Secure Service Provisioning (SSP) Framework for IP Multimedia Subsystem (IMS)

M.Sc. Muhammad Sher

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.-Ing. Thomas Sikora
Gutachter: Prof Dr.-Ing. Thomas Magedanz
Gutachter: Prof Dr.-Ing. Klaus David

Tag der wissenschaftlichen Aussprache: 14.12.2007

Berlin 2007
D 83

Zusammenfassung

Mit dem Erscheinen mobiler Multimediadienste, wie z. B. Unified Messaging, Click-to-Dial-Applikationen, netzwerkübergeifende Multimedia-Konferenzen und nahtlose Multimedia-Streming-Dienste, begann die Konvergenz von mobilen Kommunikationsetzen und Festnetzen, begleitet von der Integration von Sprach- und Datenkommunikations-Übertragungstechnik Diese Entwicklungen bilden die Voraussetzung für die Verschmelzung des modernen Internet auf der einen Seite mit der Telekommunikation im klassischen Sinne auf der anderen. Das IP Multimedia-Subsystem (IMS) darf hierbei als die entscheidende Next-Generation-Service-Delivery-Plattform in einer vereinheitlichten Kommunikationswelt angesehen werden. Seine Architektur basiert auf einem modularen Design mit offenen Schnittstellen und bietet dedizierte Voraussetzungen zur Unterstützung von Multimedia-Diensten auf der Grundlage der Internet-Protokolle. Einhergehend mit dieser aufkommenden offenen Technologie stellen sich neue Sicherheits-Herausforderungen in einer vielschichtigen Kommunikationsinfrastruktur, im Wesentlichen bestehend aus dem Internet Protokoll (IP), dem SIP-Protokoll (Session Initiation Protocol) und dem Real-time Transport Protokoll (RTP).

Die Zielsetzung des *Secure Service Provisioning*-Systems (SSP) ist, mögliche Angriffsszenarien und Sicherheitslücken in Verbindung mit dem IP Multimedia Subsystem zu erforschen und Sicherheitslösungen, wie sie von IETF, 3GPP und TISPAN vorgeschlagen werden, zu evaluieren. Im Rahmen dieser Forschungsarbeit werden die Lösungen als Teil des SSP-Systems berücksichtigt, mit dem Ziel, dem IMS und der Next-Generation-SDP einen hinreichenden Schutz zu garantieren. Dieser Teil, der als Sicherheitsschutzstufe 1 bezeichnet wird, beinhaltet unter anderem Maßnahmen zur Nutzer- und Netzwerk-Authentifizierung, die Autorisierung der Nutzung von Multimediadiensten und Vorkehrungen zur Gewährleistung der Geheimhaltung und Integrität von Daten im Zusammenhang mit dem Schutz vor Lauschangriffen, Session-Hijacking- und Man-in-the-Middle-Angriffen. Im nächsten Schritt werden die Beschränkungen untersucht, die für die Sicherheitsschutzstufe 1 charakteristisch sind und Maßnahmen zu Verbesserung des Sicherheitsschutzes entwickelt. Die entsprechenden Erweiterungen der Sicherheitsschutzstufe 1 führen zu einem *Intrusion Detection and Prevention*-System (IDP), das Schutz vor Denial-of-Service- (DoS) / Distributed-Denial-of-Service (DDoS)-Angriffen, missbräuchlicher Nutzung und Täuschungsversuchen in IMS-basierten Netzwerken bietet. Weder 3GPP noch TISPAN haben bisher Lösungen für diesen Bereich spezifiziert. In diesem Zusammenhang können die beschriebenen Forschungs- und Entwicklungsarbeiten einen Beitrag zur Standardisierung von Lösungen zum Schutz vor DoS- und DDoS-Angriffen in IMS-Netzwerken leisten.

Der hier beschriebene Ansatz basiert auf der Entwicklung eines (stateful / stateless) Systems zur Erkennung und Verhinderung von Einbruchsversuchen (Intrusion Detection and Prevention System). Aus Entwicklungssicht wurde das IDP in zwei Module aufgeteilt: Das erste Modul beinhaltet die Basisfunktionen des IDP, die sich auf Flooding-Angriffe auf das IMS und ihre Kompensation richten. Ihr Ziel ist es, das IMS-Core-Netzwerk und die IMS-Ressourcen vor DoS- und DDoS-Angriffen zu schützen. Das entsprechende Modul basiert auf einer Online Stateless-Detection-Methodologie und wird aktiv, sobald die CPU-Auslastung der P-CSCF (Proxy-Call State Control Function) einen vordefinierten Grenzwert erreicht oder überschreitet. Das zweite Modul (IDP-AS) hat die Aufgabe, Angriffe, die sich gegen IMS Application Server (AS) richten abzufangen. Hierbei konzentrieren sich die Maßnahmen auf den Schutz des ISC-Interfaces zwischen IMS Core und Application Servern. Das betreffende Modul realisiert eine Stateful Detection Methodologie zur Erkennung missbräuchlicher Nutzungsaktivitäten. Während der Nutzer mit dem Application Server kommuniziert, werden dabei nutzerspezifische Zustandsdaten aufgezeichnet, die zur Prüfung der Legitimität herangezogen werden. Das IDP-AS prüft alle eingehenden Requests und alle abgehenden Responses, die von IMS Application Servern stammen oder die an IMS Application Server gerichtet sind, auf ihre Zulässigkeit im Hinblick auf die definierten Attack Rules.

Mit Hilfe der Kriterien Fehlerfreiheit und Processing Delay bei der Identifikation potenzieller Angriffe wird die Leistungsfähigkeit der IDP-Module bewertet. Für die entsprechenden Referenzwerte werden hierbei die Zustände Nomallast und Überlast verglichen. Falls die Leistungsfähigkeit des IDP nicht unter den Erwartungen zurückbleibt, wird ein IDP-Prototyp zur Evaluation im Open IMS Playground des Fokus Fraunhofer 3Gb-Testbeds eingesetzt, um unter realen Einsatzbedingungen z. B. in VoIP-, Videokonferenz- , IPTV-, Presence- und Push-to-Talk-Szenarien getestet werden zu können.

Abstract

With the emergence of mobile multimedia services, such as unified messaging, click to dial, cross network multiparty conferencing and seamless multimedia streaming services, the fixed–mobile convergence and voice–data integration has started, leading to an overall Internet–Telecommunications merger. The IP Multimedia Subsystem (IMS) is considered as the next generation service delivery platform in the converged communication world. It consists of modular design with open interfaces and enables the flexibility for providing multimedia services over IP technology. In parallel this open based emerging technology has security challenges from multiple communication platforms and protocols like IP, Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP).

The objective of Secure Service Provisioning (SSP) Framework is to cram the potential attacks and security threats to IP Multimedia Subsystem (IMS) and to explore security solutions developed by IETF, 3GPP and TISPAN. This research work incorporates these solutions into SSP Framework to secure IMS and next generation Service Delivery Platform (SDP). We define this part as level 1 security protection which includes user and network authentication, authorization to access multimedia services, providing confidentiality and integrity protection etc. against eavesdropping, session hijacking and man-in-the middle attacks etc. In the next step, we have investigated the limitations and improvements to level 1 security and proposed the enhancement and extension as level 2 security by developing Intrusion Detection and Prevention (IDP) system against Denial-of-Service (DoS)/Distributed DoS (DDoS) flooding attacks, misuses and frauds in IMS-based networks. These security threats recently have been identified by 3GPP and TISPAN but no solution is recommended and developed. Therefore our solution may be considered as recommendation in future.

Our approach based on developing both stateless and stateful intrusion detection and prevention system. From development point of view, we have divided the work into two modules: the first module is IDP-Core; addressing and mitigating the flooding attacks in IMS core. Its objective is to protect the IMS resources and IMS-core entities from DoS/DDoS flooding attacks. This module based on online stateless detection methodology and activates when CPU processing load of P-CSCF (Proxy-Call State Control Function) reaches or crosses the defined threshold limit. The second module is IDP-AS; addressing and mitigating the misuse attacks facing to IMS Application Servers (AS). Its focus is to secure the ISC interface between IMS Core and Application Servers. This module is based on stateful misuse detection methodology by creating and comparing user state (partner) when he/she is communicating with application server to check whether user is performing legitimate or illegitimate action with attacks rules. The IDP-AS also compared the incoming request and outgoing response to and from IMS Application Servers with the defined attacks rules.

In the performance analysis, the processing delay and attacks detection accuracy of both Intrusion Detection and Prevention (IDP) modules have been measured at Fraunhofer FOKUS IMS Testbed which is developed for research purpose. The performance evaluation based on normal and overload conditions scenarios. The results showed that the processing delay introduced by both IDP modules satisfied the standard requirements and did not cause retransmission of SIP REGISTER and INVITE requests. The developed prototype is under testing phase at Fraunhofer FOKUS 3Gb Testbed for evaluation in real world communication scenarios like VoIP, video conferencing, IPTV, presence, push-to-talk etc.

Key Words: IP Multimedia Subsystem (IMS), Security Threats, Flooding Attacks, Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS), Fraud and Misuses of NGN Service, Authentication and Key Agreement (AKA), Confidentiality and Integrity, Inter-Domains Security, Intrusion Detection and Prevention (IDP) System.

Acknowledgement

I am highly indebted to express my sense of gratitude to Professor Dr. Ing. Thomas Magedanz, Head of the Chair for Next Generation Network (AV), Institute for Telecommunication Systems, Faculty of Electrical Engineering and Computer Science, Technical University Berlin, and Head of Next Generation Network Integration (NGNI) Competence Center, Fraunhofer FOKUS Open Communication Institute Berlin, for his kind supervision from start to end of my research work. He guided me in every step from the development of innovative ideas, modern trends in Information Technology (IT) and relationship between research and IT industries. I have learned from my supervisor research ability, impressive style of presentation, technical talk and writing technical reports and papers. I am very impressed from his commitment to profession and hardworking and hope that it will help me during my career.

My respects go to Professor Dr. Dr. h.c. Radu Popescu-Zelitin, Director Fraunhofer FOKUS Open Communication Institute Berlin, for his valuable suggestions during my frequent research talks and presentations. He guided me a lot to carry the research work according to the need of current IT and telecommunication industries.

I am very grateful to Professor Dr. Ing. Klaus David, Head of the Chair for Communication Technology, University of Kassel, for reviewing my research work as a second advisor.

I thank to all members of Fraunhofer Institute FOKUS (Forschungszentrum für Offene Kommunikations Systeme), especially NGNI Competence Center for their technical support through the research work. I am thankful to Shaoke Wu for helping to implement the research ideas into reality at Open IMS Fraunhofer FOKUS Testbed. Many regards to Reinhard Ruppelt, Fabricio Carvalho de Gouveia, Florian Schreiner and Niklas Blum for preparing Management Summary in Deutsch and fruitful discussion.

Many thanks to my parents for moral support and my wife for giving much time to kids, managing home independently and sparing me for the research.

At the end, I would like to acknowledge the financial support from Higher Education Communication of Pakistan (HEC) and German Academic Exchange Service (DAAD -Deutscher Akademischer Austausch Dienst). I pay special thanks to Fraunhofer FOKUS (Research Center for Open Communication System), Berlin for technical support and resources, additional research and conference funding.

Table of Contents

List of Figures

List of Tables

PART-A

Research Domain and State-of-the-Art Review

Chapter 1 Introduction

1.1 Motivation

The foundation for this thesis stems from the future trends of Fixed-Mobile Convergence (FMC), All-IP Networks and next generation Service Delivery Platform (SDP) as a result of merger of Internet and mobile communication, computer networks and Information Technology (IT). In the vision of All-IP Networks, the IP Multimedia Subsystem (IMS) [1] has been developed by Third Generation Partnership Project (3GPP) [2] and 3GPP2 [3]. The IMS is overlay architecture for the provision of multimedia services such as Voice over IP (VoIP), video conferencing, presence, push-to-talk etc. on top of all IP networks and the future technology for the convergence of data, speech and mobile networks. The IMS provides easy and efficient ways to integrate different value added services and seamless integration of legacy services. It enables consistent interactions with packet switched, circuit switched, and IP domains. The IMS manages event oriented quality of service policies e.g. use of VoIP and HTTP in a single session; VoIP has quality of service (QoS) while HTTP provides best effort delivery. These emerging systems based on event oriented charging policies; i.e. to change specific events on the appropriate level. If two events have the same IP resources, the system may charge them differently for the same user in the single session. These characteristics make the IMS as the future technology in a comprehensive service delivery and application oriented network environment.

The IMS is based on the principles and protocols of the Internet defined by the IETF, which have been adapted by 3GPP and TISPAN for their use within a secure and scalable fixed-mobile communication. The Session Initiation Protocol (SIP) [4] is used as the standard signalling protocol that establishes, controls, modifies and terminates voice, video and messaging sessions between two or more participants. The Call State Control Functions (CSCF) servers implement and manage the SIP functionalities. The Authentication, Authorization and Accounting (AAA) related functionality provision within the IMS is based on the Diameter protocol [5] and is implemented in the Home Subscriber Server (HSS). Media Gateways and Media Server support potentially required adaptation of multimedia information for specific QoS requirements. The top level view of IP Multimedia Subsystem (IMS) as Next Generation Service Delivery Platform (SDP) [6] is depicted in *figure 1.1.*

The IP Multimedia Subsystem (IMS) specifies a comprehensive and service oriented architecture providing value added services and standardized interfaces for application service integration. With this technical revolution, the promising value added services suppose to change the entire communication environment and the IMS Application Server (AS) [7] is one of the proposed and developed service containers.

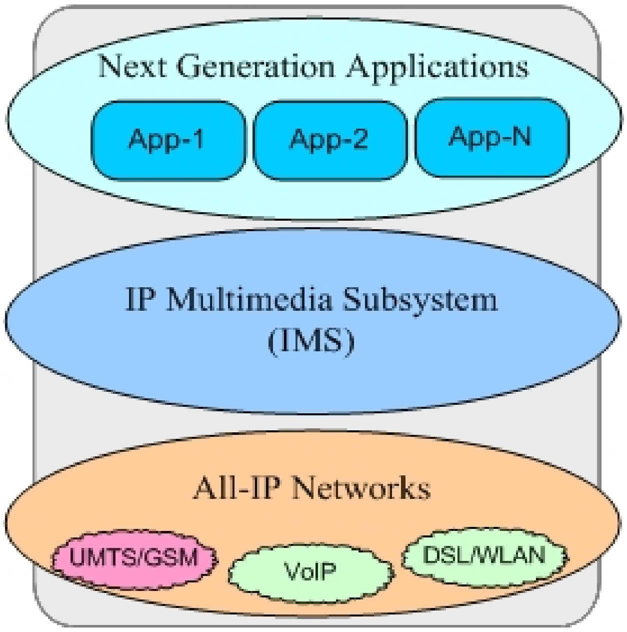


Figure 1.1 IMS Top Level View

The IMS is overlay architecture on top of TCP/IP protocol stack [8] providing value added services. It is like other IP-based network is open and distributed architecture that can enable easy access to services, information, and resources. But on the other side the hackers can access open architecture to launch attacks on IMS networks. Therefore strong and complex security solution and mechanisms such as secure data transmission, confidentiality, authentication, data integrity, anti-replay protection and intrusion detection system are essential to implement independent and robust security framework for IMS. In the following section we explore the potential security threats challenges to IMS.

1.2 IMS Security Challenges

Security and information protection is the core of all computer networks and communication systems. The convergence of fixed-mobile and voice-data networks has opened the door for the innovative and fancy next generation services and applications like integrated multimedia services, combining web browsing, email, instant messaging, presence, VoIP, video conferencing, application sharing, telephony, unified messaging, multimedia content delivery, etc. on top of different network technologies including IPv6, 3GPP (Third Generation Partnership Project) IMS (IP Multimedia Subsystem) [1], 3GPP2 Multimedia Domain (MMD) [3], TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks) NGN (Next Generation Network) [9], UMTS (Universal Mobile Telecommunication Systems) [10] and DSL (Digital Subscriber Line) [11] etc. In the context of converged communication world, network security is a big challenge to protect multi-dimensional and hybrid technology networks resources and to provide confidentiality and integrity protection to users.

The introduction of IP in telecommunication domain signifies not only a shift towards packet switching communication, but also a step towards completely open and easily accessible protocols. In terms of security, this implies an array of new threats and risks that have to be counter. The IMS is vulnerable to different types of other attacks because users are always being connected, online and the network structure based on new SIP (Session Initiation Protocol) [5] technology which is open architecture and vulnerable to different types of Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS) attacks..

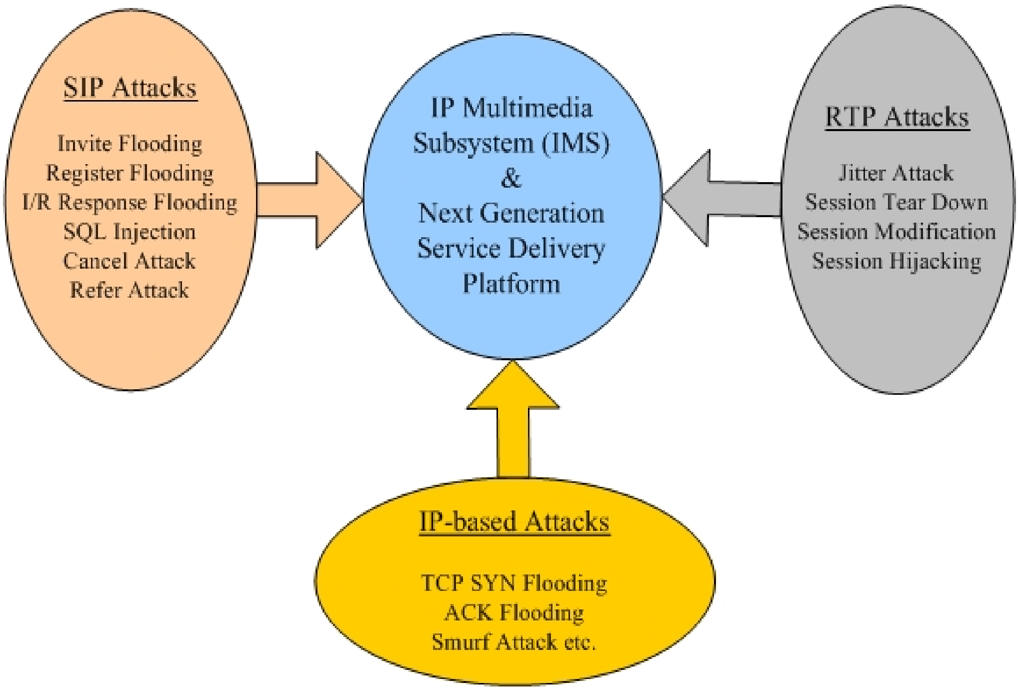


Figure 1.2 IMS Security Challenges

The IMS potential threats are from multiple communication domains and protocols including Session Initiation Protocol (SIP), Media Streaming (RTP) and Internet (IP) as depicted in *figure 1.2.* These security challenges are summarized as follows:

- Denial-of-Service (DoS) attacks on IMS Core and NGN Services.
- Distributed Denial-of-Service (DDoS) attacks on IMS.
- Misuses of IMS Services and Applications.
- Threats from open-based IP infrastructure.
- SIP signalling attacks like REGISTER and INVITE flooding.
- Media flow attacks like drop and modify session.
- Vulnerability threats on access links.

In order to minimize the risk of theft of information and data form hackers and protection of network and services, there is strapping requirement to develop an independent security framework for IP Multimedia Subsystem (IMS).

1.3 Research Domain and Proposed Solution

The IP Multimedia Subsystem (IMS) provides seamless Service Delivery Platform (SDP) [6] for next generation fixed-mobile convergence (FMC) applications and services [12]. From security prospective, it is very important to protect IMS network resources and SDP to provide security and confidentiality to costumers and users from intelligent hackers and criminal attackers.

The security and privacy in IMS is standardized by 3GPP in release 5 and onward releases [13], [14]. We define this level 1 security and are achieved during registration and session management to authenticate and authorize users before accessing the applications and services. Level 1 security is not sufficient to protect the IMS resources from DoS flooding attacks, message tempering like SQL-injection [15] and misuse of resources etc. Similarly if the hacker is able to penetrate into the network and break this security level, then the network is corrupted and multiple active attacks could be launched. In this situation there should be additional level 2 security to protect the network resources and users confidential information. The extended Level 2 security focuses on Open IMS Core and Application Servers from Denial-of-Service (DoS)/Distributed DoS (DDoS) attacks, misuse of services and fraud detection from both legitimate and illegitimate users. The research domain and scope is depicted in *figure 1.3,* focusing on securing two platforms i.e. IMS core and IMS Service Delivery Platform (SDP).

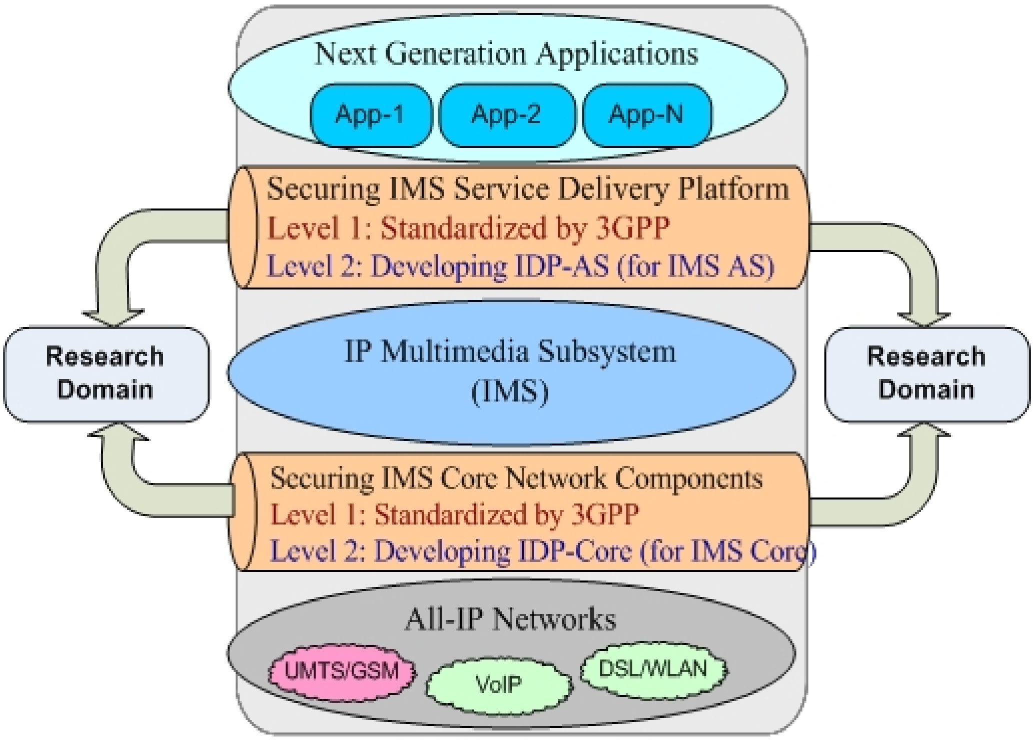

Next Generation Applications
App-1
App-2
App-N
Securing IMS Service Delivery Platform
Level 1: Standardized by 3GPP
Level 2: Developing IDP-AS (for IMS AS)
Research Domain
IP Multimedia Subsystem (IMS)
Research Domain
Securing IMS Core Network Components
Level 1: Standardized by 3GPP
Level 2: Developing IDP-Core (for IMS Core)
All-IP Networks
UMTS/GSM
VoIP
DSL/WLAN

Figure 1.3 Research Scope

The development of Secure Service Provisioning (SSP) Framework incorporates both security levels and providing security protection shield to IMS. The IMS security shield is depicted in *figure 1.4* consisting of two parts each has two modules.

IMS Level 1 Security protection focuses on:

- Developing IMS security architecture.
- Based on IETF, 3GPP and TISPAN Standards Mechanism and Specifications.
- Providing AKA, Encryption and Integrity, and Inter-Domains Security.

Extended Level 2 Security protection focuses on:

- DoS/DDoS flooding attacks on Open IMS Core.
- Misuse of services and fraud control for IMS Application Server (AS).
- Developing Intrusion Detection and Prevention (IDP-Core) system for Open IMS Core.
- Developing Intrusion Detection and Prevention (IDP-AS) system for IMS Application Servers.

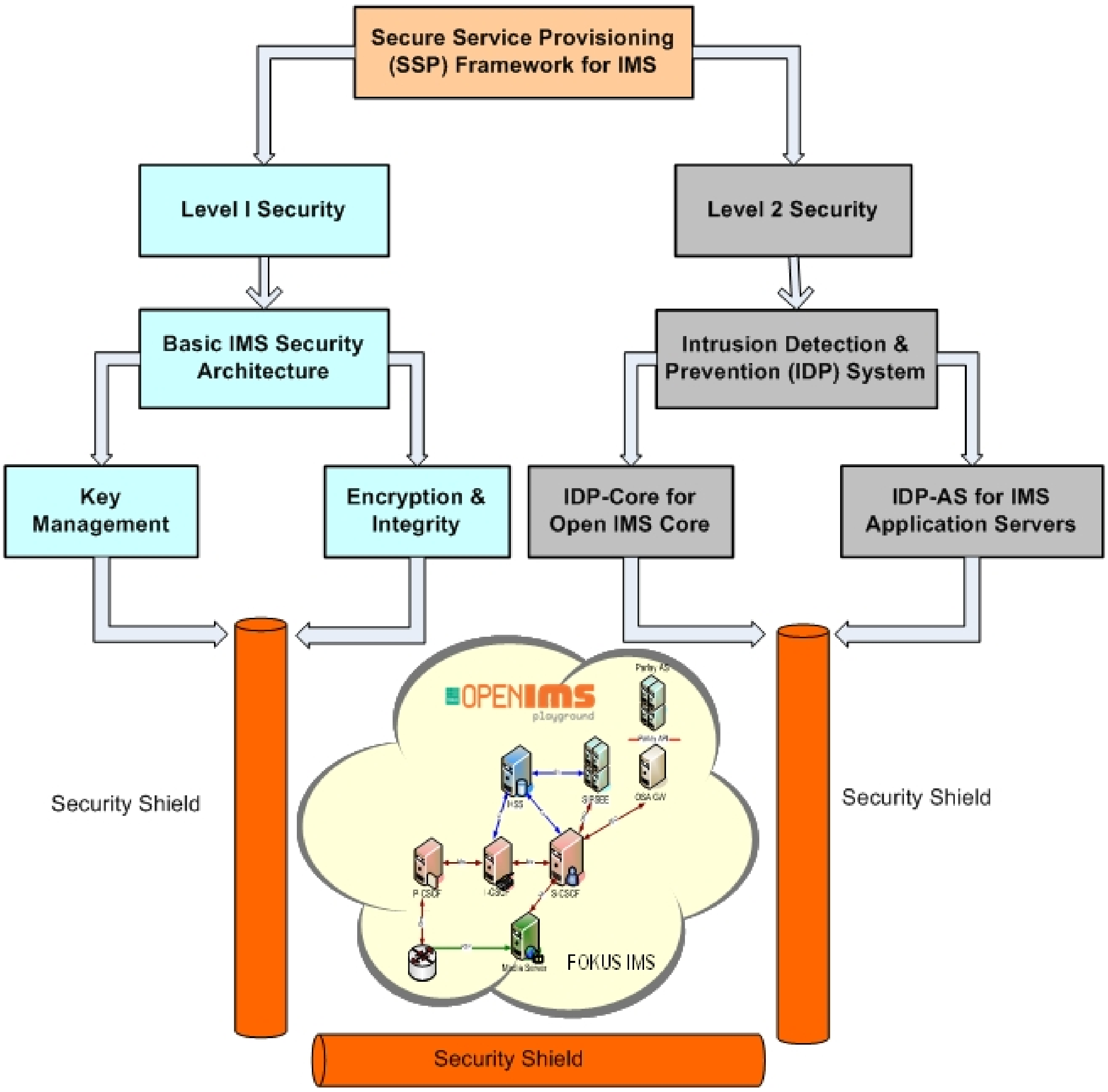


Figure 1.4 Secure Service Provisioning (SSP) Framework Overview

1.4 Thesis Outline

The thesis consists of six parts labelled A-F and further each part consists of multiple chapters as depicted in *figure 1.5*. The brief description of each part and is as follows:

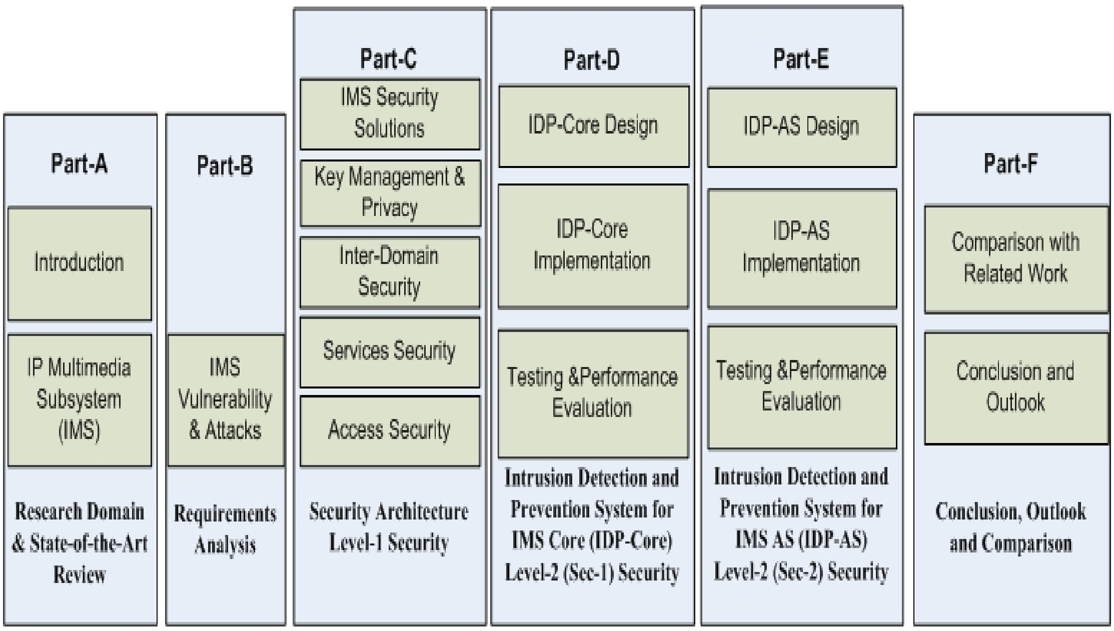

Part-A
Introduction
IP Multimedia Subsystem (IMS)
Research Domain & State-of-the-Art Review
Part-B
IMS Vulnerability & Attacks
Requirements Analysis
Part-C
IMS Security Solutions
Key Management & Privacy
Inter-Domain Security
Services Security
Access Security
Security Architecture Level-1 Security
Part-D
IDP-Core Design
IDP-Core Implementation
Testing &Performance Evaluation
Intrusion Detection and Prevention System for IMS Core (IDP-Core) Level-2 (Sec-1) Security
Part-E
IDP-AS Design
IDP-AS Implementation
Testing &Performance Evaluation
Intrusion Detection and Prevention System for IMS AS (IDP-AS) Level-2 (Sec-2) Security
Part-F
Comparison with Related Work
Conclusion and Outlook
Conclusion, Outlook and Comparison

Figure 1.5 Thesis Outlines and Division

Part-A focuses on the problem domain and state-of-the-art review. It consists of two chapters. The first chapter “Introduction” highlights the motivation, problem domain and scope of the thesis. The security challenges to IP Multimedia are presented. Chapter 2 “IP Multimedia Subsystem” is the state of art review, explaining the IMS architecture and important interfaces where security is considered very critical. The user’s registration in IMS and session establishment scenarios are presented. These scenarios are important to understand the attacks possibilities on the IMS signalling flow and communication.

Part-B defines the requirement analysis and consists of chapter 3 “IMS Vulnerability and Attacks”. The main focus is on the SIP signalling and media flow attacks. These attacks are grouped into two categories i.e. time dependent like flooding attacks and time independent attacks like message tampering and SIP message flow attacks. This categorization helps to develop the proper solution for mitigating these attacks.

Part-C explains the level 1 IMS security solutions based on standards protocols and mechanisms recommended by Third Generation Partnership Project (3GPP) and TISPAN. It consists of five chapters (from 4 to 8) developing IMS security architecture providing level 1 security measures. Chapter 4 “IMS Security Solutions” draws the outline of “Secure Service Provisioning (SSP) Framework”. IMS security attacks verses existing and extended solutions are presented. Chapter 5 “IMS Key Management and Privacy” explains keys generation and secure exchange of keys between client and network during the authentication procedure. The used of these keys for securing the session signalling are also presented in this chapter. Chapter 6

"Inter-Domains Security" provides secure communication when user is roaming. The architecture of Security Gateways (SEGs) and PKI-based Authentication Framework (AF) are discussed to implement the IMS inter-domains security. Chapter 7 "Services Security" is protecting the HTTP-based IMS services. The Generic Bootstrapping Architecture (GBA) and Generic Authentication Architecture (GAA) are presented to authenticate user before accessing the 3G services. Chapter 8 "Access Security" explains to establish security mode setup during connection establishment, and access link data integrity and confidentiality between mobile user and Universal Mobile Telecommunication System (UMTS).

Part-D presents level 2 extended security solutions. Level 2 extended security works has two sections; (1) design and development of Intrusion Detection and Prevention (IDP) system for IMS core against Denial-of-Service (DoS) attacks, and (2) design and development of Intrusion Detection and Prevention (IDP) system for IMS Application Server (AS) against fraud and misuses of services. The first component is described in part-D which consists of three chapters (from 9 to 11) focusing on the design, development, implementation, testing and performance evaluation of Intrusion Detection and Prevention (IDP-Core) system for IMS core.

Part-E explains second section of level 2 extended IMS security. It consists of three chapters (from 12 to 14) focusing of the design and development, implementation, testing and performance evaluation of Intrusion Detection and Prevention System for IMS Application Server (IDP-AS).

Part-F is the last part consisting of two chapters. Chapter 15 describes the existing approaches of Intrusion Detection and Prevention (IDP) systems developed for IP Multimedia Subsystem (IMS) and Voice over IP (VoIP) technology. The comparison with our approach is also presented in this chapter. Chapter 16 summarizes the research work. The limitations and future improvements for developed prototype are presented.

Chapter 2 IP Multimedia Subsystem (IMS)

2.1 Introduction

Today telecommunication world is passing through the evolutionary phase i.e. the merger of two of the most successful paradigms: the Internet and the cellular networks. The Internet is based on packet switching communication to provide fancy services like www, emails, instant messaging, presence, VoIP, Video Conferencing and shared whiteboard etc. with best effort quality services where as the cellular networks provides call and multimedia services i.e. SMS, MMS based on circuit switching and modem based techniques to transmit IP packet over circuits. As we know that the deployment and maintenance of data networks is much easier than the voice networks, so it is straight forward to think about relaying all communications on the data networks rather than maintaining in parallel two network technologies [16]. On the other hand we see today the increasing demand for integrated multimedia services, bringing together internet applications with telecommunications.

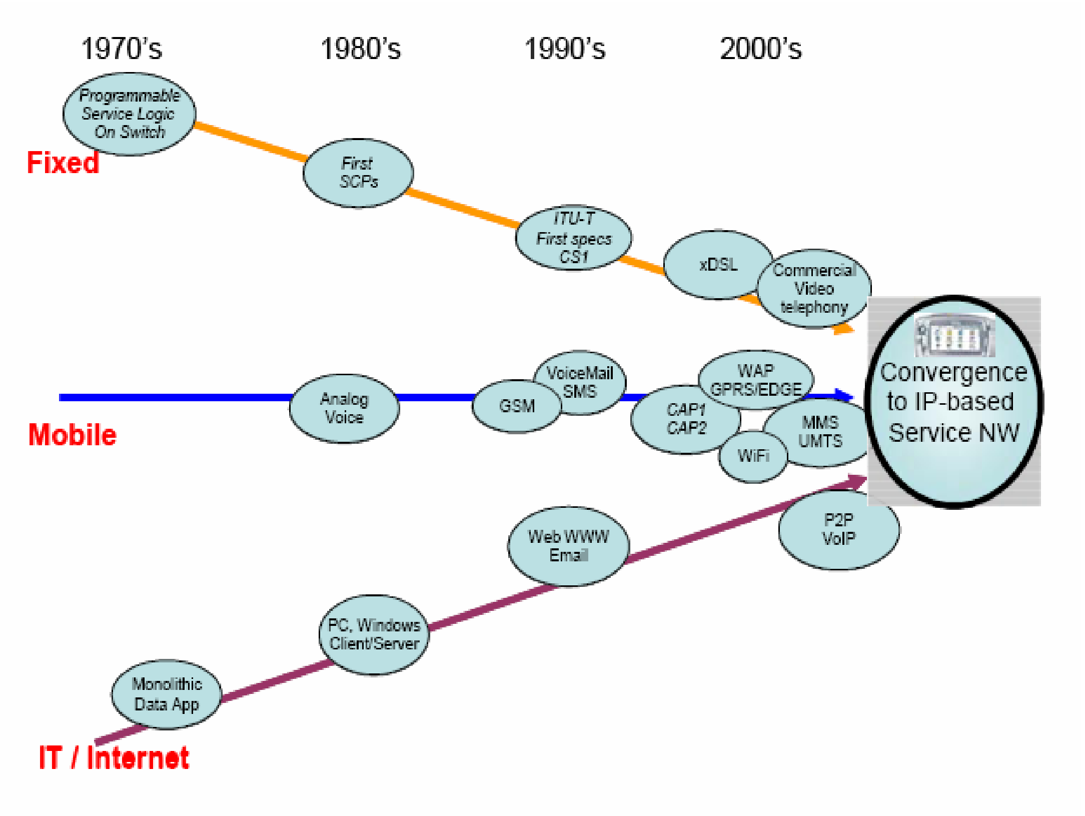


Figure 2.1 Towards Fixed-Mobile-Internet Convergence

With the emergence of mobile multimedia services, such as unified messaging, click to dial, across network multiparty conferencing and seamless multimedia streaming services, the convergence of networks is started, leading to an overall Internet–Telecommunications convergence as shown in *figure 2.1*. In face of such convergence, the need for universal SDPs supporting integrated services emerged. This means that SDP should in principle enable the rapid and uniform programming and provision of seamless multimedia services on top of any network environment. There is no doubt, however, that today two main trends are of pivotal importance for SDPs design, namely the support of mobile users and the support of (mobile) multi media data services.

The IMS is an approach to provide overlay Service Delivery Platform (SDP) [6] architecture for IP networks, entirely build on Internet protocols defined by the Internet Engineering Task Force (IETF), which have been extended on request of 3GPP to support telecommunications requirements. Mobile operator face today the problems that mobile users can gain access to the Internet and make use of Internet services and define a minimum SDP architecture for providing QoS, security and charging for IP based services, while providing maximum flexibility for the realisation of value added and content services.

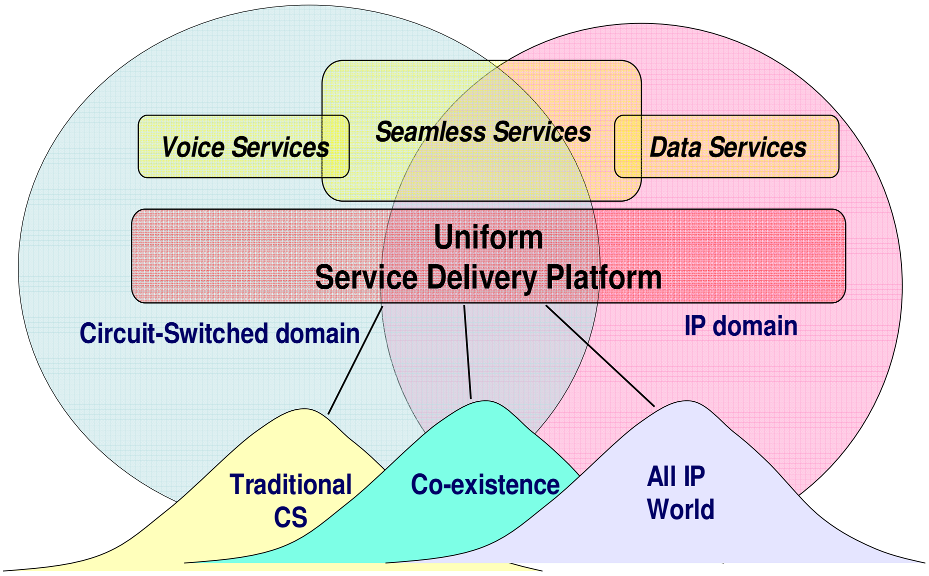


Figure 2.2 Networks & Services Convergence

2.2 IMS Standardization

The IMS has been standardized by 3GPP [2] and 3GPP2 [3] since the beginning of this century in release 5 and will be extended in higher releases as a part of UMTS and fixed network. The release 5 standard has been driven by the vision to define the

IMS for providing multi media services including VoIP on top of GPRS networks. The IMS is supposed to be standardized access-independent IP-based architecture that interiors with existing voice and data networks for both fixed, Internet and mobile users etc. The IMS architecture makes it possible to establish peer-to-peer IP communications with all types of clients with quality of services and complete service delivery functionalities.

The release 6 IMS has fixed the short comings of previous releases and also contains novel features like presence, messaging, conferencing, group managements and local services. The release 6 has optimized the IMS to provide the envisaged IMS killer application e.g. push to talk over cellular. The release 7 IMS is looking at unified IMS for all IP access networks. In addition, since 2004, ETSI TISPAN [9] is looking at service infrastructures for fixed-mobile convergence and next generation networks which extends the IMS to make it applicable on top of various access networks, i.e. WLANs and particular fixed Internet (i.e. DSL). The recent IMS Release 7 is joint cooperation work of 3GPP and TISPAN addressing All IP Networks.

2.3 IMS Architecture and Key Protocols

The IMS defines service provision architecture, and it can be considered as the next generation service delivery platform framework. It consists of modular design with open interfaces and enables the flexibility for providing multimedia services over IP technology. The IMS does not standardize specific services but uses standard service enablers e.g. presence, and supports inherently multimedia over IP, VoIP, IM and presence [16]. In the IMS architecture, the SIP protocol is used to establishes, controls, modifies and terminates voice, video and messaging sessions. The related signalling servers in the architecture are referred to as Call State Control Functions (CSCFs) and distinguished by their specific functionalities.

IMS layered architecture consists of three planes as shown in *figure 2.3*: the user, control, and application planes. In spite of the fact that IMS was initially designed (in release 5) for cellular IP networks (GPRS and UMTS), all access-specific issues have been separated in release 6 from the IMS core. This means that transport and bearer services (user plane) are separated from signalling network and session handling services (control plane).

It is important to note that an IMS compliant end user system has to provide the necessary IMS protocol support, namely SIP, and the service related media codecs for the multimedia applications in addition to the basic connectivity support, e.g. GPRS, WLAN, etc.

The important IMS components, protocols and interfaces are follows:

2.3.1 IMS Components and Entities

The IMS entities and key functionalities can be classified in six categories [7] i.e. session management and routing family (CSCFs), databases (HSS, SLF), interworking elements (BGCF, MGCF etc.), services (application server, MRCF, MRFP), support entities (THIG, SEG, PDF) and charging.

Proxy Call State Control Function (P-CSCF):- It is the first contact point within the IP Multimedia Core Network subsystem. Its address is discovered by UEs following Packet Data Protocol (PDP) context activation. The P-CSCF behaves like a proxy accepting requests and services them internally or forwards them. It performs functions like authorize the bearer resources for the appropriate QoS level, emergency calls, monitoring, header (de)compression and identification of I-CSCF.

Interrogating Call State Control Function (I-CSCF):- It is the contact point within an operator's network for all connections destined to a subscriber of that network operator, or a roaming subscriber currently located within that network operator's service area. There may be multiple I-CSCFs within an operator's network. I-CSCF performs functions like assigning an S-CSCF to a user performing SIP registration/charging and resource utilisation i.e. generation of Charging Data Records (CDRs)/acting as a Topology Hiding Inter-working Gateway (THIG).

Serving Call State Control Function (S-CSCF):- It performs the session control services for the endpoint and maintains session state as needed by the network operator for support of the services. The important functions performed by S-CSCF include user registration/interaction with services platforms for the support of services. The S-CSCF decides whether an AS is required to receive information related to an incoming SIP session request to ensure appropriate service handling. The decision at the S-CSCF is based on filter information received from the HSS. This filter information is stored and conveyed on a per application server basis for each user.

Home Subscriber Server: - The HSS is equivalent of the HLR (Home Location Register) in 2G systems; however, extended with two Diameter based reference points. It is the master database of IMS that stores IMS user profiles including individual filtering information, user status information and application server profiles.

Application Servers: - It provides service platform in IMS environment. It does not address how multimedia/value added applications are programmed but only well defined signalling and administration interfaces (ISC and Sh) and SIP and Diameter protocols are supported. The SIP AS is triggered by the S-CSCF which redirects certain sessions to the SIP AS based on the downloaded filter criteria or by requesting filter information from the HSS in a user based paradigm. The SIP AS itself comprises filter rules to decide which of the applications deployed on the server should be selected for handling the session.

Media Processing: - The Media Resource Function (MRF) can be split up into Media Resource Function Controller (MRFC) and Media Resource Function Processor (MRFP). It provides media stream processing resources like media mixing, announcements, analysis and media transcoding as well speech [7]. The other three components are Border Gateway Control Function (BGCF), Media Gate Control Function (MGCF) and Media Gate (MG) which perform the bearer interworking between RTP/IP and the bearers used in the legacy networks.

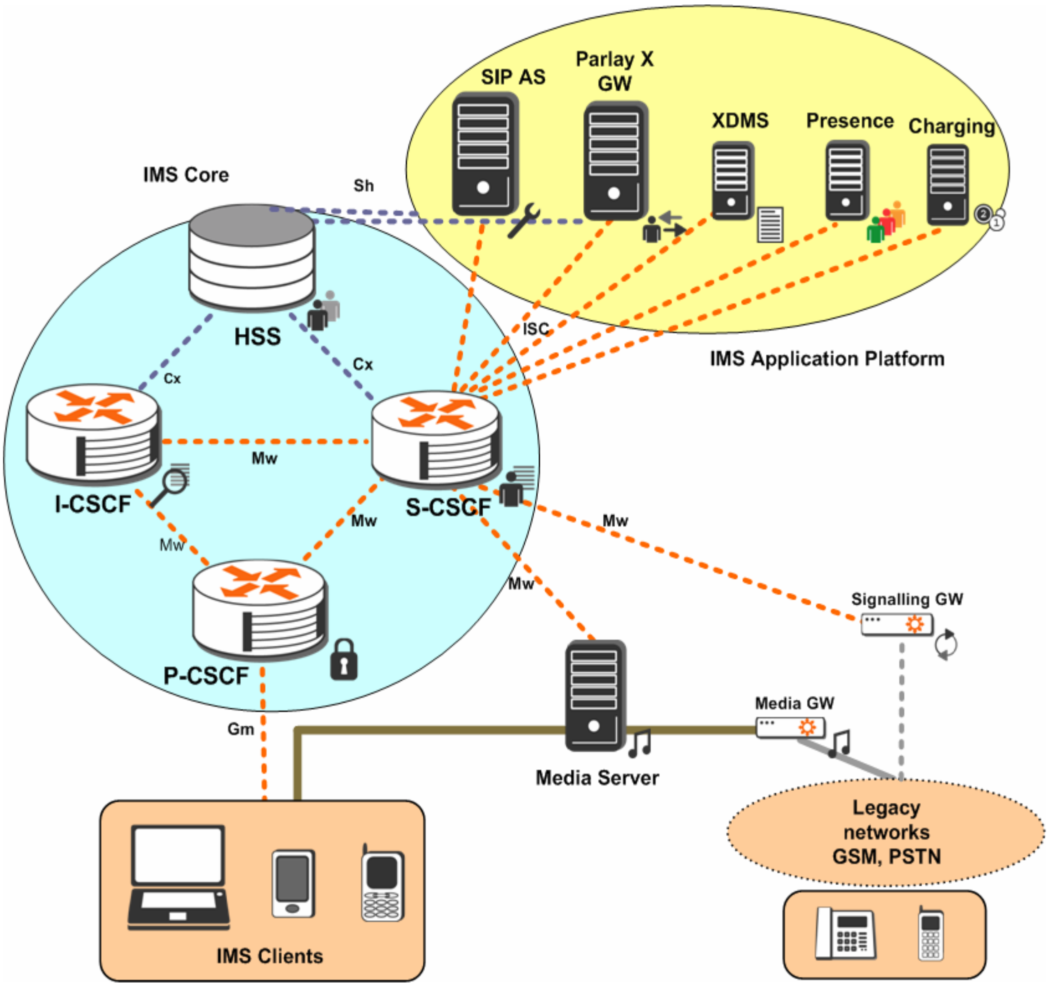


Figure 2.3 IMS Layered Architecture

IMS End User System: - It is important to note that an IMS compliant end user system has to provide the necessary IMS protocol support, namely SIP, and the service related media codecs for the multimedia applications in addition to the basic connectivity support, e.g. GPRS, WLAN, etc.

2.3.2 IMS Key Protocols

The IMS is based on Internet protocols defined by IETF, basically Session Initiation Protocol (SIP) [4] is used for session control, the Diameter [5] is for Authentication, Authorisation, and Accounting (AAA) and Real-time Transport Protocol (RTP) [17] is for media transport.

2.3.2.1 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) is an application layer protocol for establishment, modification and termination of multimedia sessions. It has support for registration and modification of multiple user location information, caller and callee authentication/call authorization, and privacy for call signalling and media streams and media path with ensured QoS. The SIP was created with the design goals to provide transport protocol neutrality, request routing direct or through proxy, separation of signalling and media description, extensibility and roaming. SIP as part of IETF process, is based on the Hyper Text Transfer Protocol (HTTP) [18] and the Simple Network Management Protocol (SNMP) [19]. SIP has some inbuilt service capabilities, allowing SIP elements to implement some intelligent network services like call forwarding, call screening, etc.

2.3.2.2 Diameter Protocol

Based on requirements of standardization bodies (such as IETF groups or 3GPP) and the industry, the IETF AAA Working Group [20] designed Diameter [5] which includes major improvements to existing AAA protocol RADIUS [21]. The Diameter is defined in terms of base protocol and set of applications. The base protocol provides an extensible framework for the use of AAA services. Each application relies on services of the base protocol to support a specific type of AAA requests. While applications may reuse the Diameter base protocol accounting commands, the base protocol is always used in combination with a particular application which implements the actual authentication and authorization. This design allows the protocol to be extended to new access technologies by specifying a new diameter application. All Diameter clients and servers must use the base protocol in conjunction with at least one diameter application e.g. diameter relay agents only needs to implement the base protocol since it does not need authentication or authorization functionality.

The Diameter is a peer-to-peer protocol and any diameter node can initiate a request. Diameter has three kinds of network nodes: servers, clients and agents. A diameter server handles the authentication, accounting and authorization requests from the clients. Diameter clients are usually the end devices of the network that perform access control and originate AAA requests. The agent provides relay, proxy, redirect or translation services. Diameter messages are routed according to the network access identifier of a particular user. The flexibility to define new Diameter applications and vendor-specific attributes allows customization without threatening interoperability. This feature of Diameter is recognized by standardization bodies worldwide and 3GPP chose it as the AAA protocol in IMS [22].

2.3.2.3 Real-time Transport Protocol (RTP)

The other protocol which is important for multimedia contents is Real-time Transport Protocol (RTP) [17]. It provides end-to-end delivery for real-time data. It also contains end-to-end delivery services like payload-type (codec) identification, sequence numbering, time stamping and delivering monitoring for real-time data. RTP provides QoS monitoring (but does not address resource reservation or QoS guarantees) using the Real Time Transfer Control Protocol (RTCP) [23]. This monitoring of data delivery provides minimal control and identification functionality, such as provision of information about reception quality which the application can use to make local adjustments (e.g. when congestion is forming, the application could decide to lower the data rate. RTCP also conveys information about media session participants.

2.3.3 IMS Reference Points and Interfaces

To connect different IMS entities with each other and carrying signal and information, interfaces and reference points are defined by 3GPP. We will discuss only those interfaces where signalling information is necessary to protect because we are proposing security solution for IMS signalling. In this context, the terms *interfaces* and *reference point*s are used synonymously.

Gm Interface: It connects user equipment (UE) to the IMS Core Network. It is used to transport all SIP signalling messages between the UE and the P-CSCF. Procedures in the Gm reference point can be divided into three main categories: registration, session control and transactions.

