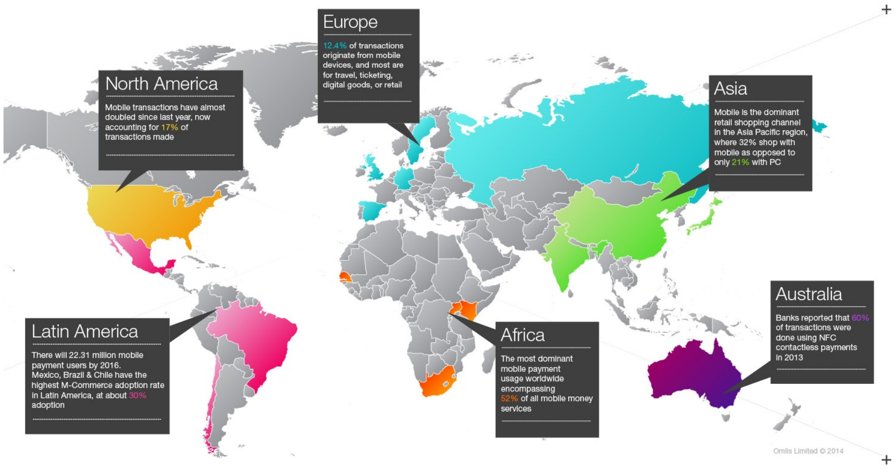

Europe
12.4% of transactions originate from mobile devices, and most are for travel, ticketing, digital goods, or retail
North America
Mobile transactions have almost doubled since last year, now accounting for 17% of transactions made
Asia
Mobile is the dominant retail shopping channel in the Asia Pacific region, where 32% shop with mobile as opposed to only 21% with PC
Australia
Banks reported that 60% of transactions were done using NFC contactless payments in 2013
Latin America
There will 22.31 million mobile payment users by 2016.
Mexico, Brazil & Chile have the highest M-Commerce adoption rate in Latin America, at about 30% adoption
Africa
The most dominant mobile payment usage worldwide encompassing 52% of all mobile money services
Omlis Limited © 2014

Figure 5.1: Worldwide use of mobile payments 2014 (Thompson, 2014)

using their own closed-loop networks. The prototype described in this work and its commercially launched version (Deutsche Telekom *myWallet*) is an example for the first type as are all other offerings by German mobile network operators. Into the other category fall applications from Yapital (Otto Group) using QR codes, Starbucks (one of the biggest mobile payment players in the United Stated with 11% of annual revenue generated through Starbucks own app by eight million customers (Roemmele, 2014)) using bar codes, and PayPal using face recognition by the cashier via a customer's photo shown on the POS register's display.

Apple's and Starbuck's successes are both limited by either the missing share of NFC-enabled POS terminals or by their (intented) limitation to Starbuck's shops only. Japan's existing mobile payment technology is literally an island solution despite its millions of users. But within these constraints, the eight-digit number of customers for these systems each dwarf the number of mobile payment users in Germany, where the combined active user count for the available NFC-based applications is between ten to twenty thousand as of end of 2014 (insights gained by the author, official numbers unpublished). The number of active users for all other solutions offered in Germany is possibly even less.

Recent studies show that (data) security is still paramount for users and being the number one requirement for mobile payment use by a wide margin (Krol and Stender, 2014). As system flaws which could be used for potential fraud are covered on mainstream media, a main asset of a mobile payment app is a well-perceived security method (Emms et al., 2014). Although the individual effect of any implemented security method is small as experiments and subsequenting models revealed, any security *hole* will probably be disastrous to any payment app's reputation.

The research presented in this thesis features several useful findings applicable to the marketability of mobile payment solutions:

- a user's personality plays a role, but (country) specific socio-cultural norms are probably prevalent;

- different security methods lead to different levels of application usage, but the overall influence of the investigated security methods is only marginal;
- nonetheless, the implemented security method is one of the few application differentiators, the "right" method could be a market advantage considering all other app elements being equal.
- the approach to use software simulation for design decisions concerning security methods is not complete enough to be economically viable yet.

The chance for existing mobile payment providers and those about to enter the market is to adapt security methods leading to more frequent use of the applications while also being perceived as more secure than others. At the moment fingerprint recognition fulfills both requirements. The historical evolution of smartphones as a direct descendent of desktop computers and their operating systems is limiting, because the designs are mainly rooted in academia and counterculture of the 1960s with a focus on sharing. This still leaves today's developers and users with limited choices concerning security concepts and methods. Developers mainly program for UNIX-derived mobile operating systems. The available security methods to users for authentication and authorization are by default 4-digit PINs, 2D-grid 3x3 patterns, and fingerprint recognition (restricted to a few smartphone models – like Apple's iPhone 5s and 6, and Samsung's Galaxy S5 and S6 – still considered expensive and high-end in 2014). A mobile payment application could make use of both: good app security and a usable security method – *usable* meaning it would lead to frequent usage of the app. The long-term goal would be to help implementing usable security through predictive behavior modeling without sacrificing efficient software development (and possibly leading to guidelines to implement appropriate security features on a mobile payment system).

Today's implementation of fingerprint recognition is different from the one used as a mock-up in the experiments. It uses either a fingerprint reader where the user either has to swipe a finger (usually the thumb) over the reader or just presses against it. The effort done by the participants to pay (in manual mode) was higher than, for example, Apple's Touch ID, where fingerprint recognition can be done effortlessly. But both the experiments and the fast increase in users of Apple Pay support the notion that an appealing security method like fingerprint recognition works in attracting users.

The models constructed in Chapter 4 explained around one third of the variance of the experimental data. The largest influence is not user personality or security method (or any other of the factors presented in Chapter 3), but probably other factors like social influences, cultural norms, and possibly trust in the mobile payment provider. A 2014 survey among Germans revealed that 55.5% would consider using mobile payment (regardless of technology), but only 21% found it to be a secure way for payment transactions (TNS Infratest, 2014). This is in line with only 23% being able to explain QR codes, and NFC and BLE even less. These surveys are highly speculative because most of the respondents judge mobile payment without knowing the details of the underlying technology. A reference to the existing card paradigm and its transfer into a new form factor would balance the unkown security mechanisms (as they are mostly unknowm to the normal user for plastic payment cards, too). But another survey showed even if clarified half of the respondents in Germany remain sceptical because of security issues (Nordlight Research, 2014). These influences and the particular German habit of paying cash has to be examined more closely concerning mobile payment (Wörlen et al., 2012).

5.2 Future Work

The strength of MeMo's core engine – probability- and rule-based modeling, and target user group selection – could not be fully used. The model could show to some extent the effects of personality traits and security methods, but – as expected – a big part of the data remains unexplained due to the restrictions of the lab experiments. In this regard, only a longitudinal field study of an existing mobile payment app among users and a control group could reveal the influencing factors. Additionally, future studies could verify, whether one of the proposed ideas behind the task of implementing the predictive model – variable substitution – would be useful or not.

After analyzing personal factors contributing to security perception and usage of mobile payment in detail, the next step is to extend the taxonomy (and the predictive model) to include socio-cultural factors. The 2D taxonomical plane would be extended with another socio-cultural plane, where relationships between factors would extend from one plane to the other. These additional factors would probably paint a more complete picture and an improved model could be constructed.

This would include cultural influences like use of particular payment methods in a given context. The proposed factors to be researched are:

- short and long-term influence of mass media and social media;
- individual environment like friends, relatives, and colleagues;
- privacy issues;
- trust as influenced by brand awareness and reputation of the mobile payment provider;
- introduction of disruptive technology ("game changer");
- technology adoption over time.

The country-wide user base for mobile payment is still very small in Germany, so it might be very difficult to find a representative panel of participants. But the state of mobile payment in 2014 may allow to start thinking about a field study in the near future.

Chapter 6

Bibliography

Adams, A. and Sasse, M. A. (1999). Users Are Not the Enemy. *Communications of the ACM*, 42(12):40–46.

Amoroso, D. L. and Magnier-Watanabe, R. (2012). Building a Research Model for Mobile Wallet Consumer Adoption: The Case of Mobile Suica in Japan. *Journal of Theoretical and Applied Electronic Commerce Research*, 7(1):94–110.

Apple Inc. (2014a). iOS Developer Library. https://developer.apple.com/-library/ios/navigation/. Accessed: 07-06-2014.

Apple Inc. (2014b). Mac Developer Library. https://developer.apple.com/-library/mac/navigation/. Accessed: 07-06-2014.

Bagnall, B. (2006). *On the Edge: The Spectacular Rise and Fall of Commodore.* Variant Press, Winnipeg, Manitoba, Canada, first edition.

Ben-Asher, N., Meyer, J., Parmet, Y., Möller, S., and Englert, R. (2009). Security and Usability Research Using a Microworld Environment. In *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '09, pages 54–54, New York, NY, USA. ACM.

Ben-Asher, N., Sieger, H., Ben-Oved, A., Kirschnick, N., Meyer, J., and Möller, S. (2011). On the Need for Different Security Methods on Mobile Phones. In *Proceedings of the 13th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '11, pages 465–473. ACM.

Ben-Asher, N., Sieger, H., Kirschnick, N., Meyer, J., and Möller, S. (2012). Poster: On the Need for Different Security Methods on Mobile Phones. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12. ACM.

BITKOM (2014). Jeder Zweite würde biometrische Daten einsetzen. http://www.bitkom.org/files/documents/BITKOM_Presseinfo_Zahlungen_-mit_biom._Daten_15_08_2014.pdf. Accessed: 18-11-2014.

Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R., and Toval, A. (2011). Basis for an integrated security ontology according to a systematic review of existing proposals. *Computer Standards & Interfaces*, 33(4):372–388.

Brooke, J. (1996). *Usability Evaluation in Industry*, chapter SUS: A "quick and dirty" usability scale, pages 189–194. Taylor and Francis.

Bruder, C., Clemens, C., Glaser, C., and Karrer-Gauß, K. (2009). TA-EG - Fragebogen zur Erfassung von Technikaffinität. Technical report, FG Mensch-Maschine Systeme TU Berlin.

Chin, E., Felt, A. P., Sekar, V., and Wagner, D. (2012). Measuring User Confidence in Smartphone Security and Privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 1:1–1:16. ACM.

Clarke, N., Furnell, S., and Reynolds, P. (2002). Biometric authentication for mobile devices. In *Proceedings of the 3rd Australian Information Warfare and Security Conference, Perth, Western Australia, 28-29 Nov 2002*.

Collins, J. (2010). Should all hard drives be encrypted? http://www.theregister.co.uk/2010/04/19/encrypted_harddrives. Accessed: 07-06-2014.

Computer Security Laboratory of the Computer Science Department at the University of California, D., editor (1998). *Early Computer Security Papers (1970-1985) distributed on CD-ROM at the 21st National Information Systems Security Conference*, NISSC '98. Computer Security Laboratory of the Computer Science Department at the University of California, Davis.

Cranor, L. F. and Garfinkel, S. (2005). *Security and Usability: Designing Secure Systems That People Can Use.* O'Reilly, Sebastopol, CA, USA.

Dahlberg, T., Mallat, N., Ondrus, J., and Zmijewska, A. (2008). Past, Present and Future of Mobile Payments Research: A Literature Review. *Electronic Commerce Research and Applications*, 7(2):165–181.

Davidson, J. D. and Apple Computer, I. (2002). *Learning Cocoa with Objective-C.* O'Reilly, Sebastopol, CA, USA.

Dodson, B. and Lam, M. S. (2012). Micro-interactions with NFC-enabled Mobile Phones. In Zhang, J., Wilkiewicz, J., and Nahapetian, A., editors, *Mobile Computing, Applications, and Services*, volume 95 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 118–136. Springer Berlin Heidelberg.

Dörflinger, T., Voth, A., Kramer, J., and Fromm, R. (2010). "My smartphone is a safe!" The user's point of view regarding novel authentication methods and gradual security levels on smartphones. In *Proceedings of the International Conference on Security and Cryptography*, SECRYPT, pages 155–164. SciTePress.

Emms, M., Arief, B., Freitas, L., Hannon, J., and van Moorsel, A. (2014). Harvesting high value foreign currency transactions from EMV contactless cards without the PIN. In *21st ACM Conference on Computer and Communications Security*.

Engelbrecht, K.-P., Quade, M., and Möller, S. (2009). Analysis of a New Simulation Approach to Dialogue System Evaluation. *Speech Communication*, pages 1234–1252.

Field, A., Miles, J., and Field, Z. (2012). *Discovering Statistics using R.* Sage, London, UK.

Firesmith, D. G. (2005). A Taxonomy of Security-Related Requirements. In *Proceedings of the Fourth International Workshop on Requirements Engineering for High-Availability Systems*.

Fischer-Hübner, S., Iacono, L. L., and Möller, S. (2010). Usable Security und Privacy. *Datenschutz und Datensicherheit*, 34(11):773–782.

Fletcher, D. (2010). How Facebook Is Redefining Privacy. *TIME Magazine, issue May 20th, 2010*.

Freiberger, P. and Swaine, M. (2000). *Fire in the Valley: The Making of The Personal Computer.* McGraw-Hill, New York, NY, USA, 2nd edition.