Cx: This reference point is located between HSS and I- or S-CSCF. Subscriber and service data are permanently stored in the HSS. This centralized data is utilized by the I-CSCF and the S-CSCF when the user registers or receives sessions using Cx reference point and the selected protocol is Diameter. The procedure can be divided into three main categories: location management, user data handling and user authentication.

ISC: The IMS Service Control (ISC) interface is located between an S-CSCF and an application server. The AS could behave as an SIP UA or SIP Proxy on this interface. The S-CSCF process the received SIP messages based on the filter criteria stored in the user profile obtained from the HSS.

Sh: It connects Application Server with the HSS and the used protocol is Diameter. It enables the AS to obtain user data or to get to know the S-CSCF to send SIP request.

Ut Interface: It is located between a UE and an AS. HTTP is the chosen data protocol and any further communication protocol needed between user and application has to rely on HTTP.

Mw: It is the reference point between different CSCFs i.e. between P-CSCF and I-CSCF & S-CSCF. The procedures in the Mw reference point can also be divided into three main categories: registration, session control and transactions.

2.4 IMS Core Functionality & Features

The IMS is designed to provide number of key capabilities required to enable new IP services via mobile and fixed networks. The important key functionalities which enable new mobile IP services are:

- Multimedia session negotiation and management
- Quality of service management

- Mobility management
- Service execution, control and interaction

Now we discuss the important features of IMS like addressing, registration, charging and quality of services etc.

2.4.1 Addressing and Registration

The 3GPP specifies SIP as the signalling protocol in the packet-switched domain of UMTS. The addressing in IMS is called SIP URI (Uniform Resource Identifier) and looks like an email address. The SIP URI follows the guidelines defined in [24]. In order to use IMS services, the UE must perform IMS registration. First the UE must obtain an IP connectivity bearer and discover an IMS entry point i.e. P-CSCF [23]. After the P-CSCF discovery, the UE sends a SIP REGISTER request to this Proxy. The P-CSCF processes the REGISTER request and uses the provided home domain name to resolve IP address of the I-CSCF then contact the HSS to fetch the required capabilities for S-CSCF selection. After S-CSCF selection the I-CSCF forwards the REGISTER request to the S-CSCF. The S-CSCF checks the response and if it is correct downloads a user profile from the HSS and accepts the registration with a 200 OK response as shown in the *figure 2.4*. Once the UE is successfully authorized, the UE is able to initiate and receive sessions. The UE must keep its registration active by periodically refreshing its registration.

The registration procedure [7] in step wise is explained as follows:

- First, the dedicated signalling Packet Data Protocol (PDP) context is established between User Equipment (UE) and the Gateway GPRS Support Node (GGSN).
- The UE discovers the address of the Proxy Call Session Control Function (PCSCF).
- The UE sends a REGISTER message to home network to perform SIP registration.
- The Interrogating-CSCF (I-CSCF) selects the Serving-CSCF (S-CSCF).
- The S-CSCF downloads the authentication data of the user from the Home Subscriber Server (HSS).
- The UE and the P-CSCF agree on a security mechanism.
- The UE and the network (S-CSCF) authenticate each other.
- IP security (IP-sec) associations between the UE and the P-CSCF are established.
- SIP compression starts between the UE and the P-CSCF.

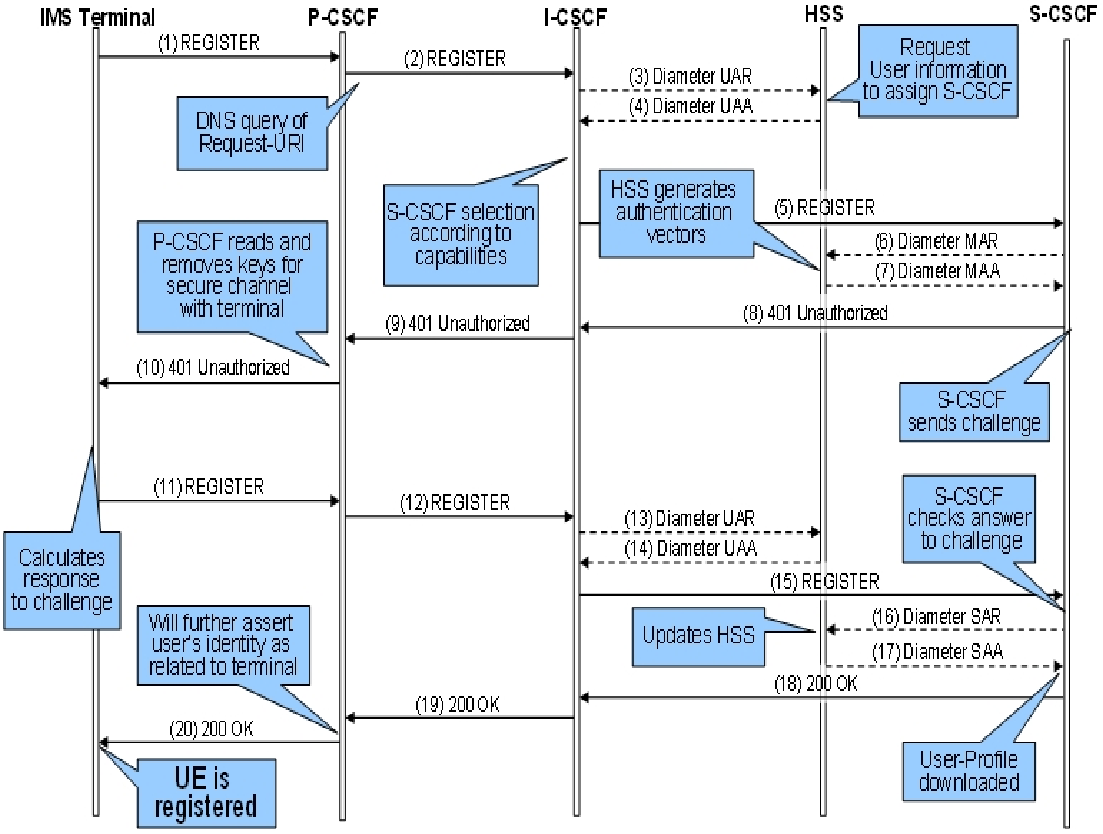


Figure 2.4 User Registration Process

- The UE learns the route to the S-CSCF.
- The S-CSCF learns the route to the UE.
- The S-CSCF downloads the user profile from the HSS.
- The S-CSCF registers the public user identity of the user.
- The UE becomes aware of public user identity and user current registration state.
- The P-CSCF becomes aware of public user identity and user current registration state.

2.4.2 IMS Session Management

After the registration, the user is able to access the services and starts session establishment process [7]. This process is briefly explained as follows and depicted in *figure 2.5*:

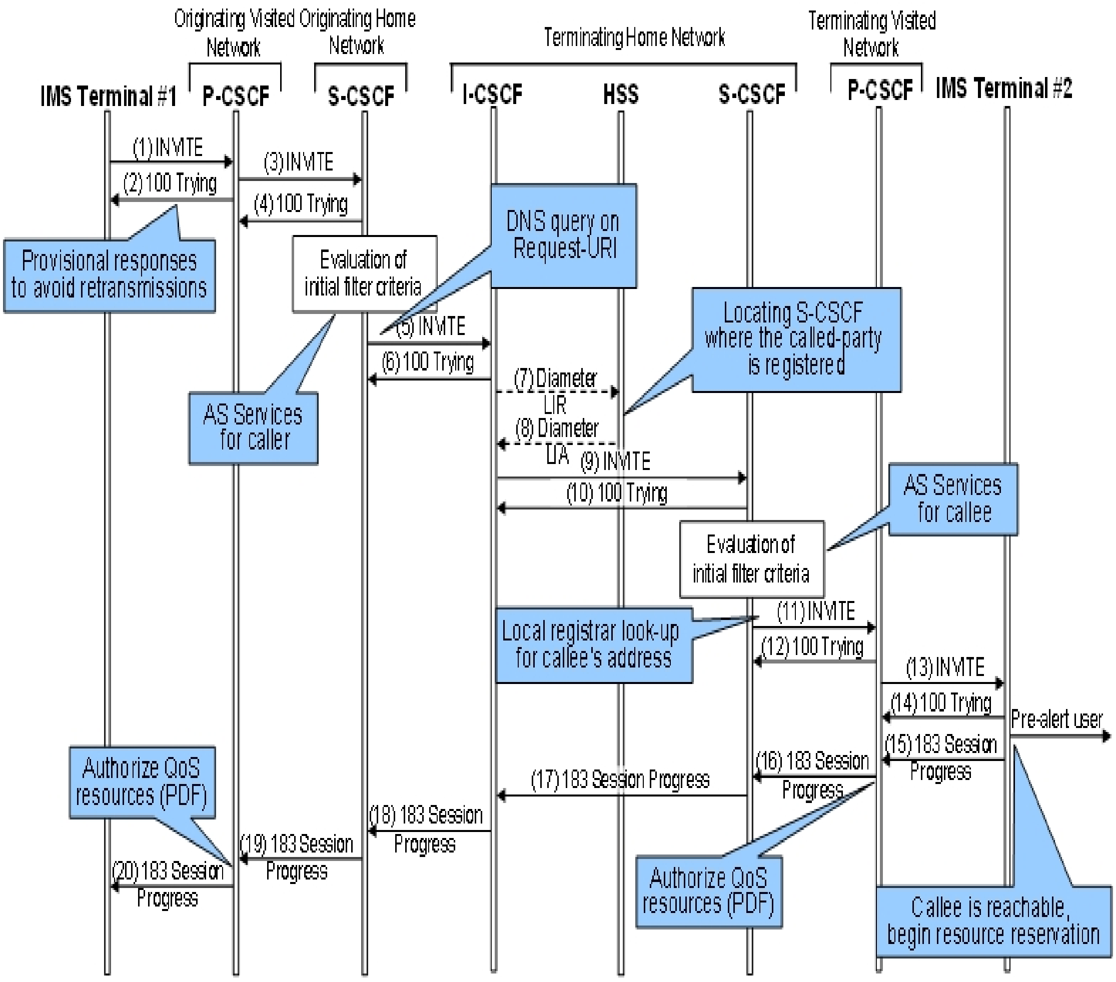

Originating Visited Network
Originating Home Network
Terminating Home Network
Terminating Visited Network
IMS Terminal #1
P-CSCF
S-CSCF
I-CSCF
HSS
S-CSCF
P-CSCF
IMS Terminal #2
(1) INVITE
(2) 100 Trying
(3) INVITE
(4) 100 Trying
Provisional responses to avoid retransmissions
Evaluation of initial filter criteria
DNS query on Request-URI
(5) INVITE
(6) 100 Trying
AS Services for caller
Locating S-CSCF where the called-party is registered
(7) Diameter LIR
(8) Diameter LIA
(9) INVITE
(10) 100 Trying
AS Services for callee
Evaluation of initial filter criteria
(11) INVITE
(12) 100 Trying
Local registrar look-up for callee's address
(13) INVITE
(14) 100 Trying
Pre-alert user
(15) 183 Session Progress
(16) 183 Session Progress
(17) 183 Session Progress
(18) 183 Session Progress
(19) 183 Session Progress
(20) 183 Session Progress
Authorize QoS resources (PDF)
Authorize QoS resources (PDF)
Callee is reachable, begin resource reservation

Figure 2.5 Session Establishment Scenario

- The Caller's UE (UE-A) constructs an INVITE request that includes a registered public user identity of called user (UE-B).

- All SIP messages must traverse the Proxy Call Session Control Function (P-CSCFs) and the Serving-CSCF (S-CSCF) of both users.

- All SIP messages are sent via the established IP Security (IPsec) security associations (ASs) between the UE and their P-CSCFs.

- All SIP messages are sent compressed between the UE and their P-CSCFs

- The UE-A and UE-B agree on the media streams that they will exchange.

- The UE-A and UE-B agree on a single codec for every media stream that they will exchange.

- The networks will authorize the media for the session, so that the users can reserve the related resources.

- The UE-A and UE-B perform resource reservation i.e. they set up the necessary media PDP contexts over which the media streams to and from the network will be transported.

- The network elements will exchange charging information.

- The S-CSCFs may initiate advanced services for their served users.

- Finally UE-B starts ringing and the called user accepts the session. This completes the session establishment phase

2.4.3 IMS Charging

Accounting is the process of collecting information about resource consumption. While accounting data can be used for multiple purposes such as capacity and trend analysis or cost allocation, it particularly forms the basis for the charging and latter billing of a user. The IMS defines two charging modes: online and offline. Online charging is a process in which the charging information can affect in real time the service rendered and therefore directly interacts with session/service control. Prepaid services are applications that need online charging capabilities. Offline charging is a process in which the charging information does not affect in real time the service rendered. This is the traditional model in which the charging information is collected over a particular period [7]. Both modes result in generated Charging Detail Records (CDRs) that are necessary for the purpose of billing a subscriber for the provided service. Offline charging is used over the Diameter-based Rf reference point which is specified between a Charging Collection Function (CCF) and either a CSCF, an AS, a MRFC, a BGCF or a MGCF. In the roaming case it is verified during authentication phase that roaming to the visited network is allowed. IMS provides a means for charging per media component, as IMS sessions may include multiple media components. This would allow a possibility to charge the called party, when a new media component is added in a session.

2.4.4 Quality of Service (QoS)

The policy-based QoS (Quality of Service) control architecture in the IMS is the key part to provide IP-based multimedia applications and services with end-to-end QoS guarantees. The IMS session setup is based on a clear separation between the IMS session signalling and the allocation of resources. This means the IMS session setup is started but afterwards set on hold. At this time, both endpoints are responsible for requesting the required resources at least in their access network, where the IMS session setup is only successfully completed if both endpoints received sufficient resources.

The IMS Release 5 specifications specifies the policy architecture only to GPRS networks [25] and Release 6 describes improvements, e.g. the specification of the PDF as a stand alone element to allow not only IMS compliant technologies but also to control of the bearer traffic to other access technologies. ETSI TISPAN is extending the IMS interconnection with fixed networks in order to have better QoS management. The approach of resource monitoring can help to perform resource management in order to get mobility and roaming QoS functionalities [26].

2.4.5 Privacy and Security

To secure the IMS resources, 3GPP has defined IMS security architecture to authenticate users and network. It protects user confidential information on radio interface and IP based infrastructure. The IMS also utilizes UMTS security features along with its own independent security framework. We shall explore all the IMS security features and services in chapter 4 describing IMS security architecture.

2.5 Provisioning of Value Added Services in IMS

IMS is designed as a platform providing service enablers and IMS-based services are not standardised. The standards bodies want to provide as much as possible freedom for service ideas and service implementations. Only the necessary and core functionality like QoS, security, charging capabilities have been standardised to enable better value added IP-based services, compared to the classic internet services. However, IMS services are important for the introduction of IMS as service delivery platform.

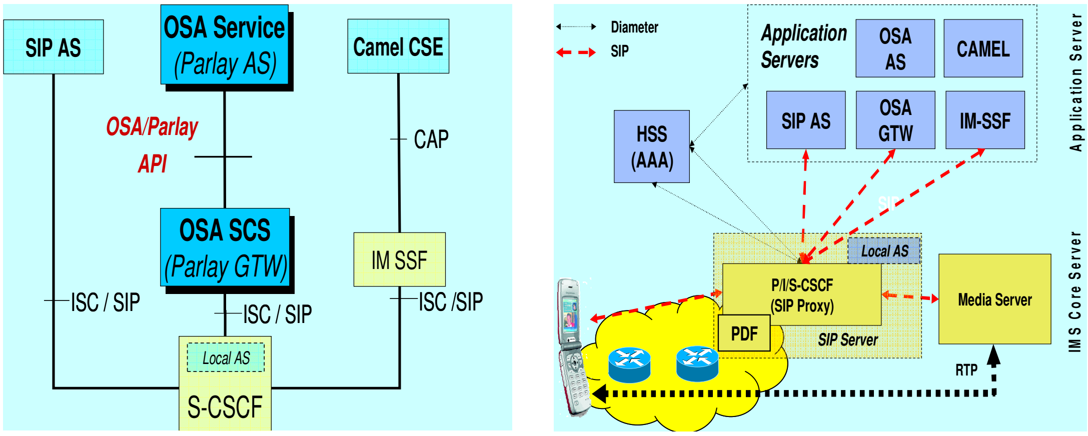


Figure 2.6 IMS Service Architecture Options

The value added services can be provided in all IP environments in principle on all involved SIP systems which are interacting via SIP. Unfortunately today there does not available any common programming paradigm for SIP value added services. Most often there is the notion of service scripts, namely, SIP servlets, call programming language (CPL) and Common Gateway Interface (CGI) scripts. All of them have compared to Intelligent Network (IN)/CAMEL and OSA/Parlay platforms that faced severe limitations in functionality and developers support [27]. However, as SIP has been selected as the universal signalling protocol in the 3GPP IP Multimedia Subsystem (IMS) domain, the notion of SIP application servers, which offer often combinations of CGI and servlets approaches, is emerging. However, also

OSA/Parlay [28] can be used on top of SIP as well as IN/CAMEL [29] as displayed in *figure 2.6*.

- **IMS services on SIP-Application Server: -** The SIP-AS is intended for new services. A multitude of widely known APIs (CGI, CPL, SIP Servlets) is available.
- **IMS services directly on the CSCF: -** It is similar to SIP AS and co-located on the CSCF. It seems to be useful for simple services and may be beneficial for the service availability and the service performance.
- **OSA Services via Open Service Access Service Capability Server:** The OSA SCS is intended for the support of third party application providers. The OSA SCS provides access and resource control.
- **CAMEL Services via Camel Support Environment (CSE):-** The CSE can be used for the support of existing intelligent services to service continuation.

The IMS services are assumed to be addressed by the Open Mobile Alliance (OMA) [30] which is created by WAP Forum in June 2002 with open mobile architecture objective and consists of about ten mobile industries. The OMA SIP-based service enablers are specified on top of IMS as common platform e.g. presence and group management [31] etc. as shown in *figure 2.7*. Now we discuss some valuable services in IMS domain.

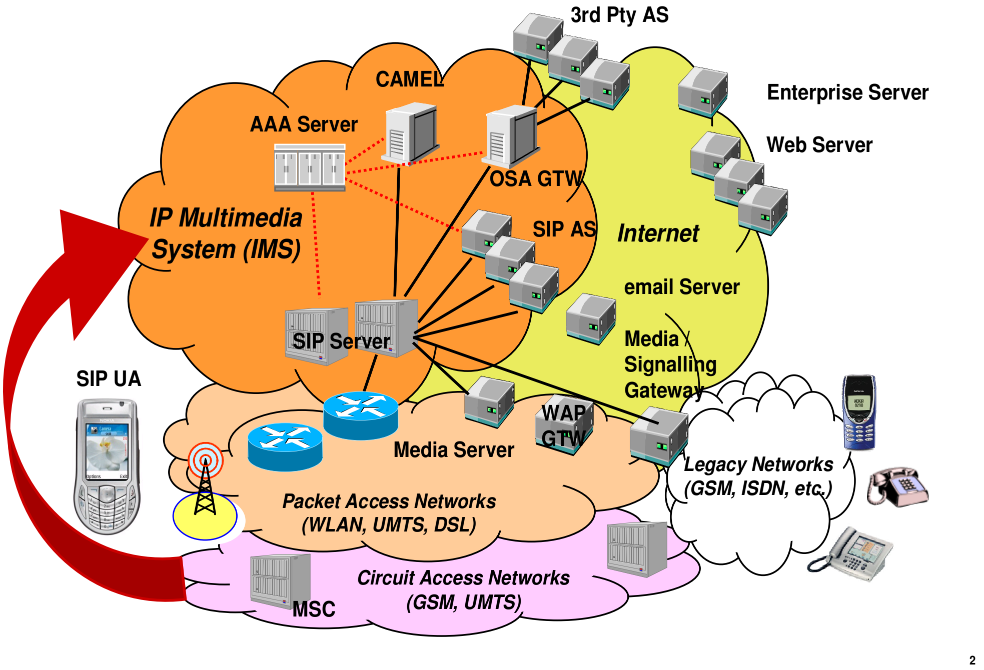


Figure 2.7 IMS as Multimedia Service Enabler

2.5.1 Push-To-Talk (PTT) over Cellular (PoC)

The PoC [32] is 1-to-n half-duplex communication, including two-way radio, using a button to switch from voice transmission mode to voice reception mode (similar to Walkie-talkie functionality) using the mobile phones.

The key PTT functions include presence, group list management, PTT media processing and the PTT application logic (including floor control handling). These are bundled tightly together in the vendor-specific PoC deployments, but from 2006 onwards IMS-based PTT implementation will be deployed. The idea is to enable the reuse of the PTT core ingredients for other service offers, such as presence based services. PoC content are short, instructional and immediate. The PoC is standardised in the Open Mobile Alliance (OMA) Release 1 in 2005, and OMA does not consider access network issues. *Figure 2.8* shows the OMA service enablers architecture and PoC scenario is shown in *figure 2.9*.

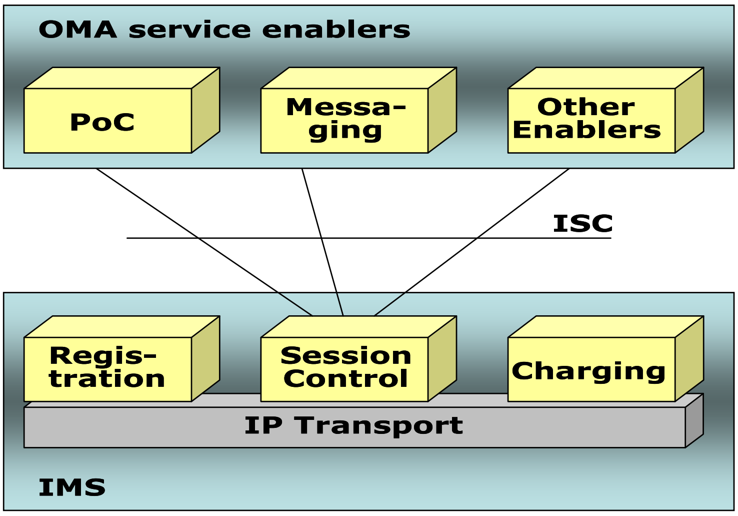


Figure 2.8 OMA Service Enabler Architecture

2.5.2 Multimedia Conferencing and Group Chat

It is a real time service that enables multiple users communicates through audio, video or text. In IMS conferences, there is always a central point of control where each conference participant has a connection. This central point provides a variety of conference services including media mixing, transcoding and participant list notifications. IMS provides functions to enable policies rules, including directives on the lifespan of the conference, definitions of roles available in the conference and policies for allowed roles [33].

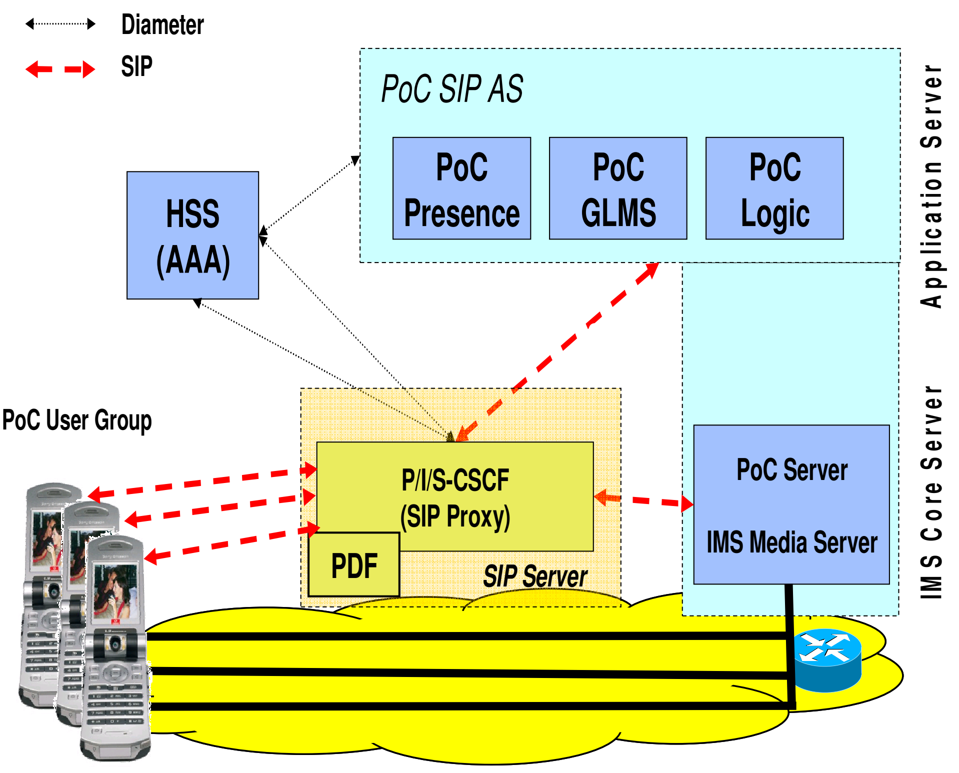


Figure 2.9 IMS Application Server options

2.5.3 Click to Dial

Click-to-dial allows a user to click on a web page when he wishes to speak to a customer or other party. The web server then creates a call between the user and this other party. When a user clicks on the screen button, IMS will negotiate and eventually set up automatically a voice session with one or more other users [34]. The end users can have this call between two phones, a phone and an IP host, or two IP hosts.

2.5.4 Presence

Presence is the capability to make the status of a user be available to others and vice-versa. The presence information may include person and terminal availability, communication preferences, terminal capabilities, current activity and location [34]. The research field actually is considering presence information to facilitate all mobile communication, not only instant messaging, as well as it will also be used as an indicator of the ability to engage in any session, including voice calls, video and gaming, and providing information to management functions like handover and QoS.

2.6 Open Issues and Summary

The new multimedia services are demanding combination of service capability features. Most likely upcoming services will also relay on features like presence, group-list management, additional logic and other features on operator network e.g. location, SMS, MMS. It is obvious that service capability features must be reused for scalability and capital expenses reasons. The open issues are:

- How to manage and orchestrate services?
- How to create stringent services that bundle service capability features?
- How to operate the network for services in a secure way?

As mentioned in the 3GPP specifications the adoption of OSA/Parlay concepts and technologies can contribute a lot. OSA/Parlay already provides an industry standard that enables unified access with gateway character to service capability features of operators' network. Even secure access by third parties can be handled by the OSA/Parlay framework. This framework may control resources by assuming there is secure access for third parties network.

Recently, there are many IMS pre-products originating from the VoIP and wireless telecommunications market. But, there is not yet any commercial IMS deployment within operator networks. However, first Push to Talk (PTT) service implementations mushrooming around the globe can be regarded as the first big trials for IMS technologies. However, there are still many open issues within the IMS architecture and the 3GPP and TISPAN IMS standardization is ongoing, particular in the field of applying the IMS on top of different wireless (WLAN, WIMAX) and wireline (DSL) networks and the IMS evolution towards All-IP Networks.

PART-B

Requirement Analysis

Requirements Analysis

This part deals with the requirement analysis and investigates the potential threats and attacks facing to IP Multimedia Subsystem (IMS). The 3GPP has done a lot of efforts for developing IMS authentication, access control and confidentiality against registration and session hijacking, man-in-the-middle, and eavesdropping and password guessing attacks. But the problems of denial-of-service, flooding and message tampering attacks are not addressed by 3GPP. The objective of this Part-B is to focus on these attacks and vulnerabilities in IMS and it consists of chapter 3. These IMS attacks are classified into two categories:

a) IMS Time Dependent (TD) Attacks

Those attacks which require time interval to produce their harmful results are called time dependent attacks. For example SIP flooding is time dependent and ultimate result of this attack is Denial-of-Service (DoS) threats. The potential IMS TD-attacks are the following:

- SIP REGISTER and SIP REGISTER Response Flooding
- SIP INVITE and INVITE Response Flooding

b) IMS Time Independent (TI) Attacks

In these attacks, even a single message or command is sufficient to launch the attack. The potential IMS TI-attacks are:

- SIP message tampering and fuzzing (e.g. SQL-injection)
- SIP message flows (BYE, CANCEL and Re-INVITE etc.) attacks.

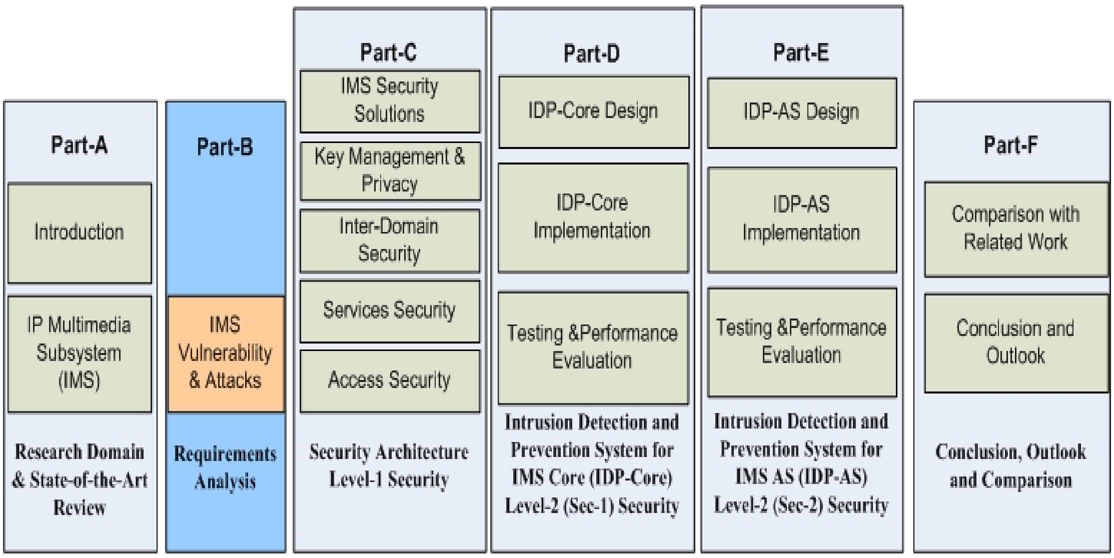

Part-A
Introduction
IP Multimedia Subsystem (IMS)
Research Domain & State-of-the-Art Review
Part-B
IMS Vulnerability & Attacks
Requirements Analysis
Part-C
IMS Security Solutions
Key Management & Privacy
Inter-Domain Security
Services Security
Access Security
Security Architecture Level-1 Security
Part-D
IDP-Core Design
IDP-Core Implementation
Testing &Performance Evaluation
Intrusion Detection and Prevention System for IMS Core (IDP-Core) Level-2 (Sec-1) Security
Part-E
IDP-AS Design
IDP-AS Implementation
Testing &Performance Evaluation
Intrusion Detection and Prevention System for IMS AS (IDP-AS) Level-2 (Sec-2) Security
Part-F
Comparison with Related Work
Conclusion and Outlook
Conclusion, Outlook and Comparison

Figure B: Requirement Analysis

Chapter 3 IMS Vulnerabilities and Attacks

3.1 Introduction

The security and data privacy is a big challenge especially due to integration of different networks and technologies. The Fixed-Mobile Convergence (FMC) based on IP Multimedia Subsystem (IMS) is considered one of the most important and open technology of this decade. This all IP based network architecture provides open and flexible interfaces to deploy innovative services. In parallel, this open IP based technology has security threats from Internet world.

The IMS is also vulnerable to different peer-to-peer attacks because users are always connected and online. The possible reasons for passive and active attacks in IMS are being an attacker could easily access wireless link, launch false based station and redirection attacks to intercept and redirect user's confidential information somewhere else.

The IMS core threats include flooding attacks which ultimately busy the network resources and as a result these sources are not available to legitimate users. The IMS Application Servers are also valuable target for intruders because they provide value-added services. Due to text-based nature of SIP, the IMS and AS are vulnerable to attacks like spoofing, hijacking and message tampering. Moreover, the AS may suffer of HTTP-based threats. Finally, intruders may launch Denial of Service (DoS) attack against applications installed on the AS.

The potential attacks and vulnerabilities suffering to IP Multimedia Subsystem (IMS) include [7]:

- **Denial of Service** - the consequence of a DOS is that the entity attacked becomes unavailable.

- **SQL Injection** – is a type of message tampering attacks and database modification or deletion.

- **Eavesdropping** - if messages are sent in clear text, any malicious user could eavesdrop and get session information to launch a variety of hijacking-style attacks.

- **Tearing down sessions** - an attacker could insert messages like a CANCEL request to stop a caller or send a BYE request to terminate the session.

- **Registration hijacking** - an attacker could register on user's behalf and could re-direct all traffic toward the attacker's machine.

- **Session hijacking** - an attacker could send an INVITE request within dialog request to modify requests en route to change session descriptions and re-direct media elsewhere.
- **Impersonating a server** - someone else pretends to be the server and forges a response. The original message could be misrouted.
- **Man in the middle** - this attack is where attacker intercepts, modifies, or fabricates the flow of messages.

3.2 IMS Security Attacks and Threats

In this part we explore potential attacks on the IMS which are classified under time-dependent and time-independent attacks. The classification is shown in *figure 3.1.* The time-dependent attack means that a time interval is required to effect or damage the victim e.g. flooding attack, but time-independent attack means that it effect instantly on the target as a data packet arrives e.g. a SQL-injection attack.

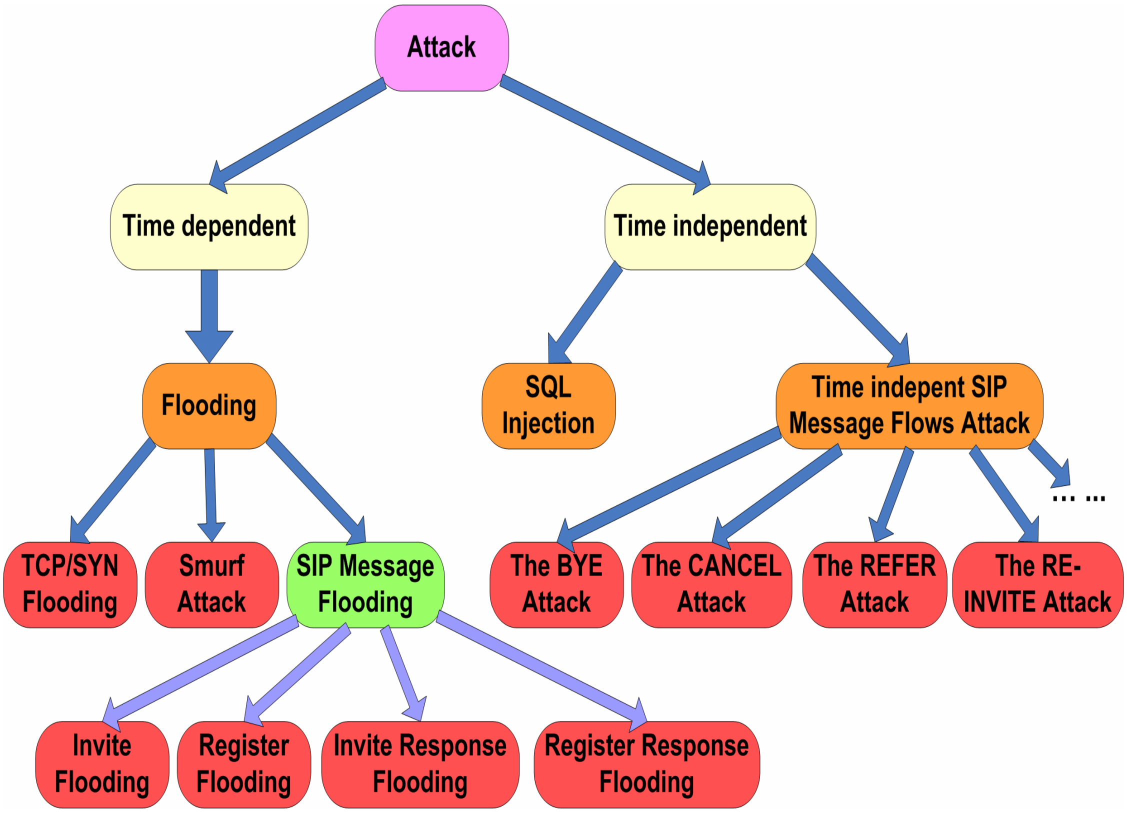


Figure 3.1 Attack Categories

3.2.1 Time Dependent (TD) Attacks

From Intrusion Detection point of view, all attacks that can be detected after the particular duration of attack instead of being detected immediately belong to Time-dependent attack. The primary feature of this category is that an attack is composed of a large amount of data packets. We describe only the SIP flooding attacks because they are the most serious threat for IMS. In flooding the attacker sends lot of fake messages to victim machine or network to produce traffic workload. In case of IMS core, the P-CSCF can be overwhelmed by SIP REGISTER flooding attacks. As a result, the resources could become congested and produce bottleneck. In case of AS, the SIP Servlet [34] server can be overwhelmed by the flooding attacks. There will be no available resources to handle the legitimate SIP- and HTTP-messages. The attacker could use a range of protocols, including Internet Control Message Protocol (ICMP) [35], User Datagram Protocol (UDP) [36], TCP, and Session Initiation Protocol (SIP) for launching flooding attacks.

3.2.1.1 REGISTER Flooding Attack

In the REGISTER flooding attack, the attacker sends a lot of REGISTER requests to the P-CSCF with fake or spoofed source address e.g. SIP URI (Uniform Resource Identifier). In case of distributed REGISTER flooding, the attacker generates multiple REGISTER requests with different spoofed and faked source addresses to overwhelm the IMS resources. It causes downfall of IMS resources and the legitimate users could not get the services. The attack is depicted in *figure 3.2*.

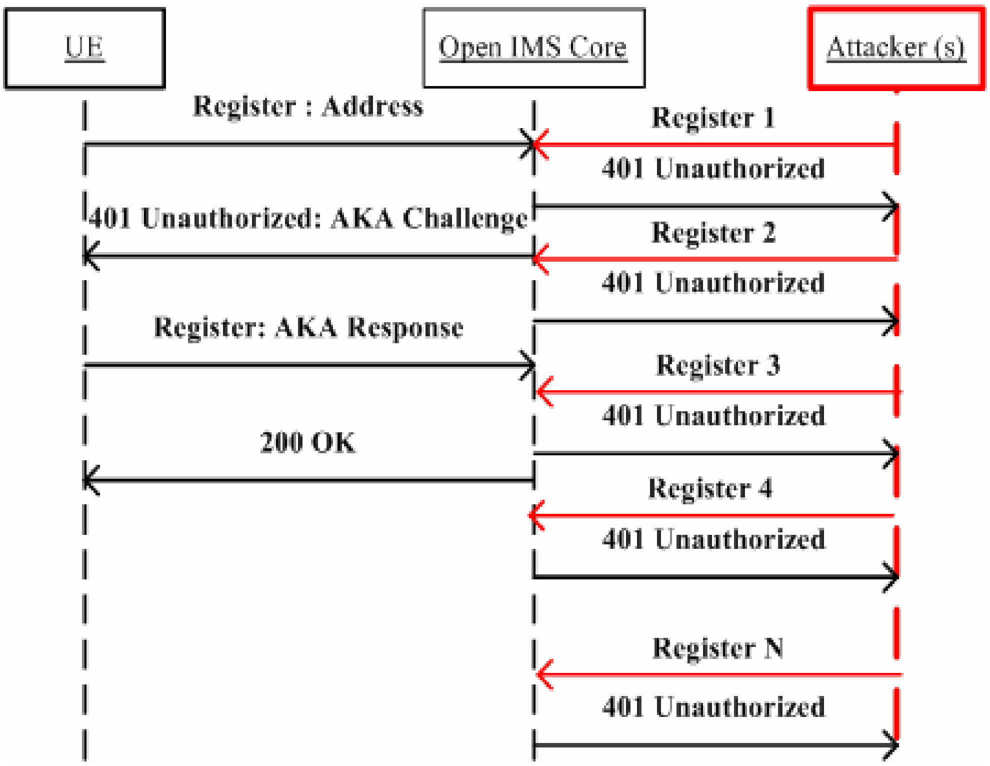


Figure 3.2 REGISTER Flooding Attack

3.2.1.2 INVITE Flooding Attack

The INVITE flooding attack is similar to the REGISTER flooding. In this attack, the attacker sends lot of INVITE SIP requests to hijack the session. The attack is depicted in *figure 3.3*. If user is able to break the IMS authentication process as mentioned in [38], then the network is under attack. In this corrupted network, the authentication process can not differentiate between legitimate and illegitimate users; therefore the extended security solution is capable of detecting solving this problem.

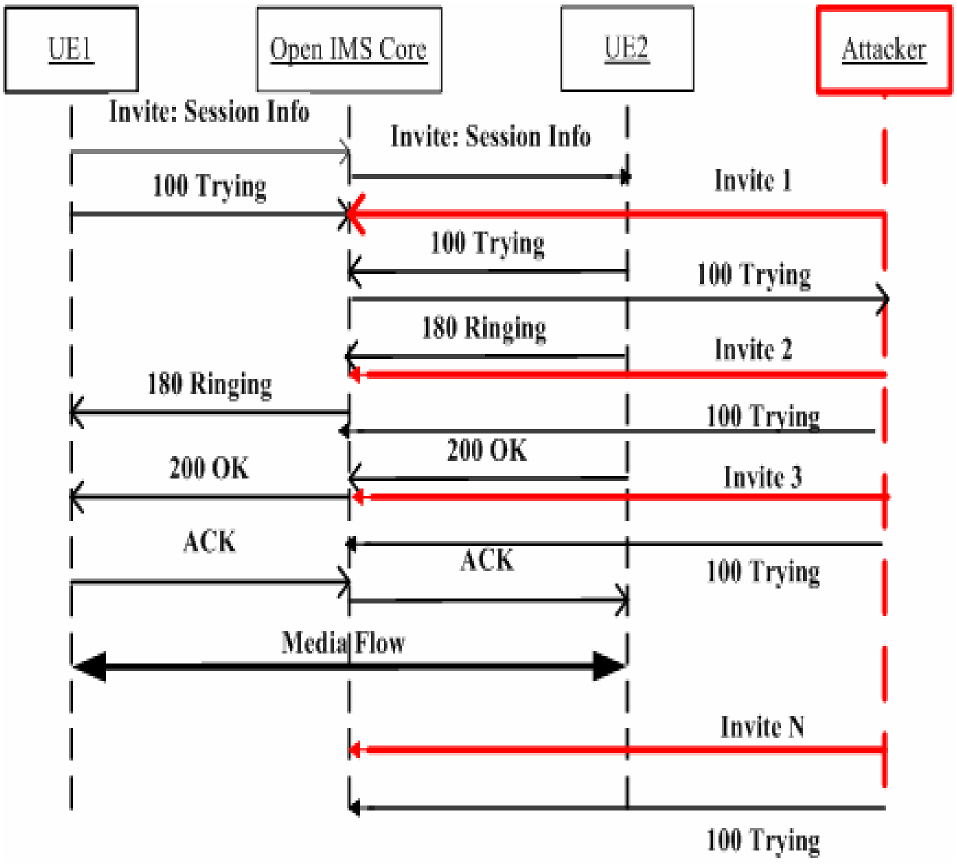


Figure 3.3 INVITE Flooding Attack

3.2.1.3 INVITE Response and REGISTER Response Flooding

The *INVITE response flooding* and *REGISTER response flooding* somewhat differ from the flooding attacks described above which always intend to overwhelm the victim. The goal of the *INVITE response flooding* is to gain valid authentication credentials using exhausted search. A lot of INVITE messages are sent in order to crack the password for the authentication. In case of the *REGISTER Response Flooding* the attacker sends lot of REGISTER messages to a SIP Proxy trying to acquire the authorization credentials.

3.2.1.4 Password Guessing Attack

It is like session hijacking attack with objective to get user session information. If an intruder is not capable to break the IMS authentication process, even than he can launch password-guessing attack in order to misuse the legitimate accounts of users. The intruder launches this attack by sending lot of REGISTER requests to P-CSCF and receives 401-Unauthorized messages [7] from IMS core. At last the attacker could get the 200 OK responses in the result of success of attack. The attack is describes in *figure 2:* the left side shows the successful authentication process from legitimate user and the right side shows the attack scenario. This attack could be launched by distributed nature with different SIP URI (Uniform Resource Identifier).

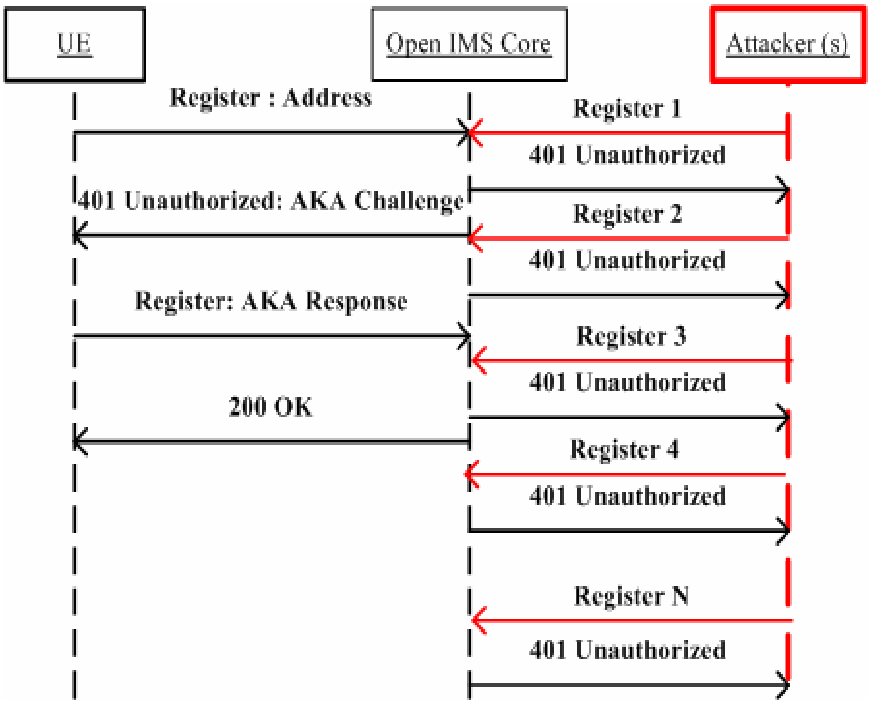


Figure 3.4 Password Guessing Attack

3.2.1.5 TCP SYN Flooding Attack

The TCP/SYN flooding attack is a common example for the flooding attack. It works by creating a quantity of half-open connections. To open a connection the client sends a SYN message to the server, which in turn answers with a SYN-ACK message. The client has to acknowledge the SYN-ACK message with an ACK. A connection is half-open as long as the server waits for the final ACK message from the client. This is achieved when the attacking system sends SYN messages to a target server with a spoofed return address. The server then sends a SYN-ACK message to the spoofed address specified in the SYN message, which is, of course, not the IP address of the attacking machine. Thus, the server never receives the final ACK because the system receiving the SYN-ACK message cannot respond to it and the connection is never fully established. These uncompleted connections are called pending connections. Eventually, as the attacking machine creates an ever increasing number of pending connections, the buffer will fill up and overflow. Just like the example given in *figure 3.5* at first the attacker sends a manipulated SYN packet whose return/source IP-address is unreachable. Then the victim will respond with a SYN-ACK message. The network does not know how to route this SYN-ACK message because of its unreachable receptor. At last the victim shall never receive an ACK message responding to the SYN-ACK message [39]. The memory occupied by the connection can be released only after the TCP connection has timed out.

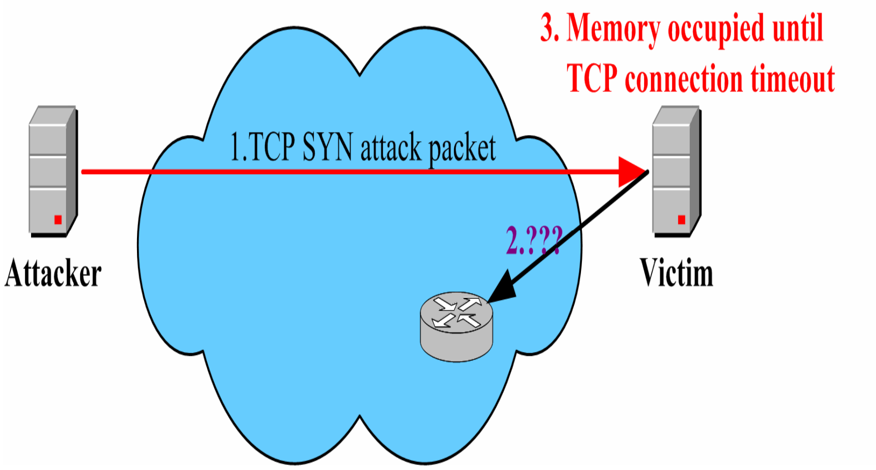


Figure 3.5 TCP/SYN Flood Attack

A similar attack is the TCP/ACKs flood attack. It is launched in the reverser direction by exploiting the answer packets. Using this technique an attacker sends packets to randomly chosen destination IP addresses and forges the source address of the packets to the victim's address. To amplify the attack the attacker can make use of the joint power of multiple systems when launching TCP/SYN flood attack called Distributed TCP/SYN flood attack.

3.2.1.6 Smurf Attack

In the smurf attack scenario, which is shown in *figure 3.6,* attackers use *ICMP echo request packets* [39] directed to IP broadcast addresses from remote locations to generate denial-of-service attacks.

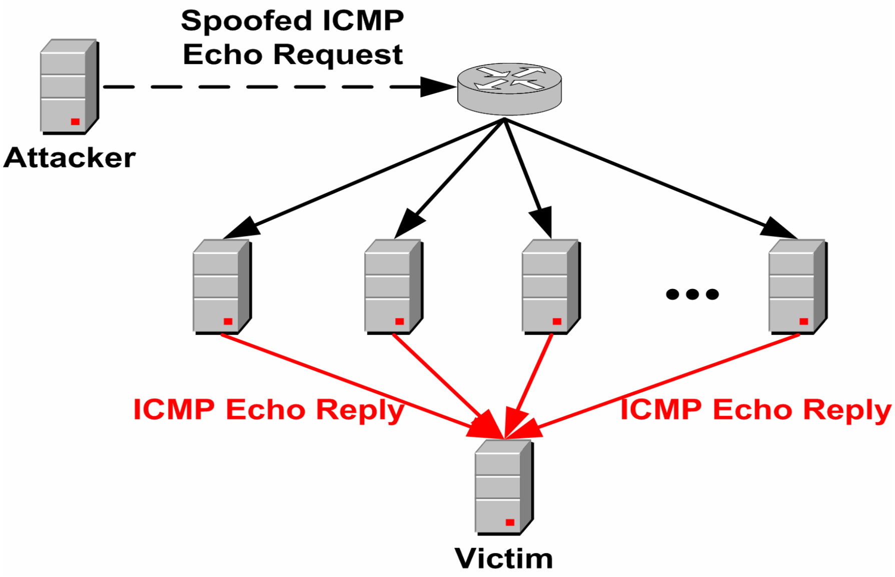


Figure 3.6 Smurf Attack

There are three parties in this attack: the attacker, the intermediary, and the victim. The intermediary receives an *ICMP echo request packet* directed to IP broadcast address of his network. If the intermediary does not filter ICMP traffic directed to IP broadcast addresses, many of the machines on the network receive this *ICMP echo request packet* and answer with an *ICMP echo reply packet*. When (potentially) all the machines on a network respond to this ICMP echo request, the result can be severe network congestion. When an attacker creates an *ICMP echo request packet*, he does not use the IP address of their own machine as the source address [39]. Instead, he creates forged packets that contain the victim’s IP address as source address. The result is that when all the machines at the intermediary's site respond to the ICMP echo requests, they send replies to the victim's machine. If there are a lot of servers at the intermediary's site, the victim is overwhelmed by the reply datagrams.

3.2.2 Time Independent (TA) Attacks

Time-independent attacks are serious threat to IMS like VoIP networks. The fake message cloud that is on behalf of an attack can immediately cause damage on the victim’s node if it is not detected and blocked immediately.

3.2.2.1 SQL injection

The SQL injection is a type of message tampering attack and the text based nature of SIP messages provides opportunity for message tampering attacks in IMS. This attack is not only targeting data modification, but causing denial-of-service by collapse of database services. The utilization of web interface for the provision of value-added services makes IMS more vulnerable to this kind of attacks.