Furnell, S. and Clarke, N. (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. *Computers & Security*, 24(7):519–527.

Gajda, B. (2011). Managing the Risks and Security Threats of Mobile Payments. *Lydian Journal*, pages 14–22.

Gancarz, M. (2003). *Linux and the Unix Philosophy.* Digital Press/Elsevier Science, Woburn, MA, USA.

Garfinkel, S. and Mahoney, M. K. (1993). *NeXTSTEP programming: Step one, object-oriented applications.* Telos.

Gartner Inc. (2014). Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013. http://www.gartner.com/newsroom/id/2665715. Accessed: 28-11-2014.

Gerlitz, J.-Y. and Schupp, J. (2005). Zur Erhebung der Big-Five-basierten Persönlichkeitsmerkmale im SOEP. *DIW Research Notes*, 4.

Gerrig, R. J. and Zimbardo, P. G. (2008). *Psychology and Life.* Allyn & Bacon, 18th edition edition.

Gruber, T. R. (1993). A Translation Approach to Portable Ontology Specifications. *Knowledge Acquisition*, 5(2):199–220.

Hartson, R. and Pyla, P. (2012). *The UX Book: Process and Guidelines for Ensuring a Quality User Experience.* Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1st edition.

Hassenzahl, M. and Monk, A. (2010). The Inference of Perceived Usability from Beauty. *Human-Computer Interaction*, pages 235–260.

Heckhausen, J. and Heckhausen, H., editors (2006). *Motivation und Handeln.* Springer.

Herley, C. (2009). So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, NSPW '09, pages 133–144. ACM.

Hertzfeld, A. (2004). *Revolution in The Valley: The Insanely Great Story of How the Mac Was Made.* O'Reilly, Sebastopol, CA, USA.

IC3 Internet Crime Complaint Center (2010). 2009 Internet Crime Report. http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf. Accessed: 28-11-2014.

Imperva Application Defense Center (2010). Consumer Password Worst Practices. http://www.imperva.com/docs/HII_Enterprise_Password_Worst_-Practices.pdf. Accessed: 28-11-2014.

Johnson, J. G., Wilke, A., and Weber, E. U. (2004). Beyond a trait view of risk-taking: A domain-specific scale measuring risk perceptions, expected benefits, and perceived-risk attitude in German-speaking populations. *Polish Psychological Bulletin*, 35(3):153–163.

Kainda, R., Flechais, I., and Roscoe, A. (2010). Security and usability: Analysis and evaluation. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, pages 275–282. IEEE.

Kim, C., Mirusmonov, M., and Lee, I. (2010a). An Empirical Examination of Factors Influencing the Intention to Use Mobile Payment. *Computers in Human Behavior*, 26(3):310–322.

Kim, C., Tao, W., Shin, N., and Kim, K.-S. (2010b). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9:84–95.

Krol, B. and Stender, T. (2014). Mobile Payment: Bezahlen mit dem Smartphone. http://www.fom.de/fileadmin/fom/presse_aktuell/-PDFs/MobilePaymentII.pdf. Accessed: 28-11-2014.

Laing, G. (2004). *Digital Retro: The Evolution and Design of the Personal Computer.* Sybex, Leves, East Sussex, UK.

Lampson, B. (2009). Privacy and Security: Usable Security: How to Get It. *Communications of the ACM*, 52(11):25–27.

Levy, S. (2001). *Hackers. Heroes of the Computer Revolution.* Penguin Books, New York, NY, USA.

Linck, K., Pousttchi, K., and Wiedemann, D. G. (2006). Security Issues in Mobile Payment from the Customer Viewpoint. In Ljungberg, J., editor, *Proceedings of the 14th European Conference on Information Systems (ECIS 2006). Goteborg, Sweden 2006, p.1-11.*

Mastercard Inc. (2014). Mobile MasterCard Approvals Process. http://mastercard-mobilepartner.com/approvals.html. Accessed: 28-11-2014.

McCLure, S., Scambray, J., and Kurtz, G. (2012). *Hacking Exposed 7: Network Security Secrets & Solutions, Seventh Edition*. McGraw Hill, New York, NY, USA, 7 edition.

Microsoft Corporation (2014). Windows Phone Dev Center. http://dev.windowsphone.com/en-us. Accessed: 07-06-2014.

Möller, S. (2010). *Quality Engineering. Qualität kommunikationstechnischer Systeme*. Springer, Heidelberg, Germany.

Möller, S., Ben-Asher, N., Engelbrecht, K.-P., Englert, R., and Meyer, J. (2011). Modeling the Behavior of Users Who are Confronted with Security Mechanisms. *Computers and Security*, 30(4):242–256.

Möller, S., Englert, R., Engelbrecht, K.-P., Hafner, V., Jameson, A., Oulasvirta, A., Raake, A., and Reithinger, N. (2006). MeMo: Towards Automatic Usability Evaluation of Spoken Dialogue Services by User Error Simulations. In *Proceedings of the 9th International Conference on Spoken Language Processing*, Interspeech 2006, pages 1786–1789, Pittsburgh, PA, USA.

NeXT Computer, I. (1994). *Nextstep 3.3 Developer Documentation Manuals*. NeXT Computer, Inc., Redwood City, CA, USA.

Nordlight Research (2014). Trendmonitor Finanzdienstleistungen 2014. http://www.nordlight-research.com. Accessed: 28-11-2014.

PCI Security Standards Council, LLC (2013). Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures Version 3.0 November 2013. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf. Accessed: 28-11-2014.

Raymond, E. S. (1999). *The Cathedral and the Bazaar*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1st edition.

Research in Motion Ltd. (2006). *BlackBerry Enterprise Solution Security. Release 4.1.2. Technical Overview.* Research in Motion, Waterloo, Ontario, Canada.

RISEPTIS (2008). *Trust in the Information Society. A Report of the Advisory Board RISEPTIS*. The Advisory Board of Research and Innovation for Security, Privacy and Trustworthiness in the Information Society. European Commission, Brussels, Belgium.

Roemmele, B. (2014). Why Is The Starbucks Mobile Payments App So Successful? *Forbes, June 13th, 2014*.

Schierz, P. G., Schilke, O., and Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: an empirical analysis. *Electronic Commerce Research and Applications*, 9(3):209–216.

Schulz, M., Engelbrecht, K.-P., and Möller, S. (2012). Simulating interaction of older adults with unfamiliar devices. In *Proceedings of the IADIS International Conference Information Systems 2012*, pages 399 – 403. IADIS Press.

Shabtai, A., Fledel, Y., and Elovici, Y. (2010). Securing Android-Powered Mobile Devices Using SELinux. *Security Privacy, IEEE*, 8(3):36–44.

Shin, D.-H. (2009). Towards an understanding of the consumer acceptance of mobile wallet. *Computers in Human Behavior*, 25(6):1343–1354.

Sieger, H., Kirschnick, N., and Möller, S. (2010). Poster: User preferences for biometric authentication methods and graded security on mobile phones. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10. ACM.

Sieger, H., Kirschnick, N., and Möller, S. (2011). Poster: Towards a User Behavior Model in Computer Security. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11. ACM.

Sieger, H., Kirschnick, N., and Möller, S. (2012). Poster: User perception of usability and security of a mobile payment system. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12. ACM.

Sieger, H. and Möller, S. (2012). Poster: Gender Differences in the Perception of Security of Mobile Phones. In *Proceedings of the 14th International Conference on Human-computer Interaction with Mobile Devices and Services Companion*, MobileHCI '12, pages 107–112. ACM.

Thompson, E. (2014). Omlis Global Mobile Payment Snapshot 2014. http://www.omlis.com/omlis-media-room/worldwide-use-of-mobile-payments/. Accessed: 28-11-2014.

TNS Infratest (2014). Relevanz von M-Payment. Technical report, TNS Infratest, Munich, Germany.

Tognazzini, B. (2005). Design for Usability. In Cranor, L. F. and Garfinkel, S., editors, *Security and Usability: Designing Secure Systems That People Can Use*, chapter 3, pages 31–46. O'Reilly.

Torvalds, L. and Diamond, D. (2001). *Just For Fun. The Story of an Accidentcal Revolutionary.* HarperBusiness, New York, NY, USA.

Turner, F. (2006). *From Counterculture to Cyberculture. Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism.* University of Chicago Press Books, Chicago, IL, USA.

Turner, F. (2014). Tal der Egomanen. *Die ZEIT, December 17*, page 8.

van Dyk, D. (2012). The End Of Cash. *TIME Magazine, issue January 9th, 2012.*

Venkatesh, V. and Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 46(2):186–204.

Venkatesh, V., Thong, J. Y. L., and Xu, X. (2012). Unified theory of acceptance and use of technology (UTAUT, UTAUT2), habit, hedonic motivation, price value, mobile internet, consumer, technology adoption. *MIS Quarterly*, 36(1):157–178.

Vermaas, R. (2013). The Security Risks of Mobile Payment Applications Using Near-Field Communication. Master's thesis, Erasmus University Rotterdam.

Wakabayashi, D. (2014). Apple CEO Tim Cook Happy With New Apple Pay Service. *The Wall Street Journal, Oct. 28, 2014*.

Wash, R. (2010). Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 11:1–11:16. ACM.

Weber, E. U. and Milliman, R. A. (1997). Perceived Risk Attitudes: Relating Risk Perception to Risky Choice. *Management Science*, Vol. 43,(No. 2):123–144.

Weir, C., Douglas, G., Carruthers, M., and Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1-2):47–62.

West, R. (2008). The Psychology of Security. *Communications of the ACM*, 51(4):34–40.

Wörlen, H., Altmann, M., Winter, H., Klocke, J., Novotny, J., and Uhlitzsch, R. (2012). *Payment behaviour in Germany in 2011. An empirical study of the utilisation of cash and cashless payment instruments*. Deutsche Bundesbank, Frankfurt am Main, Germany.

Yang, S., Lu, Y., Gupta, S., Cao, Y., and Zhang, R. (2012). Mobile payment services adoption across time: An empirical study of the effects of behavioral beliefs, social influences, and personal traits. *Computers in Human Behavior*, 28.

Young, J. S. and Simon, W. L. (2006). *iCon Steve Jobs*. John Wiley & Sons, Hoboken, NJ, USA.

Zhou, T. (2010). An empirical examination of continuance intention of mobile payment services. *Computers in Human Behavior*, 26(3):310–322.

Zmijewska, A. and Lawrence, E. (2006). Implementation Models in Mobile Payments. In *Proceedings of the 2Nd IASTED International Conference on Advances in Computer Science and Technology*, ACST'06, pages 19–25, Anaheim, CA, USA. ACTA Press.

Zuckerman, M. and Kuhlman, D. (2000). Personality and risk-taking: Common biosocial factors. *Journal of Personality*, 68:999–1029.

Chapter 7

Appendices

7.1 Store concept

The following pictures show one of the stores set up for test 2 and test 3. Test 1 did not use a store, test 4 and 5 reduced the design to two stores in one room, but the individual set up was very similar.