The SQL injection could be launched simply by inserting SQL statement when UE and P-CSCF starts authentication procedure. The UE’s initial REGISTER request utilizes the HTTP Digest [40] Authorization header to transport user’s identities. This REGISTER request looks like:

```
REGISTER SIP: home1.de SIP/2.0
Authorization: Digest Username=″user_private@home1.de″,
realm=″home1.de″, nonce=″ “, uri=″SIP: home1.de″,
response=″ “
```

When malicious user tries to launch SQL injection in IMS, he spoofs the SIP message and inserts the malicious SQL code in its authorization header. The malicious code infected with SQL injection looks like:

```
REGISTER SIP: home1.de SIP/2.0
Authorization: Digest
Username=″user_private@home1.de;delete table subscriber″,
realm=″home1.de″, nonce=″ “, uri=″SIP: home1.de″,
response=″ “
```

When P-CSCF receives a SIP message with an infected authorization header, it generates and executes the illegitimate SQL statement which may delete data in the database [41]. The existing solutions do not provide mitigation against this attack. The IMS also integrates HTTP Servlet container, therefore attacker can also utilize the HTTP message to launch the SQL injection attacks.

3.2.2.2 The BYE Attack

The BYE request is used to terminate an established session. An attacker could utilize the BYE request to tear down a session. The attacker sends a faked BYE message, which is forwarded from P-CSCF to UE1 and it assumes that it is from UE2 that wants to tear down the connection by sending the BYE message. As a result UE1 stops the RTP flow immediately, while UE2 continues to send RTP packets to UE1 because UE2 has no notion that the connection should be terminated [42]. To launch this kind of attack, the attacker needs to learn all necessary session parameters. This can be accomplished either by sniffing the network or performing a man-in-the-middle attack to insert a BYE request into the session. This attack is depicted in *figure 3.7*.

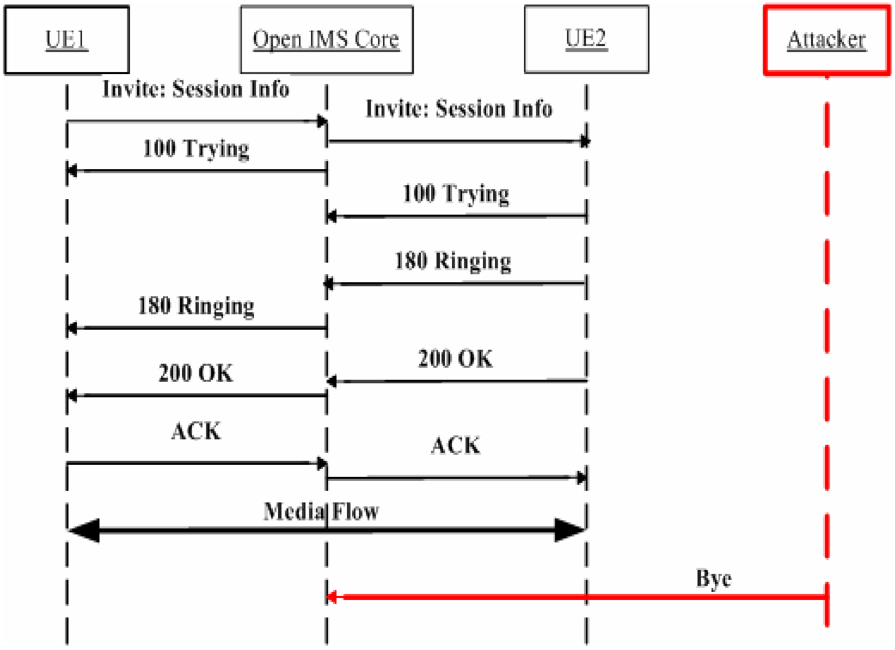


Figure 3.7 Session Tear-Down Attack

3.2.2.3 The CANCEL Attack

The CANCEL terminates a pending request. The attacker could utilize the CANCEL method to cancel an INVITE request generated by a legitimate user as illustrated in *figure 3.8*. Before the final response is generated for an INVITE request, the attacker sends a faked CANCEL message to the P-CSCF that assume that it is from legitimate user. The IMS Core acknowledges the CANCEL message and ceases the processing of INVITE request. A CANCEL request can only be used to cancel an INVITE request.

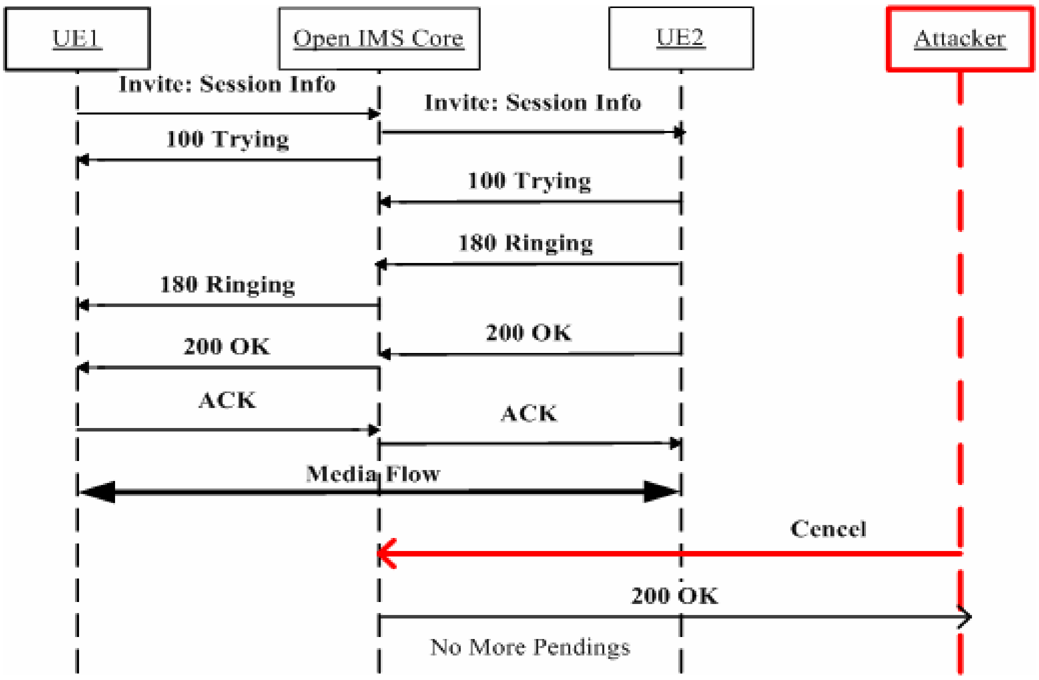


Figure 3.8 CANCEL Attack

3.2.2.4 The Re-INVITE Attack

The INVITE request establishes session or dialog between two user devices (UE). The objective of the Re-INVITE message is used to modify the actual session information, for example changing the addresses or ports, adding a media stream, deleting a media stream, and so on. Therefore the attacker could launch a DoS attack by sending a forged Re-INVITE message to modify the session.

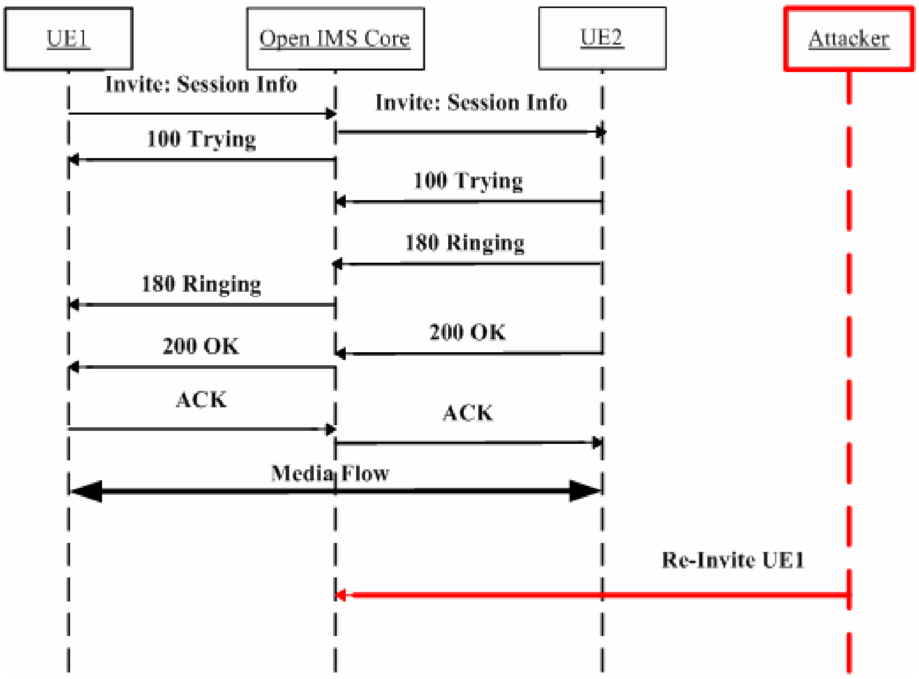


Figure 3.9 Re-INVITE Attacks

3.2.2.5 The REFER Attack

The REFER method indicates that the recipient (identified by the Request-URI) should contact a third party using the contact information provided in the request. RFC 3892 [43] extends this method by allowing the *referrer* to provide information to the *refer target* using the *referee* as an intermediary. The refer target can use this information to decide whether to accept the referenced request from the referee or not. This scheme enables the referee to act as an eavesdropper, giving him the ability to launch man-in-the-middle attacks. For example, as shown in *figure 3.10* the referee can forge the Referred-By header or/and eavesdrop on the referred-by information. The referee may also copy all the related information into future unrelated requests.

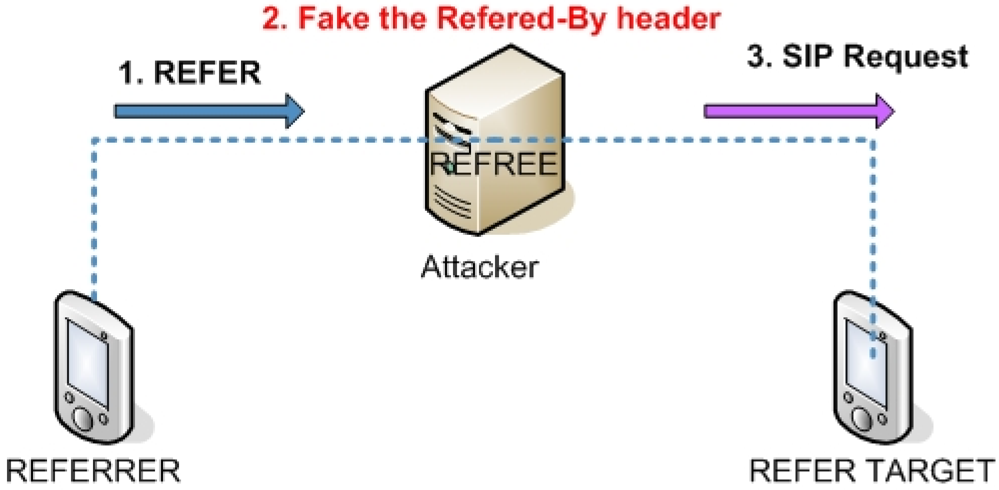


Figure 3.10 REFER Attack

3.3 Summary

This chapter explored different IMS SIP signalling attacks. These attacks are categorized into time depends and time independent attacks. The time dependent (TD) attacks includes SIP REGISTER and INVITE flooding, SIP REGISTER Response and INVITE Response flooding, TCP/SYN flooding and smurf attacks. The time independent (TA) attacks are SQL injection and SIP message flow attacks e.g. BYE, CANCEL and Re-INVITE attacks. This categorization helps us to develop optimum and effective security solution for IMS.

Part-C

IMS Security Architecture

(Level 1 Security)

Level 1 IMS Security Architecture

The Part-C deals with level 1 IMS security solutions based on standards protocols and mechanisms recommended by Third Generation Partnership Project (3GPP) and TISPAN. It consists of five chapters (from 4 to 8) developing IMS security architecture providing level 1 security measures. The functionalities of these chapters are briefly explained in the following:

Chapter 4 "IMS Security Solutions" draws the outline of "Secure Service Provisioning (SSP) Framework". IMS security attacks verses overviews of existing and extended solutions are presented.

Chapter 5 "IMS Key Management and Privacy" explains keys generation and secure exchange of keys between client and network during the authentication procedure. The uses of these keys for securing the session signalling are also presented in this chapter.

Chapter 6 "Inter-Domains Security" provides secure communication when user is roaming. The architecture of Security Gateways (SEGs) and PKI-based Authentication Framework (AF) are discussed to implement the IMS inter-domains security.

Chapter 7 "Services Security" is protecting the HTTP-based IMS services. The Generic Bootstrapping Architecture (GBA) and Generic Authentication Architecture (GAA) are presented to authenticate user before accessing the 3G services.

Chapter 8 "Access Security" explains to establish security mode setup during connection establishment, and access link data integrity and confidentiality between mobile user and Universal Mobile Telecommunication System (UMTS).

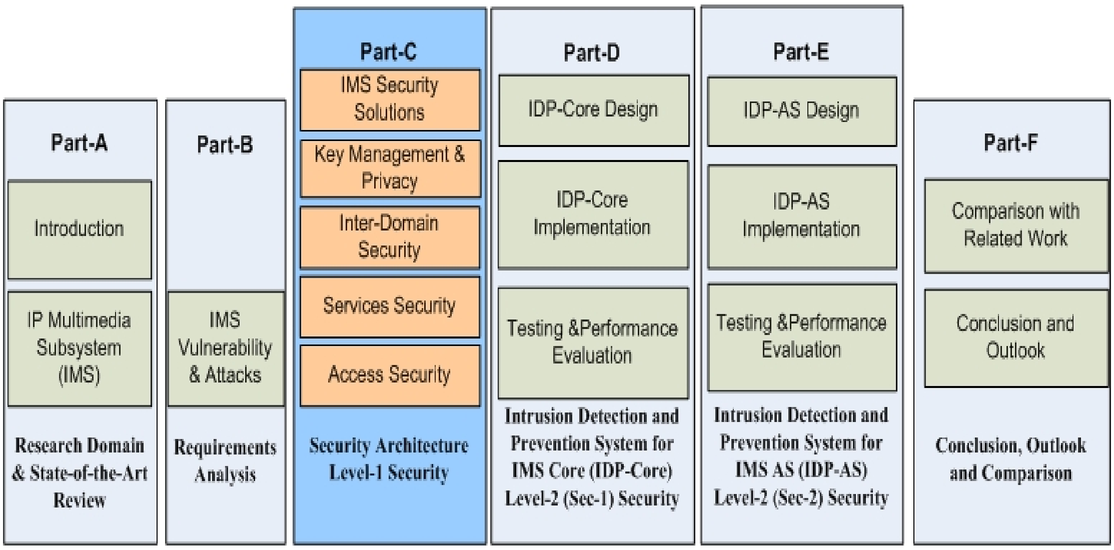

Part-A
Introduction
IP Multimedia Subsystem (IMS)
Research Domain & State-of-the-Art Review
Part-B
IMS Vulnerability & Attacks
Requirements Analysis
Part-C
IMS Security Solutions
Key Management & Privacy
Inter-Domain Security
Services Security
Access Security
Security Architecture Level-1 Security
Part-D
IDP-Core Design
IDP-Core Implementation
Testing &Performance Evaluation
Intrusion Detection and Prevention System for IMS Core (IDP-Core) Level-2 (Sec-1) Security
Part-E
IDP-AS Design
IDP-AS Implementation
Testing &Performance Evaluation
Intrusion Detection and Prevention System for IMS AS (IDP-AS) Level-2 (Sec-2) Security
Part-F
Comparison with Related Work
Conclusion and Outlook
Conclusion, Outlook and Comparison

Figure C: Overview of Part-C (IMS Level 1 Security Architecture)

Chapter 4 IMS Security Solutions

4.1 Introduction

The objective of the IMS security solutions is to develop IMS security architecture to ensure user privacy and network protection against misuses. The important security features and security services provided by these solutions includes:

User Confidentiality: This entity provides user identity confidentiality, user location confidentiality and user un-traceability. To achieve these characteristics the user is assigned by a temporary identity so that the user's permanent identity to which services are delivered cannot be eavesdropped on the radio access link and in addition user data and signalling that might reveal the user's identity is ciphered on the radio access link.

Entity Authentication: Authentication entity is based on user authentication and network authentication, and should apply at connection setup between the user and the network. It involves authentication mechanism using an authentication vector delivered by the user's HE to the serving network and a local authentication mechanism using the integrity key establishment between the user and the serving network.

Data Confidentiality: It provides confidentiality of user data and signalling data. It is achieved by using cipher algorithm and key agreement.

Data Integrity: It provides data integrity and origin authentication of signalling data. Data integrity is achieved by integrity algorithms and integrity key agreement.

Network and Services Availability: Its objective is to make sure that network resources and services should be available all the time to the users. To ensure the availability of services and resources, the network should be protected from Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks.

Fraud Control: Its objective is to protect the precious assets and value added services from the illegitimate users and hackers. In IMS, these services could be protected by securing Application Servers (ASs).

4.2 IMS Attacks and Corresponding Security Solutions

The attacks in IP Multimedia Subsystem (IMS) and the corresponding existing and extended solutions are highlighted in mapping diagram in *figure 4.1*. The existing solutions include IMS AKA (Authentication and Key Agreement) [44], Digest Authentication [40] and TLS (Transport Layer Security) [45] or IPsec (Internet Protocol Security) [46] to provide authentication, integrity and confidentiality by securing SIP messages. These solutions could not prevent application layer attacks, e.g. SIP message flooding, SIP message flow, fuzzing and SQL injection [15]. The proposed solution focuses on developing intrusion detection and prevention system along with these existing solutions to enhance IMS security by detecting and preventing such application layer attacks.

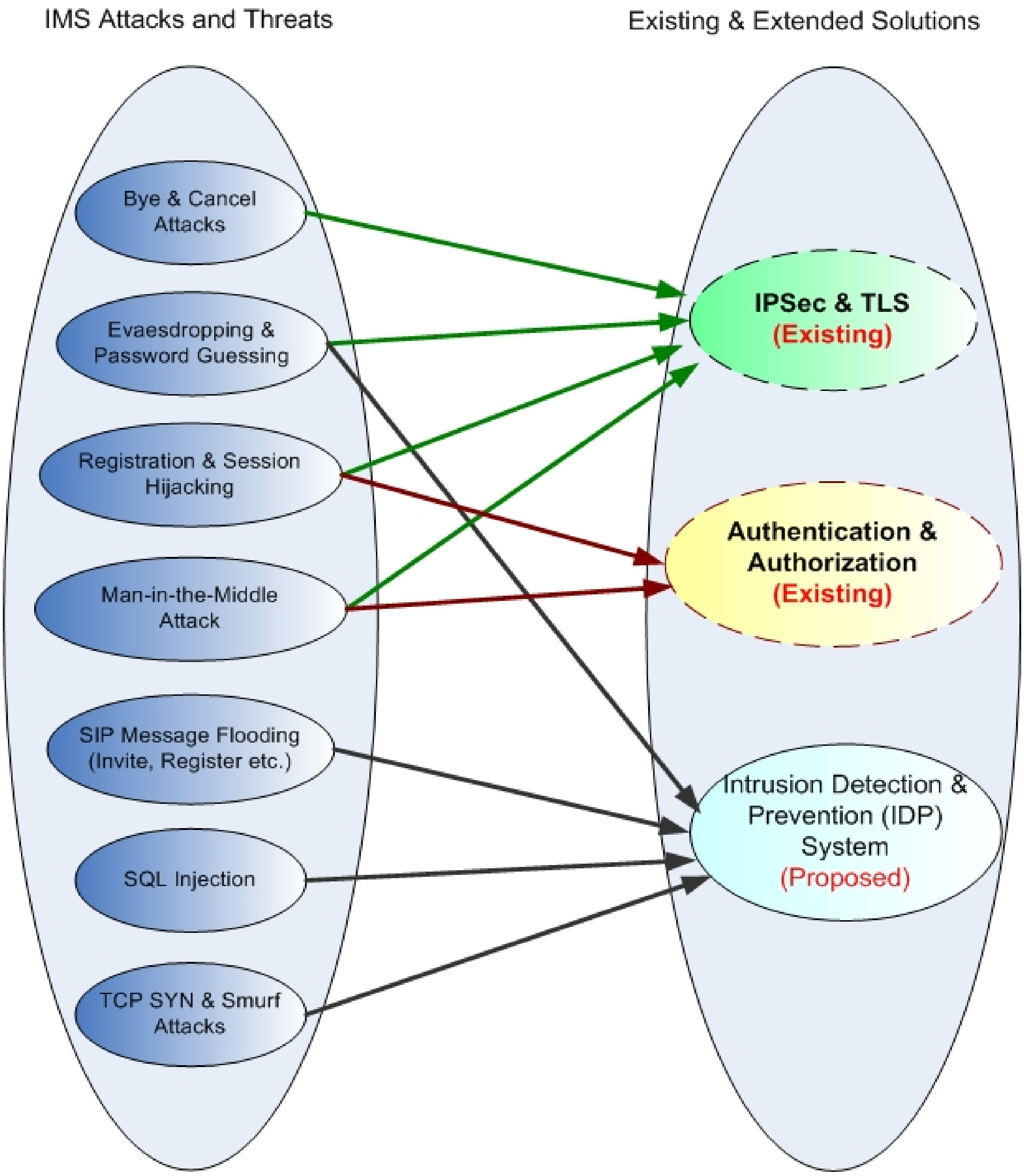

IMS Attacks and Threats
Existing & Extended Solutions
Bye & Cancel Attacks
Evaesdropping & Password Guessing
Registration & Session Hijacking
Man-in-the-Middle Attack
SIP Message Flooding (Invite, Register etc.)
SQL Injection
TCP SYN & Smurf Attacks
IPSec & TLS (Existing)
Authentication & Authorization (Existing)
Intrusion Detection & Prevention (IDP) System (Proposed)

Figure 4.1 IMS Attacks vs. Solutions

The 3GPP standards specify two security solutions for IMS i.e. early IMS security and complete IMS security solutions.

Early IMS Security Solution: standardized in 3GPP Release 5 [13] which provides limited security functionality and aiming to protect early IMS deployment and offer less security. It provides authentication of subscribers for services access and identity confidentiality on the radio interface. It also provides radio interface encryption.

Complete IMS Security Solution: standardized in 3GPP Release 6 [14] with full security functionality and it builds on the early security solutions with objective to improve it. It offers new security features and secures new services to protect network and terminals with data protection. It consists of network domain security and access security that defines SIP security with hop-by-hop fashion. The end-to-end security is not supported.

The overall security for IP Multimedia System (IMS) consists of following mechanisms and is depicted in *figure 4.2*:

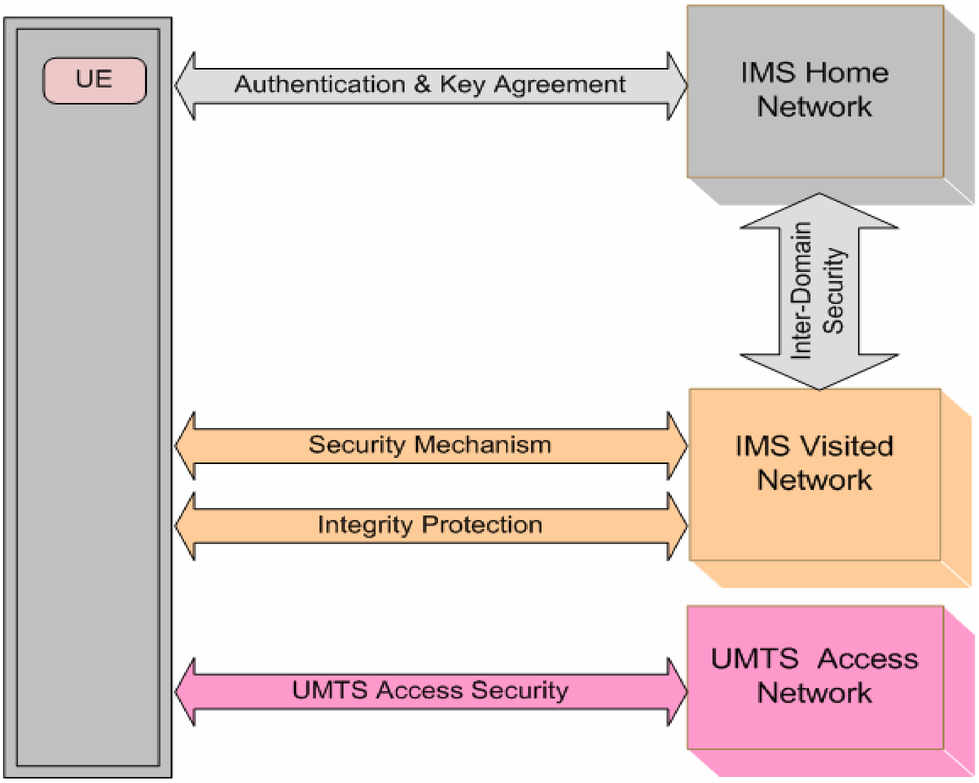


Figure 4.2 IMS Existing Security Solutions

- Authentication & Key Agreement between IM subscriber and home network
- Security Mechanism Agreement between IM client and visited network
- Integrity Protection and Confidentiality
- Network Domain Security between different Domains
- Existing GPRS/UMTS Access Security

4.3 IMS Security Associations

The architecture of IMS security management framework for Open IMS Fraunhofer FOKUS Testbed consists of following seven security associations and agreements [47] (presented in *figure 4.3*) that are mandatory to protect IMS environment for secure and safe communication over wireless and wireline networks including both circuit switched (CS) and packet switched (PS) domains.

4.3.1 Security Association 1 (SA1)

It provides mutual authentication of user and network. The HSS is responsible for generating keys and challenges and then delegate's subscriber authentication to Serving-CSCF (S-CSCF). The long-term key in ISIM and HSS is associated with the IMPI. The detailed process will be explained in chapter 5.

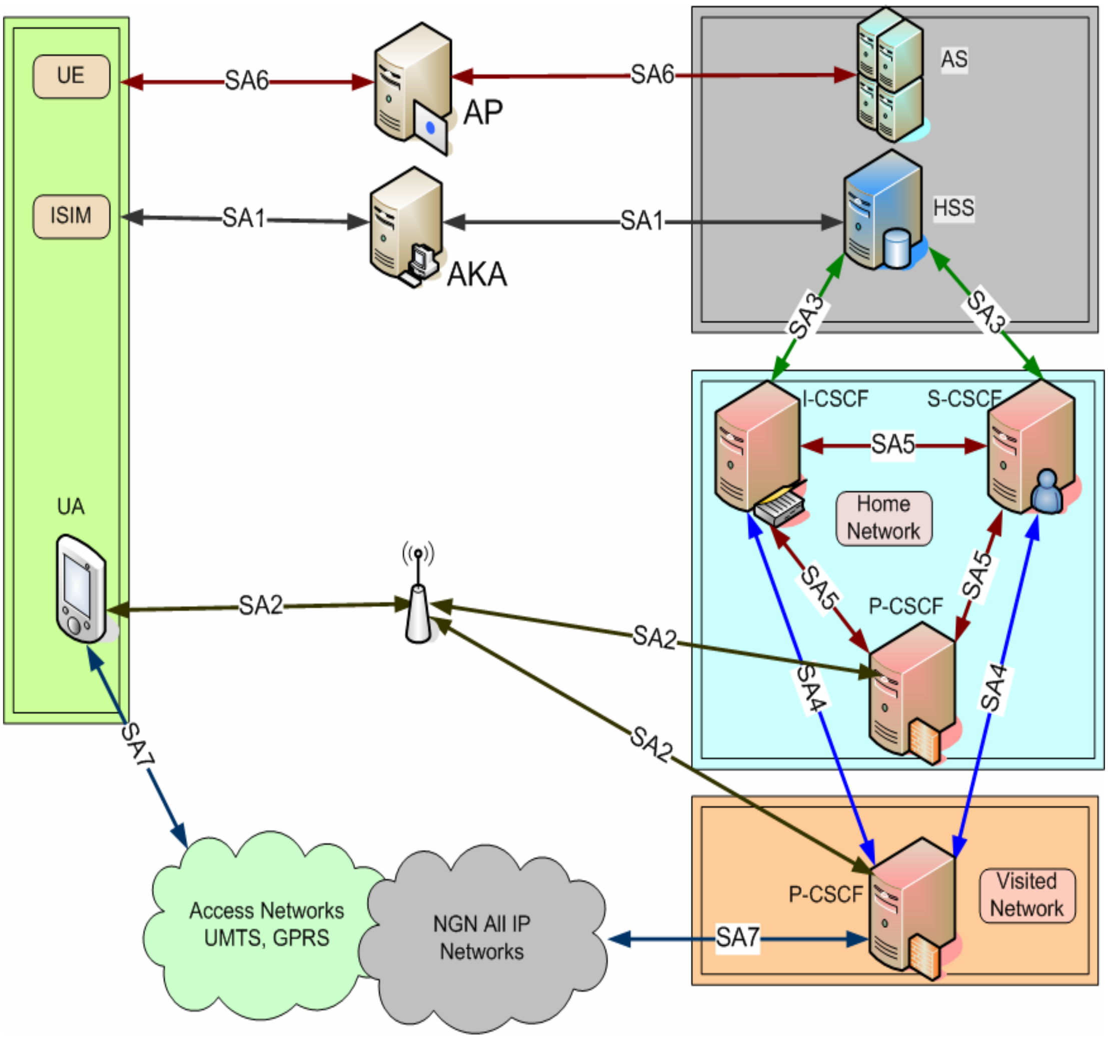


Figure 4.3 IMS Security Associations

4.3.2 Security Association 2 (SA2)

It provides a secure link and a security association between UE and Proxy-CSCF (P-CSCF) for protecting of Gm reference point (air contact). In IMS, NDS/IP is used to protect SIP signalling, but SIP communication at Gm interface between UE and P-CSCF is outside the scope of NDS/IP and needs additional measures for security. It will be explained in chapter 5.

4.3.3 Security Association 3 (SA3)

It provides security within network domain internally for Cx-interface. Home Subscriber Server (HSS) stores subscriber and service data permanently and this centralized data is utilized by I-CSCF and S-CSCF when the user registers or receives sessions through Cx interface and the selected management protocol is Diameter. Diameter messages over Cx and Dx interfaces make use of Stream Control Transmission Protocol (SCTP) [23] with IPsec for secure communication.

4.3.4 Security Association 4 (SA4)

It provides security between different networks for SIP capable nodes and only applicable when P-CSCF resides in visited network i.e. user is roaming. When P-CSCF resides in visited network than by virtue of AKA protocol, the shared secret is only accessible in home network, which means that while authentication needs to take place in visited network, certain delegation of responsibility needs to be assigned to P-CSCF, as IPsec SAs exist between P-CSCF and UE.

4.3.5 Security Association 5 (SA5)

It provides security within network internally between SIP capable nodes and also applies when P-CSCF resides in home network. The IMS protects all IP traffic in core network using Network Domain Security/IP (NDS/IP) [48] which provides confidentially, data integrity, authentication and anti-replay protection for traffic using combination of cryptographic security mechanisms and protocol security mechanisms applied is IP Security (IPsec). The security procedure for SA4 and SA5 will be explained in chapter 6.

4.3.6 Security Association 6 (SA6)

The protocols working across Ut interface performs functionality to manage data traffic for HTTP based applications. Thus securing Ut interface means to achieve confidentiality and data integrity protection of HTTP-based traffic. The authentication and key agreement for Ut interface is also based on AKA which generates session keys. The IMS defines Generic Bootstrapping Architecture (GBA) [49] which utilizes Generic Authentication Architecture (GAA) [50] that performs mutual authentication before accessing services. The authentication in the Ut interface is performed by authentication proxy. Traffic in the Ut interface goes through the authentication proxy and is secured using the bootstrapped session key. The Ut interface employs the Transport Layer Security (TLS) for both confidentiality and integrity protection. We shall discuss the detail procedure in chapter 7.

4.3.7 Security Association 7 (SA7)

It manages to protect user and user's information on access networks e.g. UMTS, GPRS, WLAN and xDSL. The security association takes place independently either in CS service domain or PS service domain. For UMTS access network, security management architecture consists of User Service Identity Module (USIM), Mobile Equipment (ME), Access Network (AN), Service Network (SN) and Home Environment (HE) [44]. The USIM is required for accessing Packet Switched (PS) domain in General Packet Radio System (GPRS) and identifies particular subscriber. USIM contains security parameters for accessing PS-domain, International Mobile Subscriber Identity (IMSI), list of allowed access points, MMS-related information. In serving network, the Serving GPRS Support Node (SGSN) links Radio Access Network (RAN) to packet core network in the PS-service domain. It is responsible for performing both control and traffic handling functions for PS domain. The control parts deal with mobility management and session management. The SGSN also ensures appropriate QoS and generates charging information. In CS-service domain, the related part is Visitor Location Register (VLR). The authentication and key agreement procedure involves Authentication Centre (AUC) within HE, SGSN or VLR and Mobile Station (MS) networks entities [7]. The detailed architecture is explained in chapter 8.

4.4 Extended IMS Security Solution

In this section, we present the overview of additional security measures and solutions in the form of developing Intrusion Detection and Prevention (IDP) system for IMS. The functionalities and types of Intrusion Detection System (IDS) are briefly explained as follows:

The IDSs are divided functionality wise into two types, i.e. anomaly detection or misuse detection. Anomaly detection depends upon models of the normal behaviour of a computer system. The focus of the models could be users, applications, or the network. An anomaly detection system compares actual usage profiles or patterns against established profiles to identify abnormal of activity on the system.

The misuse detection systems depend upon the attacks descriptions or defined attacks rules. The input data is compared with these attacks descriptions to find an evidence that particular attack is occurring. The advantage of anomaly detection systems is being able to detect unknown attacks but the disadvantage are generating large number of false positives and difficult to train the security system for new environment. The advantage of misuse detection system is to generate less false positive but its scope is to detect only known attacks. Most of the practical intrusion detection systems are misuses detection systems. The misuse detection analysis based on stateless or stateful. The stateless analysis examines each event in the input stream independently, while stateful analysis considers the relationships between events and is able to detect event histories that represent attacks. This stateful approach is more powerful and more expensive in terms of CPU and memory requirements [51].

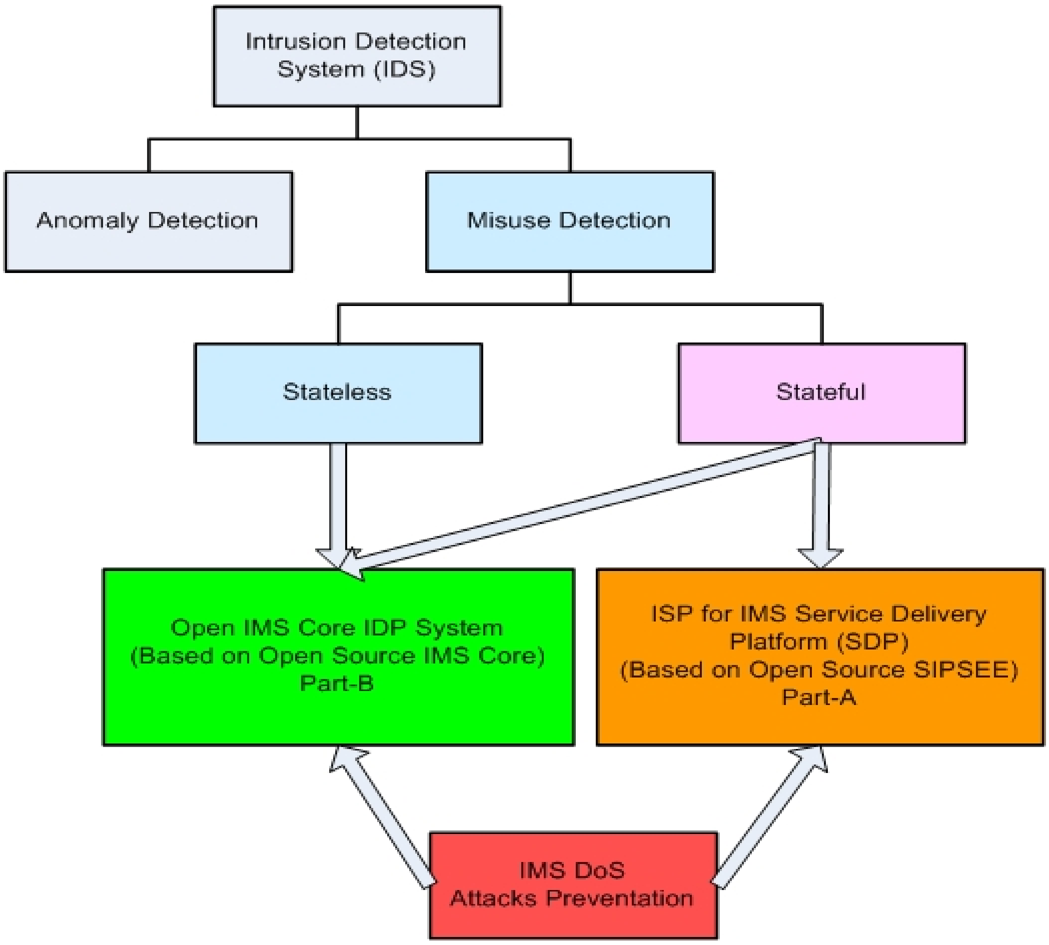

Intrusion Detection System (IDS)
Anomaly Detection
Misuse Detection
Stateless
Stateful
Open IMS Core IDP System (Based on Open Source IMS Core) Part-B
ISP for IMS Service Delivery Platform (SDP) (Based on Open Source SIPSEE) Part-A
IMS DoS Attacks Preventation

Figure 4.4 Proposed Extended IMS Security Solution

The developed prototype based on both stateless and stateful detection methodologies and applies additionally attacks preventions to protect the IMS core and Application Servers. The definition and scope of each module is as follows:

4.4.1 IDP-Core

The Intrusion Detection and Prevention (IDP-Core) system is deployed within P-CSCF as depicted in *figure 4.4*. The IDP-Core performs detection and prevention function in two modes i.e. normal and overload. In normal mode, IDP-core performs detection and prevention for SIP message tampering and SIP message flow attacks. In overload mode (when P-CSCF's CPU is overloaded), it detects and prevents SIP flooding attacks causing denial-of-services. The detail design, detection algorithm, architecture, implementation and performance evaluation of IDP-Core is presented in Part-D.

4.4.2 IDP-AS

The second module, Intrusion Detection and Prevention (IDP-AS) system is deployed within IMS Application Server to monitor the state of partner as well as SIP request/response from and to application server to verify that it is from legitimate user. This module is based on SIP Servlet Exection Environment (SIPSEE), an IMS Application Server prototype developed by Fraunhofer FOKUS [52] for research purpose to develop next generation services. The SIPSEE is based on Jetty [53], an open source, standard-based web server. The IPD-AS analysis is based on stateful misuse detection. The outline of IDP-AS is depicted in *figure 4.4.* The detail design, architecture, attacks detection methodology, implementation, testing and performance evaluation is presented in Part-E.

4.5 Summary

In this chapter we have presented the mapping of IMS security threats and the corresponding IMS security solutions. The existing IMS security solutions and security associations are outlined. The type and functionality of extended solution is discussed. The definition and scope of proposed two modules i.e. IDP-Core and IDP-AS are presented.

Chapter 5 Key Management and Secrecy

5.1 Introduction

This chapter focuses on the generation and management of session keys for securing IP multimedia signalling and data. These keys (confidentiality key and integrity key) are derived from the secret key (K) and shared secret stored in SIM/USIM. In order to get IP Multimedia Services, user's one public identity which is called IP Multimedia Public Identity (IMPU) needs to be registered and user's private identity which is called IP Multimedia Private Identity (IMPI) has to be authenticated by the IP Multimedia Subsystem (IMS).

The IMS authentication procedure is based on the Authentication and Key Agreement (AKA) protocol. The secret key (K) and AKA algorithms are stored in IP Multimedia Services Identity Module (ISIM) which is normally embedded on Universal Integrated Circuit Card (UICC) like a smart card based device. The IMS security is based on a long-term secret key (K) shared between ISIM and Home Network (HN) Authentication Centre (AUC). The AKA performs mutual authentication of ISIM and AUC, and generates Cipher Key (CK) and Integrity Key (IK) [7]. Section 5.2 describes the key generation and distribution process during authentication process. Section 5.3 explains the confidentiality and integrity protection procedures.

5.2 IMS Key Management Procedure

In this section we shall explain IMS AKA procedure for unregistered IP Multimedia client and successful mutual authentication with no synchronization error case. For authentication purpose, the client sends SIP REGISTER request to S-CSCF via P-CSCF and I-CSCF. This request contains User Private Identity (IMPI) and User Public Identity (IMPU). After receiving this request, the S-CSCF sends Authentication Vector Request (AV-Req (IMPI, m)) to Home Subscriber Server (HSS) for getting authentication vector (AV) vector and the HSS generates and sends an n-ordered array of AVs to S-CSCF and sequence number in AV-Req-Response. Each AV consists of CK, IK, RAND, XRES and AUTHN as given in *equation 5.1.*

$$AV = RAND || AUTN || XRES || CK || IK \tag{5.1}$$

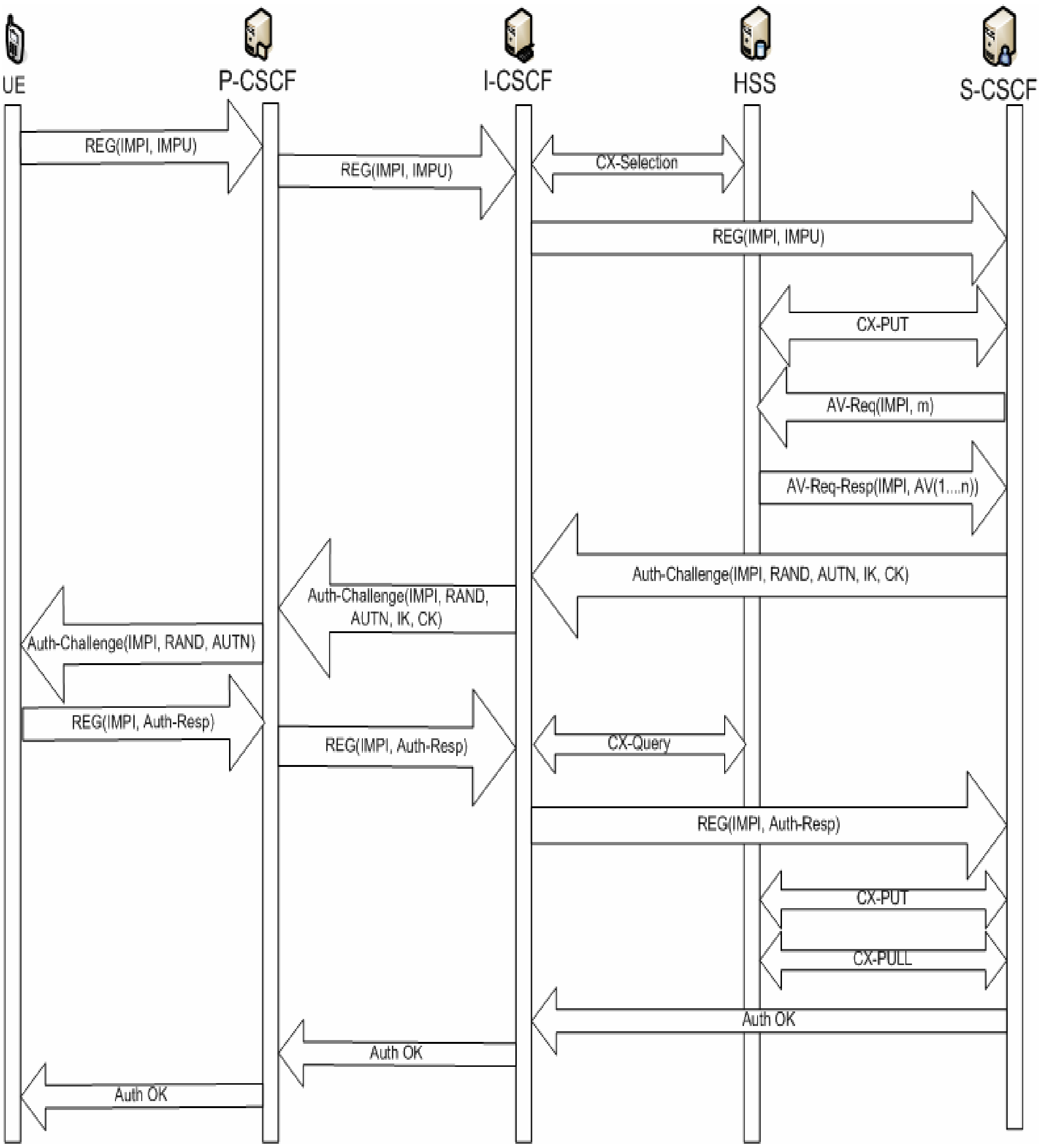


Figure 5.1 IMS Authentication Process

Each AV is required for one authentication process and is selected on first-in/first-out basis. The S-CSCF sends SIP authentication challenge (Auth-Challenge) to P-CSCF via I-CSCF and the P-CSCF stores the keys (IK, CK) and forward the remaining message (Auth-Challenge (IMPI, RAND, AUTN)) to the client. The network starts authentication procedure by using authentication request that contains a random challenge (RAND) and authentication token (AUTN).

The AUTN is calculated as:

$$AUTN = SQN + AK \oplus AMF \oplus MAC \qquad (5.2)$$

Where SQN is sequence number, $\oplus$ is XOR addition & AMP is an authentication and key management field. AK = $F5_K$ (RAND); F5 is a key generating function.

Upon receiving challenge, the client takes AUTN which includes MAC and SQN. The client calculates XMAC as given in *equation 5.3*, and verify that XMAC = MAC and SQN in correct range.

$$XMAC = F1_K\ (SQN \oplus RAN \oplus AMF) \tag{5.3}$$

If both are ok, the client calculates Auth-Response including RES and some other parameters and sends back to P-CSCF in REG (IMPI, Auth-Response) message. The client also calculates the CK and IK keys at this stage as given in *equation 5.4.*

$$CK = F3_K(RAND)\ \&\ \ IK = F4_K\ (RAND) \tag{5.4}$$

Where F3, F4 are key generating functions and RAND is a random value.

The P-CSCF forwards this response to I-CSCF which quires the HSS to find the address of S-CSCF and the I-CSCF forwards this response to the S-CSCF. The S-CSCF retrieves RES from the Response and compare with XRES [40]. If verification is successful the client has been authenticated and user's public identity (IMPU) is registered in the S-CSCF. The complete procedure is explained in *figure 5.1.*

The ISIM verifies the AUTN for network authenticity. The ISIM and the HSS keep track of sequence numbers SQN_{ISIM} and SQN_{HSS} respectively for each round of authentication procedures. If the ISIM detects an authentication whose sequence number is out of range, then it aborts the authentication and reports back to network with a synchronization failure message, including with correct sequence number [54]. This technique is used to provide for anti-replay protection. The ISIM produce authentication response (RES) as in *equation 5.5* from secret key and random challenge (RAND) in respond to network's authentication request.

$$RES = F2_K\ (RAND) \tag{5.5}$$

Where F2 is a message authentication function.

By this process the UE and home network have successfully authenticated and have established a secure communication channel. The device on which ISIM resides is a temper-resistant and only physical access to it is not sufficient to result in exposing the secret key. It is further protected by the PIN code from unauthorized access. Thus combination of ownership of physical device USIM/ISIM and knowledge of secret pin code makes the security architecture of IMS more robust [7].

5.3 Protection of Air Interface

The Gm reference point connects user to IP Multimedia Subsystem (IMS) netwrok. It is used to transport all Session Initiation Protocol (SIP) [4] signalling messages between UE and P-CSCF. The protection of this interface is very essential and therefore its security is considered very important. In IMS, NDS/IP is used to protect SIP signalling, but SIP communication at Gm interface between UE and P-CSCF is outside the scope of NDS/IP and needs additional measures for security. The IMS in 3GPP Releases 5 and 6 makes use of IPsec as the security mechanism between P-

CSCF and the UE. The Internet Protocol Security (IPsec) [55] is only one of several possible security mechanisms. The IMS was designed to allow alternative security mechanisms over the Gm interface as well. Allowing such openness usually creates backward compatibility problems because, for example, a Release 6-compliant UE would not be able to understand any alternative security mechanism, while it could be attached to P-CSCF of higher release that would already support alternatives to IPsec [7]. Therefore, the SIP Security Mechanism Agreement (Sip-Sec-Agree) [56] was introduced to allow UE and P-CSCF to negotiate a common security mechanism for use between them. For current releases the only security mechanism is IPsec; however, it might be that some entities already support alternative mechanisms on proprietary basis.

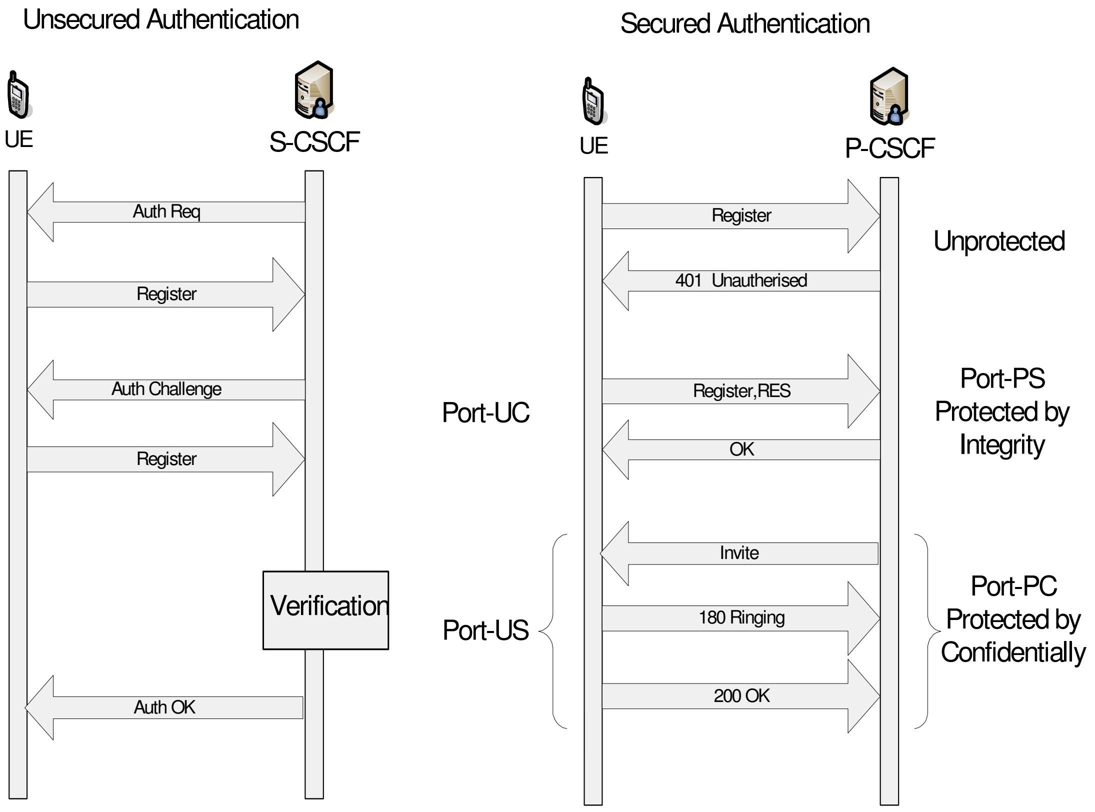


Figure 5.2 Unsecured and Secured Authentication Scenarios

During authentication of user, UE and IMS also negotiate security mechanisms for securing subsequent SIP traffic in Gm interface. SIP protocol is used for this security agreement and the UE and P-CSCF exchange their respective lists of supported security mechanisms and the highest commonly supported one is selected to provide data integrity protection. Once the security mechanism has been selected and its use started, previously exchanged list is replayed back to network in a secure fashion. This helps network to verify that the security mechanism selection was correct and the security agreement was not tampered with. An example of an attack that would be possible without this feature is bidding-down attack, where an attacker forces peers into selecting a known weak security mechanism. The IPsec ESP [57] provides both confidentially as well as data integrity and authentication which are mandatory in IMS access security. AKA session keys are used as keys for the ESP SAs i.e. IK is used as authentication key, and CK as encryption key. The AKA Protocol cannot run directly over IP and requires a vehicle to carry protocol messages between the UE and the home network. The SIP acts as vehicle for AKA protocol and it is tunnelled inside SIP and therefore IMS access is obviously to authenticate it.