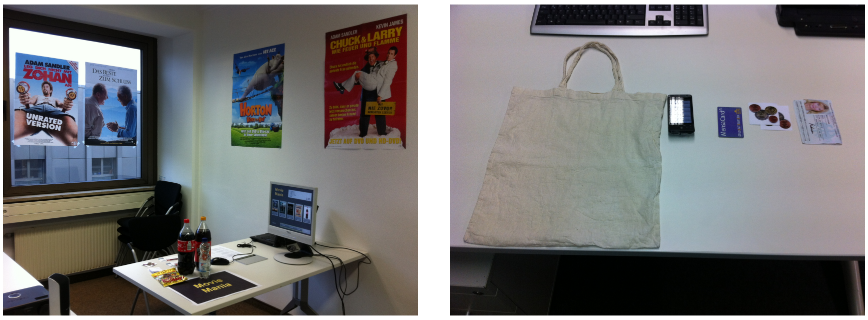
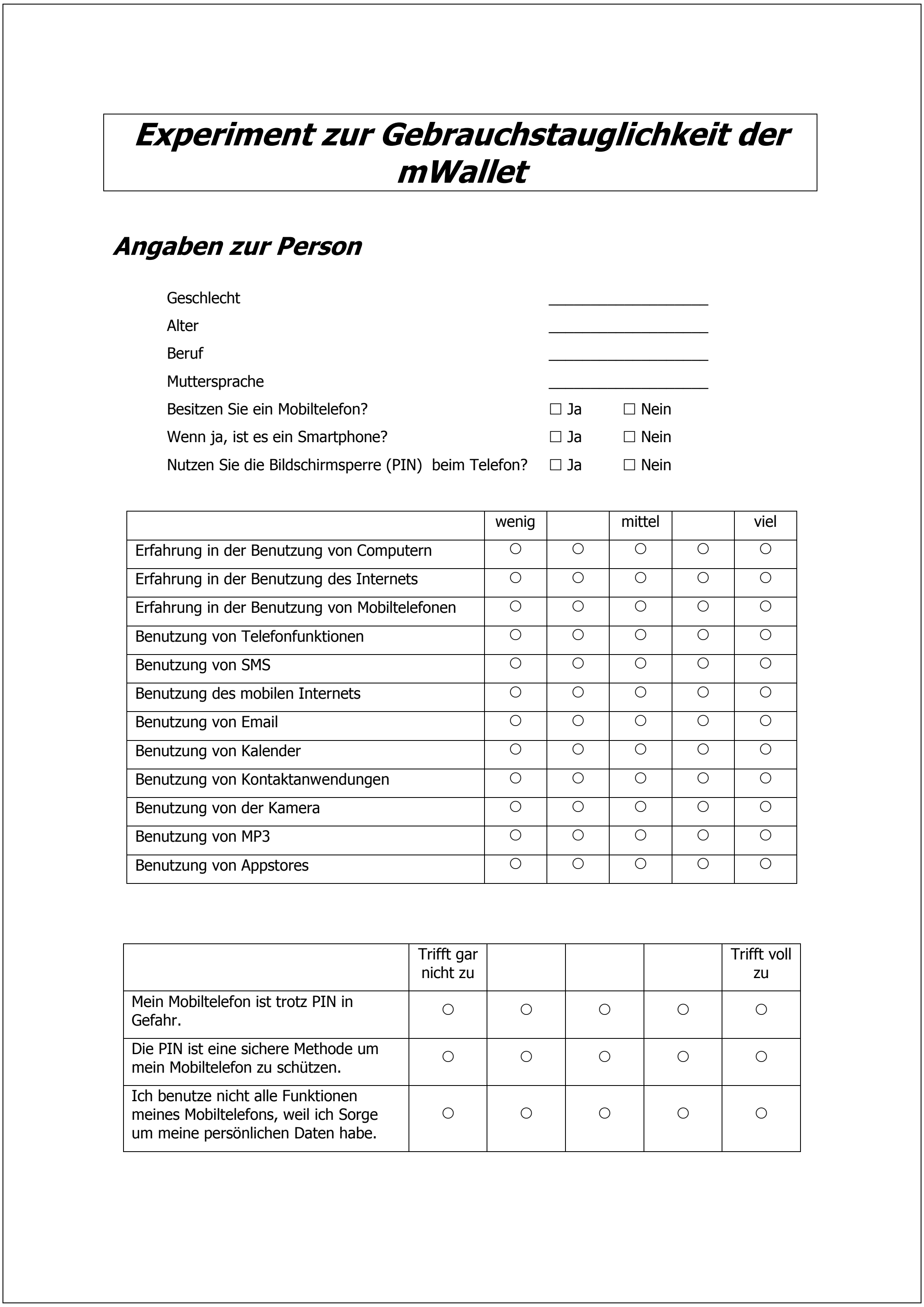


Table 7.1: *Left*: Shop environment for test 2 and 3 – cinema. *Right*: Shop environment for test 2 and 3 – bag, mWallet prototype, payment card, cash, and ID.

7.2 Questionnaires

This is the questionnaire used for test 4. The following pages show the questionnaire as presented to the participants. Pages 114-122 are the first part, page 123 was used multiple times during the practical part after each block, pages 124-127 was the third and last part.



Experiment zur Gebrauchstauglichkeit der mWallet

Angaben zur Person

Geschlecht ____________________

Alter ____________________

Beruf ____________________

Muttersprache ____________________

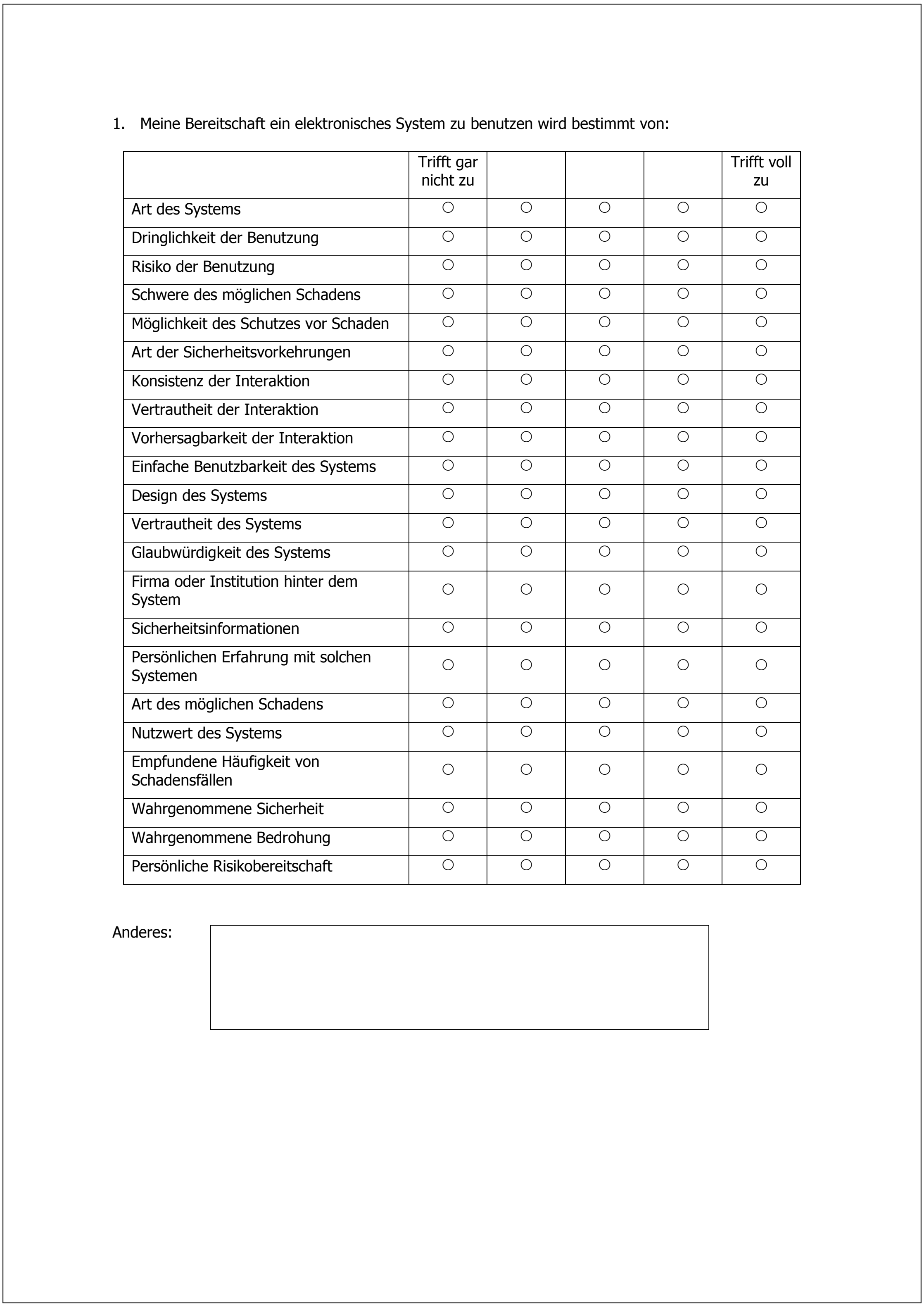
Besitzen Sie ein Mobiltelefon? □ Ja □ Nein

Wenn ja, ist es ein Smartphone? □ Ja □ Nein

Nutzen Sie die Bildschirmsperre (PIN) beim Telefon? □ Ja □ Nein

	wenig		mittel		viel
Erfahrung in der Benutzung von Computern	○	○	○	○	○
Erfahrung in der Benutzung des Internets	○	○	○	○	○
Erfahrung in der Benutzung von Mobiltelefonen	○	○	○	○	○
Benutzung von Telefonfunktionen	○	○	○	○	○
Benutzung von SMS	○	○	○	○	○
Benutzung des mobilen Internets	○	○	○	○	○
Benutzung von Email	○	○	○	○	○
Benutzung von Kalender	○	○	○	○	○
Benutzung von Kontaktanwendungen	○	○	○	○	○
Benutzung von der Kamera	○	○	○	○	○
Benutzung von MP3	○	○	○	○	○
Benutzung von Appstores	○	○	○	○	○

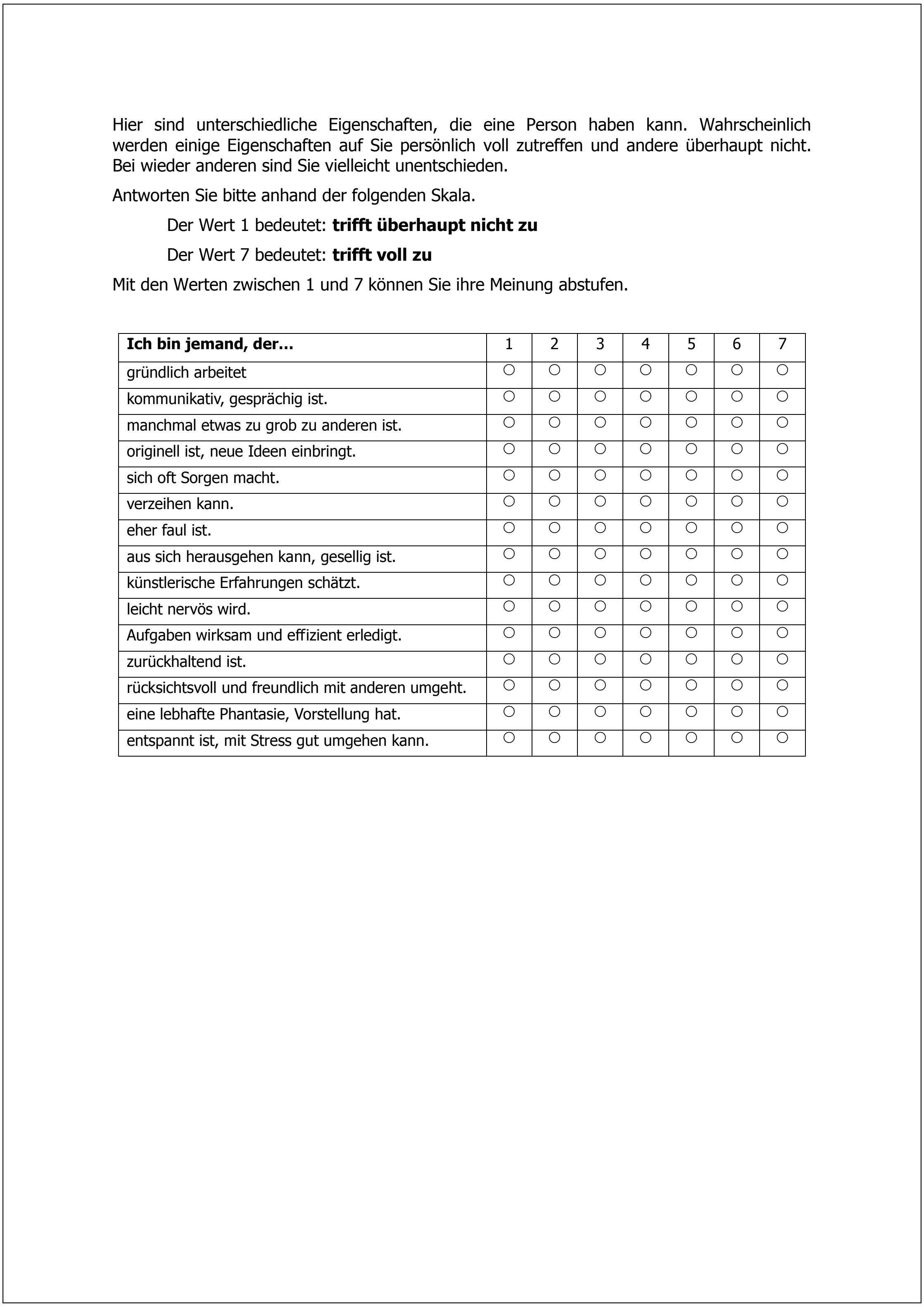
	Trifft gar nicht zu				Trifft voll zu
Mein Mobiltelefon ist trotz PIN in Gefahr.	○	○	○	○	○
Die PIN ist eine sichere Methode um mein Mobiltelefon zu schützen.	○	○	○	○	○
Ich benutze nicht alle Funktionen meines Mobiltelefons, weil ich Sorge um meine persönlichen Daten habe.	○	○	○	○	○



1. Meine Bereitschaft ein elektronisches System zu benutzen wird bestimmt von:

	Trifft gar nicht zu				Trifft voll zu
Art des Systems	○	○	○	○	○
Dringlichkeit der Benutzung	○	○	○	○	○
Risiko der Benutzung	○	○	○	○	○
Schwere des möglichen Schadens	○	○	○	○	○
Möglichkeit des Schutzes vor Schaden	○	○	○	○	○
Art der Sicherheitsvorkehrungen	○	○	○	○	○
Konsistenz der Interaktion	○	○	○	○	○
Vertrautheit der Interaktion	○	○	○	○	○
Vorhersagbarkeit der Interaktion	○	○	○	○	○
Einfache Benutzbarkeit des Systems	○	○	○	○	○
Design des Systems	○	○	○	○	○
Vertrautheit des Systems	○	○	○	○	○
Glaubwürdigkeit des Systems	○	○	○	○	○
Firma oder Institution hinter dem System	○	○	○	○	○
Sicherheitsinformationen	○	○	○	○	○
Persönlichen Erfahrung mit solchen Systemen	○	○	○	○	○
Art des möglichen Schadens	○	○	○	○	○
Nutzwert des Systems	○	○	○	○	○
Empfundene Häufigkeit von Schadensfällen	○	○	○	○	○
Wahrgenommene Sicherheit	○	○	○	○	○
Wahrgenommene Bedrohung	○	○	○	○	○
Persönliche Risikobereitschaft	○	○	○	○	○

Anderes:



Hier sind unterschiedliche Eigenschaften, die eine Person haben kann. Wahrscheinlich werden einige Eigenschaften auf Sie persönlich voll zutreffen und andere überhaupt nicht. Bei wieder anderen sind Sie vielleicht unentschieden.