5.3.1 Use of IPsec ESP for SIP Confidentiality and Integrity Protection

In order to provide the SIP Integrity protection between UE and P-CSCF, the recommended protocol is IPsec ESP (IP Security Encapsulated Security Payload) [7] which protect all SIP signalling messages at IP layer. The use of ESP for integrity protection will be applied in transport mode as shown in *figure 5.3*. In this mode TCP header, payload and padding fields are encrypted in IP packet and new ESP header which contains information like Security Parameter Index (SPI), is added between IP header and encrypted data. Finally MAC is calculated on all the data except IP header. The receiver checks integrity protection by calculating MAC and comparing with received MAC. The integrity algorithm is either Hash Message Authentication Code – Message Digest (HMAC-MD5-96) [58] or Secure Hash Algorithm (HMAC-SHA-1-96) [59]. If the selected algorithm is HMAC-MD5-96 then integrity key (IK_{ESP}) is calculated as follows which is 128 bits.

$$IK_{ESP} = IK_{IM} \tag{5.6}$$

But for other algorithm (HMAC-SHA-1-96), integrity key (IK_{ESP}) is calculated as follows to create a 160 bits key.

$$IK_{ESP} = IK_{IM} \, \| \, 32 \text{ bits zeros string} \tag{5.7}$$

In order to provide confidentiality to SIP signalling on air interface, UE and P-CSCF agree on the specific encryption algorithm, mechanism and encryption key. The IPsec ESP [60] in transport is recommended by 3GPP to provide confidentially protection of SIP signalling at Gm interface between IMS core and IMS client. The encryption algorithm is either Data Encryption Standard- Triple DES used in Cipher Block Code (DES-EDE3-CBC) [61] or Advance Encryption Standard in Cipher Block Code (AES-CBC) [62] with 128 bit key. The encryption key (CK_{ESP}) for DES-EDE3-CBC is calculated as:

$$CK_{ESP} = CK_{IM1} \, \| \, CK_{IM2} \, \| \, CK_{IM1} \tag{5.8}$$

Where CK_{IM1} (64 bits) and CK_{IM2} (64 bits) are derived from CK_{IM} (128 bits) as

$$CK_{IM} = CK_{IM1} \, \| \, CK_{IM2} \tag{5.9}$$

If the selected algorithm is AES-CBC, then encryption key (CK_{ESP}) is as:

$$K_{ESP} = CK_{IM}$$

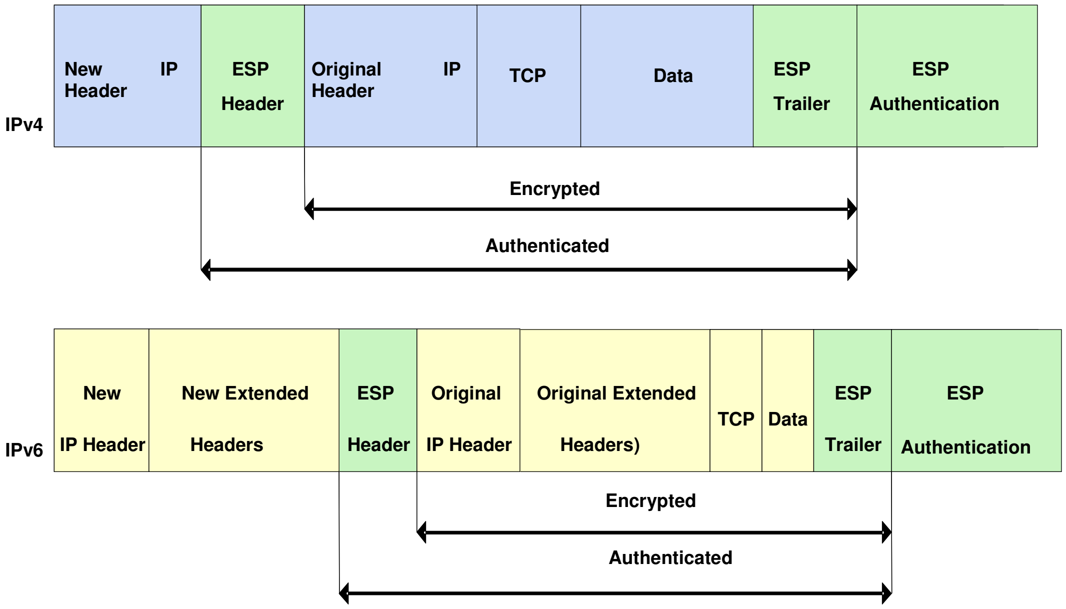


Figure 5.3 ESP Header Format

5.3.2 SIP Integrity and Confidentiality Procedure

Now we discuss the procedure to set-up security associations between client (UE) and P-CSCF for the protection of Gm interface. The client sends security-setup message in the REG (Sec-Setup = SPI-U, Port-U, UE I & E Algorithms List) message as shown in *figure 5.4.*

Where SPI-U = (SPI-UC, SPI-US); pair of Security Parameter Index values that client selects.

Port-U = (Port-UC, Port-US); pair of protected ports numbers of clients and server.

UE I & E Algorithms List = List of Integrity and Encryption Algorithms Identifiers that client supports.

Upon receipt of this message, P-CSCF stores security parameters along with client's IMPI, IMPU and IP address and adds keys IK_{IM} and CK_{IM} received from S-CSCF. Next the P-CSCF sends Auth-Challenge (Sec-Setup = SPI-P, Port-P,P-CSCF I & E Algorithms List) to client.

Where SPI-P = (SPI-PC, SPI-PS); pair of Security Parameter Index values that P-CSCF selects.

Port-P = (Port-PC, Port-PS); pair of protected ports numbers of clients and server.

P-CSCF I & E Algorithms List = List of Integrity and Encryption Algorithms Identifiers that P-CSCF supports.

The client then sends final security setup message as REG (Sec-Setup = SPI-U, Port-U, SPI-P, Port-P, P-CSCF I & E Algorithms List) to P-CSCF and it checks whether these parameters are same. If they match registration is successful. Finally P-CSCF sends REG (Integrity-Protection=Successful, Confidentiality-Protection=Successful, IMPI) to S-CSCF to inform that client messages are integrity and confidentiality protected [54].

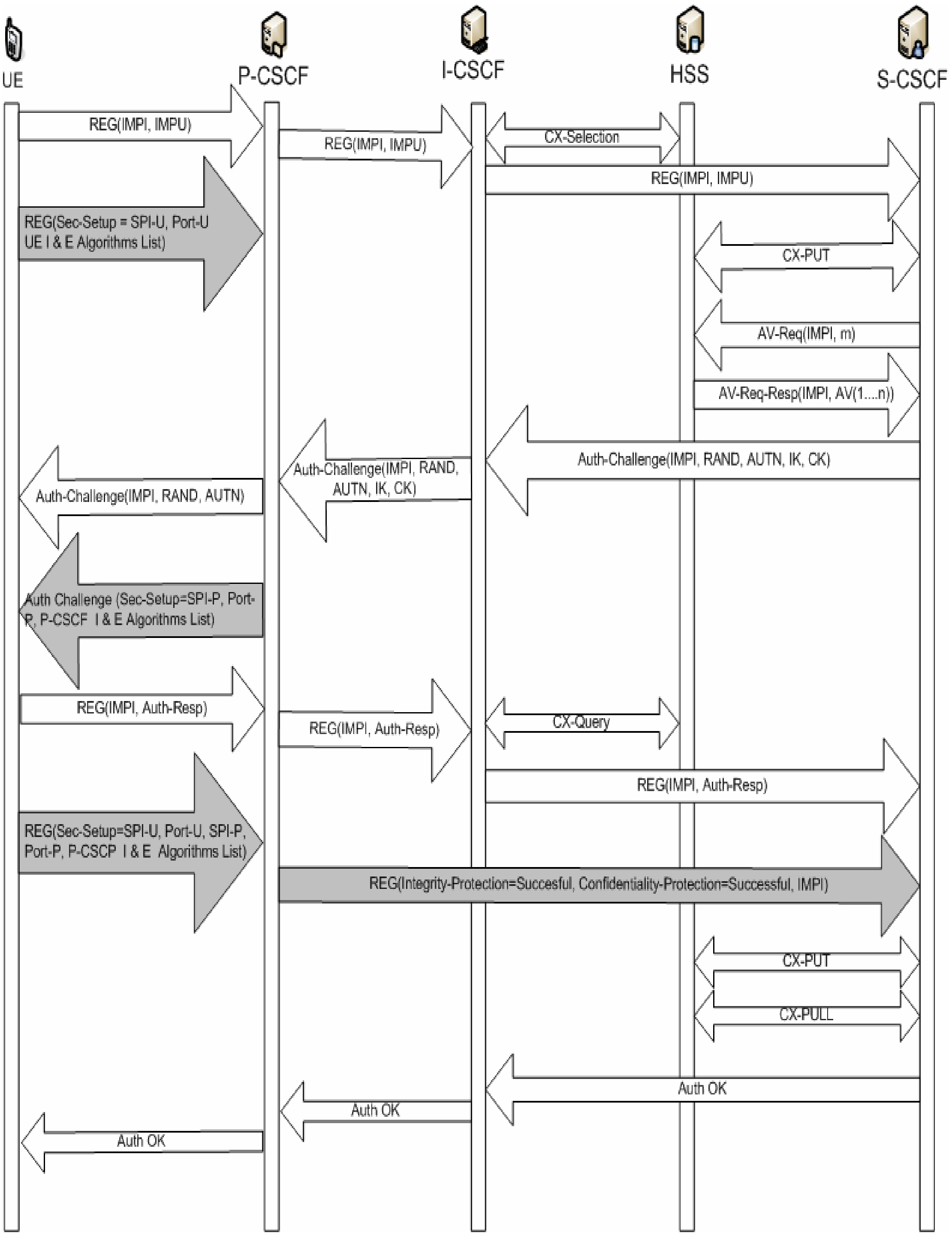

UE
P-CSCF
I-CSCF
HSS
S-CSCF
REG(IMPI, IMPU)
REG(IMPI, IMPU)
CX-Selection
REG(IMPI, IMPU)
REG(Sec-Setup = SPI-U, Port-U UE I & E Algorithms List)
CX-PUT
AV-Req(IMPI, m)
AV-Req-Resp(IMPI, AV(1....n))
Auth-Challenge(IMPI, RAND, AUTN, IK, CK)
Auth-Challenge(IMPI, RAND, AUTN, IK, CK)
Auth-Challenge(IMPI, RAND, AUTN)
Auth Challenge (Sec-Setup=SPI-P, Port-P, P-CSCF I & E Algorithms List)
REG(IMPI, Auth-Resp)
REG(IMPI, Auth-Resp)
CX-Query
REG(IMPI, Auth-Resp)
REG(Sec-Setup=SPI-U, Port-U, SPI-P, Port-P, P-CSCP I & E Algorithms List)
REG(Integrity-Protection=Succesful, Confidentiality-Protection=Successful, IMPI)
CX-PUT
CX-PULL
Auth OK
Auth OK
Auth OK

Figure 5.4 Authentication with Integrity and Confidentiality Protection

5.4 Summary

This chapter presented IMS authentication and key agreement (AKA) procedure for user and network authentication, the generation and secure transfer of confidentiality and integrity keys. The used of these key and related protocols to provide confidentiality and data integrity on Gm interface is discussed in detail.

Chapter 6 IMS Inter-Domains Security

6.1 Introduction

The IP Multimedia Subsystem (IMS) supports communication between home network and visited network, creating two scenarios weather IMS terminal is in home network or roaming. In first scenario UE's first point of contact to IMS, called P-CSCF is located in home network and in the second scenario the P-CSCF is located in visited network (roaming) as depicted in *figure 6.1*. The traffic between the visited and home network are protected using Network Domain Security/Internet Protocol (NDS/IP) at IP layer [63]. The NDS/IP only protects traffic between network elements in IP layer.

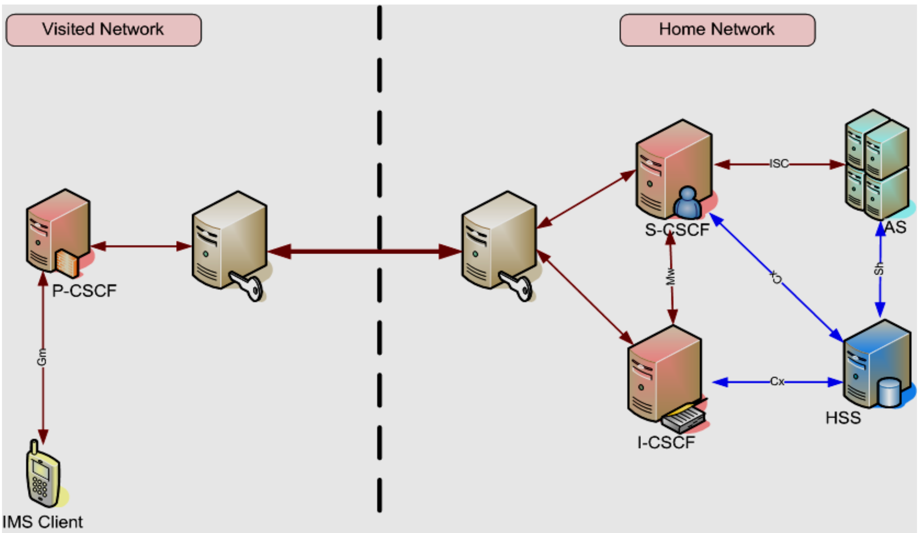


Figure 6.1 IMS Roaming User

A security domain is a network operated by a single administrative authority that implements a uniform security policy within that domain. As a result the level of security will be the same within a security domain. Mostly the security domain is related directly to an operator's core network but it is however possible to run several security domains making subset of operator's entire core network. IMS protects all IP traffic in the core network using NDS/IP which provides confidentially, data integrity, authentication and anti-replay protection for traffic using combination of cryptographic security mechanisms and protocol security mechanisms applied in IP security (IPsec). In NDS/IP platform the interfaces between elements inside security domain are denoted by Zb and interfaces between different security domains are denoted by Za as shown in *figure 6.2*. Use of Za interface is always mandatory between different security domains while use of Zb interface is optional and up to the security domain's administrator. Data authentication and integrity is mandatory for both interfaces, while use of encryption is recommended for Za and optional for Zb.

The NDS/IP is used to protect operators IMS Core Network as well as traffic between visited and home network. The fundamental idea of NDS/IP architecture is to provide hop-by-hop security, according to the *chained-tunnels* or *hub-and-spoke* models of operation. And utilizing hop-by-hop security also makes it easy to maintain separate security policies internally, and towards other external security domains. The Network Entities (NEs) establish and maintain ESP (Encapsulated Security Payload) Security Associations (SAs) as needed towards a SEG (Security Gateway) or other NEs within the same security domain. All NDS/IP traffic from NE in one security domain towards NE in other security domain is routed via SEG, and will receive hop-by-hop security protection towards the final destination [63].

The operators may decide to establish only one ESP Security Association between two communicating security domains, which will lead to coarse-grained security granularity. This has a benefit that a certain measure of protection against traffic flow analysis is given. But the disadvantage is that it is not possible to differentiate the security protection provided between the communicating entities. This does not preclude negotiation of finer grained security granularity at the discretion of the communicating entities.

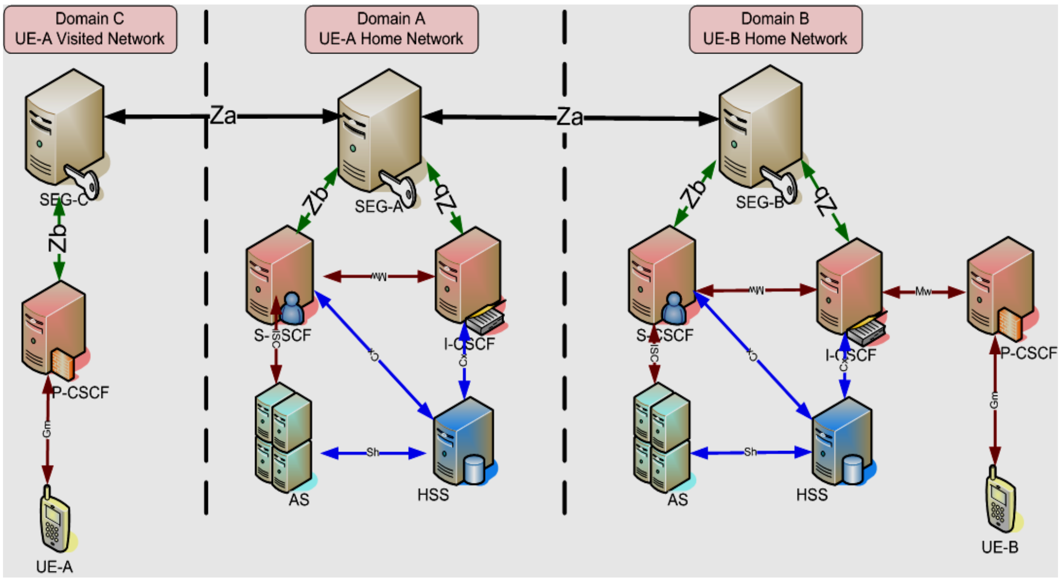


Figure 6.2 Visited and Home Network Scenarios

6.2 Network Domain Security (NDS) Architecture

Network domain is a network controlled by single operator or administrator authority to implement uniform security policy within the domain. Hence, the level of security and the available security services will be the same within security domain. The domain security is applied on the border of operator's network and protected by Security Gateways (SEGs) [63] which are responsible to enforce security policy of security domain towards other security domain's SEGs.

The NDS/IP is used to protect the operators IMS core network as well as the traffic between the visited and home network. The fundamental idea of the NDS/IP architecture is to provide hop-by-hop security, according to the *chained-tunnels* or *hub-and-spoke* models of operation. By utilizing hop-by-hop security helps to maintain separate security policies internally and towards other external security domains [64]. In NDS/IP, Security Gateways maintain IPsec secure ESP (Encapsulated Security Payload) Security Associations in tunnel mode between security domains. All NDS/IP traffic from network entities of security domain is routed via SEG to other security domain using hop-by-hop security protection to the end destination.

Different entities and interfaces of network domain security architecture are given below:

6.2.1 NDS Interfaces

As we know that security between different domains is implemented by NDS/IP protocol through Security Gateways (SEGs). The interfaces between security domains are represented as *Za* while the interfaces within the security domain are represented as *Zb* as shown in *figure 6.3*. Za-interface covers all NDS/IP traffic between security domains.

For Za-interface, authentication and data integrity protection is required and data encryption is recommended. These three security features are implemented by using ESP (Encapsulated Security Payload) protocol [57] and SEGs use IKE (Internet Key Exchange) to negotiate, establish and maintain secure ESP tunnel between them for forwarding NDS/IP traffic between security domains. The security policy over Xa-interface depends upon the roaming agreement.

For Zb-interface, authentication and data integrity protection is required and implemented by using ESP protocol. Data encryption is optional on this interface and depends upon the decision of security domain operator.

6.2.2 Security Gateways (SEGs)

Security Gateways (SEGs) are network entities on the borders of IP security domains, providing security to IP based protocols and establish the communication over the Za-interface. All NDS/IP traffic goes through SEG before entering or leaving the security domain. A security domain can have more than one SEG and it depends upon number of destinations, avoid single point failure and traffic load balancing etc. Each SEG is defined to handle NDS/IP traffic by well-defined rules to reach IP security domain.

When protecting inter-domain IMS traffic it is mandatory to provide confidentiality, data integrity, and authentication in the NDS/IP. The security gateways enforce the security policies for the interworking between networks. The security may include filtering policies as well as firewall functionality. The SEGs are responsible for security sensitive operations and need to be physically secured.

As we have discussed the SEGs establish and maintain an IPsec secured ESP Security Association in tunnel mode between security domains. The SEG will normally provide at least one IPsec tunnel at all times to a particular peer SEG. Each SEG is responsible for setting up and maintaining IPsec security associations (SAs) with its peer SEGs. These SAs are negotiated using the Internet Key Exchange (IKE) [65] protocol, where authentication is done using long term keys stored in the SEGs. Each SEG maintains two SAs per connection: one for inbound traffic and other for outbound traffic. In addition, it maintains a single Internet Security Association and Key Management Protocol (ISAKMP) SA [66] for key management. The prerequisite for the ISAKMP SA is that the peers should be authenticated. In the NDS/IP, authentication is based on pre-shared secrets. The architecture for SEGs is presented in *figure 6.3.*

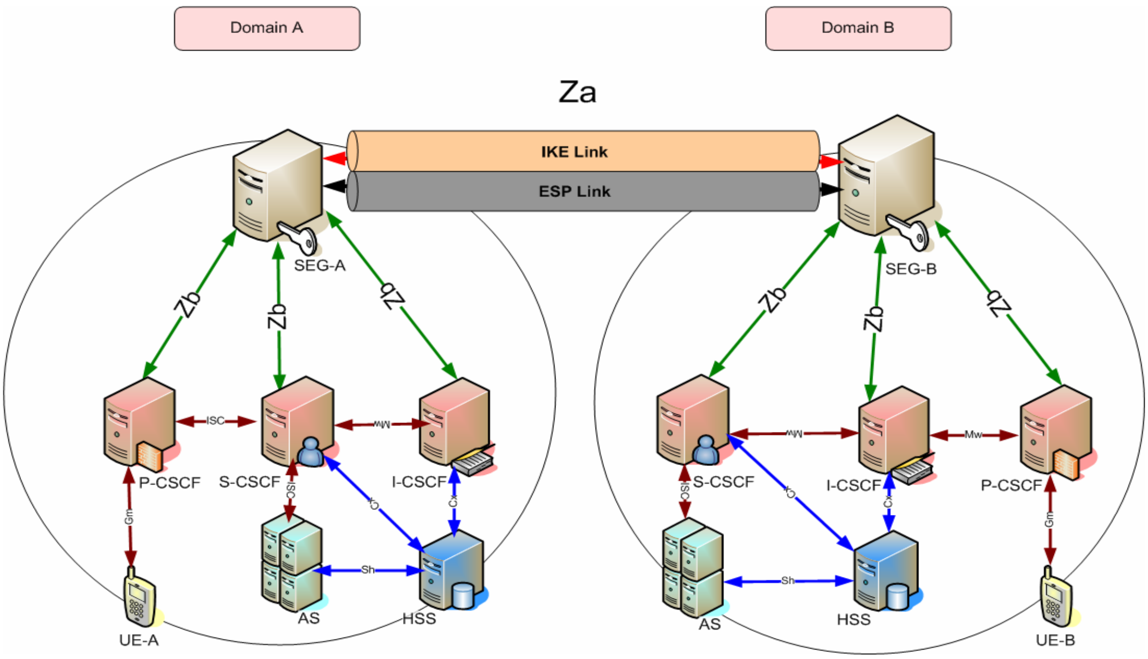


Figure 6.3 Security Gateways Architecture

The SEG will maintain logically separate Security Associations Database (SAD) and Security Policy Database (SPD) for each interface [63]. Their functionalities are given below:

6.2.2.1 Security Policy Database (SPD)

It contains the policies by which all inbound and outbound traffic is categorized by security gateways. In general, packets are selected for one of three processing modes based on IP and transport layer header information matched against entries in the database (SPD). A packet is either afforded IPsec security services, discarded, or allowed to bypass IPsec, based on the applicable database policies identified by the selectors.

6.2.2.2 Security Associations Database (SAD)

It is a container for all active SAs, and related parameters. A set of selectors—IP layer and upper layer (e.g., TCP and UDP) protocol field values—is used by the SPD to map traffic to a specific SA. This relationship is represented by a set of information that can be considered as a contract between the SEGs. The information must be agreed upon and shared between all the SEGs. All SEGs must adhere to the SA for secure communications to be possible. When accessing SA attributes, SEGs use a pointer or identifier referred to as the Security Parameter Index (SPI) [63].

6.3 Use of IPsec in NDS/IP Environment

This section provides an overview of the features of IPsec that are used by NDS/IP and defines a minimum set of features that must be supported. The security services provided by NDS/IP are data integrity, data origin authentication, anti-replay protection and limited protection against traffic flow analysis and confidentiality. IPsec provides security services at the IP layer by enabling a system to select the required security protocols, determine the algorithms to be use for the service, and to provide the cryptographic keys required for the requested services. It can be used to protect one or more links between a pair of SEGs, or between a SEG and a host. The set of security services that IPsec can provide includes access control, connectionless integrity, data origin authentication, rejection of replayed packets and confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol. The components of the IPsec security architecture are:

6.3.1 Security Protocols

The IPsec uses two protocols to provide traffic security i.e. Authentication Header (AH) and Encapsulating Security Payload (ESP). These protocols may be applied alone or in combination with each other to provide a desired set of security services in Ipv4 and Ipv6. Each protocol supports two modes of use i.e. *transport mode* and *tunnel mode*.

In transport mode the protocols provide protection primarily for upper layer protocols. Tunnel mode is typically used to tunnel IP traffic between two SEGs. The difference is that in transport mode IPsec offers limited protection to IP headers, whereas in tunnel mode the full IP datagram is protected.

The security protocol used in the NDS/IP for encryption, data integrity protection and authentication is the IPsec Encapsulating Security Payload (ESP) [57] in tunnel mode i.e. the full IP datagram, including the IP header, is encapsulated in the ESP packet. The ESP provides confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and limited traffic flow confidentiality. The set of services provided depends on options selected at the time of security association establishment and on the placement of the implementation. The anti-replay service may be selected only if data origin authentication is selected, and its selection is solely at the discretion of the receiver [57].

The ESP is used to provide security services in IPv4 and IPv6. To process outbound traffic, a host or security gateway first uses a set of selectors in the SPD to determine the outbound SA used. It then follows a set of steps to process the outbound packet:

- The entire original outbound IP datagram is encapsulated in an ESP payload field in tunnel mode.
- Appropriate padding is added to the payload data.
- The results are encrypted using an encryption key and an algorithm.
- The sequence number is incremented as appropriate.
- If authentication is enabled, then the ICV is calculated.
- Possible fragmentation of the IP datagram is performed

On receiving an IP datagram the recipient follows the following steps to process the packet:

- Possible reassembly of the IP datagram is performed.
- Using the SPI, security protocol and destination IP address, an appropriate SA is looked up from the SAD.
- If anti-replay protection is enabled, the sequence number is inspected.
- If authentication is enabled, then the ICV is verified.

The packet is decrypted, padding is removed and the original IP datagram is reconstructed. The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. The ESP header is inserted before an encapsulated IP header in tunnel mode. Thus the format of ESP packets for a given SA is fixed, for the duration of the SA. The tunnel mode ESP is employed by the SEGs to protect transit traffic. The *inner* IP header carries the ultimate source and destination addresses, while an *outer* IP header may contain distinct IP addresses usually addresses of security gateways. In tunnel mode, ESP protects the entire inner IP packet, including the entire inner IP header [66].

If authentication is selected, encryption is performed first, before the authentication, and the encryption does not encompass the Authentication Data field. This order of processing facilitates rapid detection and rejection of replayed or counterfeit packets by the receiver, prior to decrypting the packet, hence potentially reducing the impact of *denial of service attacks*. It also allows for the possibility of parallel processing of packets at the receiver, hence decryption can take place in parallel with authentication.

6.3.2 Security Associations

The concept of a security association is germane to IPsec. A security association (SA) is a set of policy and key(s) used to protect information and is defined as the relationship between two SEGs that allows the protection of information communicated between them and that defines how they are going to use security services to secure their communications. It includes information on authentication and/or encryption algorithms, cryptographic keys and key lengths as well as the initialization vectors (IV) that are shared between the entities. A SA is unidirectional; so typically two SAs are needed for a bidirectional flow of traffic—one for inbound (read) traffic and one for outbound (write) traffic. Security protocols make use of security associations (SAs) as they provide security services. This relationship includes a shared symmetric key and security attributes describing the relationship. It is uniquely identified by security parameter index (SPI) [57] and destination IP address.

With regard to the use of IPsec security associations in the network domain of NDS/IP-networks, the NDS/IP requires support for tunnel mode IPsec SAs and support for ESP SAs. The specification of IPsec SAs is available in RFC-2401 [55].

With regard to the use of ISAKMP security associations in the network domain of NDS/IP-networks, the NDS/IP only requires support for ISAKMP SAs with pre-shared keys. The specification of ISAKMP SAs is available in RFC-2408 [66].

6.3.3 Key Management

The process for the distribution of cryptographic keys to be used with the security protocols (namely, the Internet Key Exchange (IKE)) is called key management. In the IMS/UMTS network domain security architecture, the key distribution between SEGs is handled by IKE protocol [66]. The main purpose of IKE is to negotiate, establish and maintain Security Associations between network entities that are used to establish secure communications. The IKE automatically negotiates IPsec security associations (SAs) and enables IPsec secure communications [65].

There are two basic methods used to establish an authenticated key exchange i.e. *Main Mode* and *Aggressive Mode*. Each mode generates authenticated keying material from an ephemeral Diffie-Hellman exchange. *Main Mode* must be implemented but *Aggressive Mode* should be implemented. In addition, *Quick Mode* must be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services and *New Group Mode* should be implemented as a mechanism to define private groups for Diffie-Hellman exchanges [60].

Specifically, IKE provides the following benefits:

- It eliminates the need to manually specify all the IPsec security parameters in the crypto maps at both peers.
- IKE allows specifying a lifetime for the IPsec security association.
- It allows encryption keys to change during IPsec sessions.
- IKE allows IPsec to provide anti-replay services.

- It permits Certification Authority (CA) support for a manageable, scalable IPsec implementation.

- IKE allows dynamic authentication of peers.

The Internet Key Exchange protocol is used for negotiation of IPsec SAs with the following additional requirement for inter-security domain SA negotiations over the Za-interface [67].

6.3.3.1 IKE phase-1 (ISAKMP SA)

- The use of pre-shared secrets for authentication will be supported [68];

- Only ISAKMP Main Mode will be used;

- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;

- Support of 3DES in CBC mode [69] shall be mandatory for confidentiality;

- Support of AES in CBC mode [62] shall be mandatory for confidentiality;

- Support of SHA-1 [59] shall be mandatory for integrity/message authentication;

- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange [70].

Phase-1 IKE SAs shall be persistent with respect to the IPsec SAs i.e. IKE SAs shall have a lifetime for at least the same duration, as does the derived IPsec SAs. The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires [68].

6.3.3.2 IKE phase-2 (IPsec SA)

- Perfect Forward Secrecy is optional;

- Only IP addresses or subnet identity types shall be mandatory address types;

- Support of Notifications shall be mandatory;

- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange.

6.3.4 Encryption and Authentication Algorithms

To implement the IMS inter-domain security, 3GPP recommends for encryption, the Triple DES (3DES) [69] algorithm is mandatory, while for data integrity and authentication both MD5 [71] and SHA-1 [59] can be used. IPsec offers set of confidentiality transforms supports including ESP_NULL and ESP_DES transforms. However, Data Encryption Standard (DES) algorithm is no longer considered sufficiently strong in terms of cryptographic strength. It is mentioned by IESG in RFC 2407 [72] that the ESP_DES transform is likely to be deprecated in the near future. It is therefore explicitly recommended in NDS/IP that ESP_3DES algorithm is mandatory instead of ESP_DES. Also the support for AES-CBC cipher algorithm [62] is mandatory with key length of 128 bits.

IPsec offers data integrity transforms that compliant IPsec implementation is required to support are the ESP_NULL, the ESP_HMAC_MD5 and the ESP_HMAC_SHA-1 transforms. For NDS/IP traffic ESP shall always be used to provide integrity, data origin authentication, and anti-replay services, thus the ESP_NULL authentication algorithm is explicitly not allowed for use. ESP shall support ESP_HMAC_SHA-1 algorithm in NDS/IP.

6.4 Public Key Infrastructure (PKI)

Public key cryptography, also known as asymmetric cryptography, utilizes a pair of keys, one is private and other is public which are mathematically related. Information is encrypted with the public key, and can only be decrypted with the corresponding private key. In this system, the public keys of all users are published in an open directory, facilitating communications between all parties. The private key is not shared, only the public key is made public. Public key cryptography can also be used to create and verify digital signatures by changing the key order by encryption and decryption [70]. These can be appended to messages to provide proof of authentication, integrity and non-repudiation. The PKI Forum has provided PKI Technical Perspective [73] to use PKI technology in specific vendor environment, addressing the following issues [64]:

- Security policies that define the rules under which the cryptographic systems should operate;
- Procedures to generate, store and manage the keys; and
- Procedures how the keys and certificates are generated, distributed and used.

A Public Key Infrastructure is a combination of policies and procedures, hardware and software. PKI is based on digital IDs known as ‘digital certificates’ that bind the user’s digital signature to his or her public key. PKI consists of the following components.

6.4.1 Security Policy

A security policy sets out and defines the top-level direction on information security, as well as the processes and principles for the use of cryptography. Typically it will include statements on how to handle keys and valuable information, and will set the level of control required to match the levels of risk.

6.4.2 Certification Authority (CA)

The CA system is the trust basis of a PKI, since it manages public key certificates for their whole life cycle. The CA performs the following tasks:

- It issues certificates by binding the identity of a user or SEG to a public key with a digital signature;
- CA schedules expiry dates for certificates;
- It ensures publishing Certificate Revocation Lists (CRLs) revoke certificates when necessary.

The PKI must ensure that the CA's private key is held in a tamper-resistant security module, and provision must be made for back-up copies for disaster recovery purposes. Access to the CA and RA should be tightly controlled. All certificate requests should be digitally signed to detect and prevent hackers from deliberately generating counterfeit certificates. All significant events performed by the CA system should be recorded in a secure audit trail, where each entry is time/date stamped and signed, to ensure that entries cannot be falsified.

The trust relationship between two authorities is establishes by cross-certification. When Certification Authority A is cross-certified with Certification Authority B, this implies that A has chosen to trust certificates issued by B. The cross-certification process enables the users under both authorities to trust the other authority's certificates. Trust in this context equals being able to authenticate. There are two types of cross-certification processes:

6.4.2.1 Manual Cross-certification

In manual cross-certification, mutual cross-certifications are established directly between the Certification Authorities. The authority makes decisions about trust locally. When a Certification Authority A chooses to trust a Certification Authority B, then authority A signs the certificate of the authority B and distributes the new certificate (B's certificate signed by A) locally. The disadvantage of this approach is that it often results in scenarios where there need to be a large number of certificates available for the entities doing the trust decisions: There needs to be a certificate signed by the local Certification Authority for each security domain with which the local authority wishes to trust. However, all the certificates can be configured locally and are locally signed, so their management is often flexible.

6.4.2.2 Bridge Cross-certification

The Bridge CA is a concept that reduces the number of certificates that need to be configured for the entity that does the certificate checking. When two authorities are mutually cross-certified with the bridge, the authorities do not need to know about each other. Authorities can still trust each other because the trust in this model is transitive i.e. A trusts bridge, bridge trusts B, thus A trusts B and vice versa. The bridge CA acts like a bridge between the authorities and the two authorities shall also trust that the bridge CA is trusted and secure. Bridge CA style cross-certifications are useful in scenarios where all entities communicate a common Trusted Third Party. If an authority needs to restrict the trust or access control derived from the Bridge CA, it additionally needs to implement those restrictions [68].

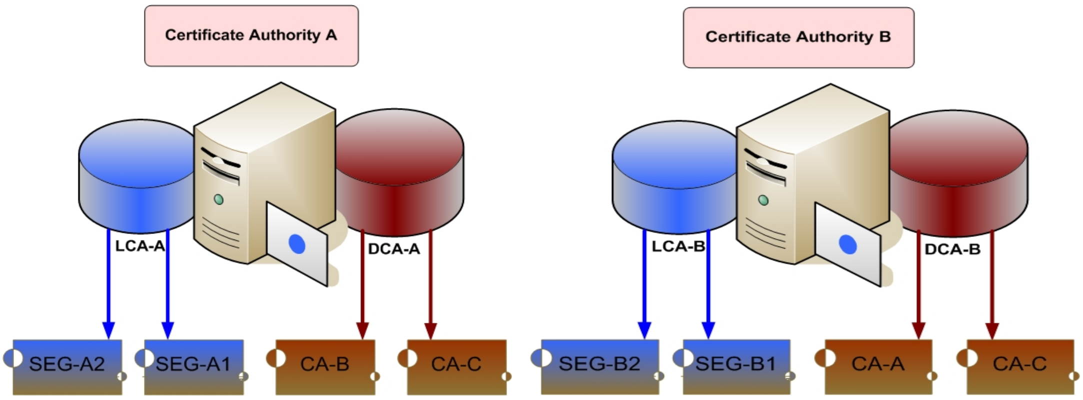


Figure 6.4 Security Gateways Architecture

6.5 PKI Based NDS Authentication Framework

This section explain the implementation of PKI based Network Domain Security/Authentication Framework which uses a simple access control method, i.e. each element that is authenticated also provides a service. The architecture uses direct cross-certifications between the security domains, which enables easy policy configurations in the SEGs [68]. Each security domain has at least one Local Certificate Authority (LCA) and one Domain Certificate Authority (DCA) as shown in *figure 6.4*. Their functionality is given as:

- The LCA of the domain issues certificates to the SEGs in the domain that have interconnection with SEGs in other domains.
- The DCA of the domain issues certificates to the LCAs of other domains with which the operator’s SEGs have interconnection.
- All the certificates are based on the Internet X.509 certificate profile [74].

The LCA issues certificates for SEGs that implement the Za interface. When SEG of the security domain A establishes a secure connection with the SEG of the domain B, they are able to authenticate each other. The mutual authentication is checked using the certificates the LCAs issued for the SEGs. When a roaming agreement is established between the domains, the DCA cross-certify the LCA of the peer operator. The created cross-certificates need only to be configured locally to each domain.

The cross-certificates issue by DCA-A of security domain A for the LCA of security domain B, will be available for SEG of domain A which implements the Za interface towards domain B. Similarly, the cross-certificates issue by DCA-B of security domain B for the LCA of security domain A will be available for SEG of domain B which implements the Za interface towards domain A. After cross-certification, the SEG-A is able to verify the following path (*figure 6.5*):

SEG-B → LCA-B → DCA-A

Similarly, the SEG-B is able to verify the path:

SEG-A → LCA-A → DCA-B

If the verification process is satisfied then both domains A and B can trust each other and use the certificates for each others.

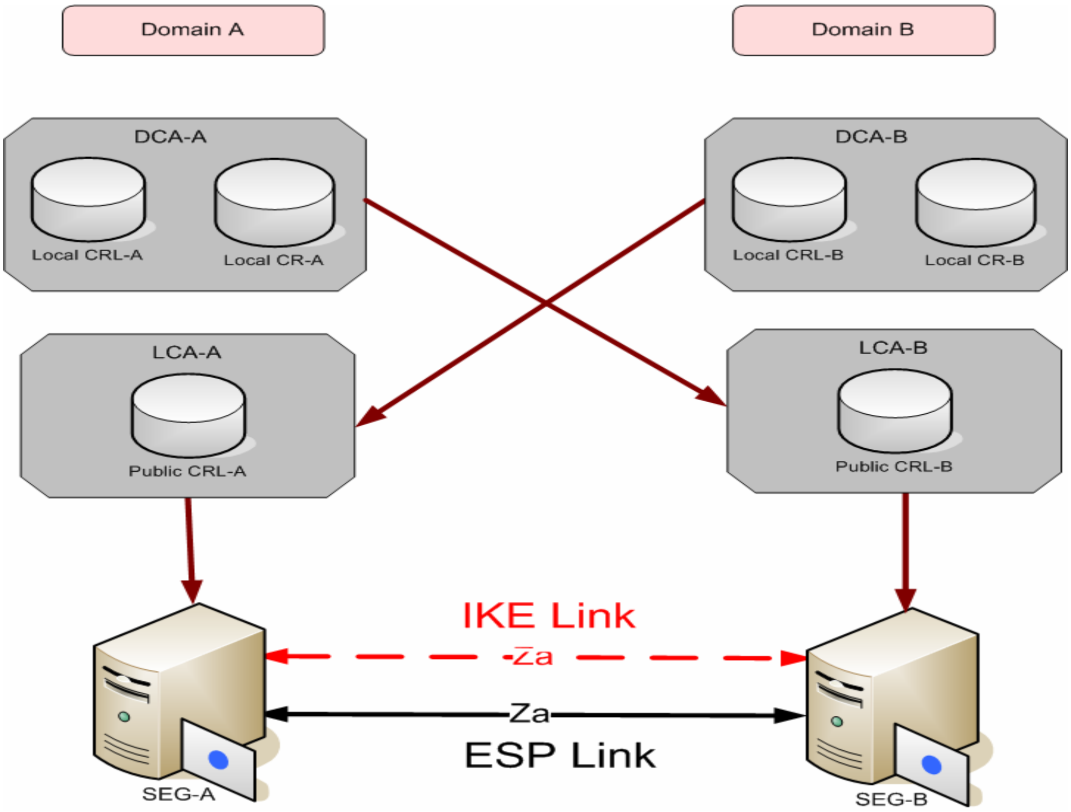


Figure 6.5 Distribution of Certificates

The public key of the DCA is stored securely in each SEG within the operator's domain. This allows the SEG to verify cross certificates issued by its operator's DCA. It is assumed that each operator domain could include 2 to 10 SEGs. An operator may decide to set up both LCA and DCA as a single CA, i.e. separation of CAs is not required. The NDS/AF is initially based on a simple trust model that avoids the introduction of transitive trust and/or additional authorisation information. The simple trust model implies manual cross-certification [68]. Now we discuss the design use cases of NDS/AF.

6.5.1 Creating/Terminating Roaming Agreement

When a roaming agreement is required, the SEGs of two different domains establish the secure tunnel using cross-certificates issued by DCA of two domains. The creation of a roaming agreement only involves use of the private keys of the DCAs. There is no need for the operators to use the private keys of their respective LCAs in forming a roaming agreement.

When creating the new cross-certificate, the DCA set the path length to zero to initiate that the new cross-certificate to be used in signing new CA certificates. When the new cross-certificate is available to the SEG, its information are configured in the SEG. The authentication can be done based on the created cross-certificates.

When a roaming agreement is terminated or due to an urgent service termination need, all concerned SEG peers will remove the IPsec SAs using device-specific management methods. Each concerned operator will also list the cross-certificate created for the DCA of the terminated operator in his local Certificate Revocation List (CRL) [68].

6.5.2 Creating VPN Tunnel

After establishing a roaming agreement and finishing the required certificate management operations, the operators configure their SEGs for SEG-SEG connection, and the SAs are established as specified by NDS/IP. In each connection configuration, the remote SEG DNS name or IP address is specified. Only the local DCA and LCA are configured as trusted CAs [68]. Because of the cross-certification, any operator who's LCA has been cross-certified can get access using this VPN connection configuration.

Now we discuss the flow of connection negotiation as mentioned in [68] from SEG-A which is initiator. The SEG-B, which is responder, will perform the same function.

- During connection initiation, the initiating SEG-A provides its own SEG certificate and the corresponding digital signature in IKE Main Mode message 3;
- SEG-A receives the remote SEG-B certificate and signature;
- SEG-A validates the remote SEG-B signature;
- SEG-A verifies the validity of SEG-B certificate by a CRL check to both the Operator A and Operator B CRL databases. If a SEG cannot successfully perform both CRL checks, it assumes as an error and abort tunnel establishment;
- SEG-A validates SEG-B certificate using the cross-certificate for LCA-B by executing the following actions:

    1. SEG-A verifies the validity of the cross-certificate for LCA-B by a CRL check to the DCA-A CRL database. If a SEG cannot successfully perform the CRL check, it will assume as an error and abort tunnel establishment;

2. SEG-A validates the cross-certificate for LCA-B using its DCA certificate if DCA is not a top-level CA, otherwise DCA public key is implicitly trusted.

In this way, the IKE Phase 1 SA is established and the Phase-2 SA negotiation proceeds as described in NDS/IP with PSK authentication.

6.5.3 Certificate Profiles

Before fulfilling any signing certificate request, the LCA and DCA will make sure that the request meets the following certificates profiles criteria:

- Certificates of version 3 are in use according to RFC 3280 [75];
- Support of SHA-1 has algorithm;
- For DCA and LCA certificates, the RSA key length will be at least 2048-bits
- For SEG certificate, the RSA key length will be at least 1024-bits

6.5.4 SEG Certificates Validation

During VPN tunnel establishment, each SEG has to verify the validity of its peer SEG certificate. SEG-A verify the validity of cross-certificate of LCA-B and certificate of SEG-B and it will be able to fetch the cross-certificate of LCA-B. SEG-B performs the same process for the validity of SEG-A certificates. At this point, the VPN tunnel is not yet available; therefore, the CRL of the peering LCA will be accessible for SEG without utilizing the Za-interface. *Figure 6.5* shows the repositories in which local CR contains cross-certificates for LCA, the local CRL contains LCA cross-certificate revocation and the public CRL contains of SEG and LCA certificates and can be accessed by other domains.

6.6 Summary

This chapter discussed the protocols, architecture and the design of Network Domain Security (NDS) model for IP Multimedia Subsystem (IMS). The architecture of IMS-NDS is based on Network Domain Security/Internet Protocol (NDS/IP) which is deployed by Domain Security Gateways (SEGs). NDS/IP utilizes IP Security (IPSec) to implement security domain services. The 3GPP Authentication Framework (AF) is introduced to authenticate the Security Gateways using NDS/IP that utilizes cryptographic security mechanisms and security protocols provided by the IP Security (IPSec) protocol. PKI is used to generate, manage and distribute digital certificates and keys in NDS/IP environment.

Chapter 7 Security Management for HTTP-Based Services

7.1 Introduction

The Ut interface is reference point between the User Equipment (UE) and Application Server (AS) that enables users to securely manage and configure their network services-related information hosted on an AS. Users can use Ut reference point to create public service identities, such as a resource list, and manage authorization policies that are used by the service. Examples of services that utilize the Ut reference point are presence and conferencing. The AS may need to provide security for the Ut reference point. HTTP is chosen data protocol for the Ut reference point that performs the functionality to manage data traffic for HTTP based applications. Thus securing the Ut interface means to achieve confidentiality and data integrity protection of HTTP-based traffic.

The authentication and key agreement for Ut interface is also based on AKA. The IMS defines Generic Bootstrapping Architecture (GBA) [49] as a part of Generic Authentication Architecture (GAA) that performs mutual authentication between Bootstrapping Server Functions (BSF) and the UE. AKA generates session keys and enable further applications provided by the Network Application Function (NAF) that issues subscriber certificates using an applications protocol secured by bootstrapped session keys. The authentication in Ut interface is performed by authentication proxy. In terms of GBA, the authentication proxy is another type of NAF. Traffic in Ut interface goes through authentication proxy and is secured using the bootstrapped session key.

The Ut interface employs Transport Layer Security (TLS) [50] for both confidentiality and integrity protection. It utilized generic bootstrapping architecture to assure that the request is coming from an authorized subscriber of mobile network operator. When HTTPS request is sent to AS through Authentication Proxy (AP) that performs UE authentication. The AP may insert the user identity when it forwards the request to application server. *Figure 7.4* presents the architectural view of using AP for different IMS SIP services e.g. presence, messaging, conferencing etc.

7.2 Generic Bootstrapping Architecture (GBA)

Different 3G Multimedia Services including video conferencing, presence, push-to-talk and messaging etc. has potential usage of Generic Bootstrapping Architecture (GBA) to distribute subscriber certificates. These certificates are used by mobile operators to authenticate the subscriber before accessing the multimedia services and applications. Now we discuss components, entities and interfaces of GBA.

7.2.1 GBA Components and Entities

The GBA consists of five entities: UE (User Equipment), NAF (Network Authentication Function), BSF (Bootstrapping Server Function) and HSS (Home Subscriber Server) which are briefly explained below and shown in *figure 7.1.*

7.2.1.1 User Equipment (UE)

The UE is UICC (Universal Integrated Circuit Card) containing USIM or ISIM related information that supports HTTP Digest AKA (Authentication & Key Agreement) and NAF (Network Authentication Function) specific protocols. A USIM (Universal Subscriber Identity Module) is an application for UMTS mobile telephony running on a UICC smartcard which is inserted in a 3G mobile phone. It stores user subscriber information, authentication information and provides with storage space for text messages. An IP Multimedia Services Identity Module (ISIM) is an application running on a UICC smartcard in a 3G telephone in the IP Multimedia Subsystem (IMS). It contains parameters for identifying and authenticating the user to the IMS. The ISIM application can co-exist with SIM and USIM on the same UICC making it possible to use the same smartcard in both GSM networks and earlier releases of UMTS.

7.2.1.2 Network Authentication Function (NAF)

The NAF has the functionality to locate and communicate securely with the subscriber's BSF (Bootstrapping Server Function). It should be able to acquire a shared key material established between the UE and the BSF during the run of the application specific protocol.

7.2.1.3 Bootstrapping Server Function (BSF)

The BSF is hosted in a network element under the control of mobile network operator. The BSF, HSS, and UEs participate in GBA in which a shared secret is established between the network and a UE by running the bootstrapping procedure. The shared secret can be used between NAFs and UEs, for example, for authentication purposes. A generic Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and a Network Application Function (NAF). The BSF shall restrict the applicability of the key material to a specific NAF by using the key derivation procedure. The key derivation procedure may be used with multiple NAFs during the lifetime of the key material. The lifetime of the key material is set according to the local policy of the BSF. The BSF shall be able to acquire the GBA User security Settings (GUSS) from the HSS [49].

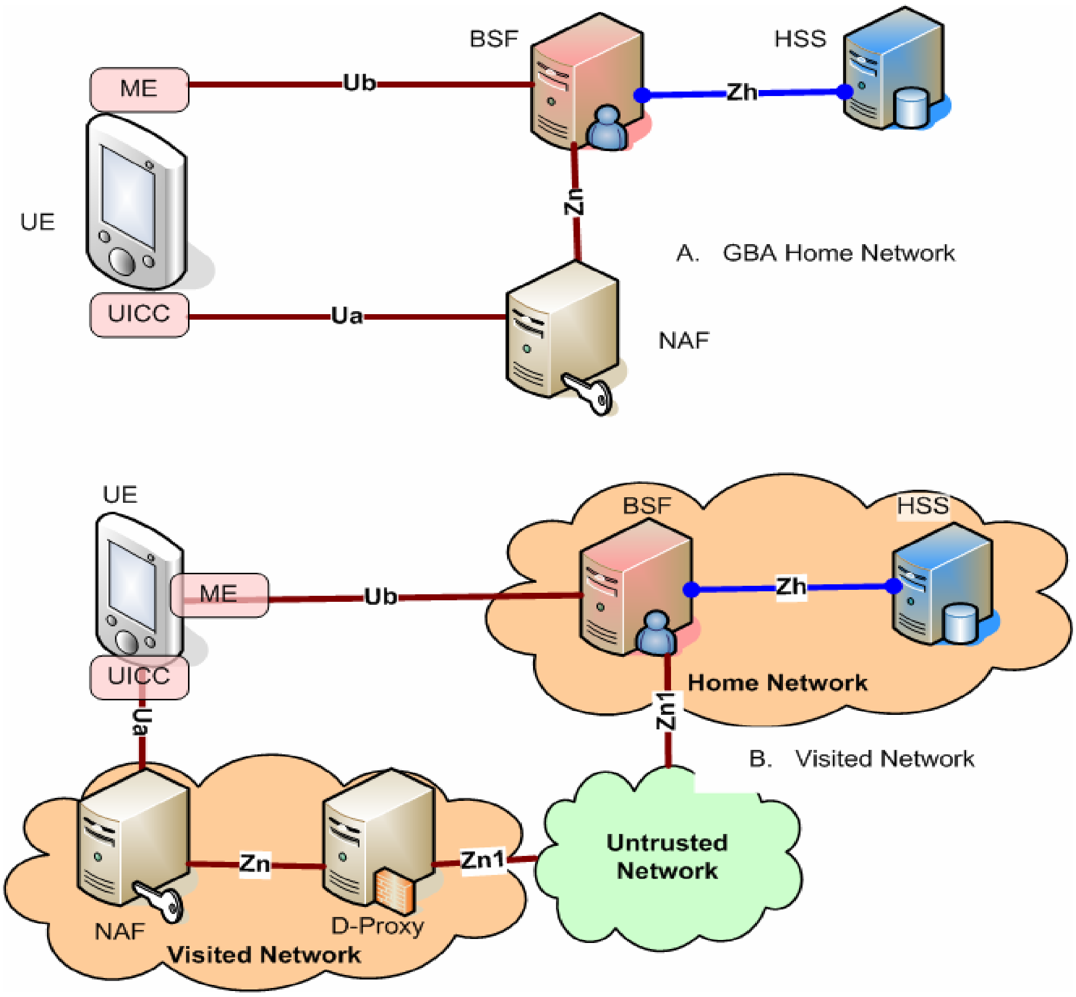


Figure 7.1 Network Entities of GBA

7.2.1.4 Home Subscriber Server (HSS)

The HSS stores GBA user security settings (GUSSs). The GUSS shall be defined in such a way that interworking of different operators for standardized application profiles is possible and also that profiles for operator specific applications and extensions to existing application profiles are supported without need for standardization of these elements. The GUSS shall be able to contain application-specific USSs that contain parameters that are related to key selection indication, identification or authorization information of one or more applications hosted by one ore more NAFs. Any other types of parameters are not allowed in the application-specific USS [49].