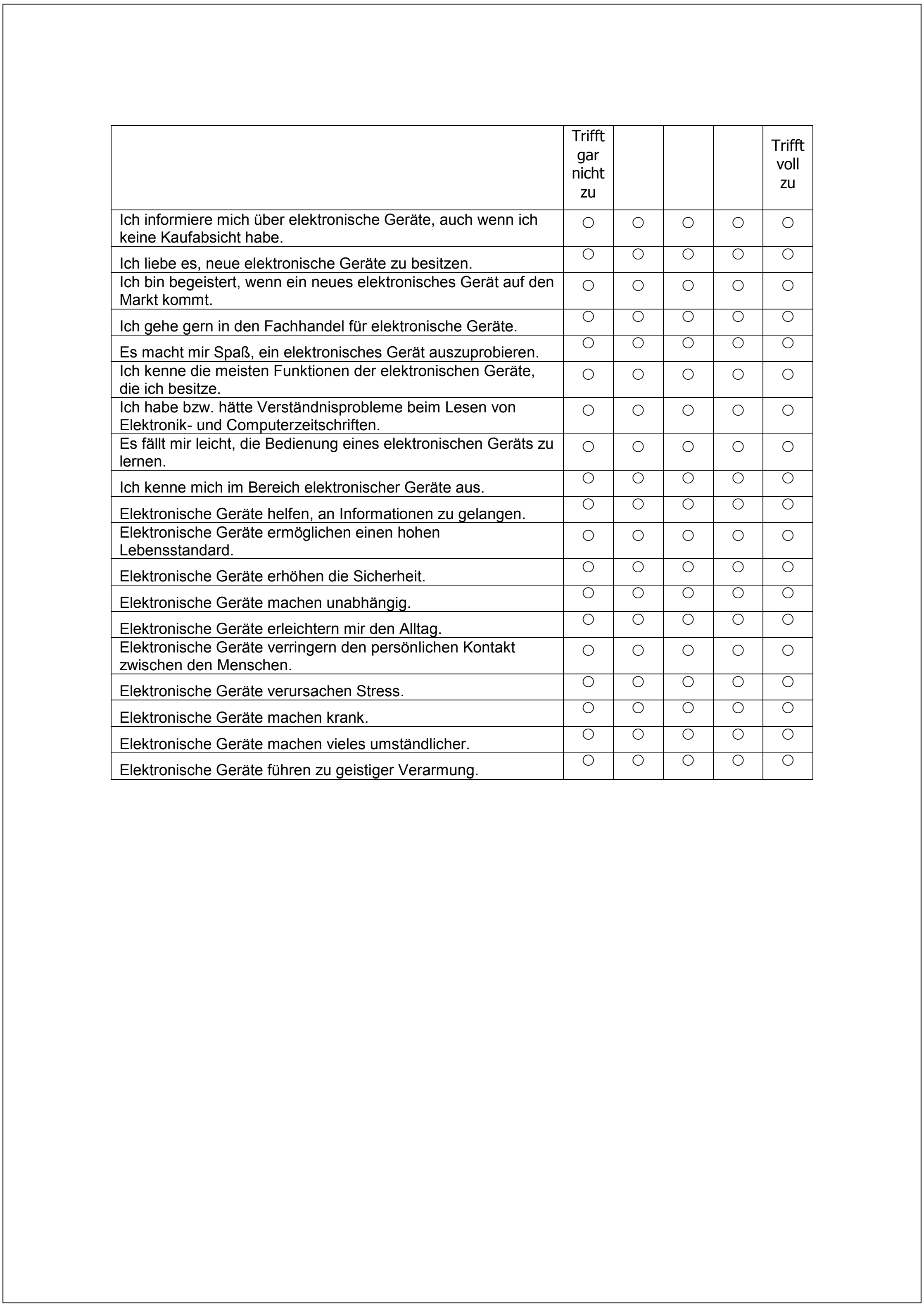
Antworten Sie bitte anhand der folgenden Skala.

Der Wert 1 bedeutet: **trifft überhaupt nicht zu**

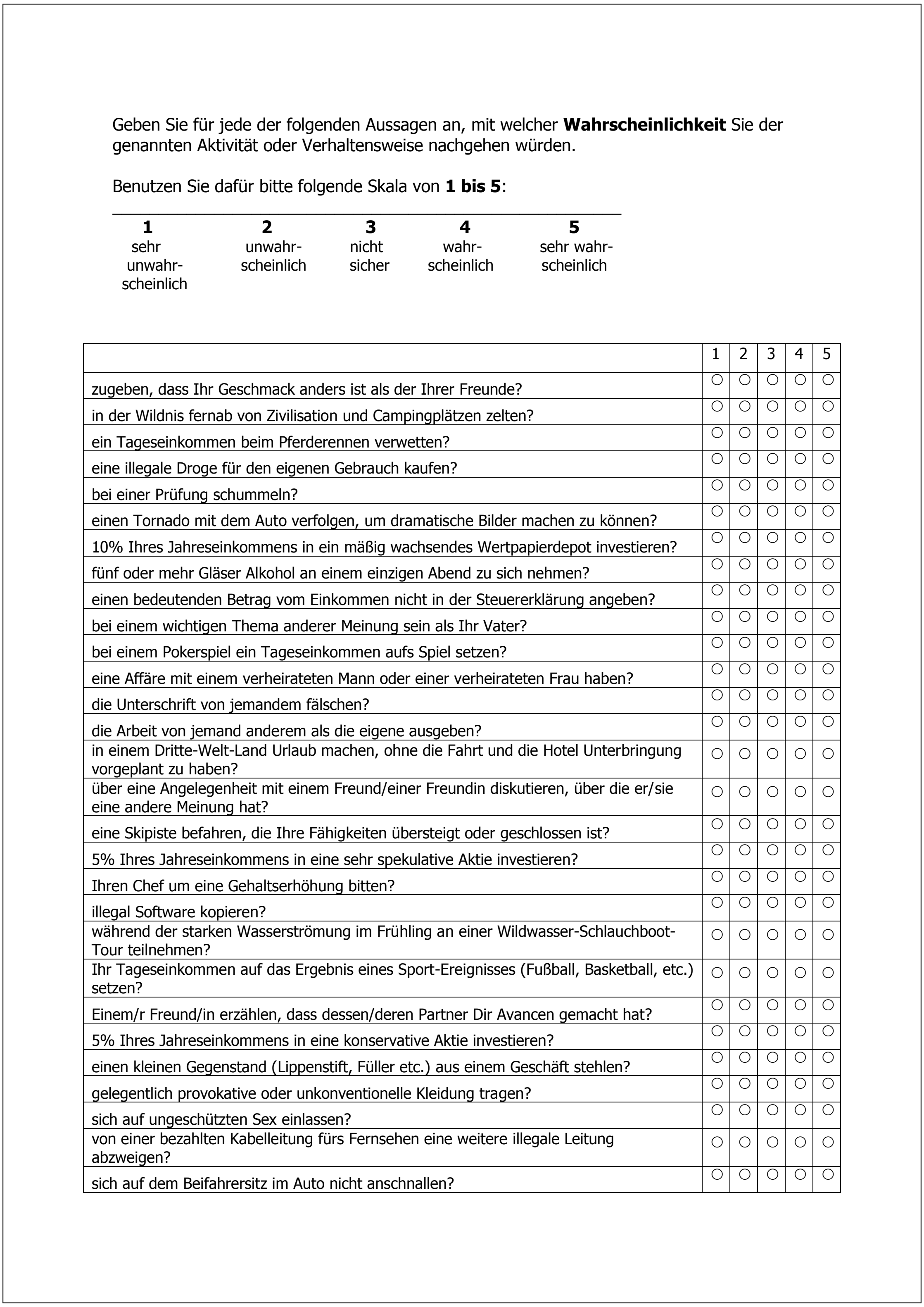
Der Wert 7 bedeutet: **trifft voll zu**

Mit den Werten zwischen 1 und 7 können Sie ihre Meinung abstufen.

Ich bin jemand, der...	1	2	3	4	5	6	7
gründlich arbeitet	○	○	○	○	○	○	○
kommunikativ, gesprächig ist.	○	○	○	○	○	○	○
manchmal etwas zu grob zu anderen ist.	○	○	○	○	○	○	○
originell ist, neue Ideen einbringt.	○	○	○	○	○	○	○
sich oft Sorgen macht.	○	○	○	○	○	○	○
verzeihen kann.	○	○	○	○	○	○	○
eher faul ist.	○	○	○	○	○	○	○
aus sich herausgehen kann, gesellig ist.	○	○	○	○	○	○	○
künstlerische Erfahrungen schätzt.	○	○	○	○	○	○	○
leicht nervös wird.	○	○	○	○	○	○	○
Aufgaben wirksam und effizient erledigt.	○	○	○	○	○	○	○
zurückhaltend ist.	○	○	○	○	○	○	○
rücksichtsvoll und freundlich mit anderen umgeht.	○	○	○	○	○	○	○
eine lebhafte Phantasie, Vorstellung hat.	○	○	○	○	○	○	○
entspannt ist, mit Stress gut umgehen kann.	○	○	○	○	○	○	○



	Trifft gar nicht zu				Trifft voll zu
Ich informiere mich über elektronische Geräte, auch wenn ich keine Kaufabsicht habe.	○	○	○	○	○
Ich liebe es, neue elektronische Geräte zu besitzen.	○	○	○	○	○
Ich bin begeistert, wenn ein neues elektronisches Gerät auf den Markt kommt.	○	○	○	○	○
Ich gehe gern in den Fachhandel für elektronische Geräte.	○	○	○	○	○
Es macht mir Spaß, ein elektronisches Gerät auszuprobieren.	○	○	○	○	○
Ich kenne die meisten Funktionen der elektronischen Geräte, die ich besitze.	○	○	○	○	○
Ich habe bzw. hätte Verständnisprobleme beim Lesen von Elektronik- und Computerzeitschriften.	○	○	○	○	○
Es fällt mir leicht, die Bedienung eines elektronischen Geräts zu lernen.	○	○	○	○	○
Ich kenne mich im Bereich elektronischer Geräte aus.	○	○	○	○	○
Elektronische Geräte helfen, an Informationen zu gelangen.	○	○	○	○	○
Elektronische Geräte ermöglichen einen hohen Lebensstandard.	○	○	○	○	○
Elektronische Geräte erhöhen die Sicherheit.	○	○	○	○	○
Elektronische Geräte machen unabhängig.	○	○	○	○	○
Elektronische Geräte erleichtern mir den Alltag.	○	○	○	○	○
Elektronische Geräte verringern den persönlichen Kontakt zwischen den Menschen.	○	○	○	○	○
Elektronische Geräte verursachen Stress.	○	○	○	○	○
Elektronische Geräte machen krank.	○	○	○	○	○
Elektronische Geräte machen vieles umständlicher.	○	○	○	○	○
Elektronische Geräte führen zu geistiger Verarmung.	○	○	○	○	○