7.2.1.5 Diameter-Proxy

In the case where UE has contacted NAF that is visited operated in another network than home network, this visited NAF shall use a diameter proxy (D-Proxy) of the NAFs network to communicate with subscriber's BSF (i.e. home BSF). General requirements for the functionality of D-Proxy are: D-Proxy shall be able to function as a proxy between the visited NAF, and the subscriber's home BSF and it will be able to locate subscriber's home BSF and communicate with it over secure channel. The D-Proxy will be able to validate that the visited NAF is authorized to participate in GBA and shall be able to assert to subscriber's home BSF the visited NAFs DNS name. The D-Proxy shall also be able to assert to the BSF that the visited NAF is authorized to request the GBA specific user profiles contained in the NAF request [49].

7.2.2 GBA Reference Points

Ub: The reference point Ub is between the UE and the BSF and provides mutual authentication between them. It allows the UE to bootstrap the session keys based on 3GPP AKA infrastructure. The HTTP Digest AKA protocol is used on the reference point Ub. It is based on the 3GPP AKA [44] protocol.

Ua: The reference point Ua carries the application protocol, which is secured using the keys material agreed between UE and BSF as a result of the run of HTTP Digest AKA over reference point Ub. For instance, in the case of support for subscriber certificates, it is a protocol which allows the user to request certificates from the NAF. In this case the NAF would be the PKI portal.

Zh: The reference point Zh used between the BSF and the HSS allows the BSF to fetch the required authentication information and all GBA user security settings from the HSS. The interface to the 3G Authentication Centre is HSS-internal, and it need not be standardized as part of this architecture.

Zn: The reference point Zn is used by the NAF to fetch the key material agreed during a previous HTTP Digest AKA protocol run over the reference point Ub from the UE to the BSF. It is also used to fetch application-specific user security settings from the BSF, if requested by the NAF.

7.3 Bootstrapping Authentication Procedure

The UE and Network Authentication Function (NAF) have to decide whether to use GBA before the start of communication between them. When UE wants to interact with NAF, it starts communication with NAF over Ua interface without GBA parameters. If the NAF requires the use of shared keys obtained by means of the GBA, but the request from UE does not include GBA-related parameters, the NAF replies with a bootstrapping initiation message [51]. When UE wants to interact with a NAF, and it knows that the bootstrapping procedure is needed, it shall first perform a bootstrapping authentication as shown in *figure 7.2*. Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a bootstrapping negotiation indication from the NAF, or when the lifetime of the key in UE has expired. The UE sends an HTTP request to the BSF and the BSF retrieves the complete set of GBA user security settings and one

Authentication Vector (AV) [54] as given in *equation 5.1* over the reference point Zh from the HSS.

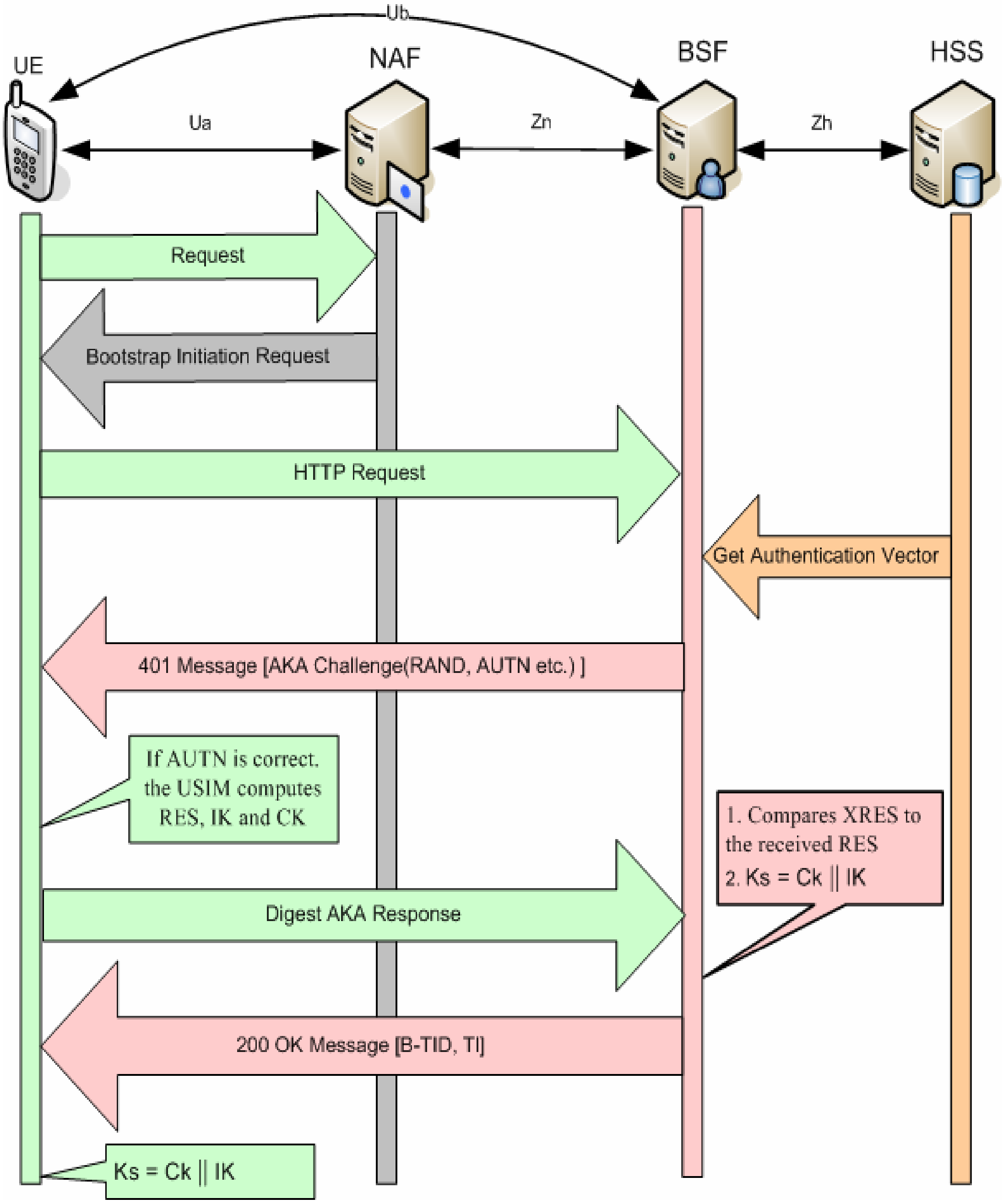

Ub
UE
NAF
BSF
HSS
Ua
Zn
Zh
Request
Bootstrap Initiation Request
HTTP Request
Get Authentication Vector
401 Message [AKA Challenge(RAND, AUTN etc.)]
If AUTN is correct, the USIM computes RES, IK and CK
1. Compares XRES to the received RES
2. Ks = Ck || IK
Digest AKA Response
200 OK Message [B-TID, TI]
Ks = Ck || IK

Figure 7.2 Bootstrapping Authentication Procedure

After that BSF forwards the RAND and AUTN to the UE in the 401 message without the CK, IK and XRES. This is to demand the UE to authenticate itself. The UE checks AUTN to verify that the challenge is from an authorized network; the UE also calculates CK, IK and RES [54]. This will result in session keys IK and CK in both BSF and UE. The UE sends another HTTP request to the BSF, containing the Digest AKA response which is calculated using RES.

The BSF authenticates the UE by verifying the Digest AKA response. The BSF generates key material Ks by concatenating CK and IK and it also generates B-TID

(Bootstrapping Transaction Identifier) which is used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn. The BSF shall send a 200 OK message, including a B-TID to the UE to indicate the success of the authentication and the lifetime of the key Ks. The key material Ks is generated in UE by concatenating CK and IK. Both the UE and the BSF shall use the Ks to derive the key material Ks-NAF which will be used for securing the reference point Ua. The Ks-NAF is computed as *equation 7.2.*

$$\text{Ks-NAF} = f_{KD}(\text{Ks}, \text{"gba-me"}, \text{RAND}, \text{IMPI}, \text{NAF-ID}) \qquad (7.1)$$

Where f_{KD} is the key derivation function and will be implemented in the ME, and the key derivation parameters consist of the user's IMPI, the NAF-ID and RAND. The NAF-ID consists of the full DNS name of the NAF, concatenated with the Ua security protocol identifier. The UE and the BSF shall store the key Ks with the associated B-TID for further use, until the lifetime of Ks has expired, or until the key Ks is updated [49].

7.4 Bootstrapping Usage Procedure

Before the start of communication between the UE and the NAF, the UE and the NAF first have to agree whether to use shared keys obtained by means of the GBA. If UE does not know whether to use GBA with this NAF, it uses the initiation of bootstrapping procedure. Once the UE and the NAF have decided that they want to use GBA then every time the UE wants to interact with NAF. The UE starts communication over reference point Ua with the NAF by supplying the B-TID to the NAF to allow the NAF to retrieve the corresponding keys from the BSF. The NAF starts communication over reference point Zn with BSF. The NAF requests key material corresponding to the B-TID supplied by the UE to the NAF over reference point Ua. With the key material request, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able verify that NAF is authorized to use that hostname. The NAF may also request one or more application-specific USSs for the applications, which the request received over Ua from UE may access.

The BSF derives the keys required to protect the protocol used over reference point Ua from the key Ks and the key derivation parameters, and supplies to NAF the requested key Ks-NAF, as well as the bootstrapping time and the lifetime of that key, and the requested application-specific and potentially NAF group specific USSs if they are available in subscriber's GUSS and if the NAF is authorized to receive the requested USSs. If the key identified by the B-TID supplied by the NAF is not available at the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a bootstrapping renegotiation request to the UE. The BSF may also send the private user identity (IMPI) and requested USSs to NAF according to the BSF's policy. The NAF continues with the protocol used over the reference point Ua with the UE. Once the run of the protocol used over reference point Ua is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to use reference point Ua in a secure way.

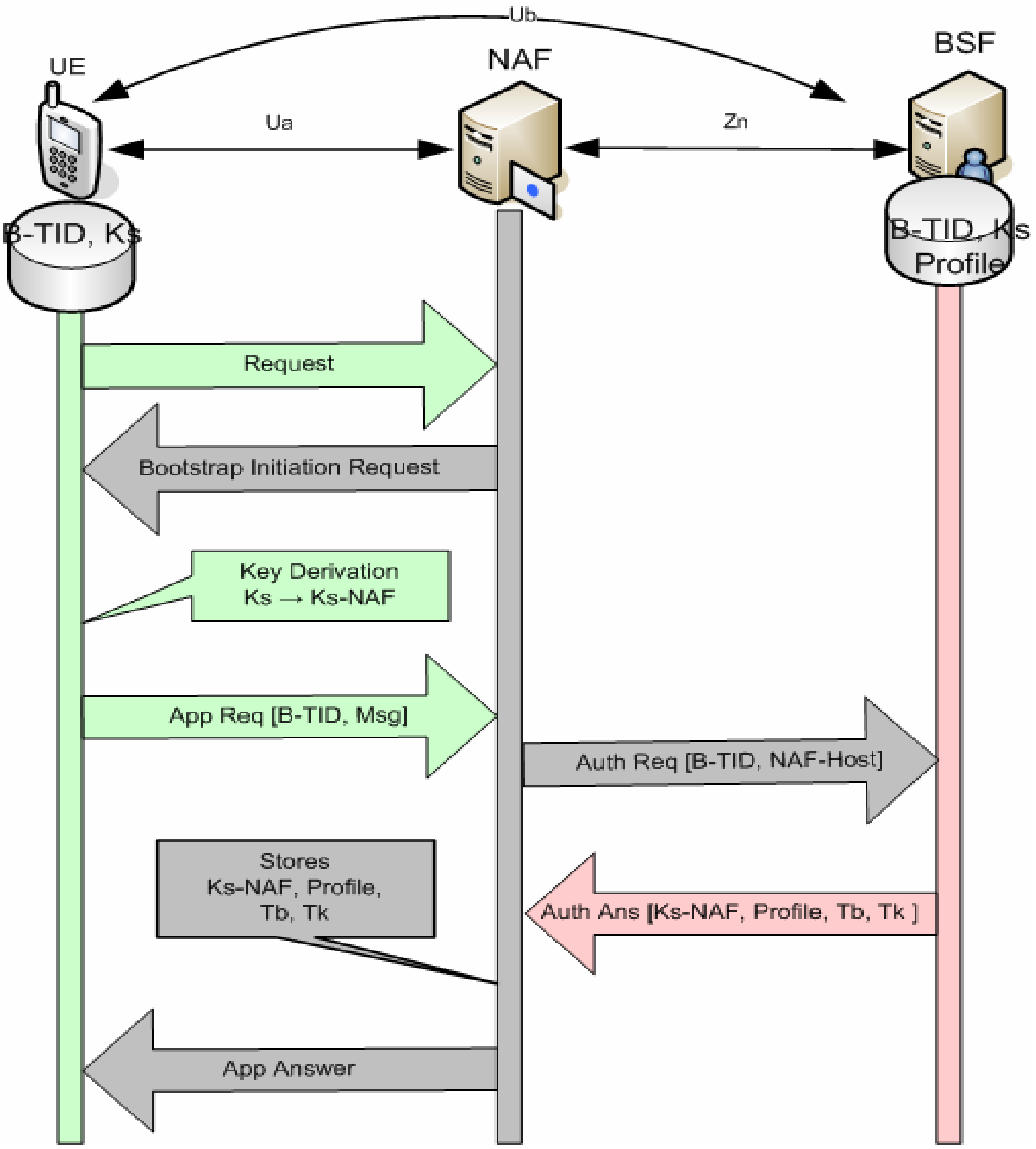


Figure 7.3 Bootstrapping Application

7.5 Authentication Proxy Usage for Multimedia Services

The Authentication Proxy (AP) is like a Network Authentication Function (NAF) and performs the function of HTTP proxy for the UE. It is responsible to handle the Transport Layer Security (TLS) and implement the secure HTTP channel between AP and UE as shown in *figure 7.4*. It utilized the generic bootstrapping architecture to assure the application servers (ASs) that the request is coming from an authorized subscriber of mobile network operator. When the HTTPS request is sent to AS through AP, the AP performs UE authentication. The AP may insert the user identity when it forwards the request to application server. Figure 5b presents the architecture view of using AP for different IMS SIP services e.g. presence, messaging, conferencing etc.

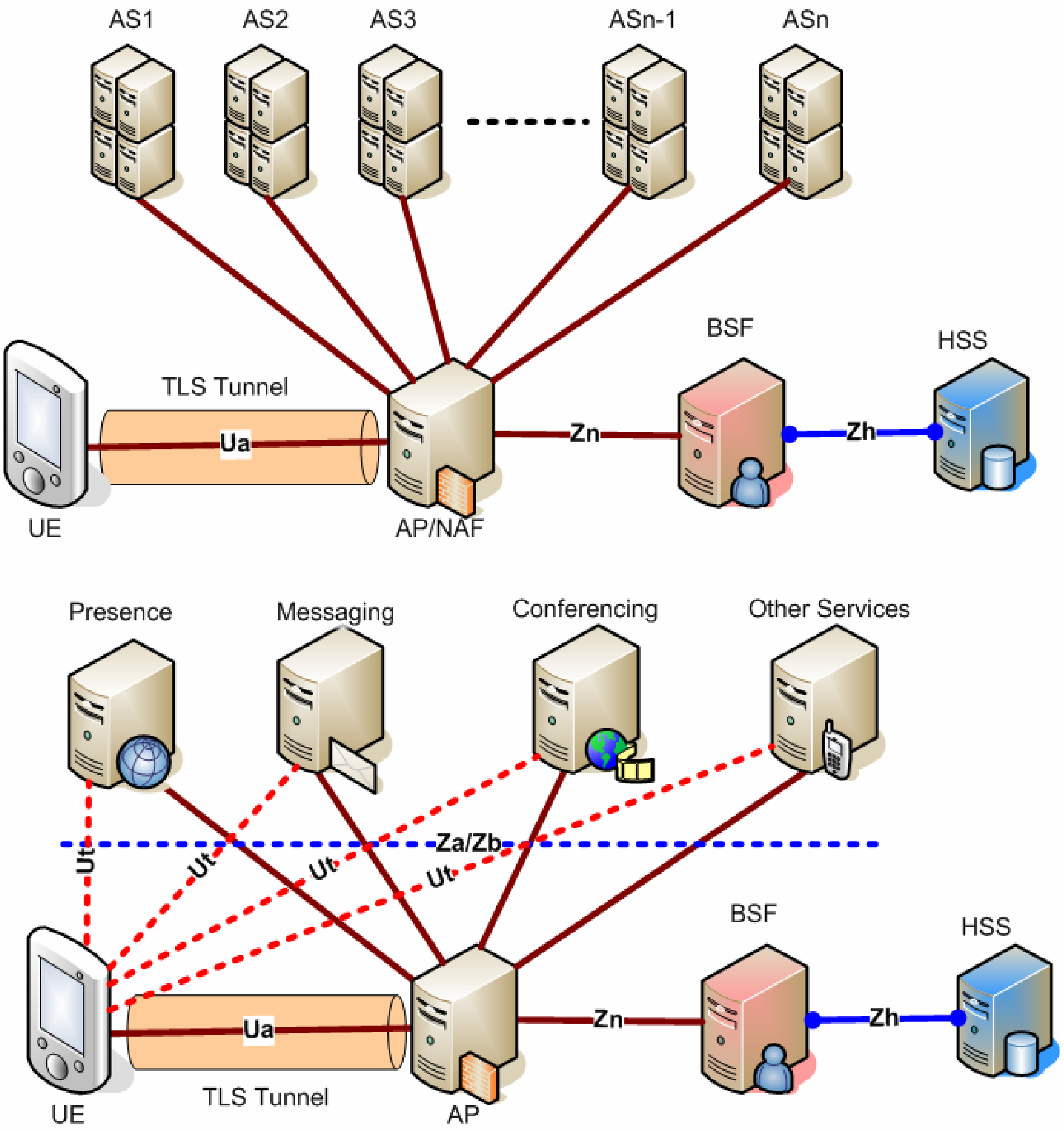


Figure 7.4 Authentication Proxy

The UE shall manipulate own data such as groups, through the Ua/Ut reference point [50]. The reference point Ut will be applicable to data manipulation of IMS based SIP services, such as Presence, Messaging and Conferencing services. When the HTTPS client starts communication via Ua reference point with the NAF, it shall establish a TLS tunnel with the NAF. The NAF is authenticated to the HTTPS client by means of a public key certificate. The HTTPS client will verify that the server certificate corresponds to the FQDN (Fully Qualified Domain Name) of the AP it established the tunnel with. We explain the procedure briefly as: the HTTPS client sends an HTTP request to NAF inside the TLS tunnel. In response to HTTP request over Ua interface, the AP will invoke HTTP digest with HTTPs client in order to perform client authentication using the shared keys. On the receipt of HTTPS digest from AP, the client will verify that the FDQN corresponds the AP it established the TLS connection with, if not the client will terminate the TLS connection with the AP. In this way the UE and AP are mutually authenticated as the TLS tunnel endpoints.

Now we discuss an example that application residing on UICC (Universal Integrated Circuit Card) may use TLS over HTTP in Generic Authentication Architecture (GAA) mechanism to secure its communication with Authentication Proxy (AP). The GBA security association between a UICC-based application and AP can be established as: The ME (Mobile Equipment) executes the bootstrapping procedure with the BSF supporting the Ub reference point. The UICC, which hosts the HTTPS client, runs the bootstrapping usage procedure with AP supporting the Ua reference point [76]. *Figure 7.5* shows the use of BIP (Bearer Independent Protocol) to establish the HTTPS connection between UICC and AP. When the UICC opens channel with AP as described in [77] than an active TCP/IP connection is established between the UICC and the AP.

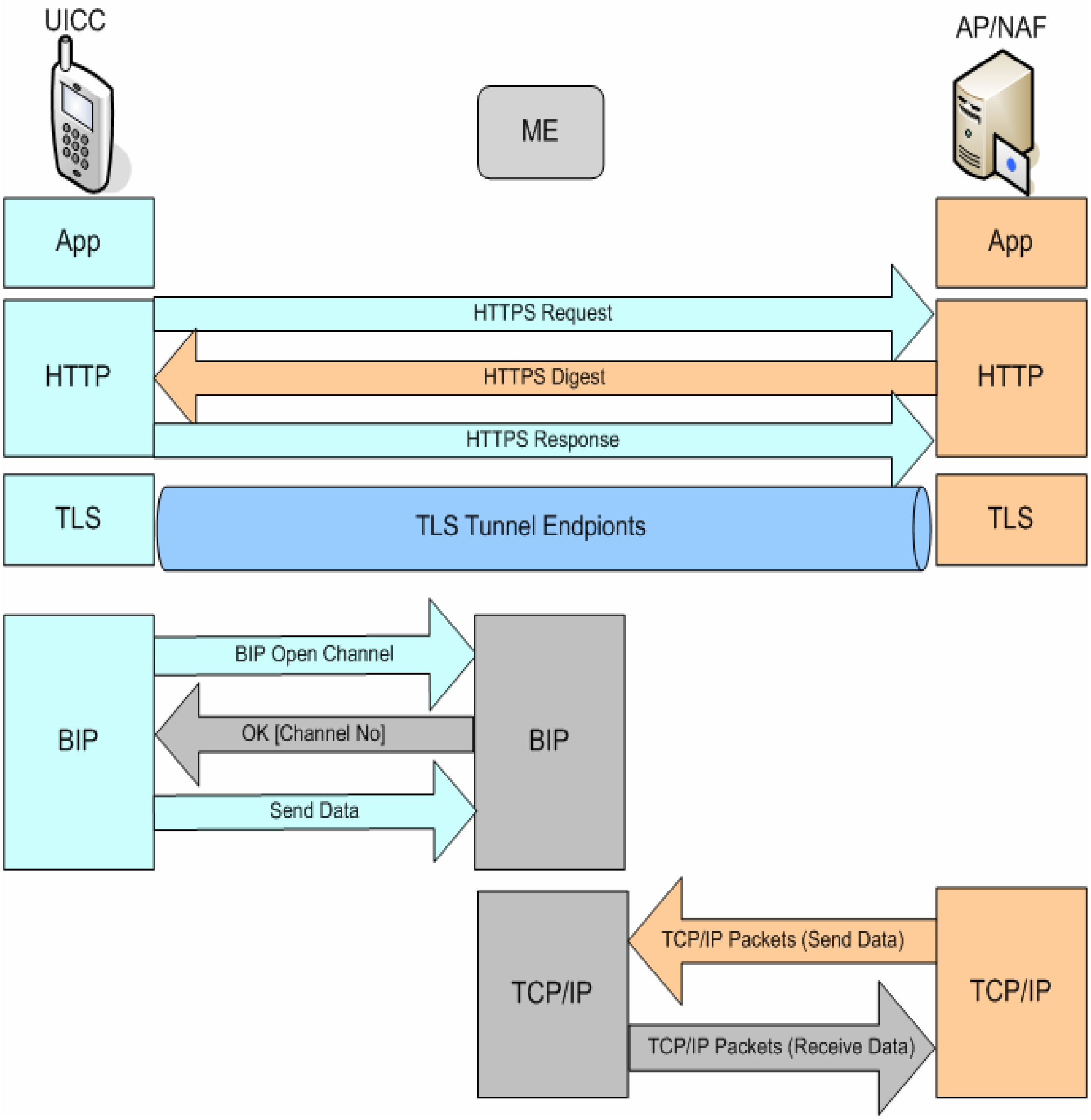


Figure 7.5 HTTPS and BIP (Bearer Independent Protocol) Procedure

7.6 Summary

This chapter focused to manage secure access to multimedia services and applications based on SIP and HTTP on top of IP Multimedia Subsystem (IMS). The solution utilized Generic Bootstrapping Architecture (GBA) to authenticate users before accessing the multimedia services offered by IMS operators. The chapter introduced the GBA-based Authentication Proxy (AP) performing mutual authentication of UE and Bootstrapping Server Function (BSF), and responsible to implement Transport Layer Security (TLS) to secure HTTP application.

Chapter 8 Access Network Security Management

8.1 Introduction

The network access security management architecture consists of User Service Identity Module (USIM), Mobile Equipment (ME), Access Network (AN), Service Network (SN) and Home Environment (HE) as shown in *figure 8.1*. The USIM is required for accessing the Packet Switched (PS) domain in General Packet Radio System (GPRS) and identifies the particular subscriber. The USIM contains the security parameters for accessing the PS-domain, International Mobile Subscriber Identity (IMSI), list of allowed access points, MMS-related information. In serving network, the Serving GPRS Support Node (SGSN) links the Radio Access Network (RAN) to the packet core network in the PS-service domain. It is responsible for performing both control and traffic handling functions for the PS domain. The control parts deal with mobility management and session management. The SGSN also ensures appropriate QoS and generates charging information [7]. In the CS-service domain, the related part is Visitor Location Register (VLR). In HE, the Authentication Centre (AUC) generates the AV vector as we have discussed in *equation 5.1.*

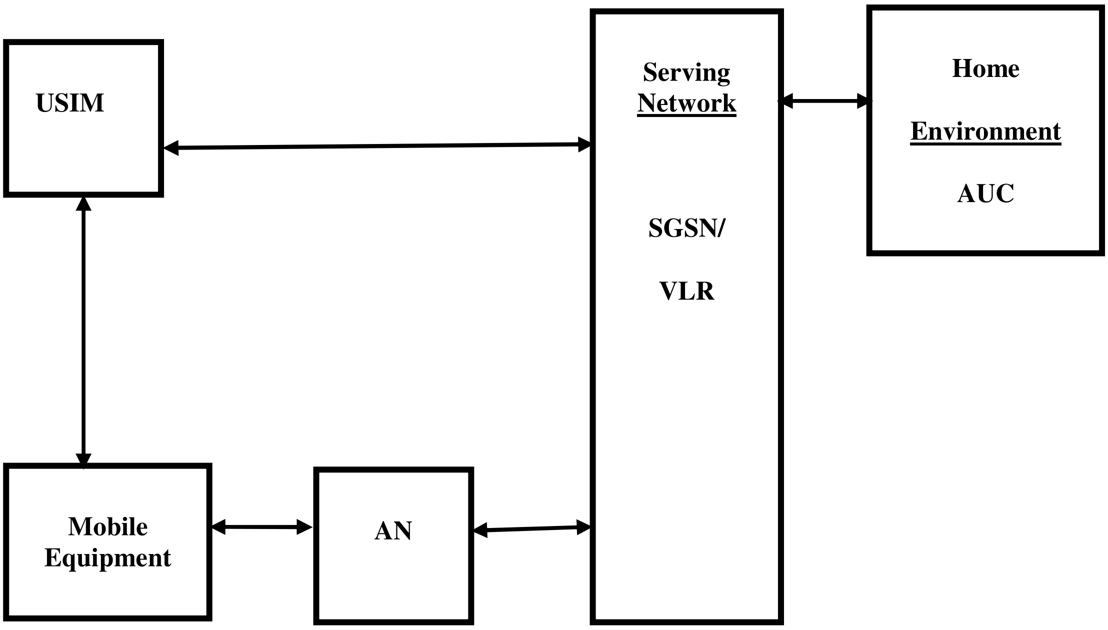


Figure 8.1 Overview of Network Access Security Model

The following security methodologies and mechanisms are required to implement the network access security architecture to protect the user and user's sensitive information on Radio Access network (RAN).

8.2 Assigning Temporary and Permanent Identities

In order to hide the identity of user on the radio access link, the user is assigned Temporary Mobile Subscriber Identity (TMSI) to identify the user on the radio link, for instance in paging, location update, attach, service, connection re-establishment and detach requests. The temporary identity has importance only in the location area or routing area in which the user is registered. Outside that area it should be accompanied by Location Area Identification (LAI) or Routing Area Identification (RAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR) for CS domain and by SGSN for PS domain depending in which domain the user is registered.

When the user could not be identified by IMSI, the serving network identifies the user by the permanent identity which is called the International Mobile Subscriber Identity (IMSI). In particular, it should be used when the user registers for the first time in a serving network, or when the serving network cannot retrieve the IMSI from the TMSI by which the user identifies itself on the radio path. The procedure is initiated by the visited SGSN/VLR that requests the user to send its permanent identity as shown in *figure 8.2*. The user's response contains the IMSI in clear text. This represents a breach in the provision of user identity confidentiality and in section 8.5 we will discuss the protection of user's temporary identities.

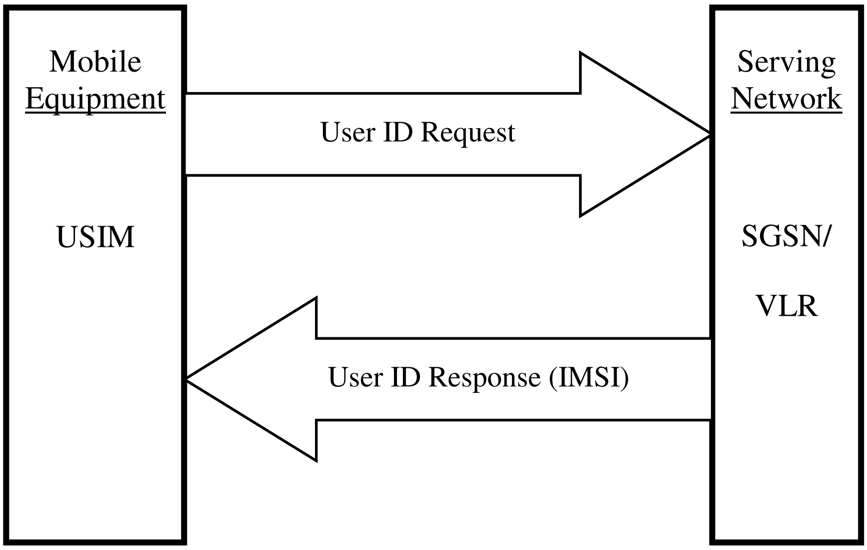


Figure 8.2 Identification by the permanent identity

8.3 Security Mode Setup during Connection Establishment

The security mode setup is achieved by the integrity protection functionality. When the SGSN is known the identity of mobile subscriber, the cipher and integrity keys setting could occurred. These keys are stored in the VLR and transferred to Radio Network Controller (RNC) as required. These keys are also stored on USIM and updated from CS domain or PS domain independently. During ME registration and connection establishment within UMTS with a CS service domain and a PS service domain, user identification, authentication and key agreement will take place independently in each service domain. The connection establishment includes the ME security capability i.e. the ciphering association and the integrity association of the MS.

8.4 Access Link Data Integrity

Most of the control signalling elements like RRC, MM, CC, GMM and SM messages between the mobile station and the RNC are considered sensitive and must be integrity protected by the message authentication function. The access link data integrity procedure is given in *figures 8.3 & 8.4*. The input parameters to the algorithm are *IK*, integrity sequence number *(COUNT-J)*, the signalling data *(S-Data)*, the direction *(DIRECT)* and the random value generated by the network side *(R-Value)*. From these four parameters the user equipment or RNC computes message authentication code *MAC-J* for data integrity using the integrity algorithm f9 as given in *equation 8.1*. The use of Kasumi for the integrity protection function f9 is specified in [78]. The *MAC-J* is then appended to the message when sent over the radio access link. The receiver computes *XMAC-J* as given in *equation 8.2*, on the message received in the same way as the sender computed *MAC-J* on the message sent and verifies the data integrity of the message by comparing it to the received *MAC-J*. There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user.

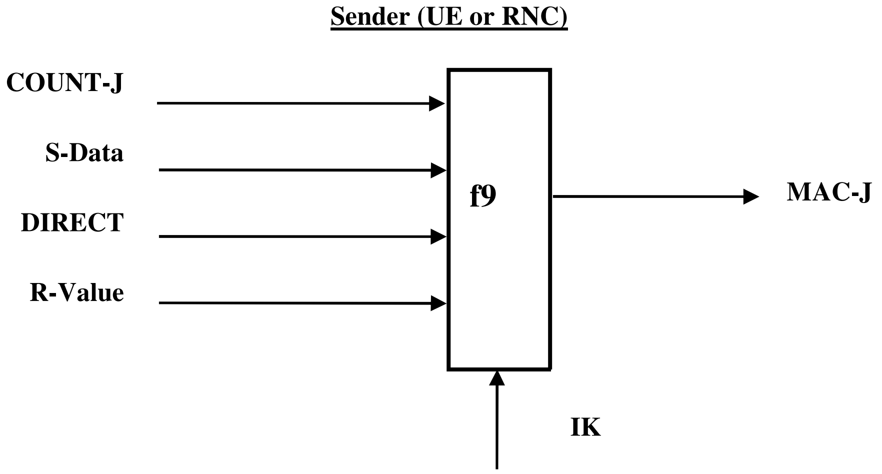


Figure 8.3 Sender's Message Authentication Function

$$\text{MAC-J} = f9_{IK}\ (\text{COUNT-J, S-Data, DIRECT, R-Value}) \quad (8.1)$$

$$\text{XMAC-J} = f9_{IK}\ (\text{COUNT-J, S-Data, DIRECT, R-Value}) \quad (8.2)$$

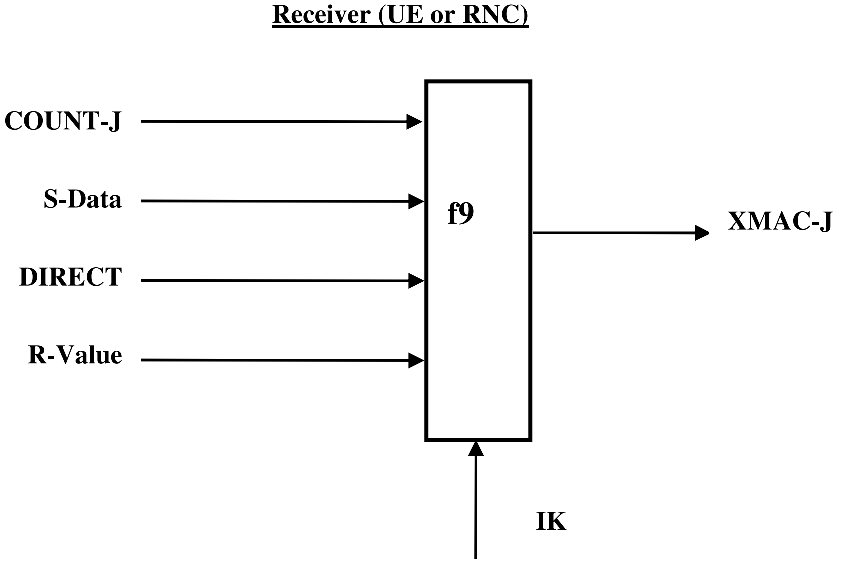


Figure 8.4 Receiver's Message Authentication Function

8.5 Access Link Data Confidentiality

User data and some signalling elements between user and network are considered sensitive and should be confidentiality protected. To ensure identity confidentiality, the temporary user identity (TMSI) should be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it. This protected mode of transmission is applied on dedicated channels between the ME and the RNC by a confidentiality function. *Figures 8.5 & 8.6* illustrate that the sender produces key-stream (Kst) by using the Ciphering Algorithm f8 [78] and gets the Cipher-text (C(x)), from bit by bit binary addition of the Plaintext (P(x)) and the key-stream as given in *equation 8.3*. At the receiver, the P(X) may be produced by generating the same key-stream using the same input parameters and bit by bit binary addition of the C(X) and key-stream as given in *equation 8.4*. The input parameters to the algorithm are the Cipher Key *(CK)*, a time counter input *(COUNT-T)*, the bearer identity *(B-ID)*, the direction of transmission *(DIRECT)* and the length of the key-stream required *(LEN)*.

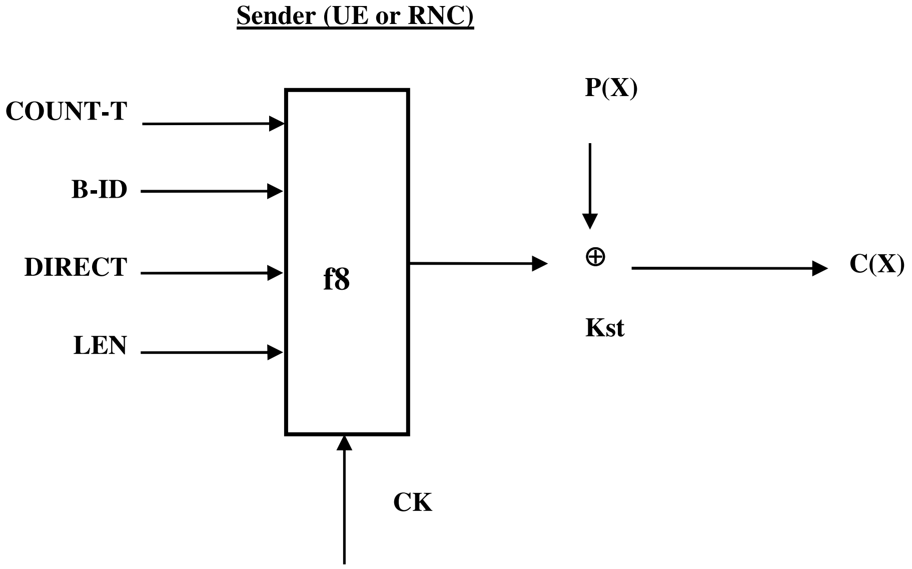


Figure 8.5 Cipher-text Production by Sender

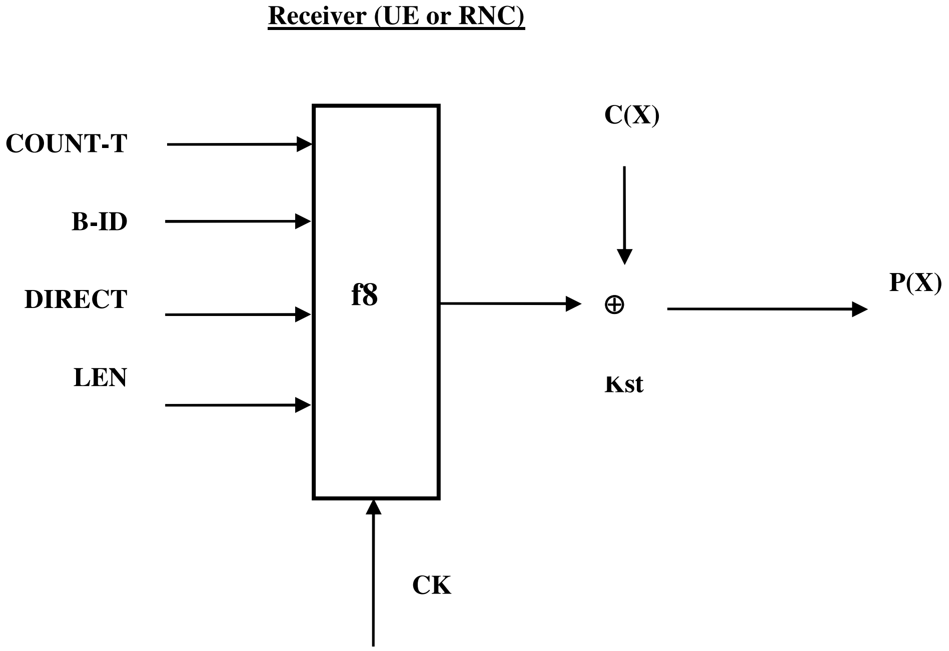


Figure 8.6 Plaintext Retrieval by Receiver

$$C(X) = P(X) \oplus f8_{CK} \text{(COUNT-T, B-ID, DIRECT, LEN)} \qquad (8.3)$$

$$P(X) = C(X) \oplus f8_{CK} \text{(COUNT-T, B-ID, DIRECT, LEN)} \qquad (8.4)$$

8.6 Summary

In this chapter we have discussed methodologies and mechanisms to provide access security including security mode setup during connection establishment, and access link data integrity and confidentiality between mobile user and universal mobile telecommunication systems. It protects the user confidential information against attacks on the radio access link of Universal Mobile Telecommunication System (UMTS).

Part-D

Design and Implementation of Intrusion Detection and Prevention System for IMS Core (IDP-Core)

(Level 2 Security – Section-1)

Design and Implementation of IDP-Core

The Part-D presents first section of level 2 IMS extended security solution. It describes development and deployment of Intrusion Detection and Prevention (IDP-Core) system for IMS core against Denial-of-Service (DoS)/Distributed DoS (DDoS) flooding and SIP message tampering/fuzzing attacks. The SIP REGISTER and SIP INVITE methods are utilized to lunch these flooding attacks in IMS. This part consists of three chapters (9 - 11) focusing on the design, detection methodology, implementation, and testing and performance evaluation of Intrusion Detection and Prevention system for IMS core (IDP-Core).

Chapter 9 “IDP-Core Design” discusses level 1 IMS security analysis, IDP-Core design requirements, reference architecture and attacks detection algorithms. Different design scenarios are explained in this chapter.

Chapter 10 “IDP-Core Implementation” explains the procedure to modify the “Main Route Block” of Open IMS core, implementation of detection algorithm, object interaction scenarios and attacks prevention procedure.

Chapter 11 “Testing and Performance Evaluation” describes Testbed environment, test scenarios, and performance evaluation at normal CPU load and overload CPU conditions of P-CSCF. These tests are preformed at Open IMS Playground within NGNI FOKUS Fraunhofer Testbed.

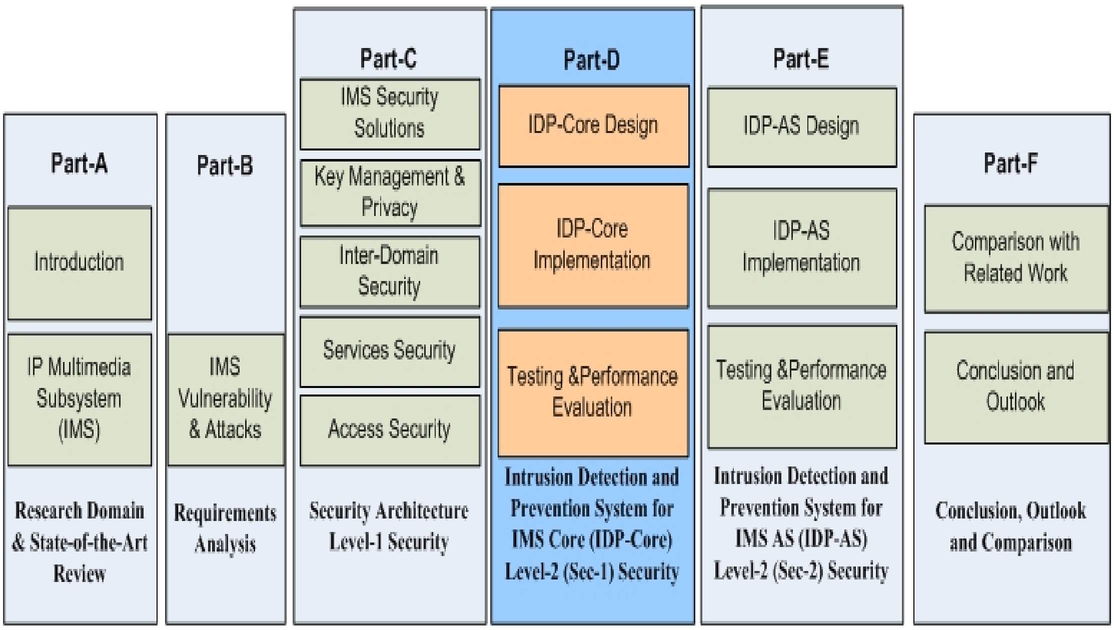

Part-A
Introduction
IP Multimedia Subsystem (IMS)
Research Domain & State-of-the-Art Review
Part-B
IMS Vulnerability & Attacks
Requirements Analysis
Part-C
IMS Security Solutions
Key Management & Privacy
Inter-Domain Security
Services Security
Access Security
Security Architecture Level-1 Security
Part-D
IDP-Core Design
IDP-Core Implementation
Testing &Performance Evaluation
Intrusion Detection and Prevention System for IMS Core (IDP-Core) Level-2 (Sec-1) Security
Part-E
IDP-AS Design
IDP-AS Implementation
Testing &Performance Evaluation
Intrusion Detection and Prevention System for IMS AS (IDP-AS) Level-2 (Sec-2) Security
Part-F
Comparison with Related Work
Conclusion and Outlook
Conclusion, Outlook and Comparison

Figure D: Design and Implementation of IDP-Core (Part-D Overview)

Chapter 9 Design and Architecture of IDP-Core

9.1 Introduction

The IP Multimedia Subsystem (IMS) employs SIP for registration and session management. The SIP protocol specification [4] describes methods to establish, end or terminate a session, cancel an invitation, redirect a call and update session parameters. But the SIP specification does not include any specific security mechanisms. It is possible that the attacker could exploit any security vulnerability in the SIP methods and cause DoS to the provided multimedia services. For example, attacker could launch REGISTER flooding attack to collapse the IMS resources. The attacker could also use a faked BYE message to tear down an established session. Moreover, the attacker could discover possible security flaws in the applications or protocols, similar to attacks launched against Internet applications and services.

The objective and scope of developing Intrusion Detection and Prevention (IDP-Core) system for IMS core is to enhance the existing security level. It protects the IMS core components i.e. P-CSCF (Proxy-Call State Control Function), I-CSCF, S-CSCF and HSS (Home Subscriber Server) from different Denial of Service (DoS)/Distributed Denial of Service (DDoS) flooding attacks, unauthorized access and misuse of IMS resources against fraud situation, both from legitimate and illegitimate users.

In this chapter first we discuss the IMS security and vulnerability analysis. The next section shows the placement of IDP-Core component in IMS core. The subsequent sections explain the IDP-Core architecture, design and detection algorithm etc.

9.2 Security and Vulnerability Analysis

We have discussed in part C (chapter 5) that in a result of successful authentication, the IMS client and P-CSCF establish the secure association providing data integrity and confidentiality [44]. The 3GPP/IMS authentication and key agreement protocol has been reported and claimed to be secure. But M. Zhang and Y. Fang [38] claim that AKA is vulnerable to different types of threats. We present here brief analysis to show that IMS AKA is vulnerable to a variant of false base station attack. The flaw of AKA could allow an attacker to redirect user traffic from one network to another. The attacker could also use the authentication vectors corrupted from one network to impersonate other networks. Thus the attacked network may make vulnerable the other secure networks. The redirection attack represents a real threat since the security levels provided by different networks are not always the same.

The redirection attack could also cause false billing problem as the service rates offered by different networks are not always the same. The following are the possible attacks occur due to vulnerability in the IMS AKA.

9.2.1 Redirection Attack

For example an attacker is using a device that has the functions of base station and emulation of mobile device. This device is called false base station. With this device the attacker could impersonate as a legitimate base station and legitimate mobile station on the radio link. In this way the attacker could transmit messages between the network and his illegitimate device.

Consider the scenario that a legitimate user is in his home network and want to establish connection in foreign network. During the connection establishment, the attacker entices the mobile station through his false base station. Once the mobile station connects with the false base station, the attacker can divert the session request signals to any foreign network. After this the attacker relays messages between legitimate user's mobile station and foreign network. The authentication process is successfully completed between the user and foreign network. The communication link is also protected through the established keys during this process [44]. Thus the redirection attack is successfully launched in this scenario.

9.2.2 Active Attack in Under Attacked Networks

In IMS AKA, the authentication vectors are traversed between networks depending upon the user is in home network or roaming. Every network is controlled by its own administrator. When a network is under attack, the attacker could access user authentication data without intercepting and breaking the security of the user's home network. Later the attacker could use the obtained authentication vectors to impersonate into his network and could mount false base station attack against legitimate users [38]. He could also launch the flooding attack by setting the counter value at high. Thus the under attack network may jeopardize or vulnerable the entire system. There is no security mechanism available to control the attacks in corrupted network to protected and secure networks.

9.2.3 Resynchronization Attack

During the IMS AKA procedure, the home network maintains a counter for each subscriber. Unlike the authentication key whose value is fixed, the value of a counter is dynamic. If there is no problem with synchronization, the network and user are successfully authenticated each other. But if there is problem with synchronization data, the authentication process is aborted and network restarts the authentication procedure to resynchronize the counter.

If the attacker is able to launch the false base station attack, he could disturb the synchronization counter. This situation produces two serious network faults: one heavy cost of authentication signalling and denial-of-service problem for legitimate users [38]. This situation becomes worst when the user is roaming. For example when authentication process started in visited network and the sequence number is not in the correct range, the mobile station decides that a synchronization failure has occurred in the home network and consequently initiates a resynchronization request to the home network.

9.3 IDP-Core Approach

The IDP-Core is based on Open Source IMS [79] and is deployed within P-CSCF as depicted in *figure 9.1*. It is placed in-line between the IMS client and IMS core and processes each incoming SIP REGISTER and other messages like INVITE or Subscribe in real time. The operation is performed online into two modes in order to increase the efficiency and performance. In first mode IDP-core checks all SIP REGISTER messages between client and IMS core against SQL-injection in normal CPU load condition. The second mode checks the DoS/DDoS flooding attacks and triggers when P-CSCF CPU load exceeds the defined threshold limit (X). The IDP-core monitors the CPU load and takes necessary measures if system is under flooding attack due to SIP REGISTER or INVITE messages.

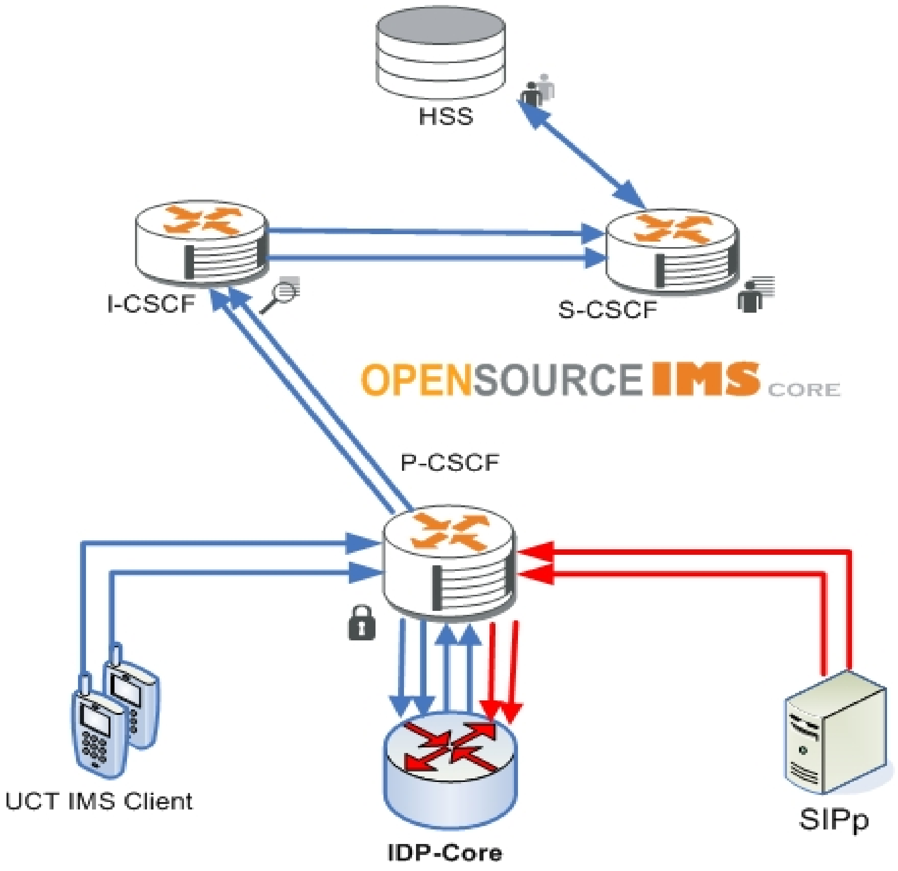


Figure 9.1 Location of IDP-Core

9.4 IDP-Core Design Requirements

The security challenges facing to IMS are the flooding attacks causing to downfall or collapse of IMS resources and network services. These attacks could not be mitigated by the standards mechanisms; therefore, the primary functionality of IDP-core is to detect and protect the DoS/DDoS flooding attacks launched against IP Multimedia Subsystem (IMS) core network. The design requirements of IDP-Core are the following:

- It should not affect the P-CSCF message processing procedure at normal load.
- It should detect and drop the SQL-injection messages.
- At P-CSCF CPU overloading, the following requirements should be considered:
    - The continued authentication process from legitimate users should be carried out.
    - The REGISTER/INVITE messages from known legitimate UEs (previously success authenticated users) will still be accepted.
    - REGISTER messages from unknown users should be blocked. These messages may be the cause of overloading of IMS core.