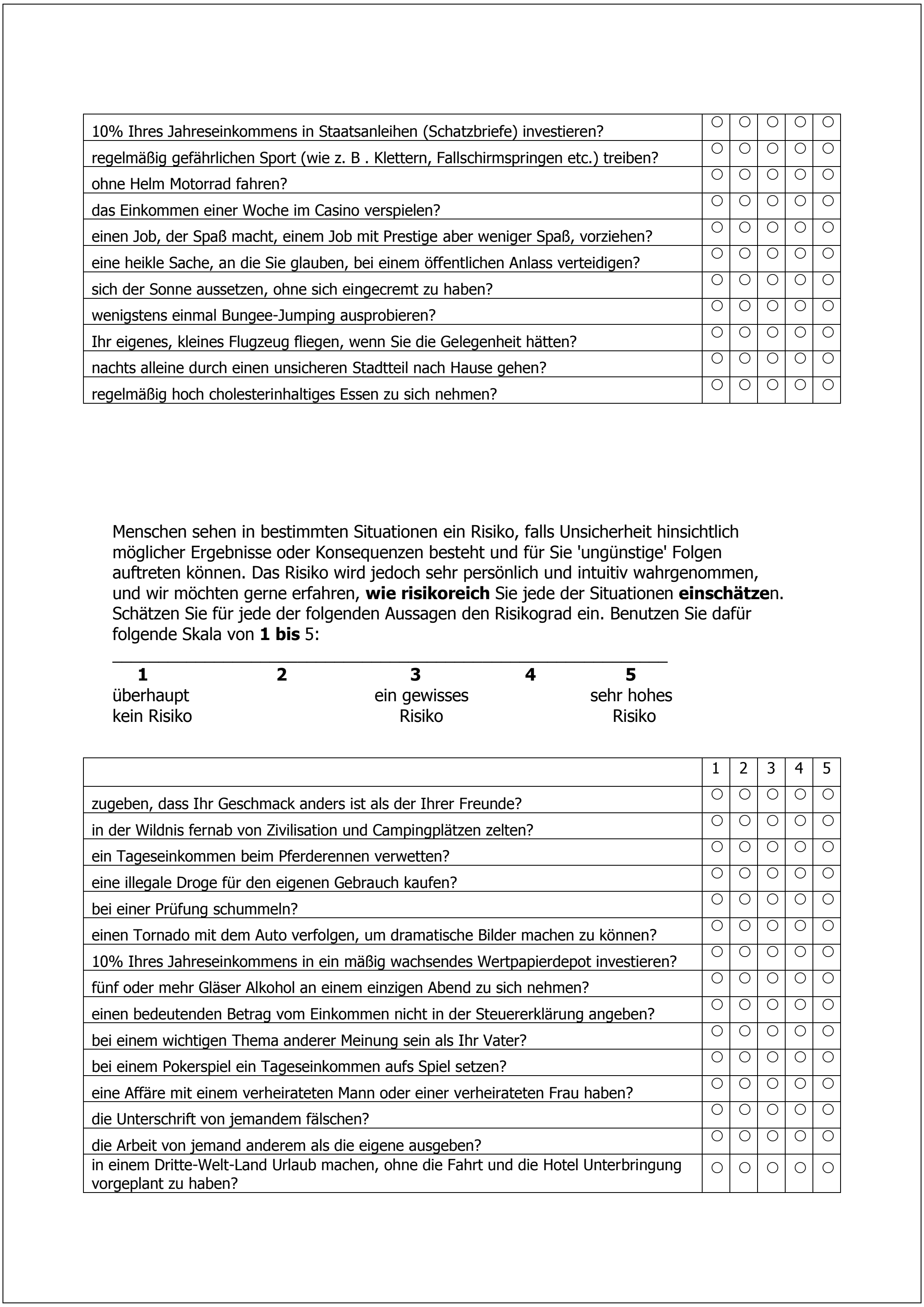


Geben Sie für jede der folgenden Aussagen an, mit welcher **Wahrscheinlichkeit** Sie der genannten Aktivität oder Verhaltensweise nachgehen würden.

Benutzen Sie dafür bitte folgende Skala von **1 bis 5**:

1	**2**	**3**	**4**	**5**
sehr unwahr-scheinlich	unwahr-scheinlich	nicht sicher	wahr-scheinlich	sehr wahr-scheinlich

	1	2	3	4	5
zugeben, dass Ihr Geschmack anders ist als der Ihrer Freunde?	○	○	○	○	○
in der Wildnis fernab von Zivilisation und Campingplätzen zelten?	○	○	○	○	○
ein Tageseinkommen beim Pferderennen verwetten?	○	○	○	○	○
eine illegale Droge für den eigenen Gebrauch kaufen?	○	○	○	○	○
bei einer Prüfung schummeln?	○	○	○	○	○
einen Tornado mit dem Auto verfolgen, um dramatische Bilder machen zu können?	○	○	○	○	○
10% Ihres Jahreseinkommens in ein mäßig wachsendes Wertpapierdepot investieren?	○	○	○	○	○
fünf oder mehr Gläser Alkohol an einem einzigen Abend zu sich nehmen?	○	○	○	○	○
einen bedeutenden Betrag vom Einkommen nicht in der Steuererklärung angeben?	○	○	○	○	○
bei einem wichtigen Thema anderer Meinung sein als Ihr Vater?	○	○	○	○	○
bei einem Pokerspiel ein Tageseinkommen aufs Spiel setzen?	○	○	○	○	○
eine Affäre mit einem verheirateten Mann oder einer verheirateten Frau haben?	○	○	○	○	○
die Unterschrift von jemandem fälschen?	○	○	○	○	○
die Arbeit von jemand anderem als die eigene ausgeben?	○	○	○	○	○
in einem Dritte-Welt-Land Urlaub machen, ohne die Fahrt und die Hotel Unterbringung vorgeplant zu haben?	○	○	○	○	○
über eine Angelegenheit mit einem Freund/einer Freundin diskutieren, über die er/sie eine andere Meinung hat?	○	○	○	○	○
eine Skipiste befahren, die Ihre Fähigkeiten übersteigt oder geschlossen ist?	○	○	○	○	○
5% Ihres Jahreseinkommens in eine sehr spekulative Aktie investieren?	○	○	○	○	○
Ihren Chef um eine Gehaltserhöhung bitten?	○	○	○	○	○
illegal Software kopieren?	○	○	○	○	○
während der starken Wasserströmung im Frühling an einer Wildwasser-Schlauchboot-Tour teilnehmen?	○	○	○	○	○
Ihr Tageseinkommen auf das Ergebnis eines Sport-Ereignisses (Fußball, Basketball, etc.) setzen?	○	○	○	○	○
Einem/r Freund/in erzählen, dass dessen/deren Partner Dir Avancen gemacht hat?	○	○	○	○	○
5% Ihres Jahreseinkommens in eine konservative Aktie investieren?	○	○	○	○	○
einen kleinen Gegenstand (Lippenstift, Füller etc.) aus einem Geschäft stehlen?	○	○	○	○	○
gelegentlich provokative oder unkonventionelle Kleidung tragen?	○	○	○	○	○
sich auf ungeschützten Sex einlassen?	○	○	○	○	○
von einer bezahlten Kabelleitung fürs Fernsehen eine weitere illegale Leitung abzweigen?	○	○	○	○	○
sich auf dem Beifahrersitz im Auto nicht anschnallen?	○	○	○	○	○

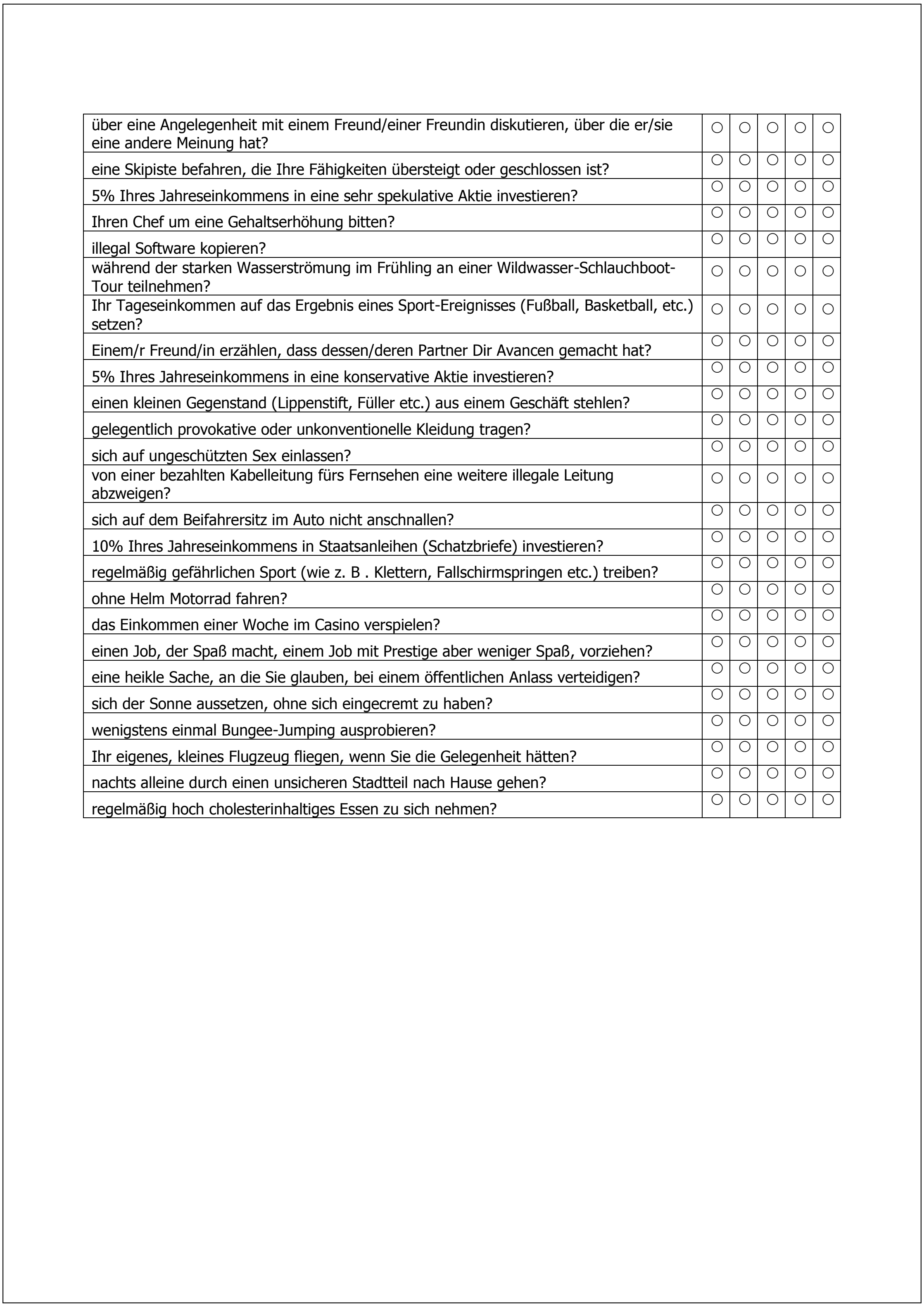


10% Ihres Jahreseinkommens in Staatsanleihen (Schatzbriefe) investieren?	○	○	○	○	○
regelmäßig gefährlichen Sport (wie z. B . Klettern, Fallschirmspringen etc.) treiben?	○	○	○	○	○
ohne Helm Motorrad fahren?	○	○	○	○	○
das Einkommen einer Woche im Casino verspielen?	○	○	○	○	○
einen Job, der Spaß macht, einem Job mit Prestige aber weniger Spaß, vorziehen?	○	○	○	○	○
eine heikle Sache, an die Sie glauben, bei einem öffentlichen Anlass verteidigen?	○	○	○	○	○
sich der Sonne aussetzen, ohne sich eingecremt zu haben?	○	○	○	○	○
wenigstens einmal Bungee-Jumping ausprobieren?	○	○	○	○	○
Ihr eigenes, kleines Flugzeug fliegen, wenn Sie die Gelegenheit hätten?	○	○	○	○	○
nachts alleine durch einen unsicheren Stadtteil nach Hause gehen?	○	○	○	○	○
regelmäßig hoch cholesterinhaltiges Essen zu sich nehmen?	○	○	○	○	○

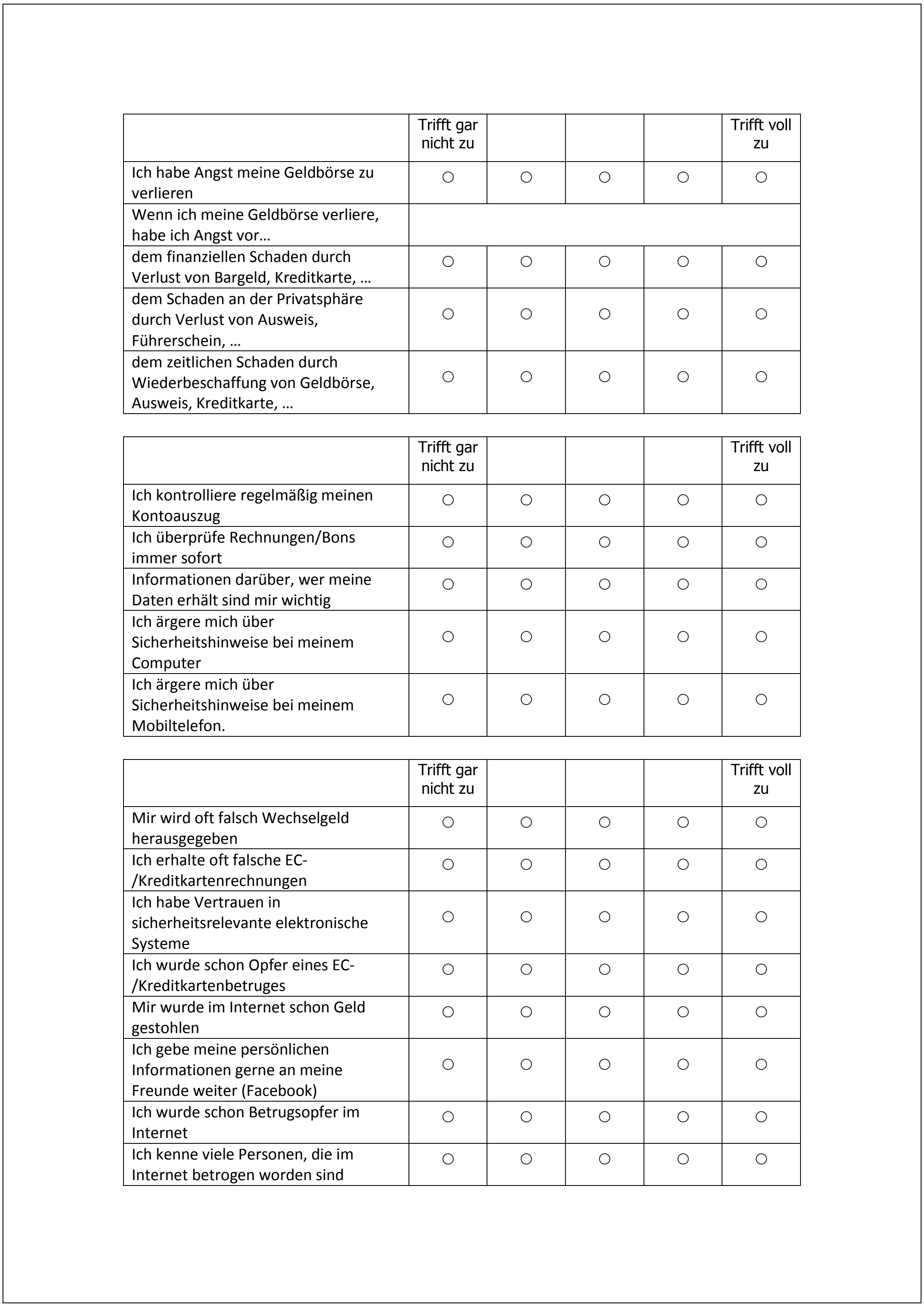
Menschen sehen in bestimmten Situationen ein Risiko, falls Unsicherheit hinsichtlich möglicher Ergebnisse oder Konsequenzen besteht und für Sie 'ungünstige' Folgen auftreten können. Das Risiko wird jedoch sehr persönlich und intuitiv wahrgenommen, und wir möchten gerne erfahren, **wie risikoreich** Sie jede der Situationen **einschätze**n. Schätzen Sie für jede der folgenden Aussagen den Risikograd ein. Benutzen Sie dafür folgende Skala von **1 bis** 5:

1	**2**	**3**	**4**	**5**
überhaupt kein Risiko		ein gewisses Risiko		sehr hohes Risiko

	1	2	3	4	5
zugeben, dass Ihr Geschmack anders ist als der Ihrer Freunde?	○	○	○	○	○
in der Wildnis fernab von Zivilisation und Campingplätzen zelten?	○	○	○	○	○
ein Tageseinkommen beim Pferderennen verwetten?	○	○	○	○	○
eine illegale Droge für den eigenen Gebrauch kaufen?	○	○	○	○	○
bei einer Prüfung schummeln?	○	○	○	○	○
einen Tornado mit dem Auto verfolgen, um dramatische Bilder machen zu können?	○	○	○	○	○
10% Ihres Jahreseinkommens in ein mäßig wachsendes Wertpapierdepot investieren?	○	○	○	○	○
fünf oder mehr Gläser Alkohol an einem einzigen Abend zu sich nehmen?	○	○	○	○	○
einen bedeutenden Betrag vom Einkommen nicht in der Steuererklärung angeben?	○	○	○	○	○
bei einem wichtigen Thema anderer Meinung sein als Ihr Vater?	○	○	○	○	○
bei einem Pokerspiel ein Tageseinkommen aufs Spiel setzen?	○	○	○	○	○
eine Affäre mit einem verheirateten Mann oder einer verheirateten Frau haben?	○	○	○	○	○
die Unterschrift von jemandem fälschen?	○	○	○	○	○
die Arbeit von jemand anderem als die eigene ausgeben?	○	○	○	○	○
in einem Dritte-Welt-Land Urlaub machen, ohne die Fahrt und die Hotel Unterbringung vorgeplant zu haben?	○	○	○	○	○



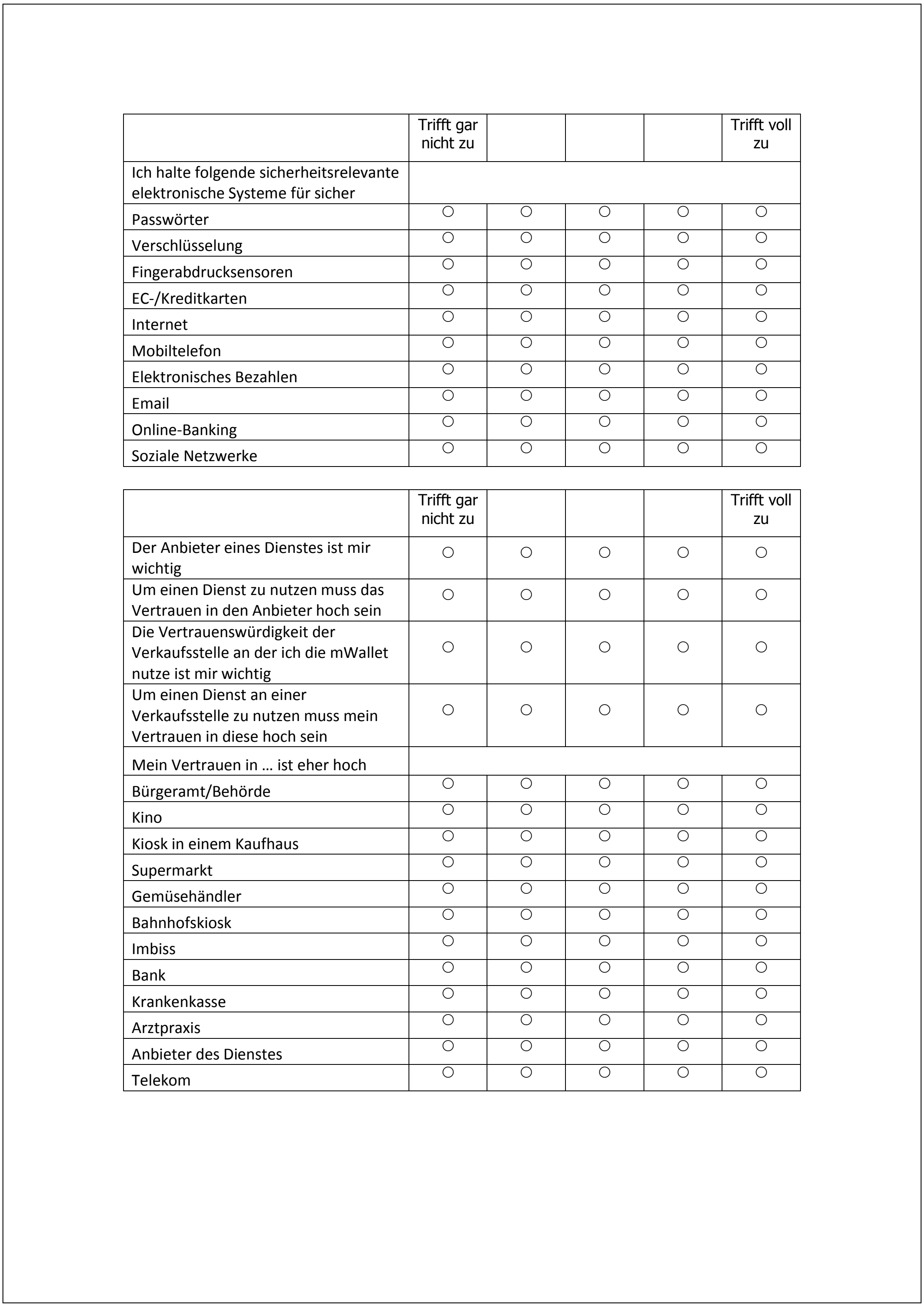
über eine Angelegenheit mit einem Freund/einer Freundin diskutieren, über die er/sie eine andere Meinung hat?	○	○	○	○	○
eine Skipiste befahren, die Ihre Fähigkeiten übersteigt oder geschlossen ist?	○	○	○	○	○
5% Ihres Jahreseinkommens in eine sehr spekulative Aktie investieren?	○	○	○	○	○
Ihren Chef um eine Gehaltserhöhung bitten?	○	○	○	○	○
illegal Software kopieren?	○	○	○	○	○
während der starken Wasserströmung im Frühling an einer Wildwasser-Schlauchboot-Tour teilnehmen?	○	○	○	○	○
Ihr Tageseinkommen auf das Ergebnis eines Sport-Ereignisses (Fußball, Basketball, etc.) setzen?	○	○	○	○	○
Einem/r Freund/in erzählen, dass dessen/deren Partner Dir Avancen gemacht hat?	○	○	○	○	○
5% Ihres Jahreseinkommens in eine konservative Aktie investieren?	○	○	○	○	○
einen kleinen Gegenstand (Lippenstift, Füller etc.) aus einem Geschäft stehlen?	○	○	○	○	○
gelegentlich provokative oder unkonventionelle Kleidung tragen?	○	○	○	○	○
sich auf ungeschützten Sex einlassen?	○	○	○	○	○
von einer bezahlten Kabelleitung fürs Fernsehen eine weitere illegale Leitung abzweigen?	○	○	○	○	○
sich auf dem Beifahrersitz im Auto nicht anschnallen?	○	○	○	○	○
10% Ihres Jahreseinkommens in Staatsanleihen (Schatzbriefe) investieren?	○	○	○	○	○
regelmäßig gefährlichen Sport (wie z. B . Klettern, Fallschirmspringen etc.) treiben?	○	○	○	○	○
ohne Helm Motorrad fahren?	○	○	○	○	○
das Einkommen einer Woche im Casino verspielen?	○	○	○	○	○
einen Job, der Spaß macht, einem Job mit Prestige aber weniger Spaß, vorziehen?	○	○	○	○	○
eine heikle Sache, an die Sie glauben, bei einem öffentlichen Anlass verteidigen?	○	○	○	○	○
sich der Sonne aussetzen, ohne sich eingecremt zu haben?	○	○	○	○	○
wenigstens einmal Bungee-Jumping ausprobieren?	○	○	○	○	○
Ihr eigenes, kleines Flugzeug fliegen, wenn Sie die Gelegenheit hätten?	○	○	○	○	○
nachts alleine durch einen unsicheren Stadtteil nach Hause gehen?	○	○	○	○	○
regelmäßig hoch cholesterinhaltiges Essen zu sich nehmen?	○	○	○	○	○



	Trifft gar nicht zu				Trifft voll zu
Ich habe Angst meine Geldbörse zu verlieren	○	○	○	○	○
Wenn ich meine Geldbörse verliere, habe ich Angst vor…					
dem finanziellen Schaden durch Verlust von Bargeld, Kreditkarte, …	○	○	○	○	○
dem Schaden an der Privatsphäre durch Verlust von Ausweis, Führerschein, …	○	○	○	○	○
dem zeitlichen Schaden durch Wiederbeschaffung von Geldbörse, Ausweis, Kreditkarte, …	○	○	○	○	○

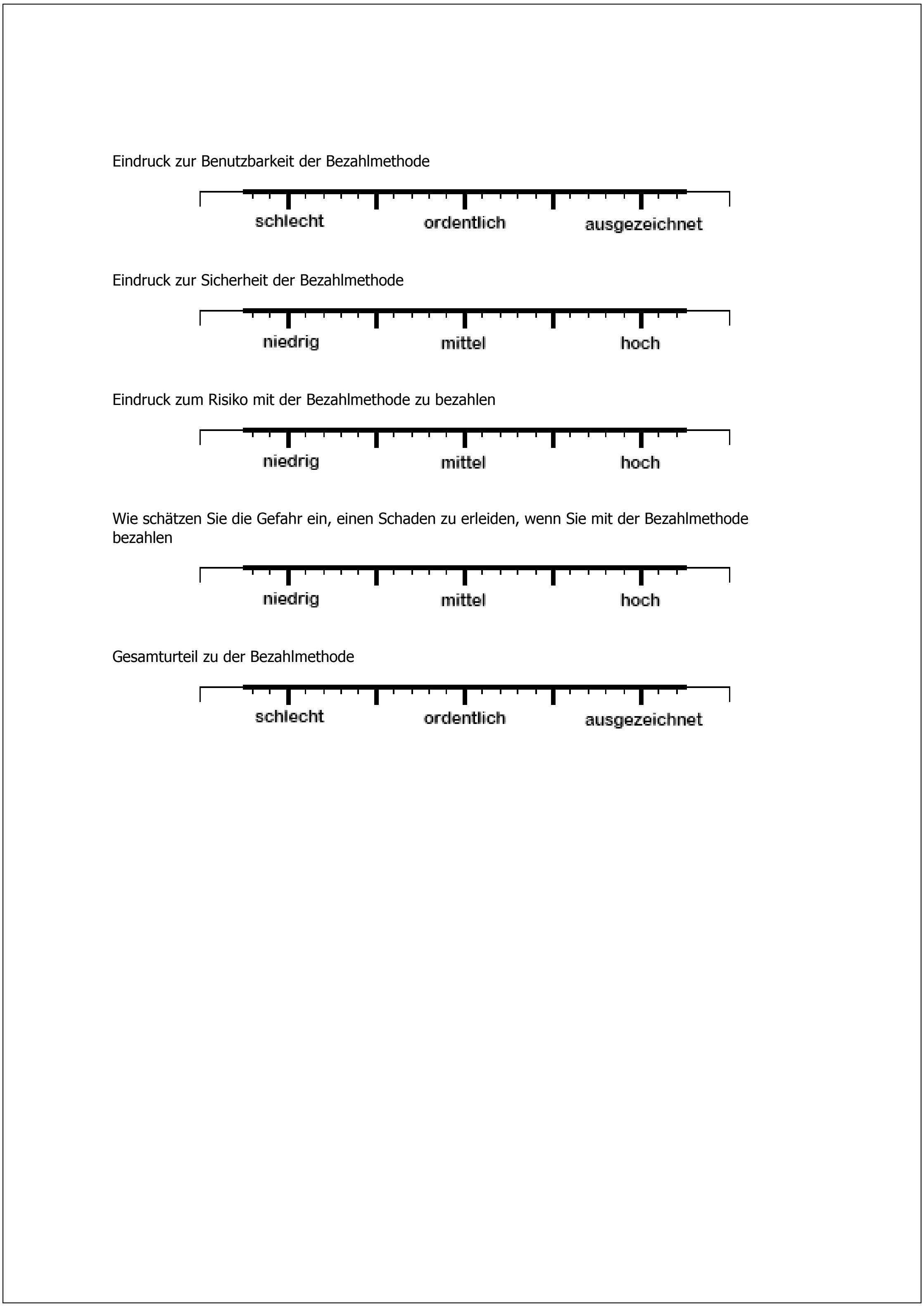
	Trifft gar nicht zu				Trifft voll zu
Ich kontrolliere regelmäßig meinen Kontoauszug	○	○	○	○	○
Ich überprüfe Rechnungen/Bons immer sofort	○	○	○	○	○
Informationen darüber, wer meine Daten erhält sind mir wichtig	○	○	○	○	○
Ich ärgere mich über Sicherheitshinweise bei meinem Computer	○	○	○	○	○
Ich ärgere mich über Sicherheitshinweise bei meinem Mobiltelefon.	○	○	○	○	○