The IDP-Core receives SIP messages from P-CSCF and processes them to check for SQL-injection and DoS/DDoS flooding attacks and then forwards to P-CSCF. Therefore P-CSCF is only the single actor of the IDP-Core as depicted in *figure 9.2*.

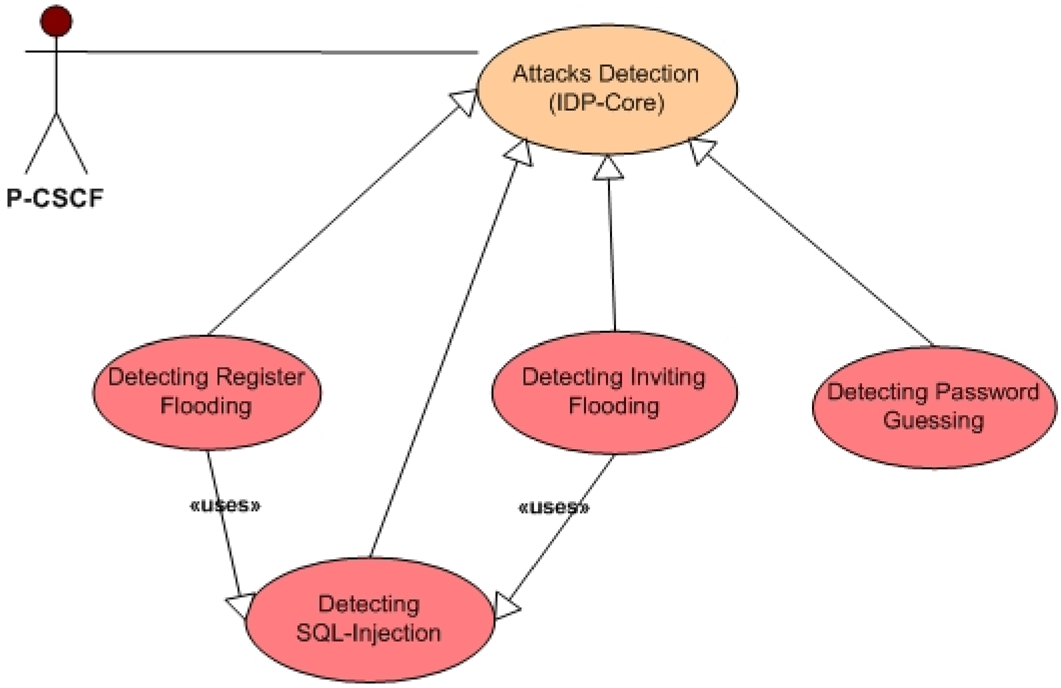

P-CSCF
Attacks Detection (IDP-Core)
Detecting Register Flooding
Detecting Inviting Flooding
Detecting Password Guessing
«uses»
«uses»
Detecting SQL-Injection

Figure 9.2 IDP-Core Use Cases

9.5 IDP-Reference Architecture

After defining the functional requirements and use cases, we focus on formulating the architecture to meet the design requirements. The top level architecture of IDP-Core is shown in *figure 9.3* consisting of following main modules:

Dispatcher: It is SP message handler. All the SIP messages either from the UE or the P-CSCF are received by the Dispatcher and it forwards them to IDP-Centre for further processing.

IDP-Centre: It is the brain of IDP-Core and performs analysis and takes decision to protect IMS core against flooding and fuzzing attacks. The analysis procedure detects the reason of overloading and decides to stop further communication from illegitimate user about defined time interval.

System Monitor: This module monitors the P-CSCF CPU processing load and compares with the defined threshold limit (X) to indicate the critical level.

Blacklist maintains the list of malicious users. If any attack is detected, the address (IP address or URI) of malicious user is inserted into the Blacklist for a defined time interval.

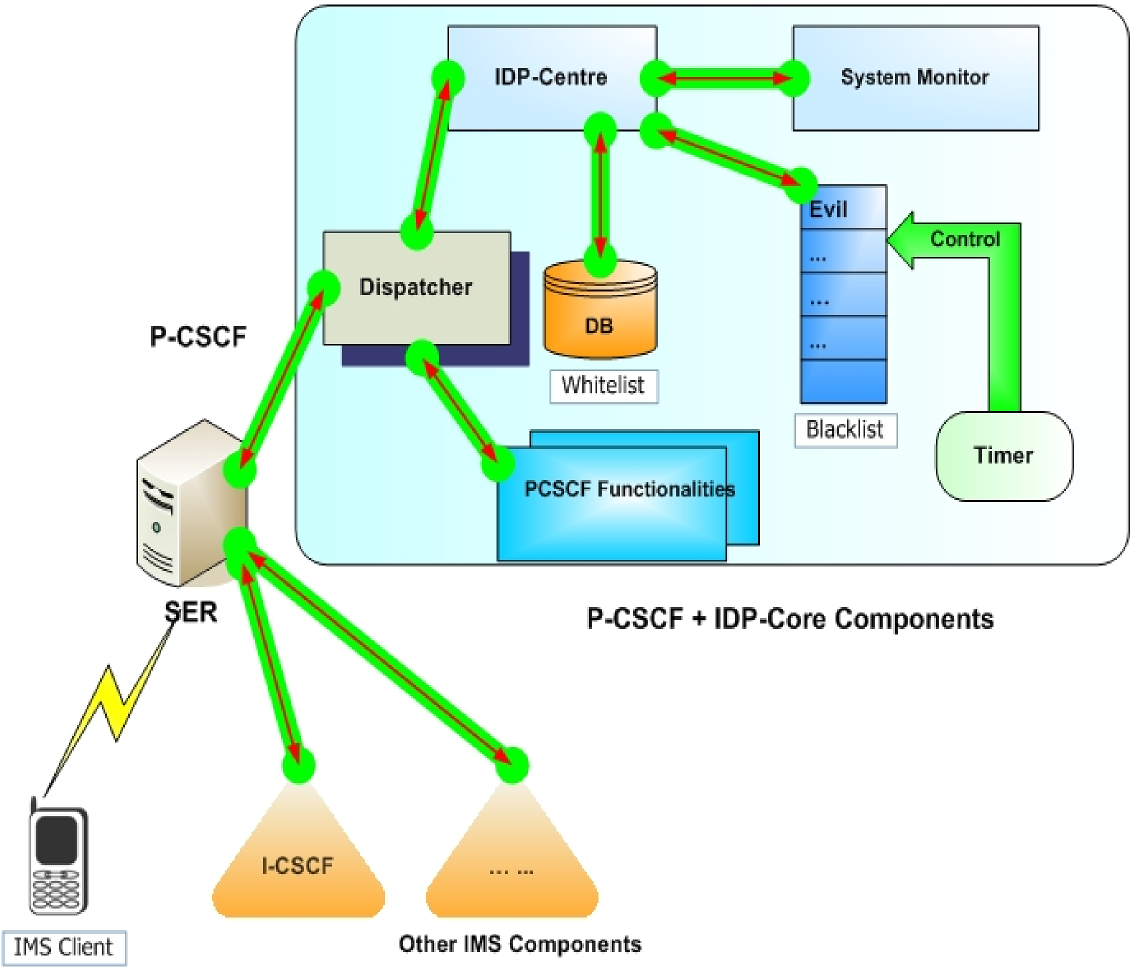


Figure 9.3 IDP-Core Architecture

Whitelist Database: It maintains the list of reliable users which are successfully registered previously within one week. These legitimate users could continue their registration procedure even system is under flooding attacks.

9.6 Attacks Detection Algorithm

The attacks detection algorithm identifies the reasons of overloading of IMS resources. The P-CSCF CPU load monitoring curve is depicted in *figure 9.4*. The detection procedure consists of three states i.e. normal, critical and under attack as shown in *figure 9.5*. In normal state, IDP-Core detects only the QSL injection. The system switches to critical state if the CPU load of P-CSCF reaches or crosses the threshold value but IDP-Core does not apply any detection algorithm. This is attack alert state and it remains 500 ms which is the round trip time of SIP REGISTER massage as mentioned in RFC 3261 [4]. If CPU load remains or crosses the threshold limit, the IDP-Core declares that the IMS-core is under flooding attack. The under attack state describes the cause of overloading i.e. it may be due to REGISTER or INVITE messages or both of them. This situation may also occur due to pick processing time, which should be avoided by deploying multiple P-CSCFs.

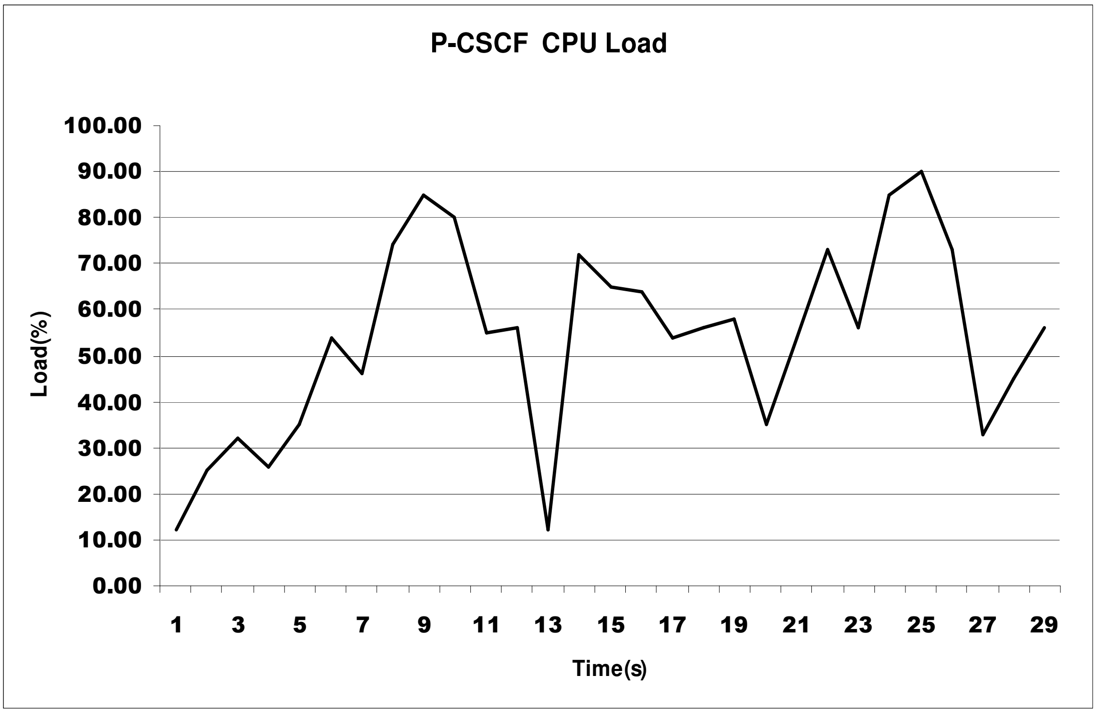
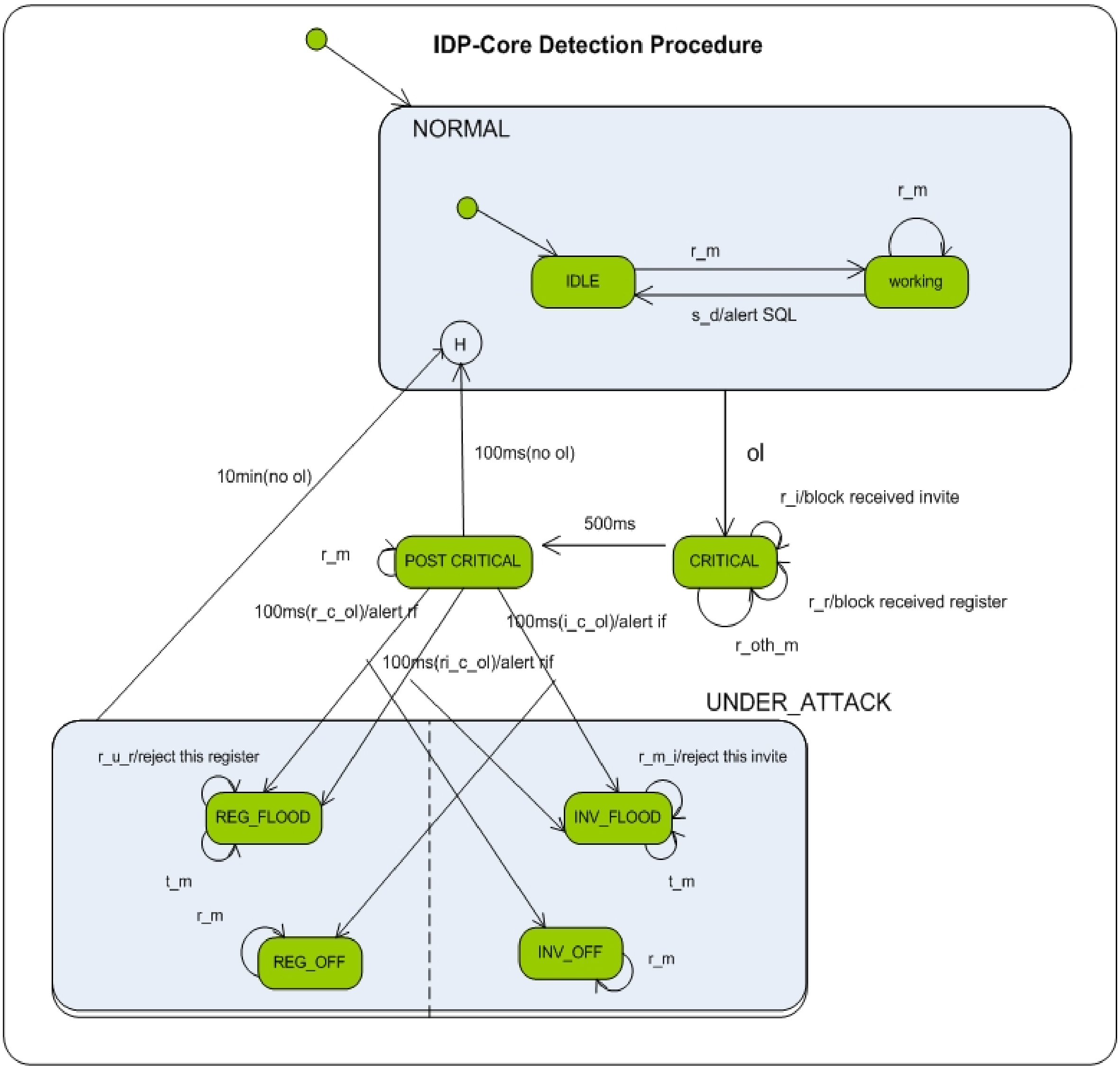


Figure 9.4 P-CSCF CPU Load Monitoring



r_m: received message

s_d: SQL Injection detected

alert SQL: alert SQL-Injection Attack

XXms: in XXms

no ol: no overload

r_u_r: received a register from a UA that is previously unknown

r_m_i: received a invite from a identified malicious UA

r_i: received an Invite Request

r_r: received a Register Request

alert rif: alert invite and register flood

r_c_ol: system is overloaded and register flood is the cause

i_c_ol: system is overloaded and invite flood is the cause

alert rf: alert register flood

alert if: alert invite flood

ri_c_ol: system is overloaded and the register flood and invite flood are the causes

r_oth_m: received the rest messages (exclude the Invite and Register request)

Figure 9.5 IDP-Core Attacks Detection Algorithm

9.6.1 SQL Injection Detection Methodology

As we have discussed that in normal state, IDP-core only detect the SQL injection with objective to cause minimum processing delay on the SIP REGISTER messages flow. The SQL injection can be launched simply by inserting SQL statement when UE and P-CSCF starts authentication procedure. The UE’s initial REGISTER request utilizes the HTTP Digest [40] Authorization header to transport user’s identities. This REGISTER request looks like:

```
REGISTER SIP: home1.de SIP/2.0
Authorization: Digest Username=”user_private@home1.de”,
realm=”home1.de”, nonce=” ", uri=”SIP: home1.de”,
response=” "
```

When malicious user tries to launch SQL injection in IMS, he spoofs the SIP message and inserts the malicious SQL code in its authorization header. The malicious code infected with SQL injection looks like:

```
REGISTER SIP: home1.de SIP/2.0
Authorization: Digest
Username=”user_private@home1.de;delete table subscriber”,
realm=”home1.de”, nonce=” ", uri=”SIP: home1.de”,
response=” "
```

When P-CSCF receives a SIP message with an infected authorization header, it generates and executes the illegitimate SQL statement which may delete data in the database [41]. The existing solutions do not provide mitigation against this attack. The IMS also integrates HTTP Servlet container, therefore attacker can also utilize the HTTP message to launch the SQL injection attacks.

To detect SQL Injection, IDP-Centre parses the SIP message and checks SIP message containing username with semicolon in the SQL-statement. If this behavior is detected, the IDP-Core alerts that SQL-injection has been identified and further processing of SIP messages will be stopped from this user and his name is inserted in the Blacklist.

9.6.2 REGISTER Flooding Detection Methodology

The REGISTER flooding attack could be launched by generating multiple REGISTER SIP messages from single or multiple hosts to collapse the IMS resources. If this attack is launched from unknown and unregistered illegitimate users, there is initial REGISTER flooding on IMS core entities. AS a result lot of half open connection will be opened and IMS resources and services will not available to serve the legitimate users.

The REGISTER flooding detection method starts when the SIP messages flow start. First the IDP-Core starts timer to perform periodical checking of CPU load and counting of SIP messages. The time period is set with 500ms and the threshold value is defined as X = 80 % CPU load. If load reaches or crosses the threshold limit, the IDP-Core shifts from normal state to critical state and keeps processing all SIP REGISTER messages. After 500ms if the load condition remains the same, the IDP-core declares that IMS core is under flooding attacks. In under attack state, IDP-core rejects all unknown REGISTER requests while continues the processing of all other SIP messages. After the expiry of time period, the timer is reset and IDP-Core again verifies the P-CSCF load. This detection procedure is explained in state chart depicted in *figure 9.6.*

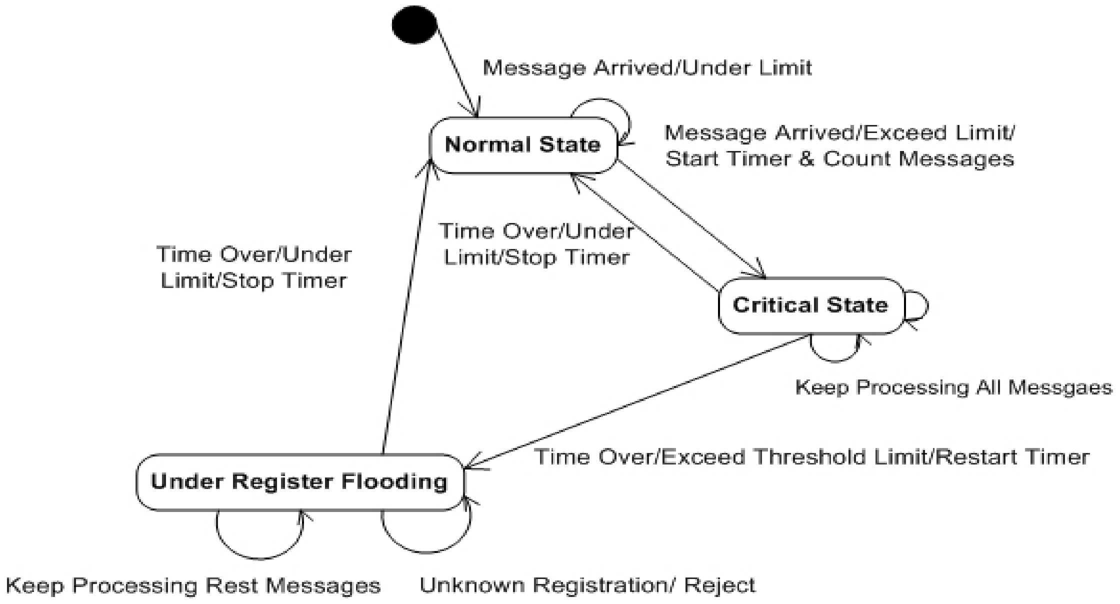

Message Arrived/Under Limit
Normal State
Message Arrived/Exceed Limit/
Start Timer & Count Messages
Time Over/Under
Limit/Stop Timer
Time Over/Under
Limit/Stop Timer
Critical State
Keep Processing All Messgaes
Time Over/Exceed Threshold Limit/Restart Timer
Under Register Flooding
Keep Processing Rest Messages
Unknown Registration/ Reject

Figure 9.6 REGISTER Flooding Detection State Chart

9.6.3 INVITE Flooding Detection Methodology

Similar to the previous method, IDP-Core starts timer to count the INVITE or Subscribe SIP messages. If flooding is detected, IDP-Core monitoring state change from normal to critical and it continues to process all the messages SIP messages. After 500 ms the timer is initialized and again it verifies the load condition. If it crosses the threshold, IDP-Core verifies that the flooding is due to INVITE messages and it stops all unknown messages. The INVITE flooding detection state chart is provided in *figure 9.7*.

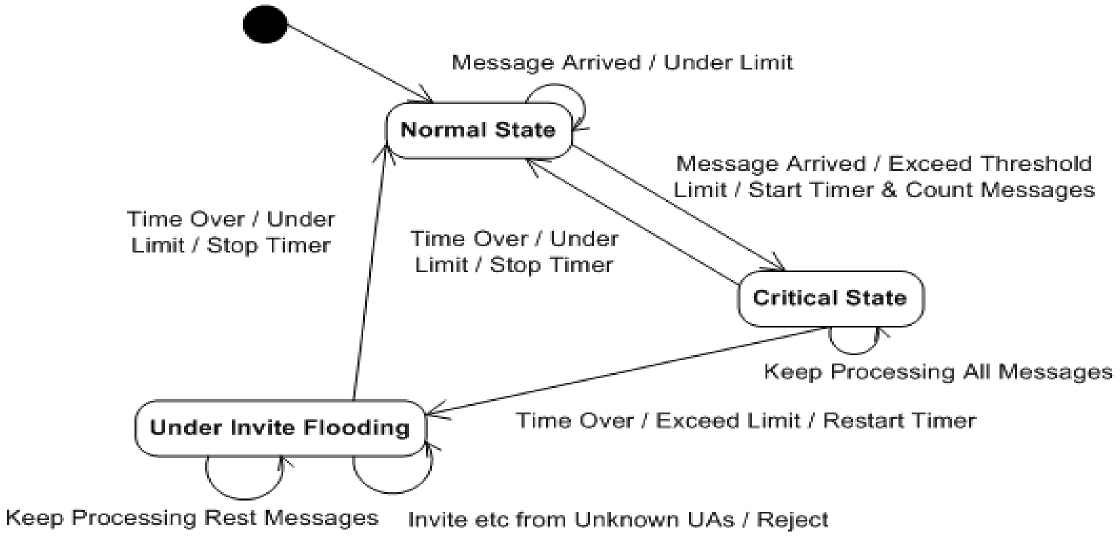

Message Arrived / Under Limit
Normal State
Message Arrived / Exceed Threshold
Limit / Start Timer & Count Messages
Time Over / Under
Limit / Stop Timer
Time Over / Under
Limit / Stop Timer
Critical State
Keep Processing All Messages
Time Over / Exceed Limit / Restart Timer
Under Invite Flooding
Keep Processing Rest Messages
Invite etc from Unknown UAs / Reject

Figure 9.7 INVITE Flooding Detection State Chart

9.7 IDP-Core Design Scenarios

After defining the attacks detection methodology, we discuss the design scenarios of IDP-Core with time-line diagrams for detecting SQL-Injection, REGISTER and INVITE DoS/DDoS flooding attacks.

9.7.1 REGISTER Flooding Design Scenario

When P-CSCF receives REGISTER messages from any user agent (UA) or user equipment (UE), the Dispatcher forwards them to IDP-Centre for secure verification. The System Monitor measures the CPU load monitoring and triggers the critical state in case of CPU overloading. The REGISTER flooding detection and prevention procedure is completed into four steps as explained in time line diagram provided in *figure 9.9*.

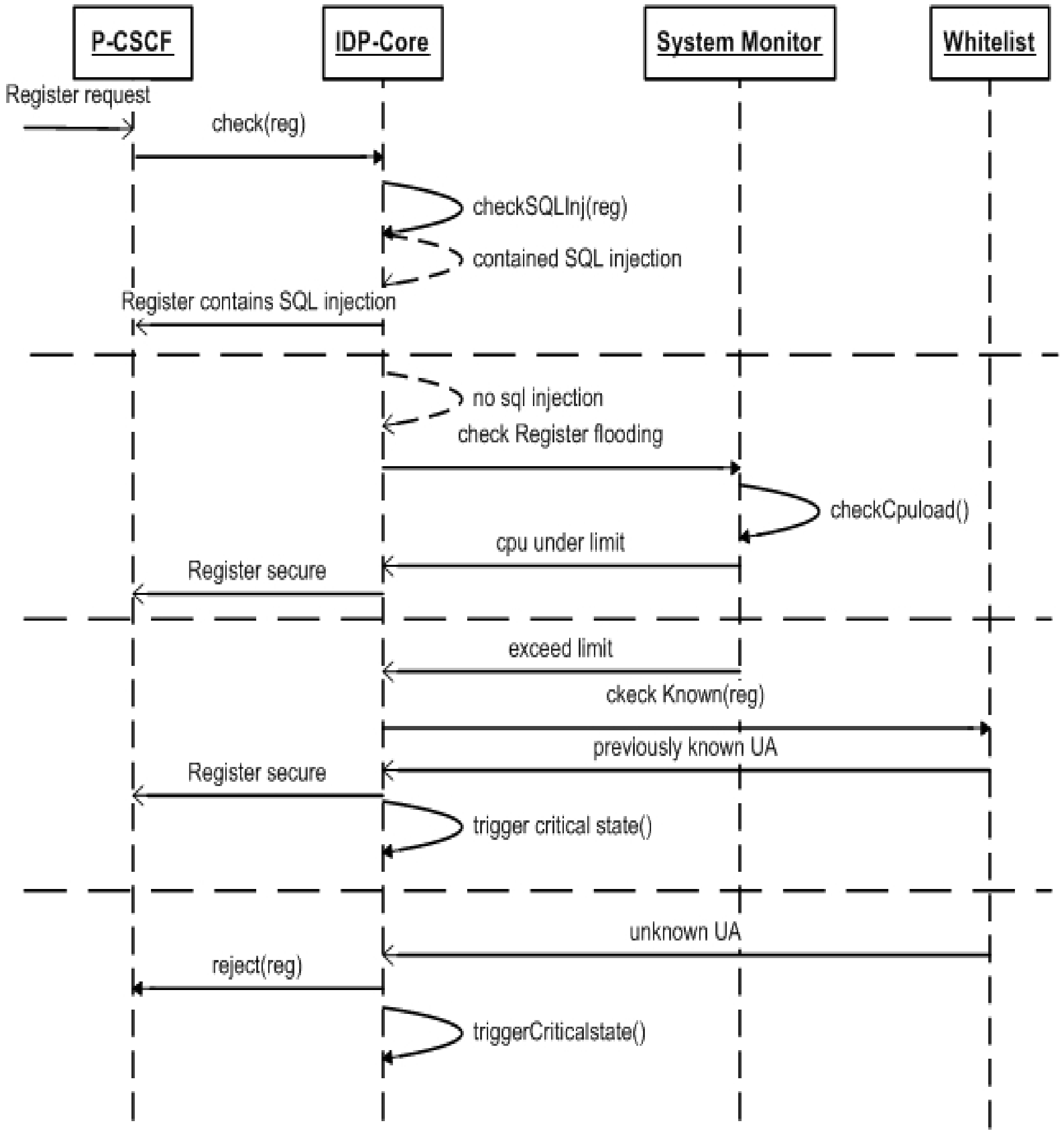


Figure 9.8 REGISTER Flooding Detection Time Line Diagram

9.7.2 INVITE Flooding Design Scenario

The INVITE flooding design scenario consists of three steps as explained in time line diagram in *figure 9.9.*

- In first step SQL injection is verified in normal state.
- In second step System Monitor performs the CPU load monitoring.
- In third step IDP-Core rejects the INVITE messages causing flooding attack.

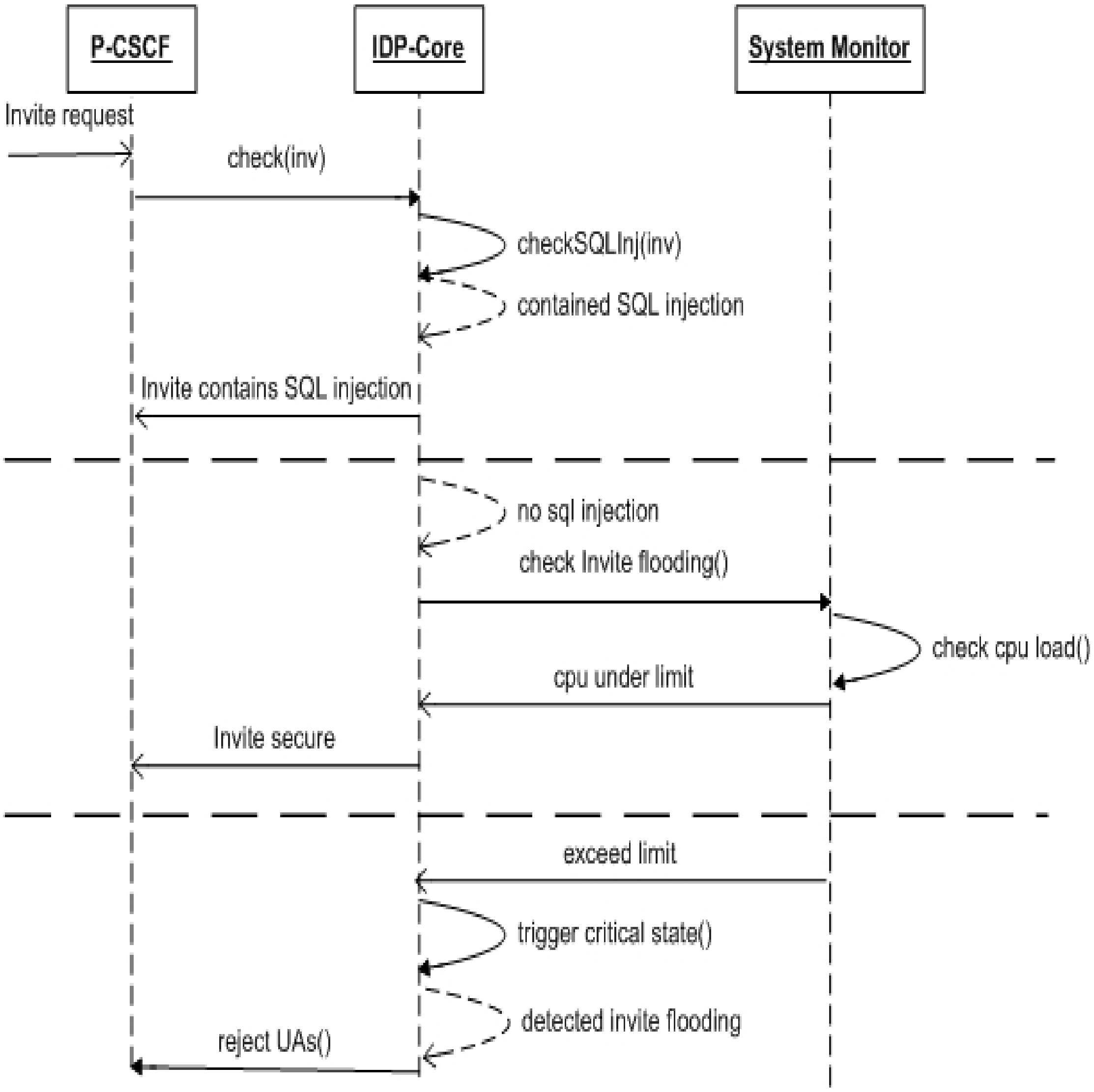


Figure 9.9 INVITE Flooding Detection Time Line Diagram

9.7.3 Password Guessing Design Scenario

In password guessing, the attacker gets a lot of 401-Response messages in reply to fake REGISTER requests to P-CSCF in order to crack the password. This attack could also be launched by legitimate user without breaking the authentication. The time line diagram is provided in *figure 9.10.*

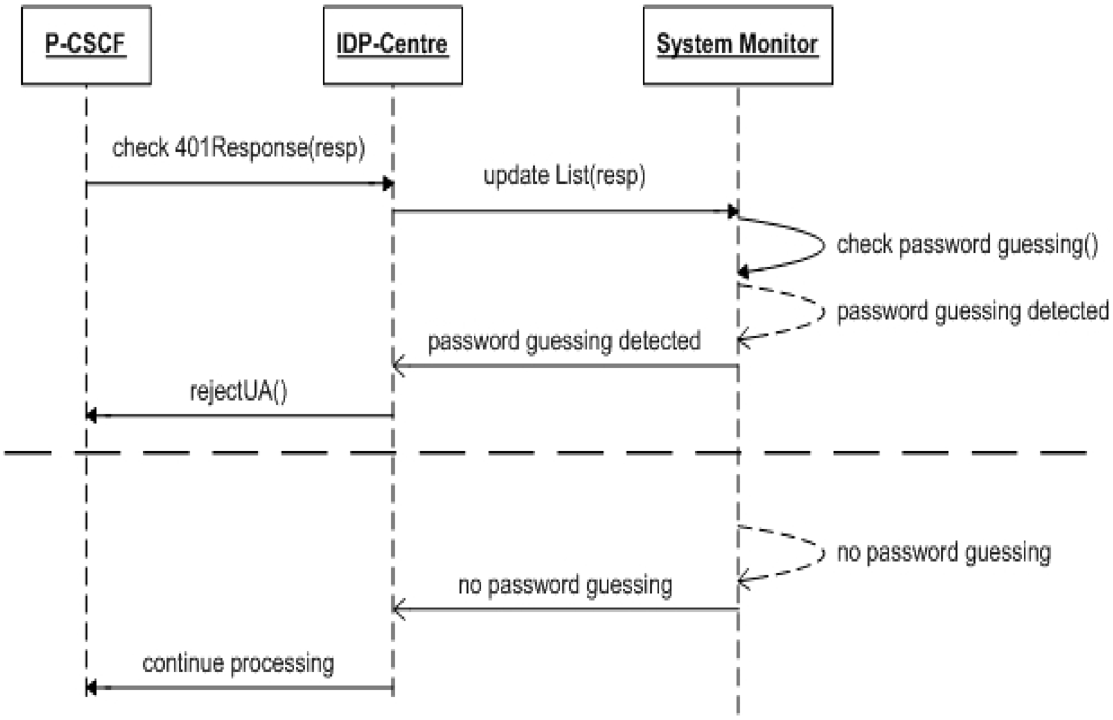


Figure 9.10 Password Guessing Time Line Diagram

9.8 Summary

This chapter covered the design and architecture of Intrusion Detection and Prevention (IDP-Core) system for IMS core. The chapter started with level 1 IMS security analysis which was necessary to understand the need of deploying IDP-Core. After that IDP-Core design requirement, reference architecture and attacks detection algorithms are discussed. Different design scenarios are elaborated at the end.

Chapter 10 IDP-Core Implementation

10.1 Introduction

This chapter describes the implementation of Intrusion Detection and Prevention (IDP-Core) system for the Open IMS core. The Fraunhofer FOKUS Open IMS core [79] is developed in C/C++; therefore IDP-Core is also developed in C/C++. In the following section, we describe the realization of the mechanism with which the IDP-Core can intercept the messages before the P-CSCF processes them. The implementation of “pids” module - kernel of the IDP-Core – and CPU load monitoring algorithm are explained in subsequent sections.

10.2 Modified Main Route Block

The components of FOKUS Open IMS Playground [80], except the Home Subscriber Server (HSS), are based on the SIP Express Router (SER) [81]. In this environment, SIP Express Router plays the roll of a SIP container that receives the SIP messages and enables the basic functionality of handling the SIP messages. Most of SERs functionality is offered through its modules. The Open IMS Playground is also based on modular approach. Hence, the P-CSCF is developed and deployed as a module within SER. An important feature of SER is to use a configuration file to manage the messages dispatching.

This configuration file has following seven main logical sections:

Global Definitions contains the IP address and listening ports, debug level, etc. Any change or setting in this section affects the SER daemon [81].

Modules Section contains a list of external libraries that are needed to expose functionality not provided by the core.

Modules Configuration defines the configuration parameters for the external libraries specified in the Modules section for their proper functionality.

Main Route Block is analogous to a C programs main function. This is the entry point of processing a SIP message and controls how each received message is handled.

Secondary Route Blocks: In addition to the main route block, the configuration file may contain additional route blocks that can be called from the main route block or from other secondary route blocks. A secondary route block is analogous to a subroutine.

Reply Route Block: Optional reply route blocks may be utilized to handle replies to SIP messages.

Failure Route Block: Optional failure route blocks may use when special processing is needed to handle failure conditions such as a busy or timeout;

The IDP-Core is a part of the modified secure P-CSCF rather than a standalone module of IMS core. In order to intercept messages, we need to export the entry function of IDP-Core in the main program of module "PCSCF".

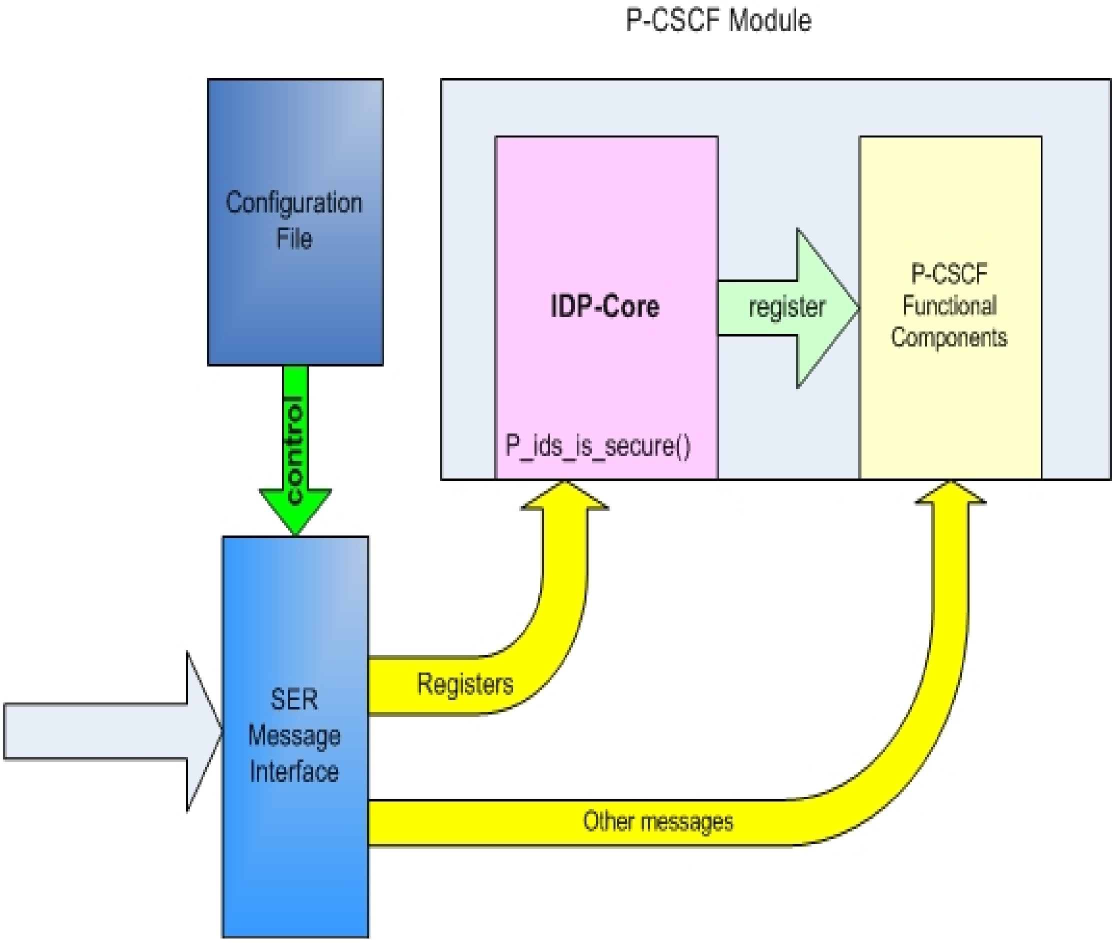


Figure 10.1 Modified Main Route Block Intercepting Approach

Look at the following the codes fragment of main program "mod.c":

```
static cmd_export pcscf_cmds[] = {
          {"P_add_path", P_add_path, 0,0, REQUEST_ROUTE},
           ... ...
          {"P_ids_is_secure", P_ids_is_secure, 0, 0,
REQUEST_ROUTE},
           ... ...
};
```

This array "pcscf_cmds" provides both name mapping of all exported function and message types to which these functions are applied. Then the export function should be included in the above "Main Route Block" corresponding to the requirement. In our case, all REGISTER requests should be checked by the function "P_ids_is_secure" before the PCSCF's procedure. The configuration of main route block is changed as follows:

```
             route{
           ... ...
             if(method=="REGISTER"){
                     if(P_ids_is_secure()){
                             route(REGISTER);
                    }
                  break;
            }
             ... ...
  }
```

The main route block intercepting approach is depicted in *figure 10.1.*

10.3 The Implementation of "P-ids" Module

The "pids" module consists of three subroutines. The first subroutine is for message processing, second for password guessing and the third subroutine for resource monitoring. The functionalities are explained with flow control diagram in the following:

10.3.1 SIP Message Processing Subroutine

The message processing routine accepts the SIP messages and processes them against message tampering and flooding attacks as illustrated in the flow control diagram in *figure 10.2.* First P-ids accepts the message and checks the overloading condition. If condition is true, then checks user is legitimate. If condition is true, forward the SIP message to the P-CSCF, otherwise block the messages and put the source IP address into IPtables.

If the overloading condition is false, then process the message against SQL-injection. If SQL-injection is detected, drop the messages, otherwise the messages is considered as secure and forwards the SIP message to P-CSCF.

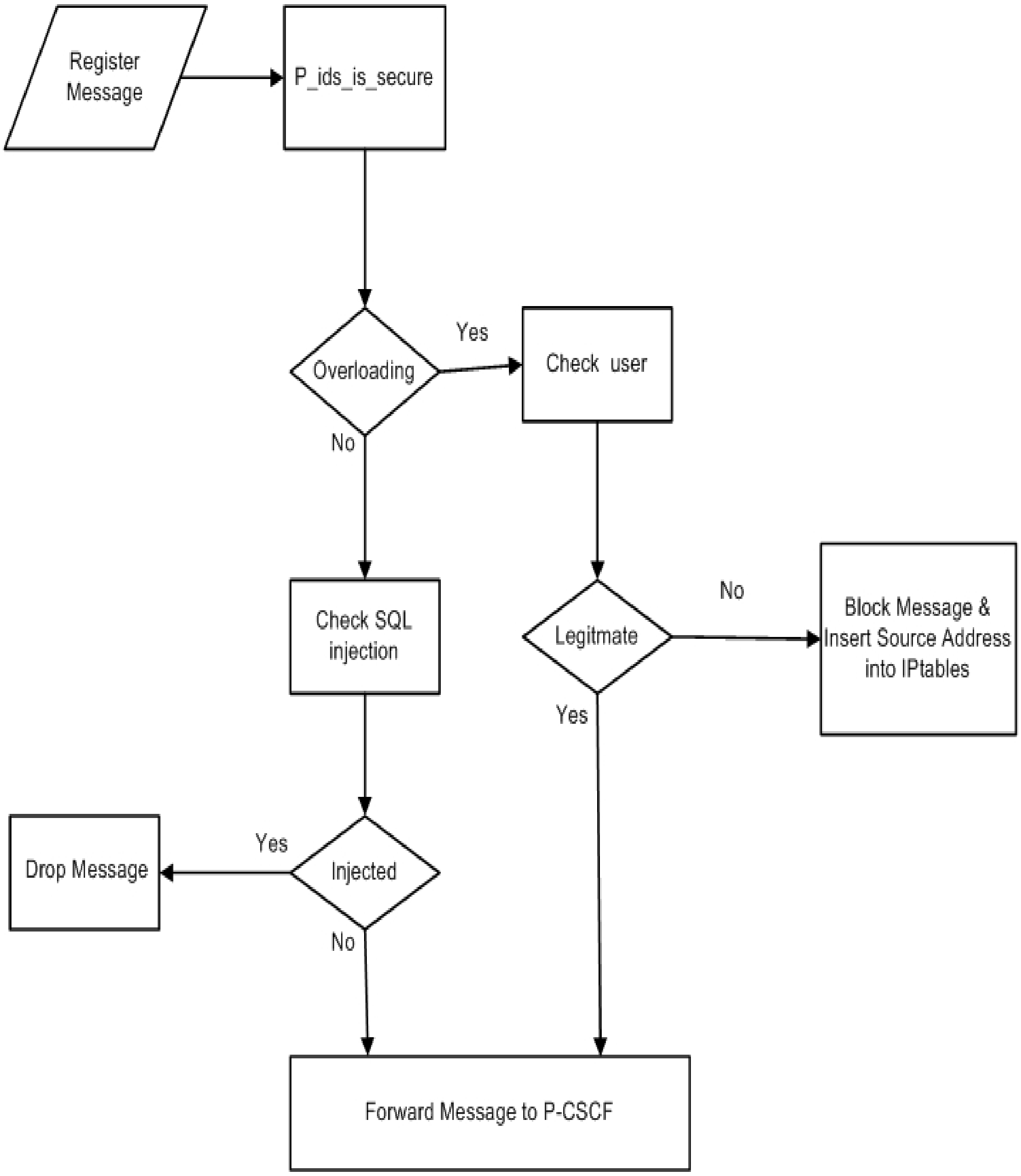


Figure 10.2 SIP Messages Processing Flow Control

10.3.2 Password Guessing Detection Subroutine

The password guessing attack detection implementation procedure is explained in flow graph as depicted in *figure 10.3.* If P-CSCF receives more than five 401 Responses within one minute from same URI/IP Address, than we assume it is password guessing attack and IDP-Core inserts this URI/IP Address in the Blacklist.

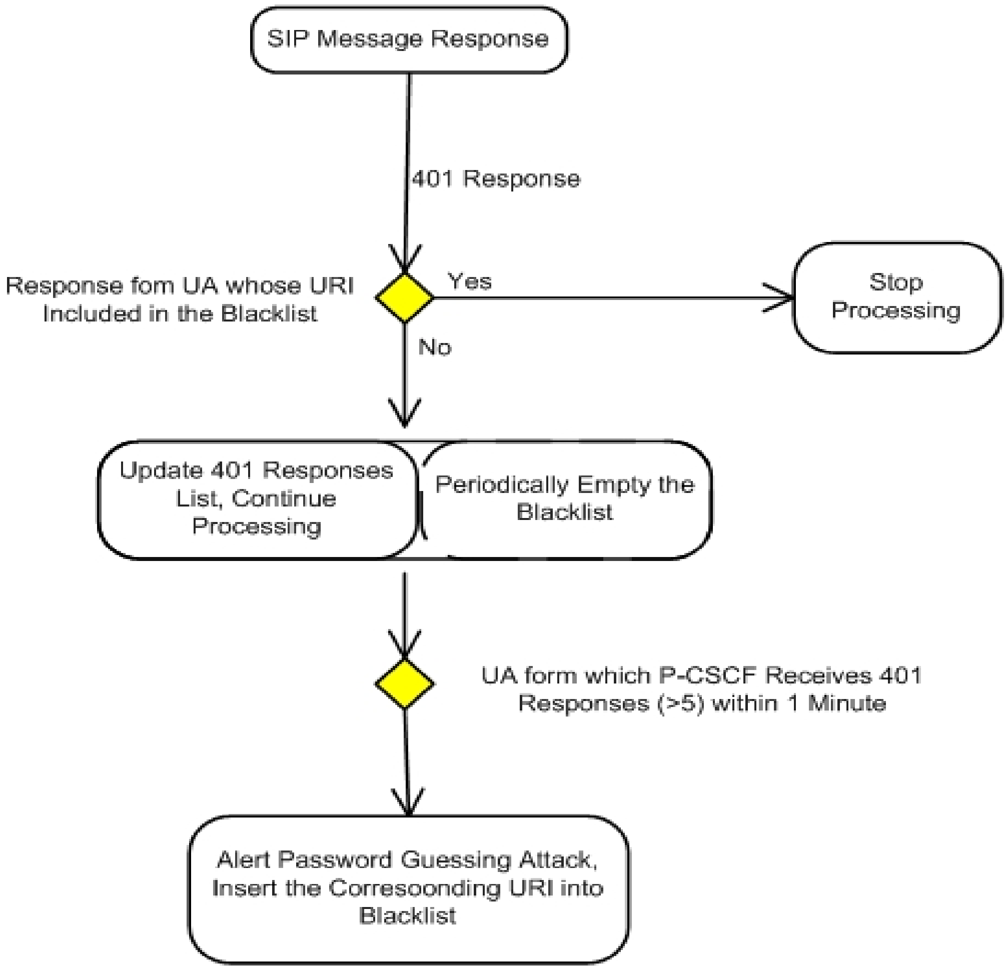

SIP Message Response
401 Response
Response fom UA whose URI Included in the Blacklist
Yes
Stop Processing
No
Update 401 Responses List, Continue Processing
Periodically Empty the Blacklist
UA form which P-CSCF Receives 401 Responses (>5) within 1 Minute
Alert Password Guessing Attack, Insert the Corresoonding URI into Blacklist

Figure 10.3 Flow Control for Processing the 401 Response

10.3.3 CPU Load Monitoring Subroutine

To measure the P-CSCF CPU load, the IDP-Core has utilized operating system Linux resource monitoring file /proc/stat [82]. The resource monitoring function has the following seven parameters about CPU performance.

- user: normal processes executing in user mode
- nice: niced processes executing in user mode
- system: processes executing in kernel mode
- idle: twiddling thumbs
- iowait: waiting for I/O to complete
- irq: servicing interrupts
- softirq: servicing soft interrupts

The parameters/columns *idle and iowait* represent the CPU free resources. These seven parameters at time T1 and at time T2 are provided in *table 10.1*.

CPU Parameters	**Parameters at Time T1**	**Parameters at Time T2**
User	USE1	USE2
Nice	NIC1	NIC2
System	SYS1	SYS2
Idle	IDL1	IDL2
IOWait	IOW1	IOW2
Irq	IRQ1	IRQ2
SoftIrq	SIRQ1	SIRQ2

Table 10.1 CPU Utilization Parameters

In light of above parameters we calculate the CPU utilization in two time frames and the corresponding CPU load. The total time T1 utilization is given in *equation 10.1*:

$$\sum T_1 = USE_1 + NIC_1 + SYS_1 + IDL_1 + IOW_1 + IRQ_1 + SIRQ_1 \qquad (10.1)$$

In this time frame, the CPU utilization is given in *equation 10.2*.

$$BUSY_1 = \sum T_1 - IDL_1 - IOW_1 \qquad (10.2)$$

The total time frame T2 and CPU utilization are provided in equations *10.3 and 10.4* respectively.

$$\sum T_2 = USE_2 + NIC_2 + SYS_2 + IDL_2 + IOW_2 + IRQ_2 + SIRQ_2 \qquad (10.3)$$

$$BUSY_2 = \sum T_2 - IDL_2 - IOW_2 \qquad (10.4)$$

From the above four equations, we calculate the P-CSCF CPU processing load given in *equation 10.4.*

$$L_{CPU} = \frac{BUSY_2 - BUSY_1}{\sum T_2 - \sum T_1} \qquad (10.5)$$

The threshold limit and sampling rate are provided in *equations 10.6 and 10.7* respectively.

$$Limit_{Threshold} = X = 80\% \tag{10.6}$$

$$Rate_{Sampling} = \frac{2}{1Sec} = 500\,ms \tag{10.7}$$

10.4 Flow Control and Object Interaction Scenarios

The implementation of SIP messages processing and resource monitoring are explained in the following with flow controls and object interaction scenarios.

10.4.1 REGISTER Message Processing

The REGISTER processing scenario is depicted in *figure 10.4*. The IDP-Core receives SIP REGISTER messages and processes them against defined attacks. The System Monitor measures the P-CSCF CPU load and Repository acts as Whitelist that maintains the list of previously successfully registered users.

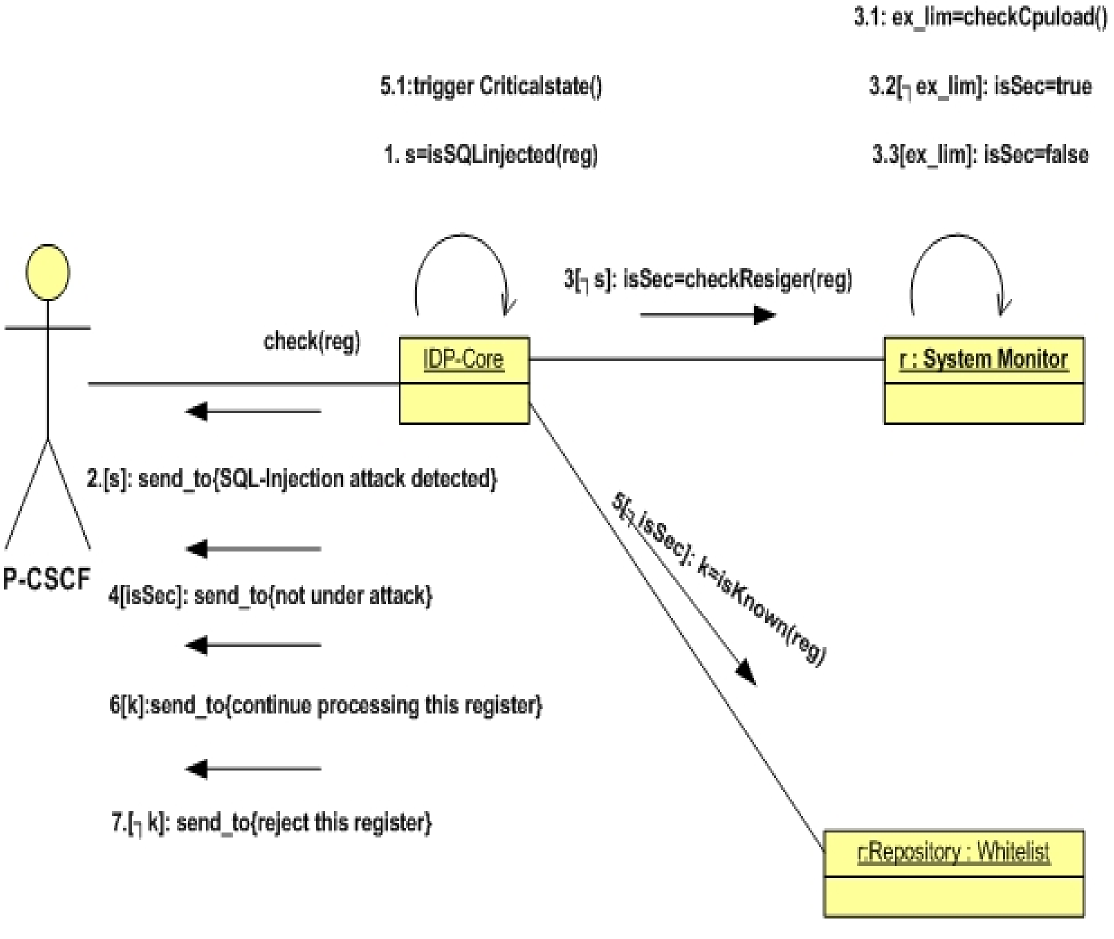

3.1: ex_lim=checkCpuload()
5.1:trigger Criticalstate()
3.2[¬ ex_lim]: isSec=true
1. s=isSQLinjected(reg)
3.3[ex_lim]: isSec=false
3[¬ s]: isSec=checkResiger(reg)
check(reg)
IDP-Core
r : System Monitor
2.[s]: send_to{SQL-Injection attack detected}
5[¬ isSec]: k=isKnown(reg)
P-CSCF
4[isSec]: send_to{not under attack}
6[k]:send_to{continue processing this register}
7.[¬ k]: send_to{reject this register}
rRepository : Whitelist

Figure 10.4 REGISTER Flooding Object Interaction Scenario

The implementation detailed procedure of SIP REGISTER processing is explained in flow control in *figure 10.5.*

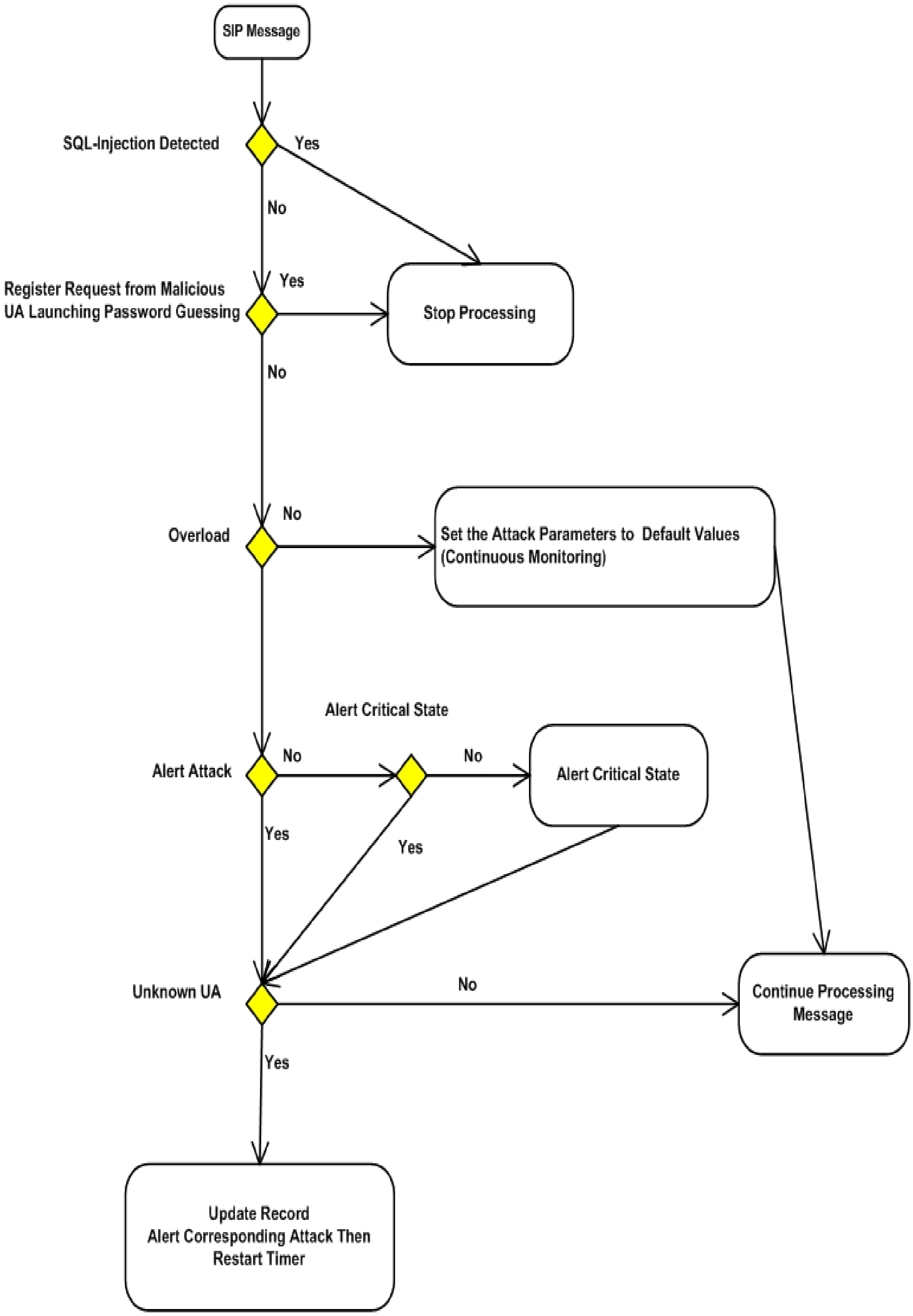

SIP Message
SQL-Injection Detected
Yes
No
Register Request from Malicious UA Launching Password Guessing
Yes
Stop Processing
No
Overload
No
Set the Attack Parameters to Default Values (Continuous Monitoring)
Alert Critical State
Alert Attack
No
No
Alert Critical State
Yes
Yes
Unknown UA
No
Continue Processing Message
Yes
Update Record Alert Corresponding Attack Then Restart Timer

Figure 10.5 REGISTER Flooding Detection Flow Control

10.4.2 INVITE Message Processing

In the second scenario, the SIP INVITE flooding detection object-interaction model depicted in *figure 10.6*, where the IDP-Centre compares the user address of each INVITE message with the addresses stored in Blacklist. While the System Monitor monitors the P-CSCF CPU load.

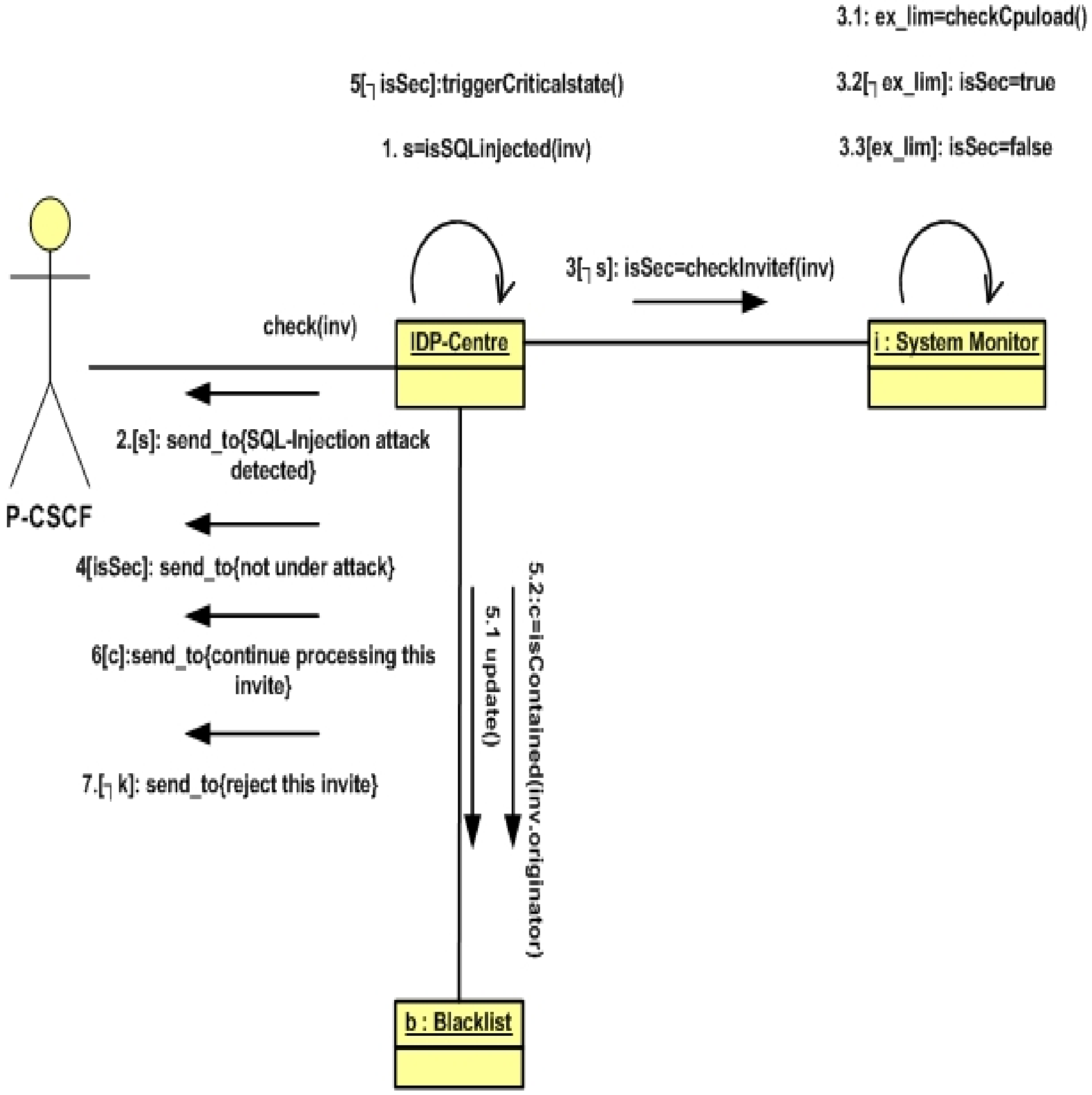

3.1: ex_lim=checkCpuload()
5[¬ isSec]:triggerCriticalstate()
3.2[¬ ex_lim]: isSec=true
1. s=isSQLinjected(inv)
3.3[ex_lim]: isSec=false
3[¬ s]: isSec=checkInvitef(inv)
check(inv)
IDP-Centre
i : System Monitor
2.[s]: send_to{SQL-Injection attack detected}
P-CSCF
4[isSec]: send_to{not under attack}
5.2:c=isContained(inv.originator)
5.1 update()
6[c]:send_to{continue processing this invite}
7.[¬ k]: send_to{reject this invite}
b : Blacklist

Figure 10.6 INVITE Flooding Object Interaction Model

The detailed implementation procedure is explained in flow control as depicted in *figure 10.7*.

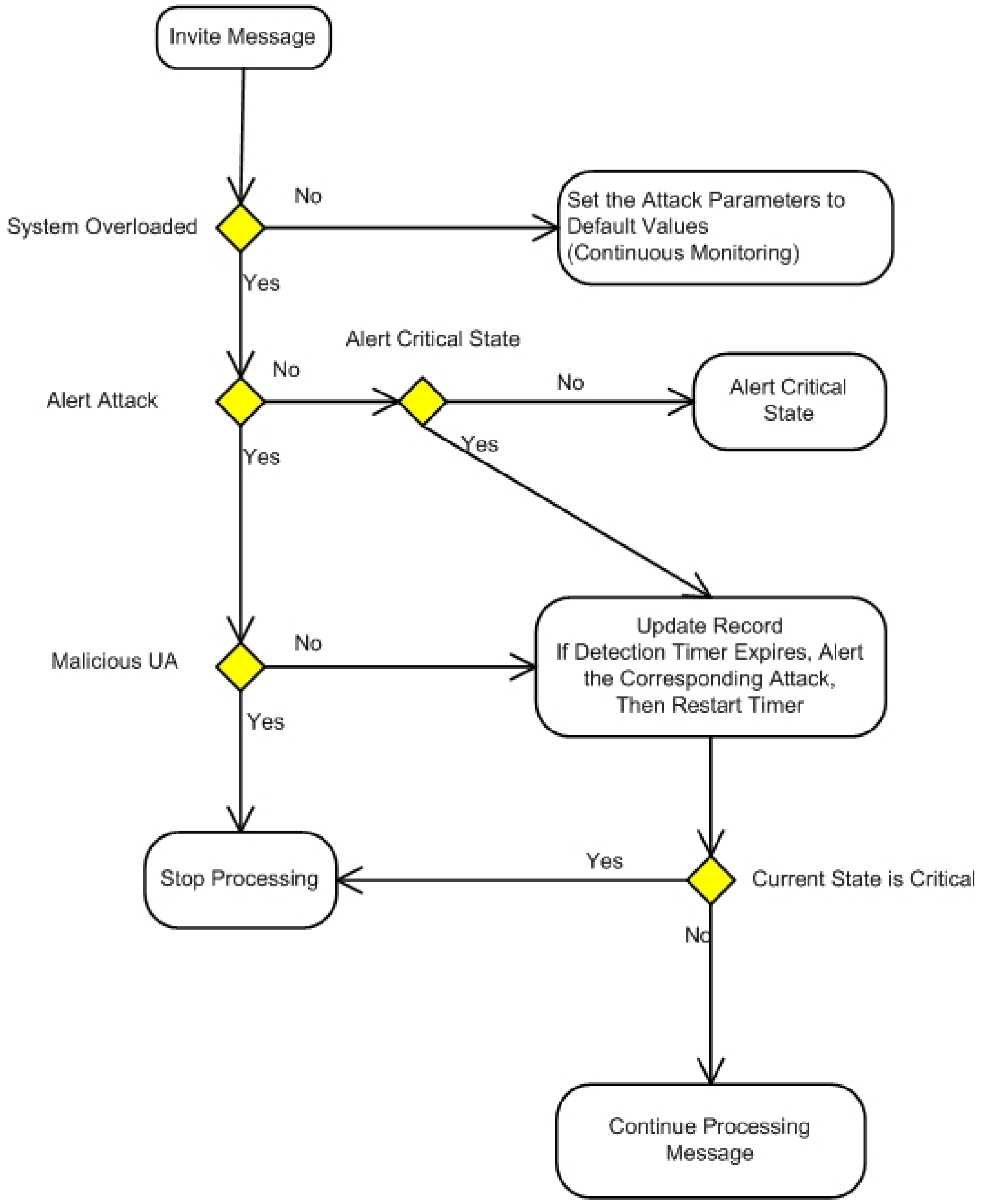

Invite Message
System Overloaded
No
Yes
Set the Attack Parameters to Default Values (Continuous Monitoring)
Alert Critical State
Alert Attack
No
No
Alert Critical State
Yes
Yes
Update Record If Detection Timer Expires, Alert the Corresponding Attack, Then Restart Timer
Malicious UA
No
Yes
Stop Processing
Yes
Current State is Critical
No
Continue Processing Message

Figure 10.7 INVITE Flooding Detection Flow Control

10.5 Mechanism for Preventing Flooding Attacks

In the design of IDP-Core we have considered two options to block the addresses of illegitimate users: (1) blocking the IP address at network layer, (2) blocking the URI (Uniform Resource Identifier) at higher layer. If we apply second approach using URI to block suspicious user at application layer, there is not significant reduce of processing overhead and flooding. It means that higher layer blocking is not efficient and consumes lot of resources. Therefore, network layer blocking approach is more efficient and consumes less system resources. The IDP-Core has utilized IPtables [83] to block the address of illegitimate users causing flooding.

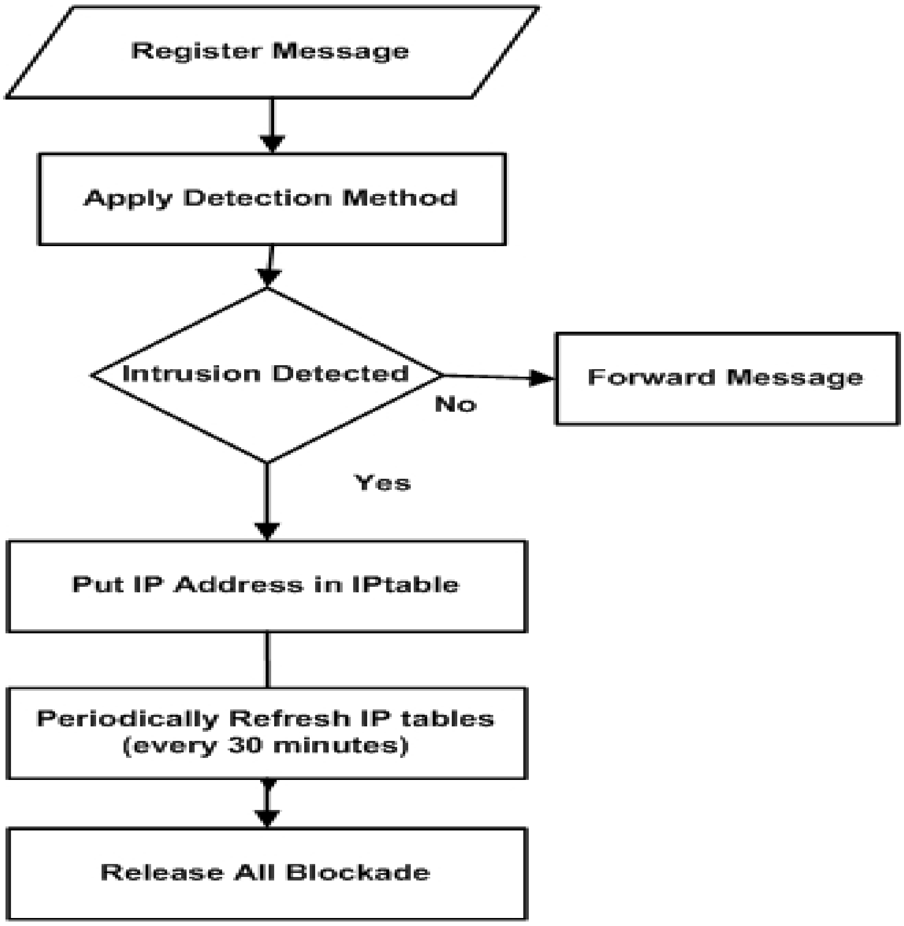


Figure 10.8 Use of IPtables to Prevent Flooding

The IPtables could be used to setup a firewall using net-filter approach. It has three rules and three policies to process the data packets.

The rules are:

(1) **Input** evaluates data packets received by the system.

(2) **Forward** processes data packets which are received and forwarded by the system.

(3) **Output** evaluates date packets sent or generated by the system.

The IPtables applies the following three policies to implement security and firewall:

(a) The **Accept Policy** accepts data packets that have not matched with any three rules.

(b) The **Reject Policy** discards the data packets matches with any three rules and sends an ICMP packet back to the source or originator.

(c) The **Drop Policy** simply rejects all data packets without applying any rule option.

We can apply any policy on the three types of data with the following commends:

```
iptables -P Input <Accept, Reject or Drop>

iptables -P Forward <Accept, Reject or Drop>

iptables -P Output  <Accept, Reject or Drop>
```

In our case, if intrusion and flooding attack is detected, the IDP-Core inserts the malicious IP address in the IPtables to block further flooding from that source as depicted in *figure 10.8*. The IPtables entries are refreshed after every 30 minutes so that these IP addresses should not blocked permanently.

10.6 Summary

In this chapter we have explained the implementation of IDP-Core within P-CSCF. The procedure "intercept SIP messages" is explained. The subroutines include SIP message processing, password guessing and CPU load monitoring of P-CSCF. The flooding prevention method utilized IPtable to block the illegitimate users and attackers.

Chapter 11 IDP-Core Testing and Performance Evaluation

11.1 Introduction

In the performance evaluation, our focus is to calculate the processing overhead and delay caused by IDP-Core in both when the IMS core is under normal load and when it is overloaded. As we know that this module is deployed in between IMS client and IMS core, and it performs attacks detection on-line and real time, therefore the processing delay of IDP-Core is very critical.

Normally all the Intrusion Detection System (IDS) performs processing offline by making copy of each message, analyzing and generating reports. We have also claimed that it is lightweight security protocol. Both features should be tested in the performance matrix. In the following we shall discuss the testbed environment, test scenarios and performance evaluation.

11.2 Testbed Environment

To test IDP-Core prototype, the testing environment consists of following components:

- Open IMS-Core [79] and IDP-Core integrated with P-CSCF
- Open source UCT IMS client [84] acts as legitimate user
- Open source SIPp [85] which acts as illegitimate user launching flooding attacks on IMS.

The testbed is depicted in *figure 11.1.* We have explained the Open Source IMS core in the state-of-art review section. Here we discuss both the clients briefly.

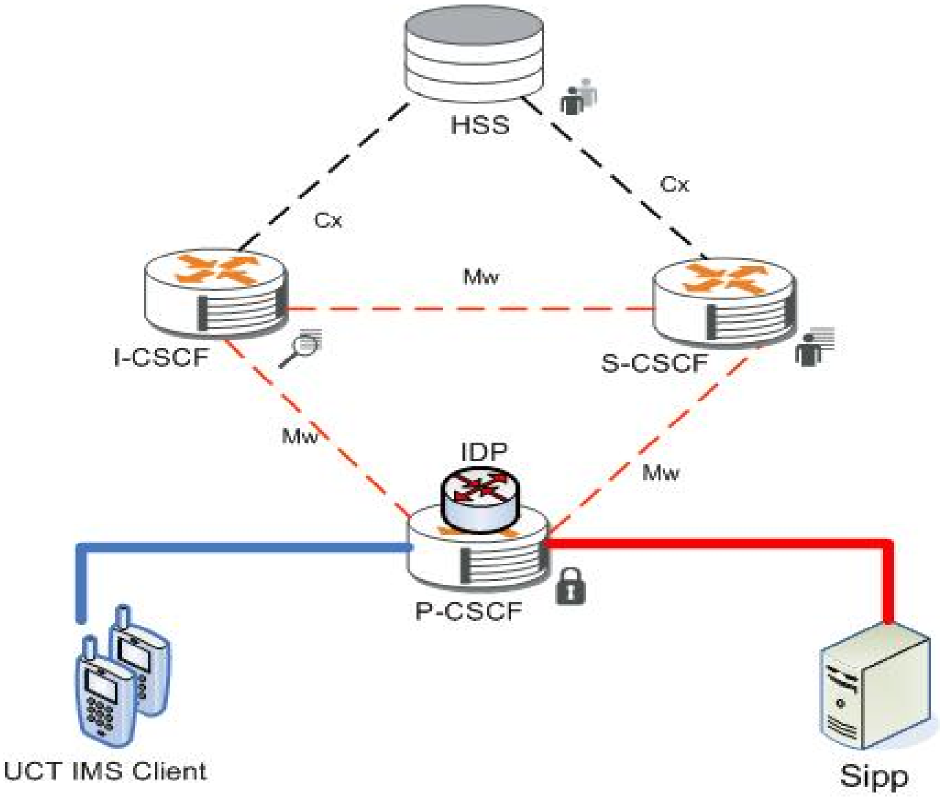


Figure 11.1 Testing Environment

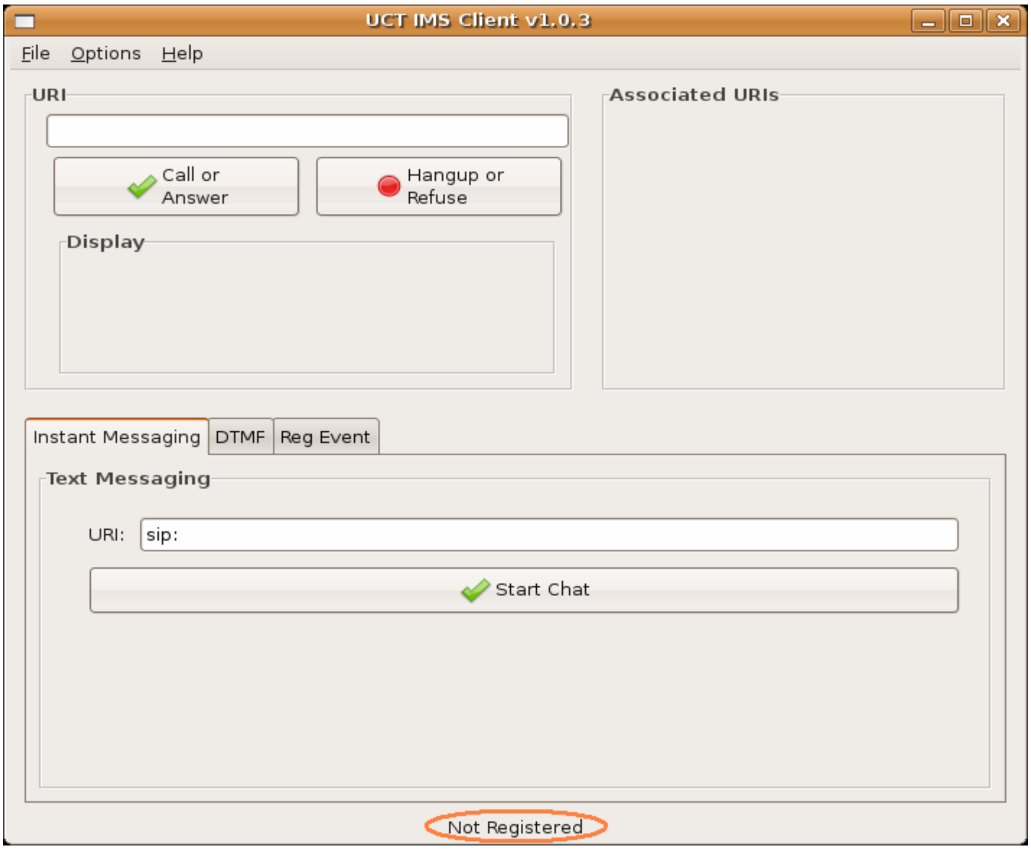
11.2.1 IMS Client

For legitimate user, we have used UCT IMS client [84] developed by Communication Research Group of University of Cape Town with objective to be used with Open IMS-Core [79] developed by NGNI Competence Center of Fokus Fraunhofer Open Communication Institute [87]. The client is still in active development and current version is 1.0.3. The UCT IMS client user interface is shown in *figure 11.2*.

The main features include:

- AKAv1 and AKAv2 registration
- Subscribe to register event
- Supports provisional response acknowledgements (PRACK) and preconditions
- Signalling follows service routes
- INVITE contains p-preferred-identity and p-access-network information
- Supports private and public user identities
- Pager-mode instant messaging
- DTMF tones via SIP INFO messages

- It could be used as a normal SIP client



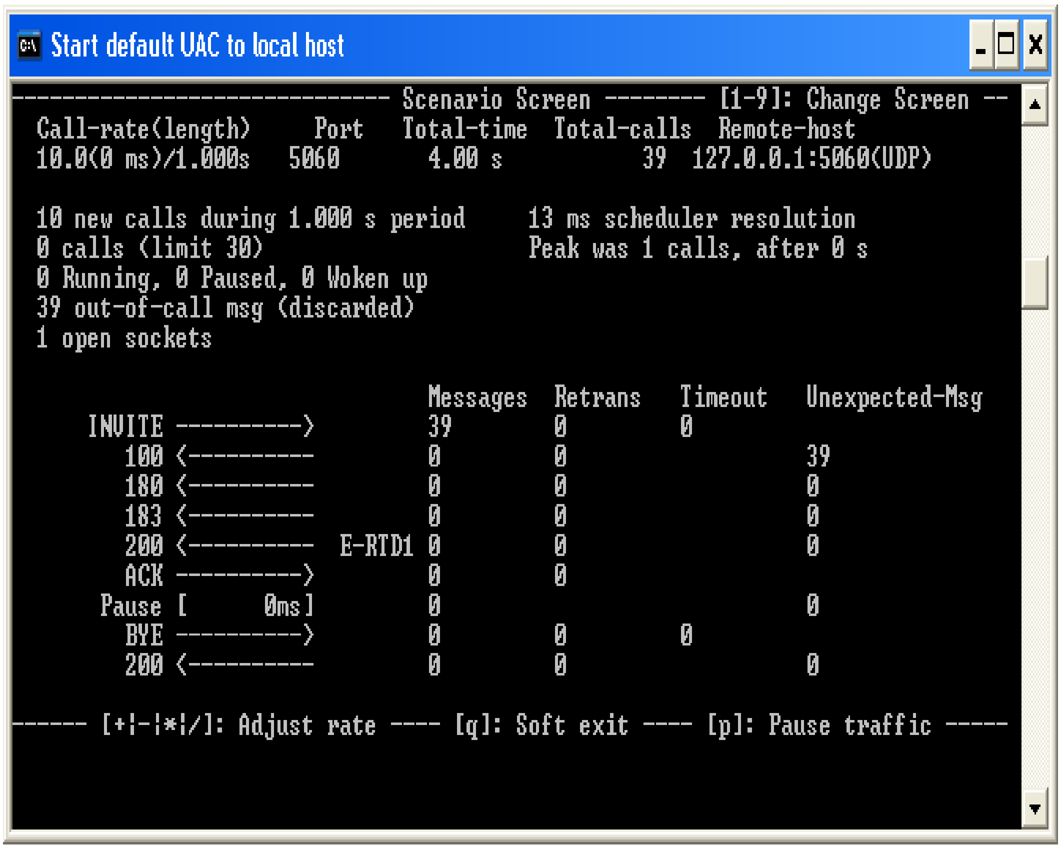
URI: sip:

Figure 11.2 UCT IMS Client Interface

11.2.2 SIPp Client

To launch attacks on IMS-Core, we have selected SIPp [85] which is open source SIP traffic generator and manages multiple calls with INVITE and BYE methods. It could generate one or more calls from one remote system. It can also transmit media traffic with RTP protocol. SIPp could be used to test SIP proxies, SIP media servers and SIP gateways etc. It helps developer to develop their own test scenarios written in XML. In our case, we have used SIPp to produce lot of SIP REGISTER requests to overload IMS Core specially P-CSCF. The user interface of SIPp is shown in *figure 11.3*. The important features of SIPp include:

- User Agent Client (UAC) and User Agent Server (UAS) scenarios
- Displays calls statistics like call rate, round trip delay etc.
- Manages multiple sockets and dynamic call rates.
- Supports of TCP, UDP, IPv6, TLS, SIP authentication etc.
- Actions like log, dump, system command, call stop etc.



```
------------------------------ Scenario Screen -------- [1-9]: Change Screen --
  Call-rate(length)     Port   Total-time  Total-calls  Remote-host
  10.0(0 ms)/1.000s   5060       4.00 s           39  127.0.0.1:5060(UDP)

  10 new calls during 1.000 s period     13 ms scheduler resolution
  0 calls (limit 30)                     Peak was 1 calls, after 0 s
  0 Running, 0 Paused, 0 Woken up
  39 out-of-call msg (discarded)
  1 open sockets

                                 Messages  Retrans   Timeout   Unexpected-Msg
      INVITE ---------->         39        0         0
         100 <----------         0         0                   39
         180 <----------         0         0                   0
         183 <----------         0         0                   0
         200 <----------  E-RTD1 0         0                   0
         ACK ---------->         0         0
       Pause [      0ms]         0                             0
         BYE ---------->         0         0         0
         200 <----------         0         0                   0

------ [+|-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----
```

Figure 11.3 SIPp Interface

11.3 Test Scenarios

To verify whether IDP-Core meets the functional requirements as discussed in design chapter, we have created following three test scenarios.

11.3.1 First Scenario: Successful Registration

In the first test scenario, the user legitimate user 'Alice' is registered in IMS via a UCT IMS Client. The IDP-Core should allow this registration and forward it to PCSCF. This scenario is described roughly in *figure 11.4.* In this case only one user agent (UA) is active; therefore the CPU load of P-CSCF is very low. The IDP-Core is almost transparent to the all UAs. The successful registration of Alice is depicted in *figure 11.5.*

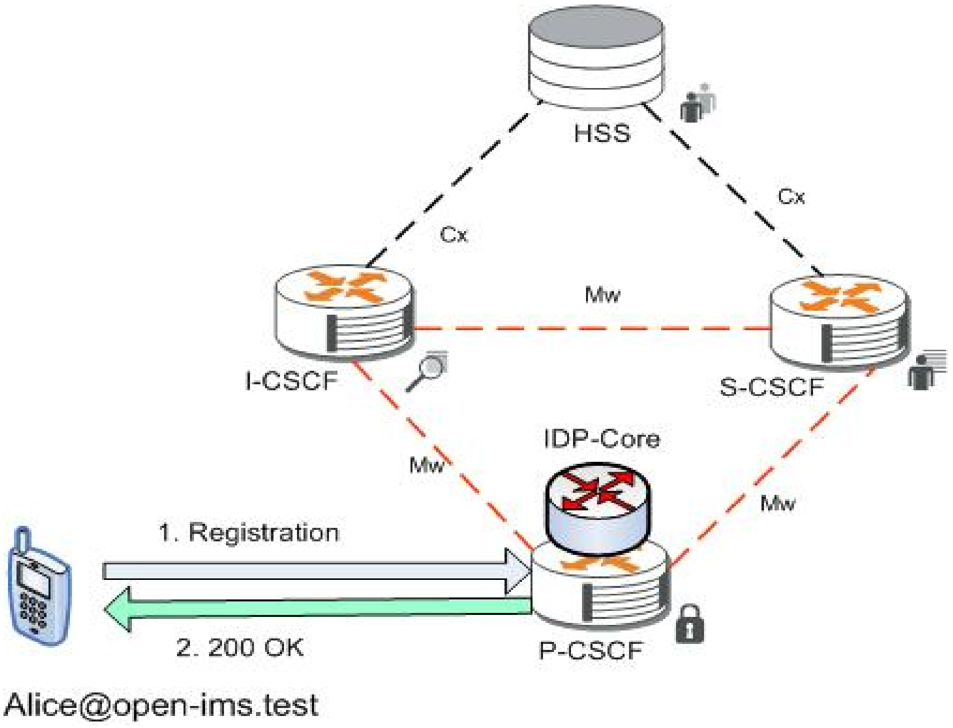
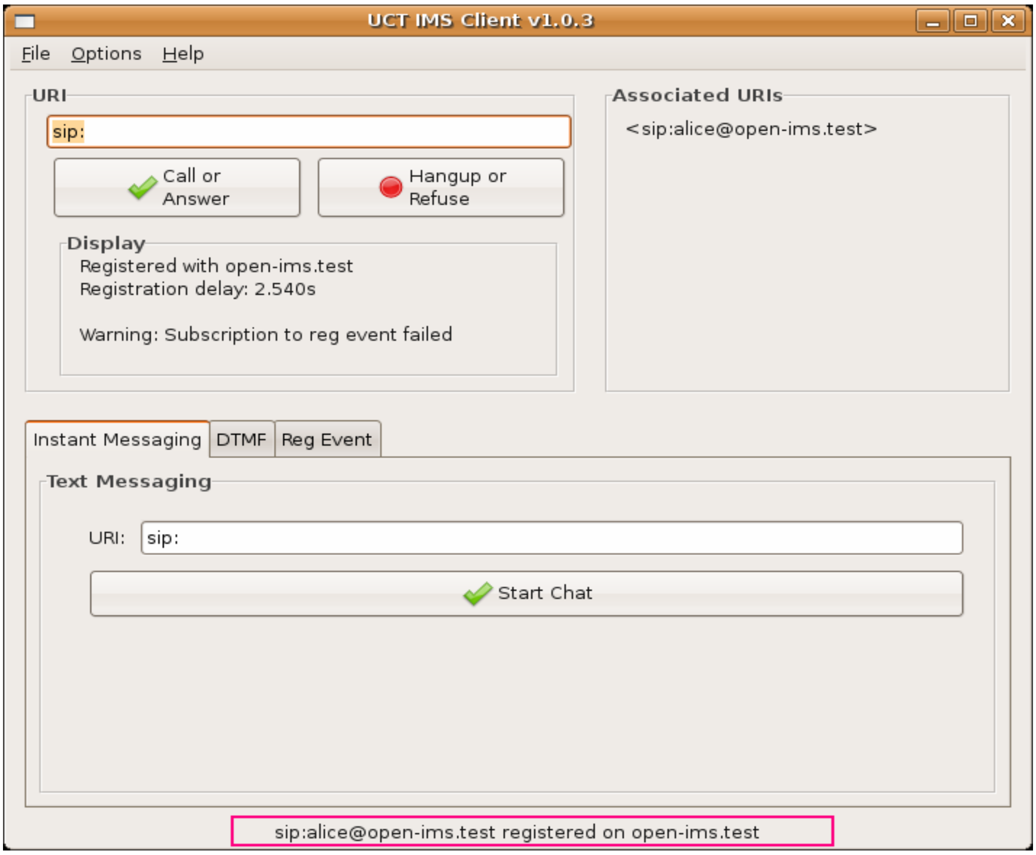


Figure 11.4 First Test Scenario



Display

Registered with open-ims.test
Registration delay: 2.540s

Warning: Subscription to reg event failed

<sip:alice@open-ims.test>

sip:alice@open-ims.test registered on open-ims.test

Figure 11.5 Alice Successful Registrations

11.3.2 Second Scenario – Illegitimate User

In the second test scenario, the attacker (SIPp) sends illegitimate REGISTER requests to P-CSCF with low rates. In this case the CPU loads remains under defined threshold limit, therefore the IDP-Core behaviour is the same as in the first scenario. It means all these illegitimate REGISTER messages are not processed by the flooding algorithm and simply passed through the IDP-Core. The I-CSCF and S-CSCF receive and forward these messages to the HSS. But the HSS replies with 4XX Response [86] as unknown user as depicted in *figure 11.6.* The consequences of this attack are not very serious and ultimately the HSS rejects these illegitimate REGISTER requests.

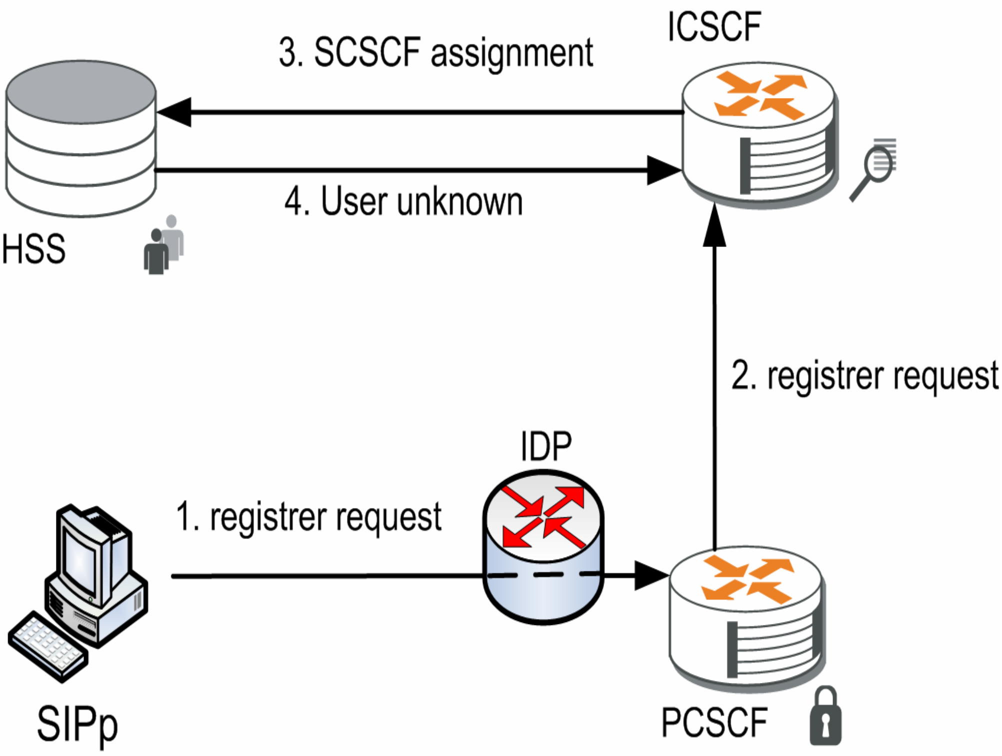


Figure 11.6 Second Test Scenario

11.3.3 Third Scenario: Flooding Condition

The third and last test scenario is serious threat to IMS core causing flooding and ultimately to overload the P-CSCF. The IDP-core should ensure that it can protect the IMS core against all types of Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks. In this case the attacker generates lot of REGISTER requests from single or multiple nodes and IDP-Core prevents them when CPU load crosses the threshold limit. Therefore IDP-Core activities and controls the REGISTER flooding attacks to protect the P-CSCF. This scenario is depicted in *figure 11.7* showing parallel actions sequence.

The SIPp client sends illegitimate random REGISTER requests at a rate of 1 million calls per second to overload the P-CSCF. Before reaching the CPU load to threshold limit, the P-CSCF routes all these flooding messages to next hop (I/S-CSCF).

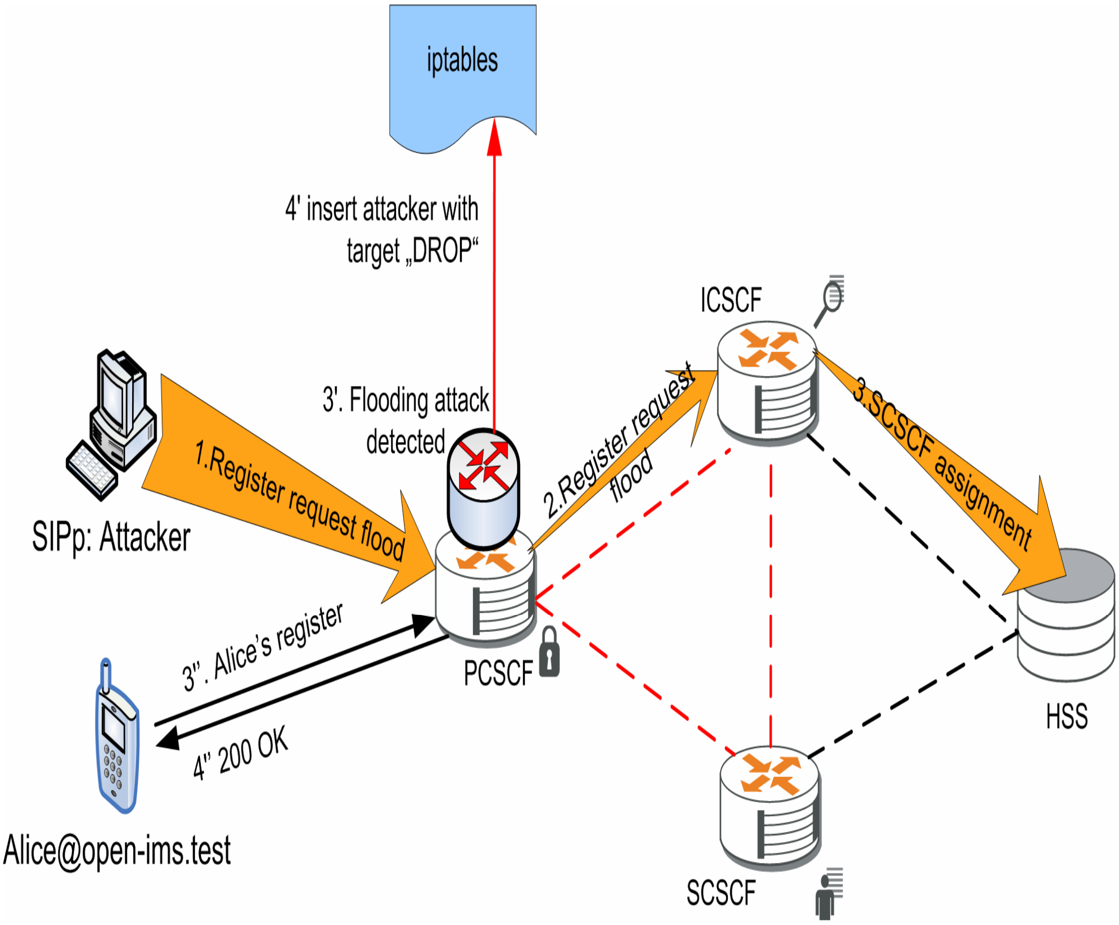
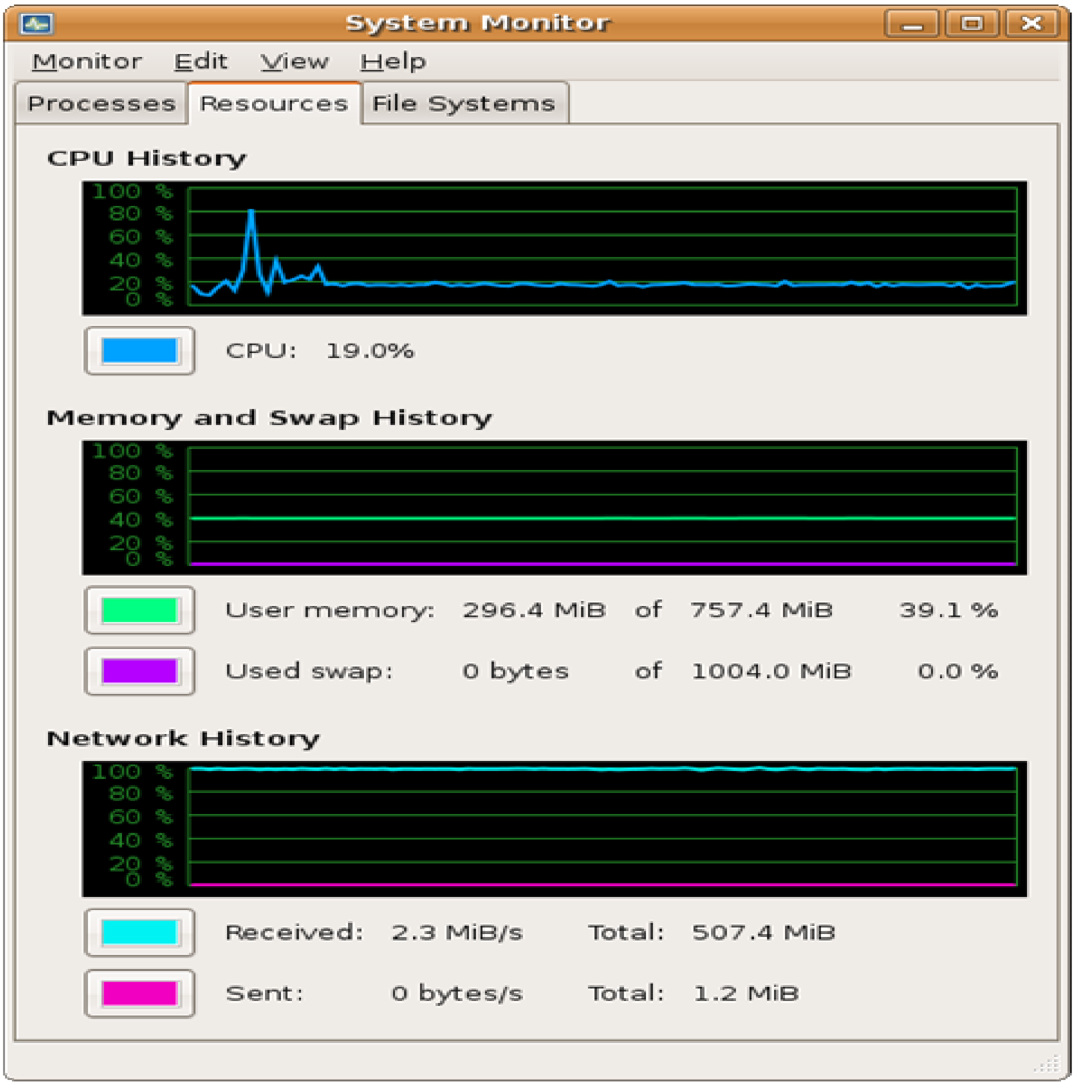


Figure 11.7 Third Test Scenario

As the CPU load reaches the threshold limit (80%) as shown in *figure 11.8*, the IDP-Core declares REGISTER flooding and the IP address of attacker (SIPp client) is inserted into Iptables. To block further REGISTER messages from attacker, the "Drop" rule of Iptables is utilized. Within very short time the CPU load goes to normal state. From the diagram, the *Network History* curve shows that the network interface or bandwidth is 100% consumed constantly by the received messages but the *CPU History* curve shows that IPD-Core has effectively controlled the flooding attack on IMS-Core.

Also it is important to note that during this attack situation what happens with the requests coming from legitimate users. The reliable user 'Alice' starts the registration procedure at the time of attack situation (step 3 = flooding and step 3 = registration). As the REGISTER request from Alice arrives at P-CSCF which is suffering flooding attack, the IDP-Core recognizes that this request is from the legitimate user agent which has previously successfully registered. Therefore P-CSCF continues this registration procedure. Only two-steps transaction between Alice and P-CSCF is shown in *figure 11.8* instead of complete registration process.



🟦 CPU: 19.0%

🟩 User memory: 296.4 MiB of 757.4 MiB 39.1 %

🟪 Used swap: 0 bytes of 1004.0 MiB 0.0 %

🟦 Received: 2.3 MiB/s Total: 507.4 MiB

🟪 Sent: 0 bytes/s Total: 1.2 MiB

Figure 11.8 System Monitoring Interface

11.4 Performance Evaluation

The important design consideration of IDP-Core is that it must not cause much delay during online and real time processing to avoid messages retransmission. In practical environment IMS Core, especially P-CSCF processes lot of registration and authentication messages. Therefore performance is very critical when IDP-Core is deployed in real world scenario. The performance metric is the average delay per message in milliseconds which we measures in normal and heavy load scenarios.

11.4.1 Performance Test at Normal Load

We start the test from 10 requests per second and gradually increase the call rate (req/s) up to 7000 requests per second as shown in *table 11.1*. The duration of each test flow is 10 seconds. The results show that there is no significant change in the processing delays due to increase of calls rate in normal load condition. The IDP

System fetches the value of a variable for each incoming SIP message and stores the latest CPU load and compares it with the defined threshold limit.

No of Requests/Sec	Average Delay (ms)
10 (req/s)	0.015
100 (req/s)	0.038
500 (req/s)	0.049
1000 (req/s)	0.053
2000 (req/s)	0.059
3000 (req/s)	0.068
4000 (req/s)	0.072
5000 (req/s)	0.081
6000 (req/s)	0.087
7000 (req/s)	0.086

Table 11.1 Average Delay under Normal CPU Load

These test results are depicted in *figure 11.9*, indicating that the average delay introduced by the IDP System is varies from 0.015 ms to 0.096 ms. This delay is negligible as compared to the entire message processing delay by IMS core.