	Trifft gar nicht zu				Trifft voll zu
Mir wird oft falsch Wechselgeld herausgegeben	○	○	○	○	○
Ich erhalte oft falsche EC-/Kreditkartenrechnungen	○	○	○	○	○
Ich habe Vertrauen in sicherheitsrelevante elektronische Systeme	○	○	○	○	○
Ich wurde schon Opfer eines EC-/Kreditkartenbetruges	○	○	○	○	○
Mir wurde im Internet schon Geld gestohlen	○	○	○	○	○
Ich gebe meine persönlichen Informationen gerne an meine Freunde weiter (Facebook)	○	○	○	○	○
Ich wurde schon Betrugsopfer im Internet	○	○	○	○	○
Ich kenne viele Personen, die im Internet betrogen worden sind	○	○	○	○	○



	Trifft gar nicht zu				Trifft voll zu
Ich halte folgende sicherheitsrelevante elektronische Systeme für sicher					
Passwörter	○	○	○	○	○
Verschlüsselung	○	○	○	○	○
Fingerabdrucksensoren	○	○	○	○	○
EC-/Kreditkarten	○	○	○	○	○
Internet	○	○	○	○	○
Mobiltelefon	○	○	○	○	○
Elektronisches Bezahlen	○	○	○	○	○
Email	○	○	○	○	○
Online-Banking	○	○	○	○	○
Soziale Netzwerke	○	○	○	○	○

	Trifft gar nicht zu				Trifft voll zu
Der Anbieter eines Dienstes ist mir wichtig	○	○	○	○	○
Um einen Dienst zu nutzen muss das Vertrauen in den Anbieter hoch sein	○	○	○	○	○
Die Vertrauenswürdigkeit der Verkaufsstelle an der ich die mWallet nutze ist mir wichtig	○	○	○	○	○
Um einen Dienst an einer Verkaufsstelle zu nutzen muss mein Vertrauen in diese hoch sein	○	○	○	○	○
Mein Vertrauen in … ist eher hoch					
Bürgeramt/Behörde	○	○	○	○	○
Kino	○	○	○	○	○
Kiosk in einem Kaufhaus	○	○	○	○	○
Supermarkt	○	○	○	○	○
Gemüsehändler	○	○	○	○	○
Bahnhofskiosk	○	○	○	○	○
Imbiss	○	○	○	○	○
Bank	○	○	○	○	○
Krankenkasse	○	○	○	○	○
Arztpraxis	○	○	○	○	○
Anbieter des Dienstes	○	○	○	○	○
Telekom	○	○	○	○	○



Eindruck zur Benutzbarkeit der Bezahlmethode

schlecht ordentlich ausgezeichnet

Eindruck zur Sicherheit der Bezahlmethode

niedrig mittel hoch

Eindruck zum Risiko mit der Bezahlmethode zu bezahlen

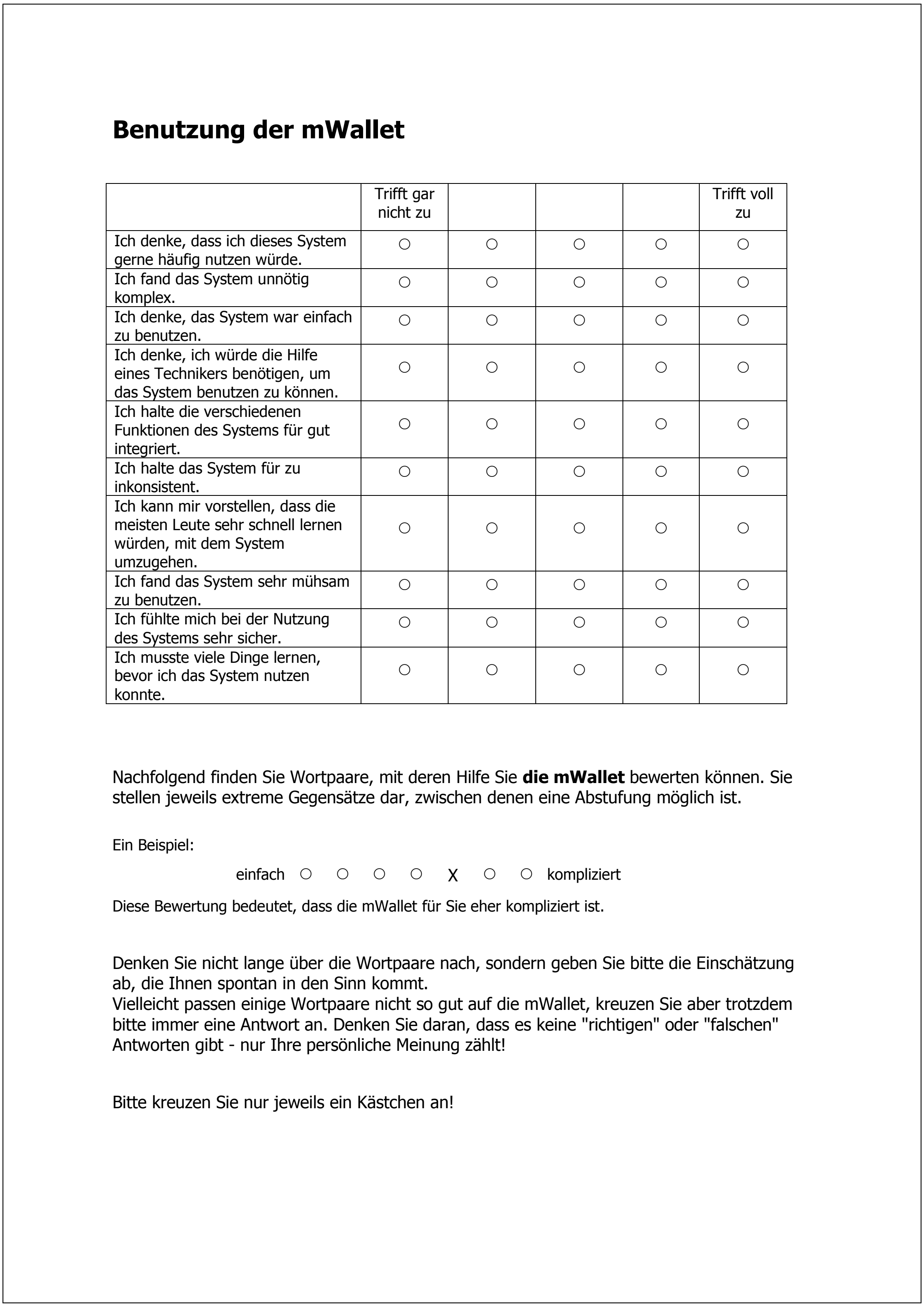
niedrig mittel hoch

Wie schätzen Sie die Gefahr ein, einen Schaden zu erleiden, wenn Sie mit der Bezahlmethode bezahlen

niedrig mittel hoch

Gesamturteil zu der Bezahlmethode

schlecht ordentlich ausgezeichnet



Benutzung der mWallet

	Trifft gar nicht zu				Trifft voll zu
Ich denke, dass ich dieses System gerne häufig nutzen würde.	○	○	○	○	○
Ich fand das System unnötig komplex.	○	○	○	○	○
Ich denke, das System war einfach zu benutzen.	○	○	○	○	○
Ich denke, ich würde die Hilfe eines Technikers benötigen, um das System benutzen zu können.	○	○	○	○	○
Ich halte die verschiedenen Funktionen des Systems für gut integriert.	○	○	○	○	○
Ich halte das System für zu inkonsistent.	○	○	○	○	○
Ich kann mir vorstellen, dass die meisten Leute sehr schnell lernen würden, mit dem System umzugehen.	○	○	○	○	○
Ich fand das System sehr mühsam zu benutzen.	○	○	○	○	○
Ich fühlte mich bei der Nutzung des Systems sehr sicher.	○	○	○	○	○
Ich musste viele Dinge lernen, bevor ich das System nutzen konnte.	○	○	○	○	○

Nachfolgend finden Sie Wortpaare, mit deren Hilfe Sie **die mWallet** bewerten können. Sie stellen jeweils extreme Gegensätze dar, zwischen denen eine Abstufung möglich ist.

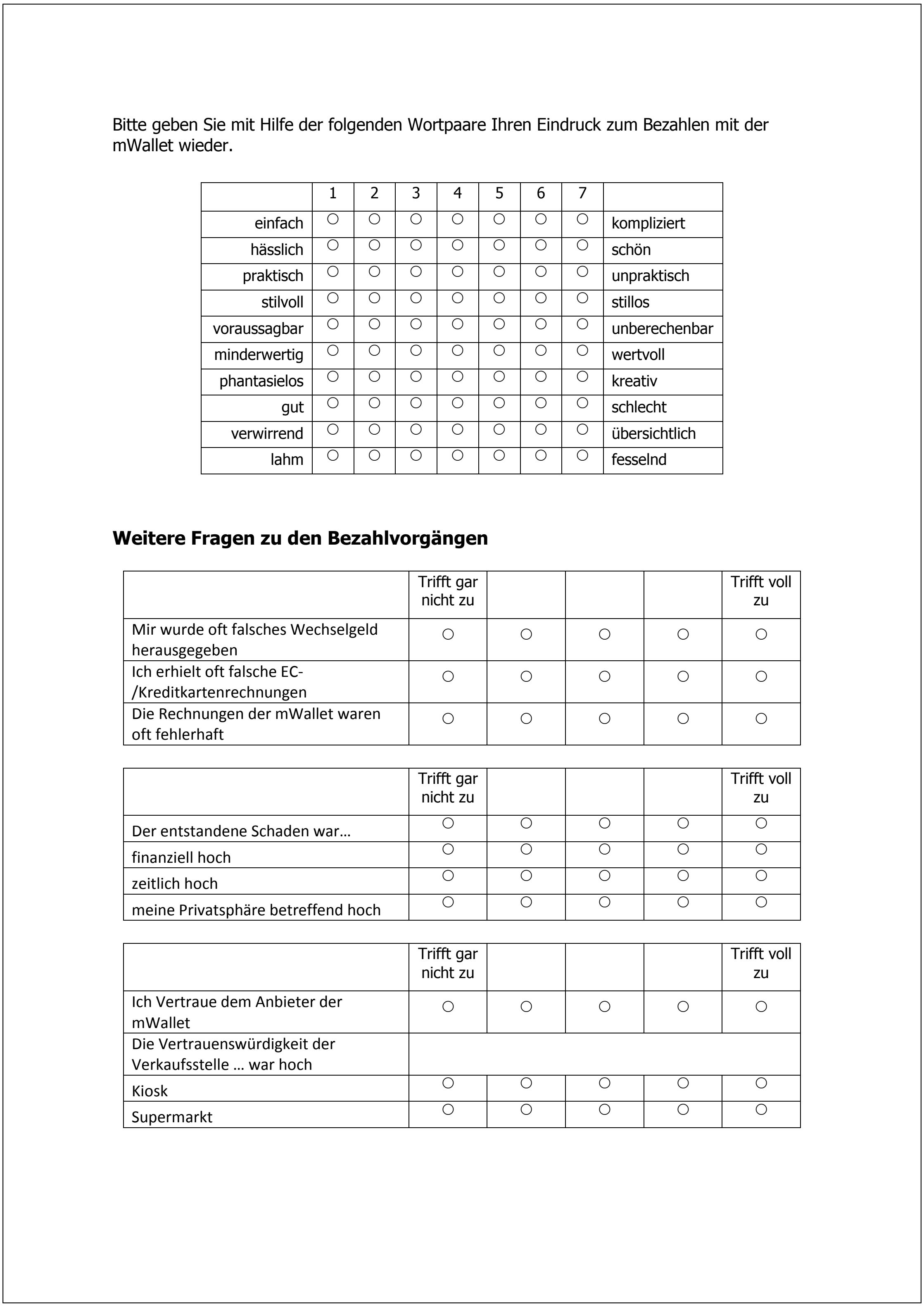
Ein Beispiel:

einfach ○ ○ ○ ○ X ○ ○ kompliziert

Diese Bewertung bedeutet, dass die mWallet für Sie eher kompliziert ist.

Denken Sie nicht lange über die Wortpaare nach, sondern geben Sie bitte die Einschätzung ab, die Ihnen spontan in den Sinn kommt.
Vielleicht passen einige Wortpaare nicht so gut auf die mWallet, kreuzen Sie aber trotzdem bitte immer eine Antwort an. Denken Sie daran, dass es keine "richtigen" oder "falschen" Antworten gibt - nur Ihre persönliche Meinung zählt!

Bitte kreuzen Sie nur jeweils ein Kästchen an!



Bitte geben Sie mit Hilfe der folgenden Wortpaare Ihren Eindruck zum Bezahlen mit der mWallet wieder.

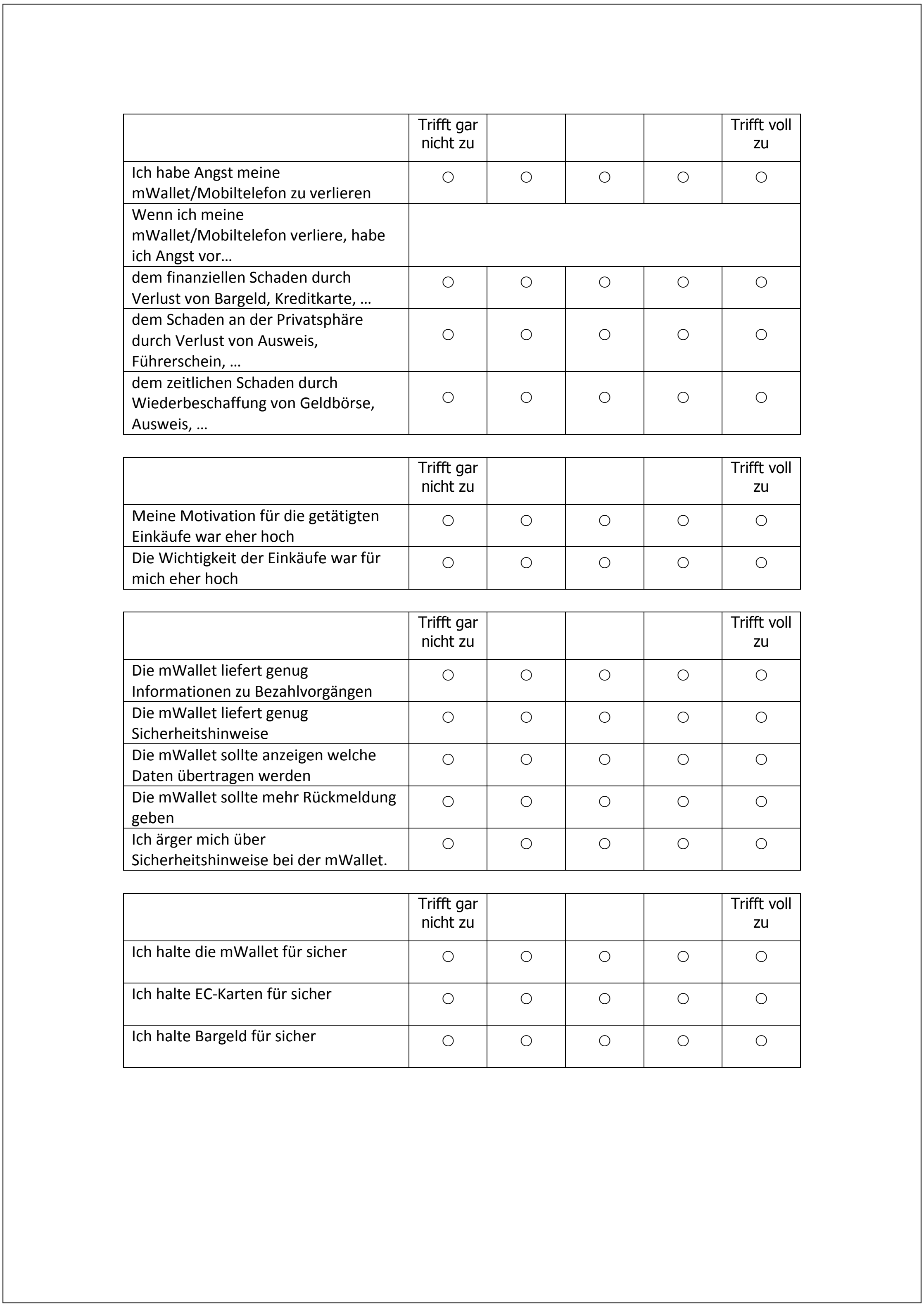
	1	2	3	4	5	6	7	
einfach	○	○	○	○	○	○	○	kompliziert
hässlich	○	○	○	○	○	○	○	schön
praktisch	○	○	○	○	○	○	○	unpraktisch
stilvoll	○	○	○	○	○	○	○	stillos
voraussagbar	○	○	○	○	○	○	○	unberechenbar
minderwertig	○	○	○	○	○	○	○	wertvoll
phantasielos	○	○	○	○	○	○	○	kreativ
gut	○	○	○	○	○	○	○	schlecht
verwirrend	○	○	○	○	○	○	○	übersichtlich
lahm	○	○	○	○	○	○	○	fesselnd

Weitere Fragen zu den Bezahlvorgängen

	Trifft gar nicht zu				Trifft voll zu
Mir wurde oft falsches Wechselgeld herausgegeben	○	○	○	○	○
Ich erhielt oft falsche EC-/Kreditkartenrechnungen	○	○	○	○	○
Die Rechnungen der mWallet waren oft fehlerhaft	○	○	○	○	○

	Trifft gar nicht zu				Trifft voll zu
Der entstandene Schaden war…	○	○	○	○	○
finanziell hoch	○	○	○	○	○
zeitlich hoch	○	○	○	○	○
meine Privatsphäre betreffend hoch	○	○	○	○	○

	Trifft gar nicht zu				Trifft voll zu
Ich Vertraue dem Anbieter der mWallet	○	○	○	○	○
Die Vertrauenswürdigkeit der Verkaufsstelle … war hoch					
Kiosk	○	○	○	○	○
Supermarkt	○	○	○	○	○

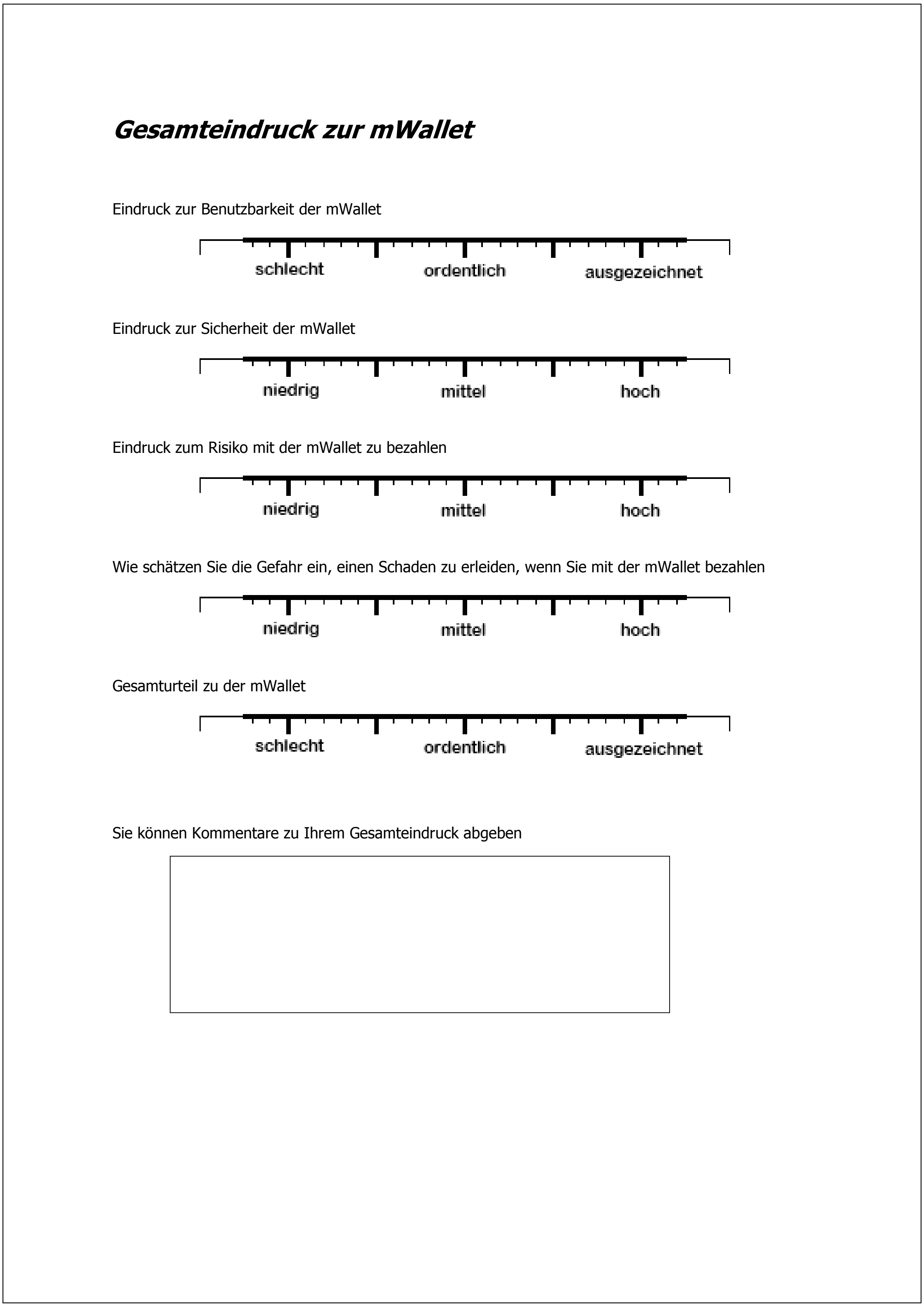


	Trifft gar nicht zu				Trifft voll zu
Ich habe Angst meine mWallet/Mobiltelefon zu verlieren	○	○	○	○	○
Wenn ich meine mWallet/Mobiltelefon verliere, habe ich Angst vor…					
dem finanziellen Schaden durch Verlust von Bargeld, Kreditkarte, …	○	○	○	○	○
dem Schaden an der Privatsphäre durch Verlust von Ausweis, Führerschein, …	○	○	○	○	○
dem zeitlichen Schaden durch Wiederbeschaffung von Geldbörse, Ausweis, …	○	○	○	○	○

	Trifft gar nicht zu				Trifft voll zu
Meine Motivation für die getätigten Einkäufe war eher hoch	○	○	○	○	○
Die Wichtigkeit der Einkäufe war für mich eher hoch	○	○	○	○	○

	Trifft gar nicht zu				Trifft voll zu
Die mWallet liefert genug Informationen zu Bezahlvorgängen	○	○	○	○	○
Die mWallet liefert genug Sicherheitshinweise	○	○	○	○	○
Die mWallet sollte anzeigen welche Daten übertragen werden	○	○	○	○	○
Die mWallet sollte mehr Rückmeldung geben	○	○	○	○	○
Ich ärger mich über Sicherheitshinweise bei der mWallet.	○	○	○	○	○

	Trifft gar nicht zu				Trifft voll zu
Ich halte die mWallet für sicher	○	○	○	○	○
Ich halte EC-Karten für sicher	○	○	○	○	○
Ich halte Bargeld für sicher	○	○	○	○	○



Gesamteindruck zur mWallet

Eindruck zur Benutzbarkeit der mWallet

schlecht ordentlich ausgezeichnet

Eindruck zur Sicherheit der mWallet

niedrig mittel hoch

Eindruck zum Risiko mit der mWallet zu bezahlen

niedrig mittel hoch

Wie schätzen Sie die Gefahr ein, einen Schaden zu erleiden, wenn Sie mit der mWallet bezahlen

niedrig mittel hoch

Gesamturteil zu der mWallet

schlecht ordentlich ausgezeichnet

Sie können Kommentare zu Ihrem Gesamteindruck abgeben