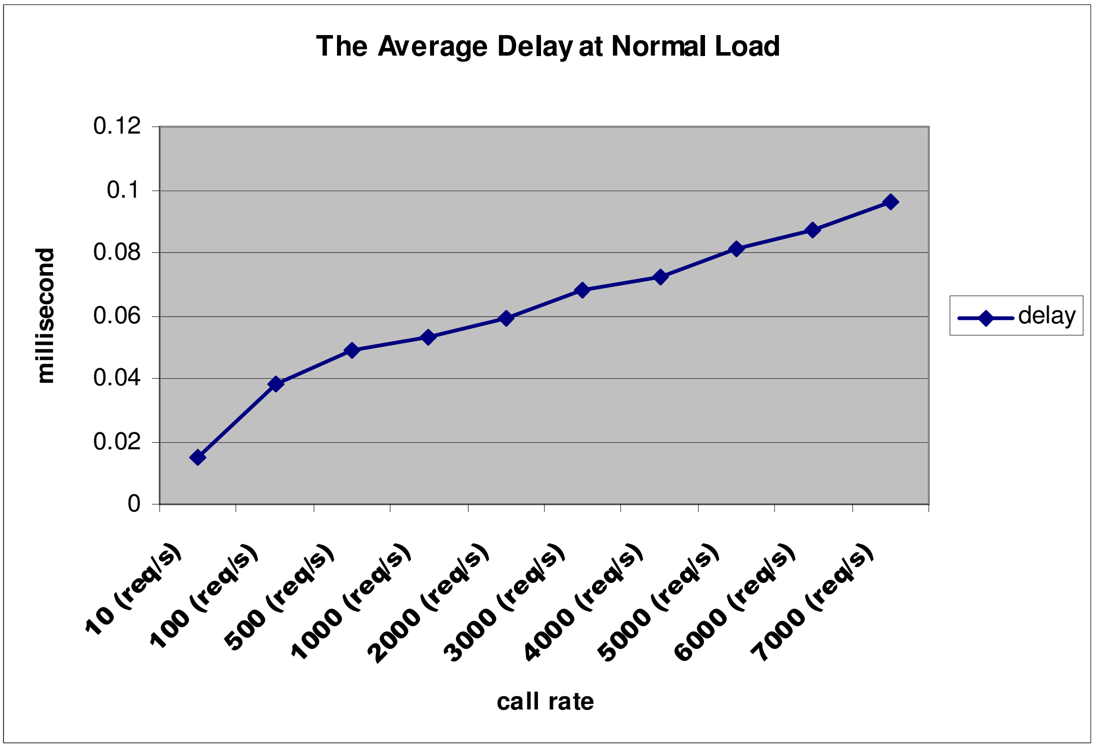


Figure 11.9 Average Message Processing Delay under Normal Load

11.4.2 Performance Test at CPU Overloading

To overload CPU of P-CSCF, we have generated lot of SIP flooding traffic by using SIPp on multiple nodes. The flooding limit starts from 10,000 requests per second which increases up to 100,000 requests per second. The duration for each test is 5 seconds.

No of Requests/Sec	Average Delay (ms)
10000(req/s)	0.031
20000(req/s)	0.053
30000(req/s)	0.055
40000(req/s)	0.067
50000(req/s)	0.077
60000(req/s)	0.078
70000(req/s)	0.083
80000(req/s)	0.084
90000(req/s)	0.091
100000(req/s)	0.101

Table 11.2 Average Delay during CPU Overloading

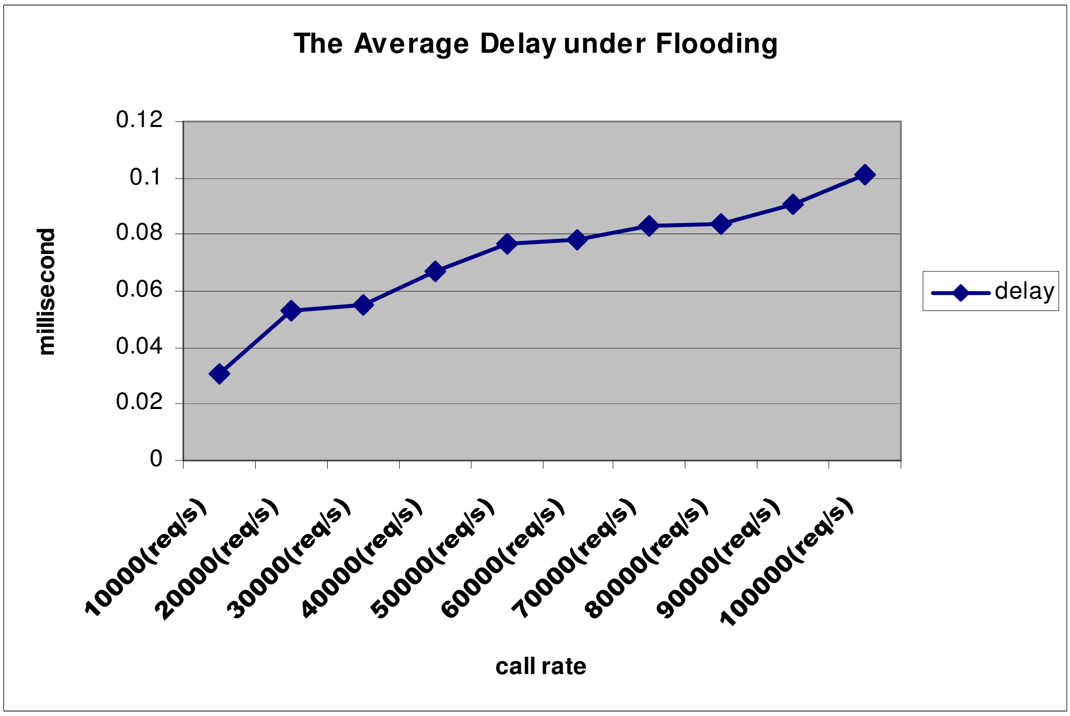


Figure 11.10 Average Delay during CPU Overloading

Once the IDP-Core detects SIP messages flooding attacks from any malicious user, it drops further requests from the attacker by inserting its IP address in the Iptable. In this scenario, the delay introduced by the IDP-Core is in the range of 0.031 ms to 0.101 ms.

These test results indicate that the IMS IDP-Core prototype performances are very reliable and the overhead delays are also very small in both test conditions.

11.5 Summary

In this chapter the performance of IDP-Core is evaluated in normal and overload flooding scenarios. The developed prototype met the design requirements in both providing safeguard against REGISTER flooding and performing real-time and online processing with very small overhead delay.

Part-E

Design and Implementation of Intrusion Detection and Prevention System for IMS Applications Servers (IDP-AS)

(Level 2 Security – Section 2)

Design and Implemenation of IDP-AS

The Part-E describes section 2 of level 2 extended IMS security solution. Its objective is to protect IMS Application Server from misuse of IMS services. This part consists of three chapters (from 12 to 14) focusing on the design and development, implementation, testing and performance of Intrusion Detection and Prevention system for IMS Application Server (IDP-AS). It is based on IMS Application Server - SIPSEE (SIP Servlet Execution Environment) developed by Fraunhofer FOKUS Open Communication Institute. The IDP-AS is developed in Java. Functionality of each chapter is briefly explained as follows:

Chapter 12 “Design and Architecture of IDP-AS” discusses the objective of Intrusion Detection and Prevention system for IMS Application Servers, The architecture and components of IDP-AS, attacks detection methodology, design scenarios with time line diagrams and object-interaction models are presented.

Chapter 13 “IDP-AS Implementation” presents the implementation of different module of IDP-AS including IDP-Centre, Partner, IDP-Filter, Rule Collection and Rule Parser.

Chapter 14 “IDP-AS Testing and Performance” explains testing environment, different test cases, and performance evaluation at Open IMS FOKUS Testbed.

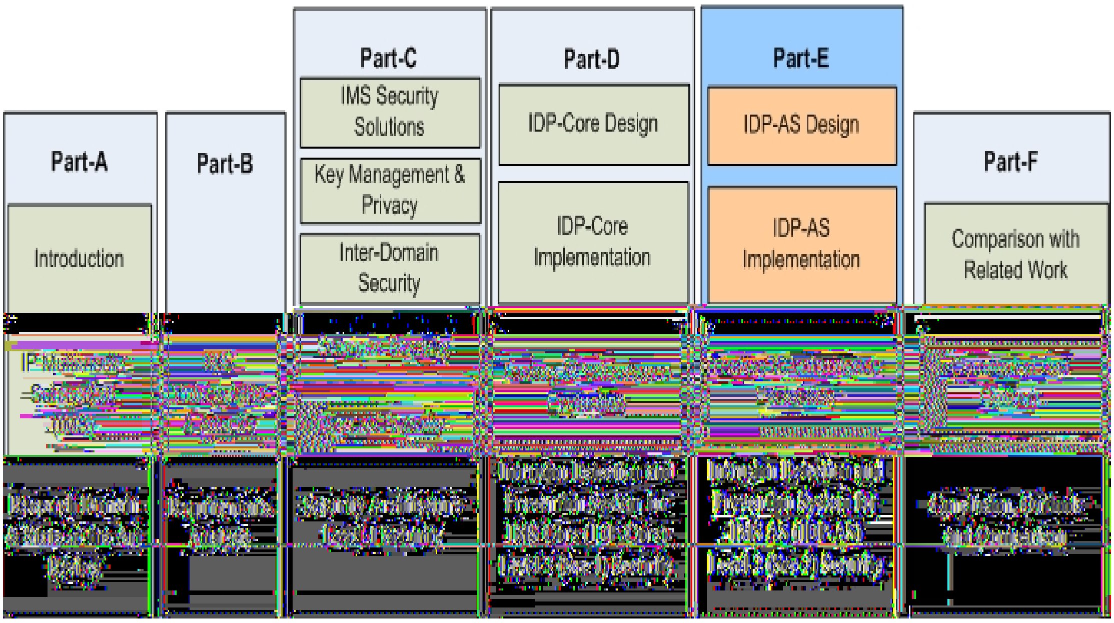


Figure E: Design and Implementation of IDP-AS (Part-E Overview)

Chapter 12 Design and Architecture of IDP-AS

12.1 Introduction

Application Servers (ASs) are functions on top of IMS and provide value-added multimedia services in the IMS. The AS is capable of processing incoming SIP session received from the IMS and able to originate SIP requests. The SIP Execution Environment (SIPSEE) developed within Open IMS Testbed at FOKUS Fraunhofer [87], is equipped with both SIP Servlet container and HTTP Servlet container and it fulfils the requirements of AS. The SIP Servlet API is developed to standardize the platform for development and deployment of SIP based services. It is one of the several possible technologies suggested by 3GPP to build a SIP Application Server (AS) which is an important part of IP Multimedia Subsystem (IMS) [1] because applications providing value added services are deployed on the application server.

The IMS Application Servers like other web-servers are ubiquitous, remotely accessible and open based architecture. They could be subjected to different kinds of intrusions, vulnerabilities and threats. These attacks could cause collapse of services e.g. flooding attacks could keep the IMS AS busy and exhaust its resources, and the SQL Injection could delete, or modify the database of IMS AS etc. To mitigate the security exposure associated with the AS, an Intrusion Detection and Prevention (IDP) is needed to analyze and screen incoming and outgoing messages. The goal is to perform early detection of malicious activity and prevent them before major damage to the AS services and to protect IMS Application Environment, which is based on SIP Servlet Container integrated with the existing HTTP Servlet Container Jetty.

The chapter starts with Intrusion Detection and Prevention (IDP) system motivation and its placement within IMS Application Server. Next, IMS AS architecture is presented. The next section explains the IDP-AS design architecture, attacks detection methodologies and algorithms, different development object interaction scenarios.

12.2 IDP-AS Movitation and Objective

The objective of Intrusion Detection and Prevention (IDP-AS) is to protect IMS Application Servers (ASs) and to secure SIP signalling on IP Multimedia Service Control (ISC) interface [7]. The ISC interface connects AS with IMS core. The 3GPP has not standardized specific security solution to secure this ISC. We concentrate the security threats that IMS ASs have challenged, especially the SIP signalling attacks on this interface and general on the whole. The lower level attacks could be prevented by using low-level security mechanisms, e.g., Transport Layer Security (TLS) and IP security (IPsec) to secure the communication channel by encryption. But the higher level attacks, like SQL injection at application level, are not mitigated by low-level security mechanisms. Hence, the task of IDP-AS is to detect and block such higher level attacks.

The IDP-AS is deployed within IMS AS. The IMS Application Server could be divided in two modules: SIP stack and SIP server. The SIP stack exchanges the SIP messages with S-CSCF via the ISC interface. The SIP server processes the incoming SIP messages and generates SIP responses. To protect IMS AS from time-dependent (TD) and time-independent (TI) attacks, all incoming and outgoing SIP messages must process by the IDP-AS, therefore it is placed between SIP stack and SIP server as depicted in *figure 12.1.*

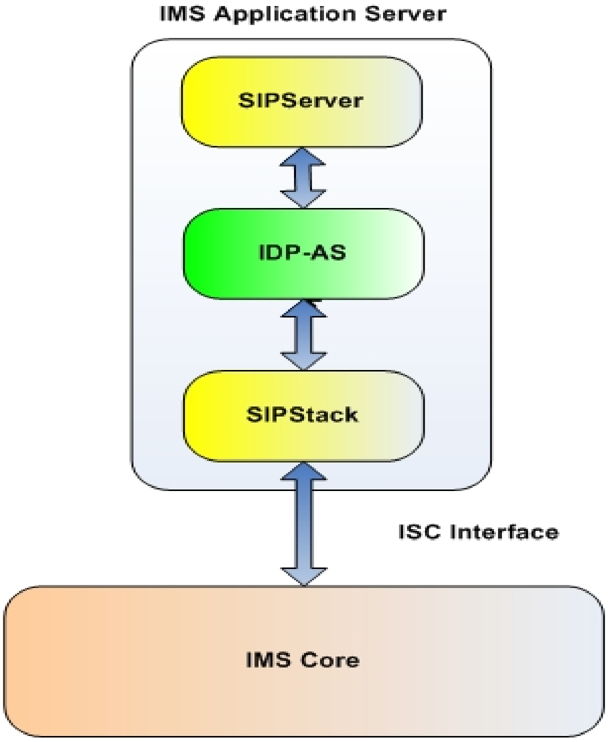


Figure 12.1 Location of IDP-AS

The proposed security mechanisms focus on protecting the IMS Application Server from attacks contained in SIP messages. Intruder could use two approaches to launch attacks relying on SIP messages. The first one is to intercept and fake the SIP messages exchanged between legitimate UAs and the Application Server. The other approach is to send malicious SIP messages directly to AS e.g. the intruder transmits a SIP message, which contains SQL-Injection. Therefore, we introduce a two tiers security mechanism shown in *figure 12.2* to safeguard IMS-AS.

The first tier utilizes the TLS (Transport Layer Security) [45] mechanism to secure the communication channel. The TLS mechanism can exclude the intruder from intercepting and forging the exchanged SIP messages. It should be noted that the SIP signalling path is hop-by-hop and from security point of view this means that the whole signalling path between the UA and the AS must be secured by the TLS [45].

TLS has many advantages over IPsec and successful introduction of the protocol in the Internet has proved its usability and effectiveness.

The major difficulty with TLS deployment is that it does not run over UDP which is usually used by SIP entities. In the future, it could be possible that TLS may be utilized for UDP traffic.

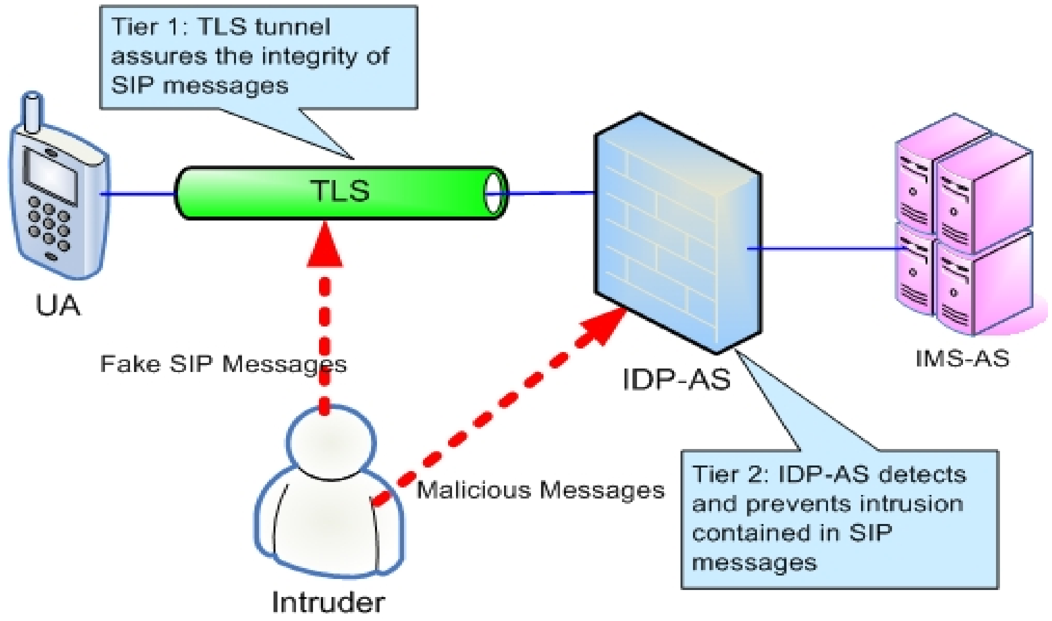

Tier 1: TLS tunnel assures the integrity of SIP messages
TLS
UA
Fake SIP Messages
IDP-AS
IMS-AS
Malicious Messages
Tier 2: IDP-AS detects and prevents intrusion contained in SIP messages
Intruder

Figure 12.2 Two-Tier Security Mechanisms

The second tier is to deploy an Intrusion Detection and Prevention (IDP) system for IMS Application Server. The task of the IDP is to detect and prevent attacks which can not debarred by the first tier technique e.g. the Bob is a legitimate and he is performing malicious activity. As a legitimate user, he is qualified to use the TLS communication channels to send SIP messages [89] to the AS. As a malicious user, Bob intends to launch SQL-Injection attack to drop a table in the database of AS. SIP provides a challenge-based mechanism for authentication that is based on authentication in HTTP and simple challenge-based authentication as illustrated in *figure 12.3.*

At the end of authentication, Bob can inject SQL statement into the Request with Credentials. The authorization Header of the injected Request may look like:

Authorization:

Digest username="Bob'; drop table films;' ",

realm="example.com",

... ...

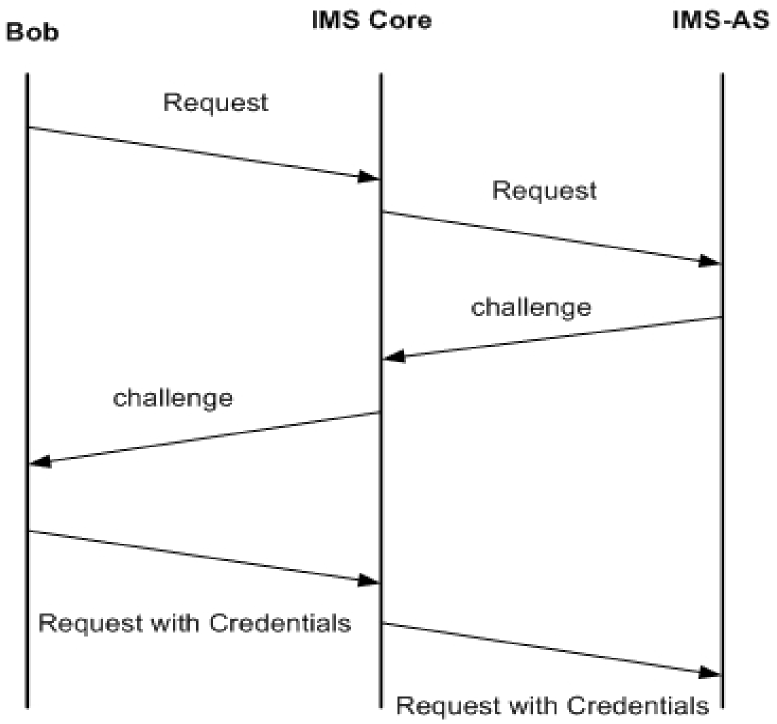


Figure 12.3 Example of Challenge-based Authentication

If the Application Server is not equipped with additional security protection like Intrusion Detection and Prevention (IDP) system, the above Request can cause loss of data, namely drop table "films" in AS.

12.3 IMS Application Server Architecture

The IMS Application Server as shown in *figure 12.4* consists of SIP Servlet Execution, SIP Message Handling, Application Deployment Environment, SIP Servlet API Compliance and Bridge components [88]. The IMS Application Server is triggered by the Serving Call State Control Function (S-CSCF) which redirects certain sessions to the SIP AS based on internal filters and criteria or by requesting filter information from the Home Subscriber Server (HSS). The SIP AS comprises filter rules to decide which applications should be selected for handling the session. During execution of service logic it is also possible for the SIP AS to communicate with the HSS to get additional information about a subscriber or to be notified about changes in subscriber profile [7]. In SIP Servlet Execution, the queue of the servlets being executed will be observed by a thread which creates separate threads for execution. SIP Message Handling component receives the SIP messages and converts them into the SIP-Servlet-Request (respectly SIP-Servlet-Response), then dispatches the SIP-Servlet-Request or SIP-Servlet-Response to the corresponding SIP Servlet. Application Deployment Environment provides approach for the deployed applications to make known to AS. Using the deployment descriptors of applications, the AS decides which servlet of specific application should handle a SIP message.

The SIP Servlet API Compliance provides the possibility for application developer to develop the applications independent of the SIP Servlet container. The SIP Servlet API is basis for creating of communication services and provides benefits to clients with applications having web into the communication process features. The AS merges with Jetty [53] -HTTP Servlet container- and Bridge component is responsible for bridging SIP servlet execution environment to the HTTP Servlet execution environment. As every specification contains its own session instance, the SIP Servlet specification introduces the concept of a spanning session, the SIP-Application-Session. The converged applications should be able to access a common SIP-Application-Session from the Http Session as well from the SIP Session.

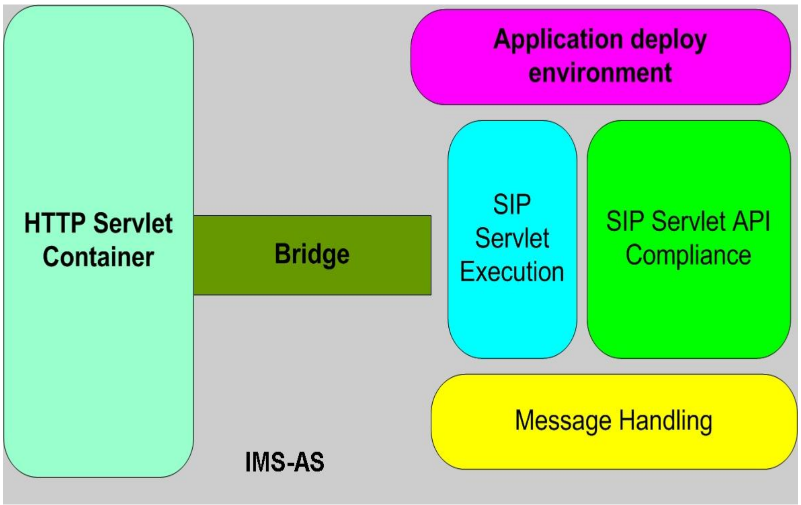
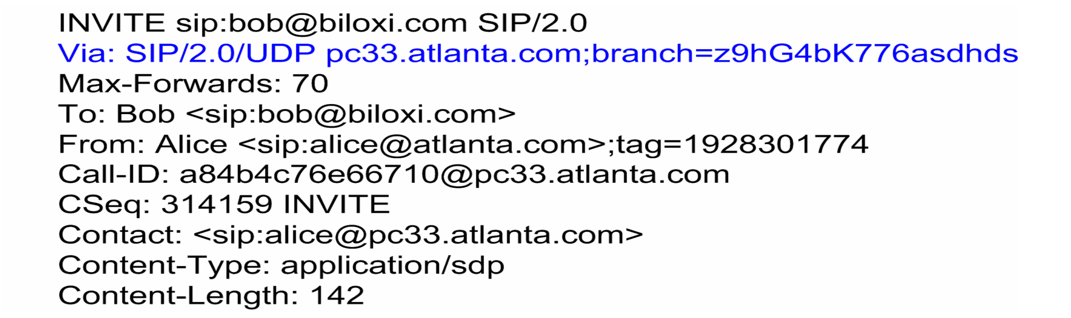


Figure 12.4 IMS-AS Architecture

12.4 Architecture of IDP-AS

This section provides top level architecture, functionality and components of IDP-AS. All the incoming SIP messages either from SIP stack or from SIP server are passed through the IDP centre that maintains a list of partners. Each partner represents a communication entity that exchanges SIP messages with the IMS AS. A partner is identified with SIP URI (Uniform Resource Identifier). For example, user Alice sends an INVITE request to the IMS-AS as shown in *figure 12.5* representing a partner with identity pc33.atlanta.com.



```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

Figure 12.5 Example of INVITE Request

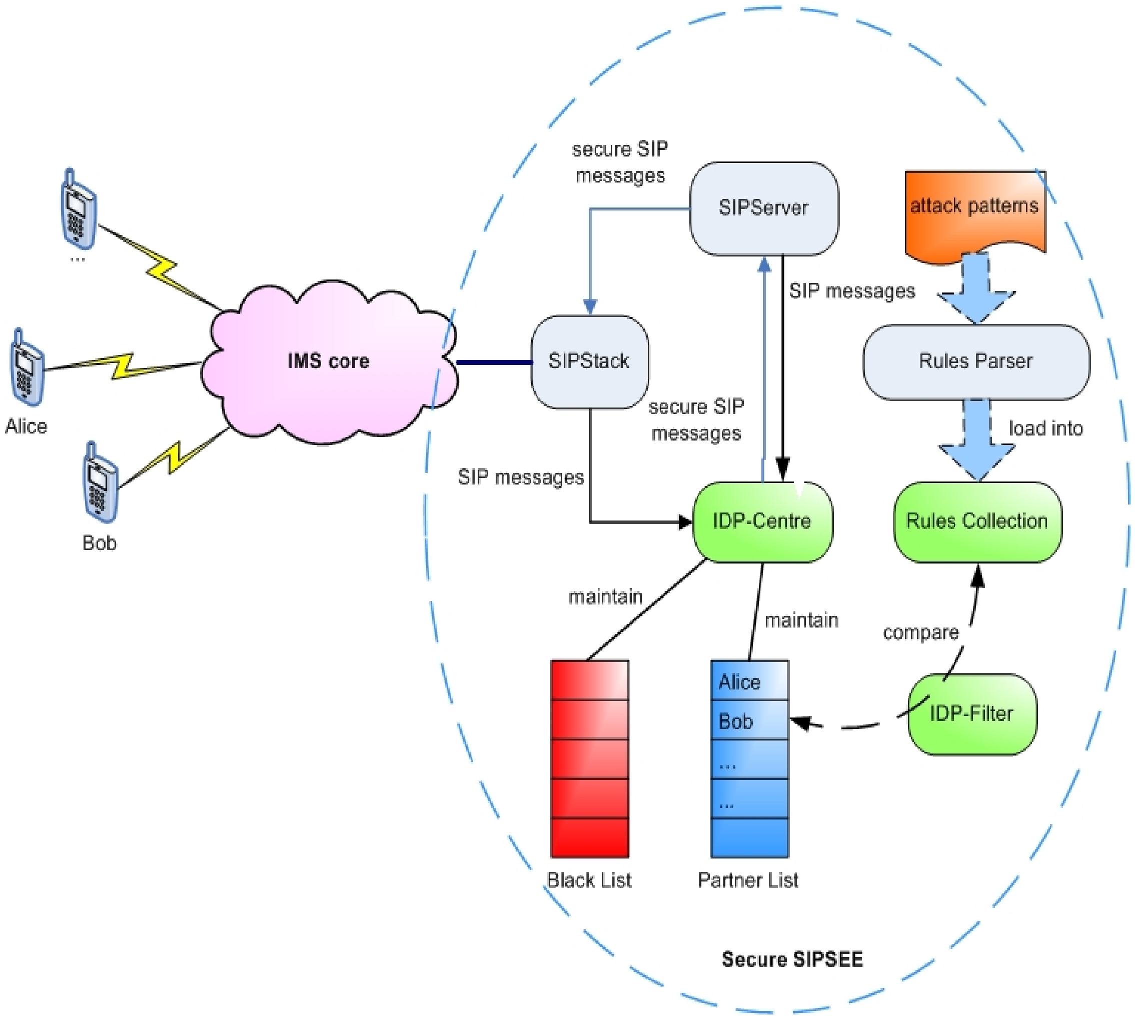


Figure 12.6 Architecture of IDP-AS

Each partner has state and number of sends or receives messages etc. When IDP-AS receives SIP message, it updates the state of corresponding partner or creates a new partner if it does not exist. After that IDP Filter compares it with the rules loaded in the Rule Collection. If a partner matches with any attack rule, the IDP Centre inserts the malicious partner into the Blacklist that contains the list of URIs of all the malicious communication partners. The reference architecture is provided in *figure 12.6*. Different components of the IDP-AS are as follows:

IDP Centre is the communication interface which receives SIP messages either from SIP stack or SIP server and process them against attacks. If an attack is detected, the IDP Centre makes a decision to generate alerts or stops further processing of malicious messages.

Partner is an Interior Agent that represents user agent (UA) or user equipment (UE) being communicating with IMS-Application Server. The partner is created during runtime and it is removed at the end of session.

Rule Collection contains and loads the defined attacks descriptions at runtime. The attacks covered the time-independent and time-dependent attacks.

IDP Filter compares both SIP messages and state of the partner with attacks descriptions stored in the Rule Collection. Through these comparisons, the IDP achieves stateless and state-based detection characteristics.

Blacklist contains a list of malicious SIP URI of illegitimate users or partners. The malicious users are identified if the state of the partner or SIP message matches with an attack rules.

12.5 IDP-AS Attacks Detection Methodology

The IDP Centre is the core of IDP-AS responsible for exchanging instances of SIP request event and SIP response event with SIP stack and SIP server. The Partner, IDP Filter and Rule Collection are entities. The object Rule represents attacks patterns described in XML.

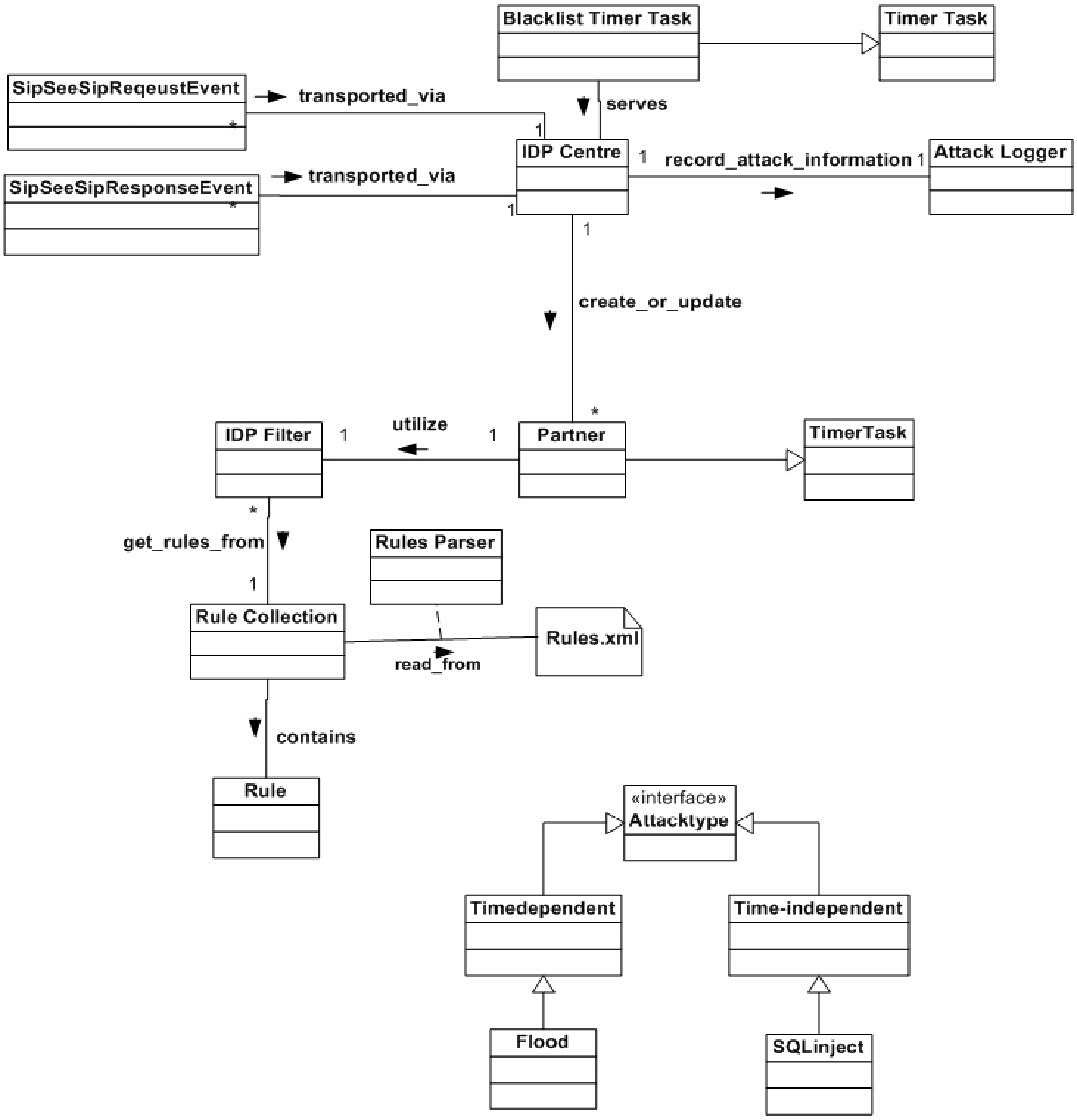


Figure 12.7 IDP-AS Attacks Detection Methodology

If IDP Centre detects an attack from malicious partner, the URI of this user is inserted into the Blacklist. Simultaneously, two actions are trigged as depicted in *figure 12.7*: first, the Attack Logger alerts the detected attack and second IDP Centre creates a new instance Blacklist timer task for deleting the corresponding URI from the Blacklist within defined time interval so that the partner is not always blocked. For example the URI bob@example.com is inserted into the Blacklist for one hour. During this time all SIP messages from or to the bob@example.com are not allowed to process. After the expiry of time interval, the URI "bob@example.com" is deleted from the Blacklist and this user is allowed to exchange SIP messages.

The attacks detection algorithm based on following two methodologies as described in flow control of *figure 12.8*:

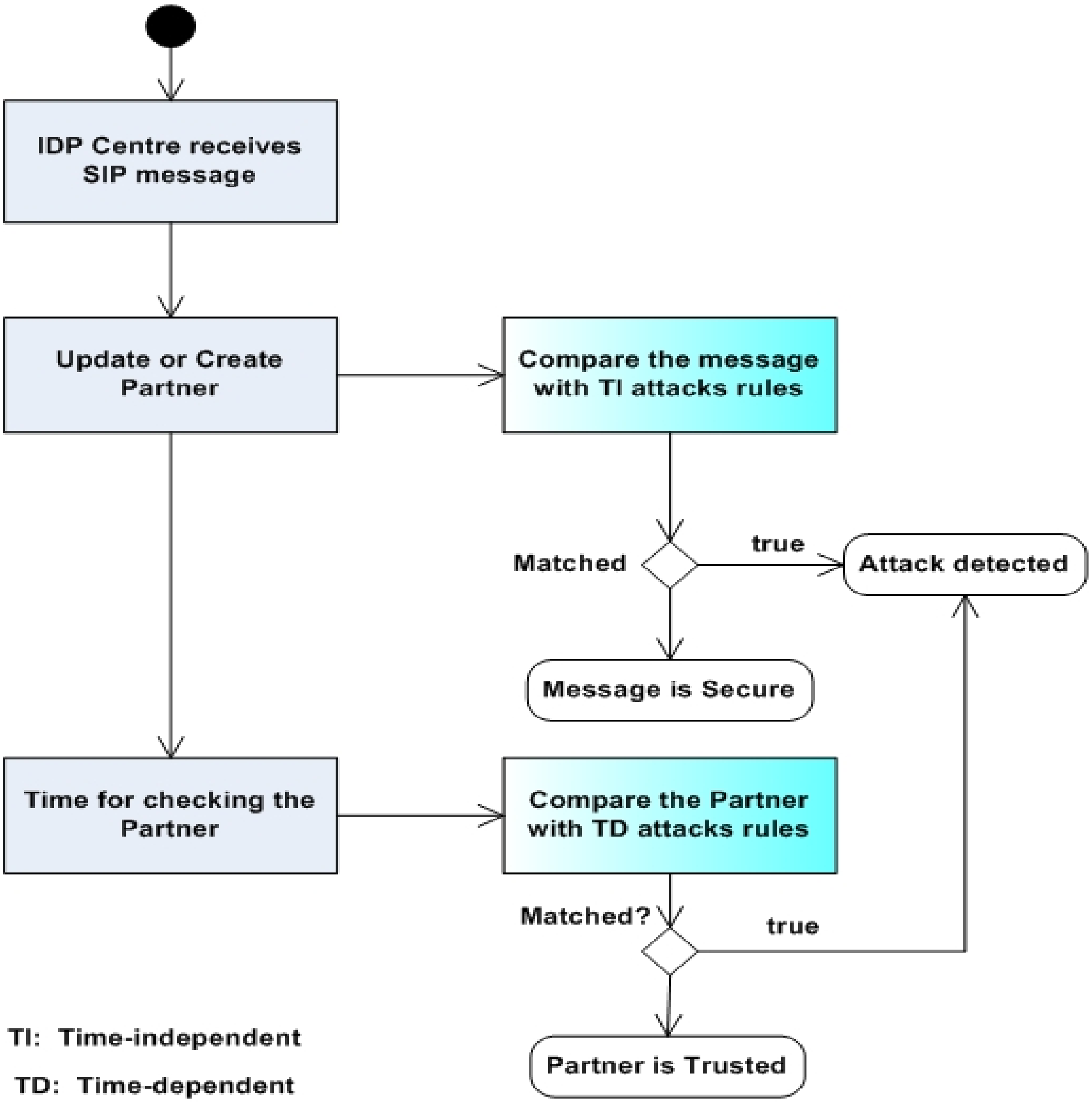

IDP Centre receives SIP message
Update or Create Partner
Compare the message with TI attacks rules
Matched
true
Attack detected
Message is Secure
Time for checking the Partner
Compare the Partner with TD attacks rules
Matched?
true
Partner is Trusted
TI: Time-independent
TD: Time-dependent

Figure 12.8 Attacks Detection Algorithm

a) To detect time-independent (TI) attack, the IDP-AS compares the message with defined attack rules, if matches, it turns the procedure attack detected, and announces the detection and block the message, otherwise the message is regarded as secure and is forwarded to the SIP Server.

b) To detect time-dependent (TD) attacks, the partner has a timer to perform periodic checking the state of user. As timer is triggered, a comparison between the current state of partner & the defined attack rules will be carried out: if matches, the procedure attack detected takes over the control. The further messages to or from the UE will be blocked.

12.6 IDP-AS Attacks Description

The attacks descriptions for INVITE Flooding, INVITE Response Flooding and SQL Injection attacks are provided in the following tables. The *table 12.1* presents INVITE flooding attack description.

	Value	**Description**
Type	Flood	The attack describes Flooding attack which is time-dependent attack.
Name	INVITE Flooding	This rule is called INVITE flooding.
Method	INVITE	The attack is launched via using SIP INVITE Request.
Status	-	The status is null because only INVITE Request is utilized to launch the attack.
Number	100	The maximal amount of INVITE request permitted by the IDS within specified time interval which is set in the property *Interval,* e.g., the number is 100 and the interval is 60 (s). It mean if UA sends 201 INVITE requests within 60 seconds to IMS AS, then the UA will be treated as an attacker.
Interval	60	Explained above.
Alert	INVITE Message Flood	If rule is matched, the IDP-AS alerts IMS AS with this message.
Whitelist	158.88.0.1	The UA whose IP is 158.88.0.1 will always be treated as secure communication partner, even though the UA matches with this rule.

Table 11.1 Description for INVITE Flooding Attack

The *table 12.2* describes the INVITE Response flood. This type of attack aims to guess the password of a legitimate user.

	Value	**Description**
Type	Flood	The attack describes Flooding attack which is time-dependent attack.

Method		The value is null. It means this rule is applied only to the Response.
Name	INVITE Response Flooding	This rule is called INVITE response flooding.
Status	407	The characteristic of attack is a lot of outgoing 407 messages.
Number	100	The maximal amount of 407 message permitted by IDS within specified time interval, which is set for the property *Interval,* e.g., the number is 100 and the interval is 60 (s). If IMS AS sends 201 "407" response within 60 seconds to a UA, then the UA will be treated as an intruder.
Interval	60	Explained above.
Alert	SIP/2.0 407 unauthenticated	If rule is matched, the IDS will alert IMS AS with this message.
Whitelist	158.88.0.1	The UA whose IP is 158.88.0.1 will always be treated as secure communication partner, even though the UA matches this rule.

Table 11.2 Description for INVITE Response Flooding

The third rule provided in *table 12.3* describes the SQL Injection attack.

	Value	Description
Type	Sql-injection	This rule describes SQL Injection attack which time-independent attack.
Name	Drop statement	This rule is called Drop Statement.
Statement	Drop	The SQL statement Drop is used to launch this attack.
Alert	Drop SQL Injection Attack is detected.	If rule is matched, the IDS will alert IMS AS with this message.

Table 11.3 Description for SQL Injection Attack

12.7 IDP-AS Design Scenarios

In this section we describes time line diagrams and object interaction models to show how a system fulfils the task of user requirements. The following four possible design scenarios are presented to check the security and reliability of each SIP message communicating with IMS AS. Each system operation defines an object interaction graph specifying the context of a system operation and the communication flow between objects to realize a system operation.

12.7.1 Incoming Request Scenario

In this scenario, the IDP-AS receives incoming SIP request from SIP stack and IDP Centre performs check-in-request action against any attack which consists of following steps. First, if the URI of the request is contained in the Blacklist, alert the attack and reject the request.

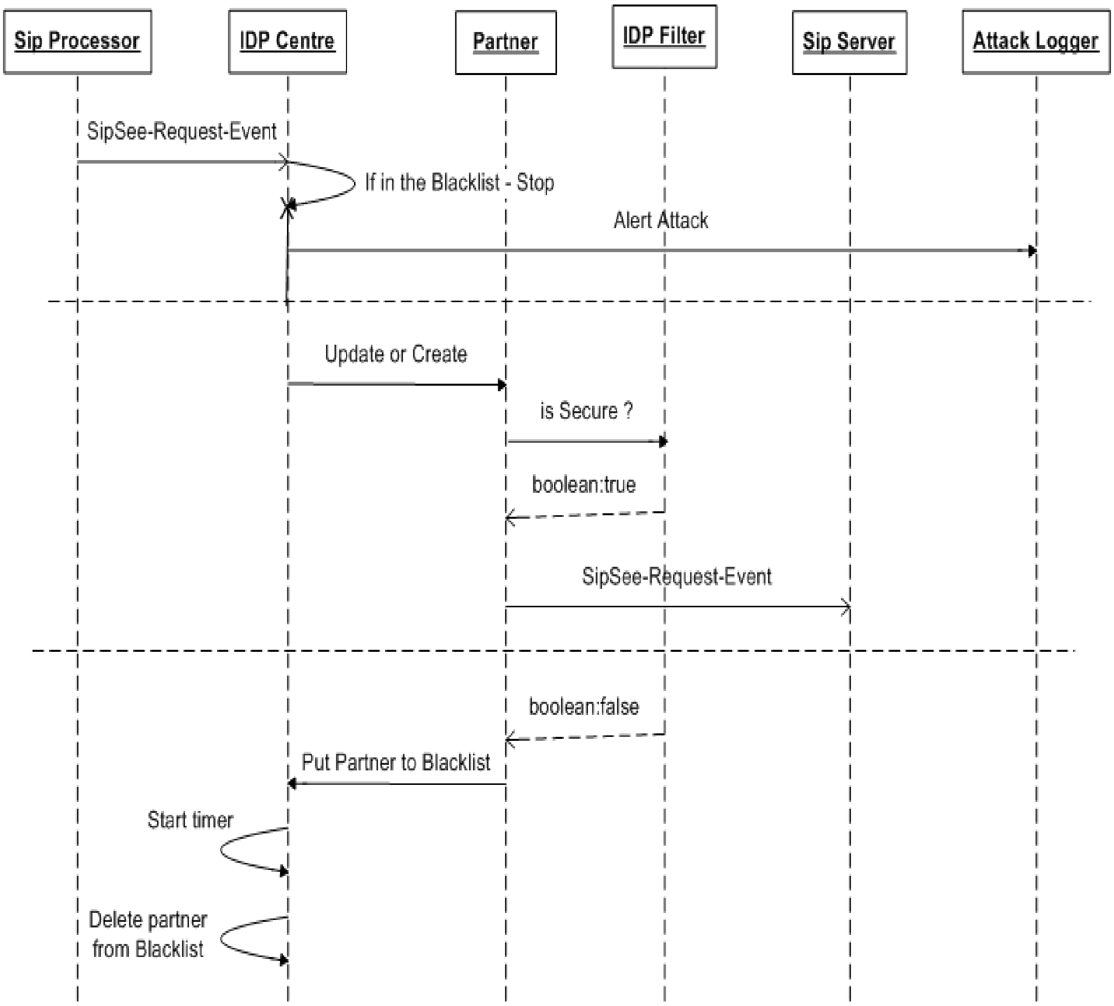


Figure 12.9 Incoming SIP Request Scenario

If the URI is not contained in the Blacklist then partner is created or updated. Second, the IDP Filter compares the request with time-independent attack rules to check SQL-injection attack. The partner has also timer task to check state of partner repeatedly in lifecycle against any attack. The scheduled task compares the partner's state with time-dependent attacks rules. If it matches, the URI of the partner is inserted in the Blacklist. Simultaneously, an instance of the Blacklist timer task is created and it is scheduled for deleting the specified URI from the Blacklist in defined time interval, in order to avoid the blocking of URI forever. If the partner is proved to be secure, the

IDP-AS forwards the request to SIP server for processing. The related time line diagram and object-interaction model is shown in *figures 12.9 & 12.10* respectively.

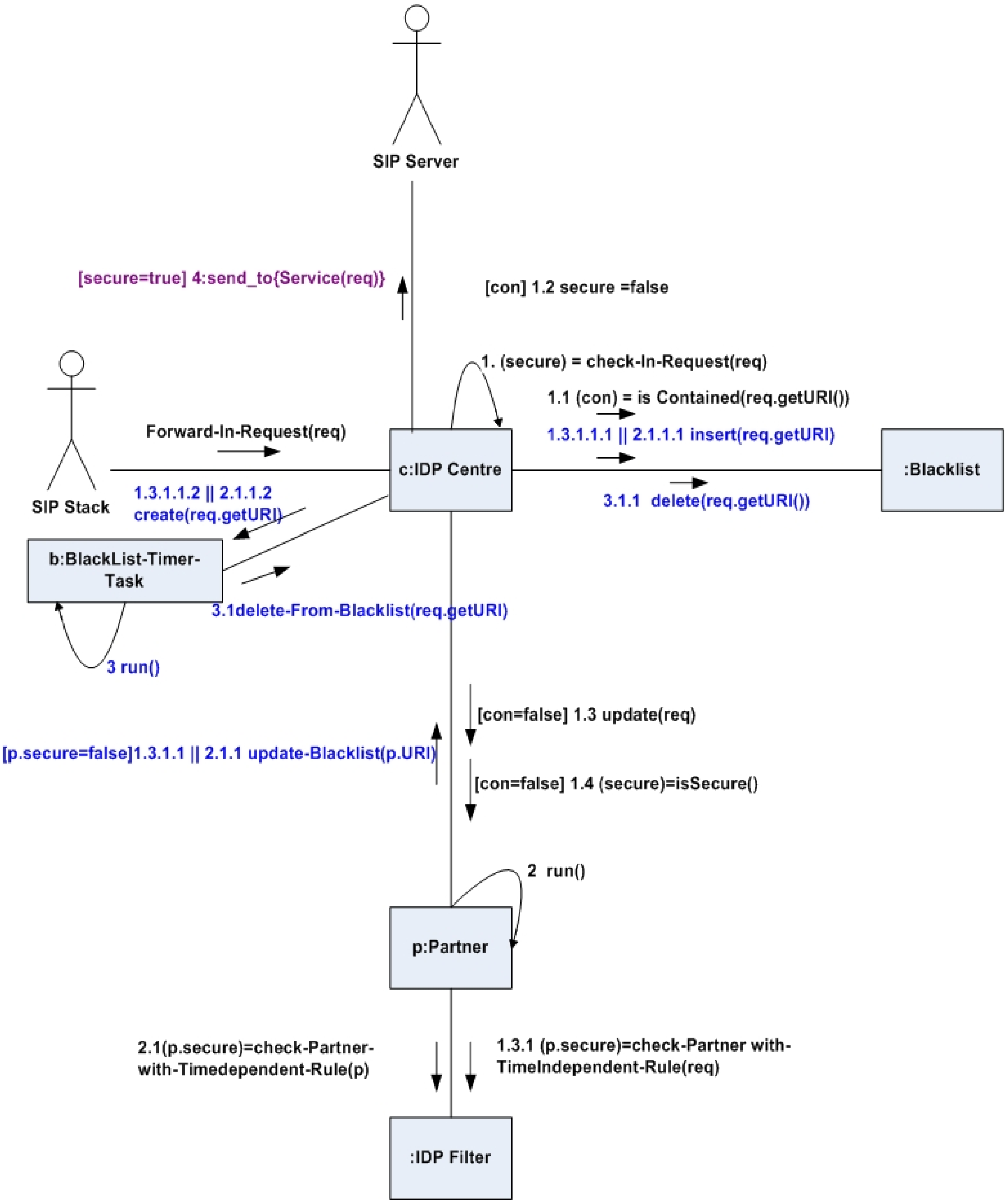

SIP Server
[secure=true] 4:send_to{Service(req)}
[con] 1.2 secure =false
1. (secure) = check-In-Request(req)
1.1 (con) = is Contained(req.getURI())
1.3.1.1.1 || 2.1.1.1 insert(req.getURI)
Forward-In-Request(req)
c:IDP Centre
:Blacklist
3.1.1 delete(req.getURI())
SIP Stack
1.3.1.1.2 || 2.1.1.2
create(req.getURI)
b:BlackList-Timer-Task
3.1delete-From-Blacklist(req.getURI)
3 run()
[con=false] 1.3 update(req)
[p.secure=false]1.3.1.1 || 2.1.1 update-Blacklist(p.URI)
[con=false] 1.4 (secure)=isSecure()
2 run()
p:Partner
2.1(p.secure)=check-Partner-with-Timedependent-Rule(p)
1.3.1 (p.secure)=check-Partner with-TimeIndependent-Rule(req)
:IDP Filter

Figure 12.10 Incoming Request Object-Interaction Graph

12.7.2 Incoming SIP Response Scenario

Similar to the first scenario, only the secure incoming responses are permitted to pass through the IDP-AS. In this scenario, the IDP Centre checks that if the URI of the response is contained in the Blacklist, the response is treated an attack and it is rejected. If the URI of response is not contained in the Blacklist, it is assumed that the response is secure. The IDP centre will not create or update the partner to compare with attack rules or with the state of the partner of incoming response. The time line diagram and object-interaction graph is provided in *figure 12.11 & 12.12* respectively.

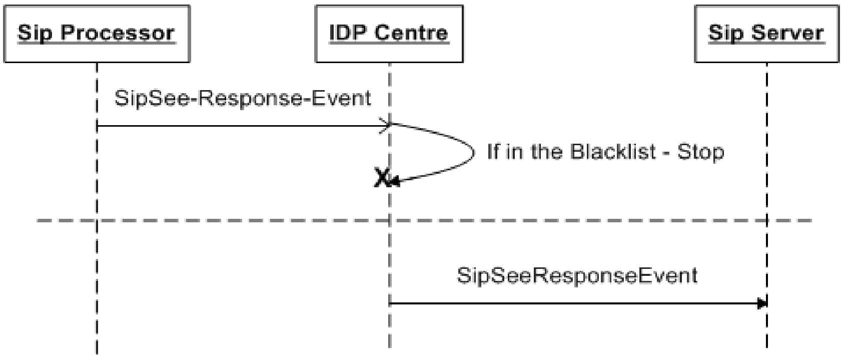


Figure 12.11 Incoming SIP Response Scenario

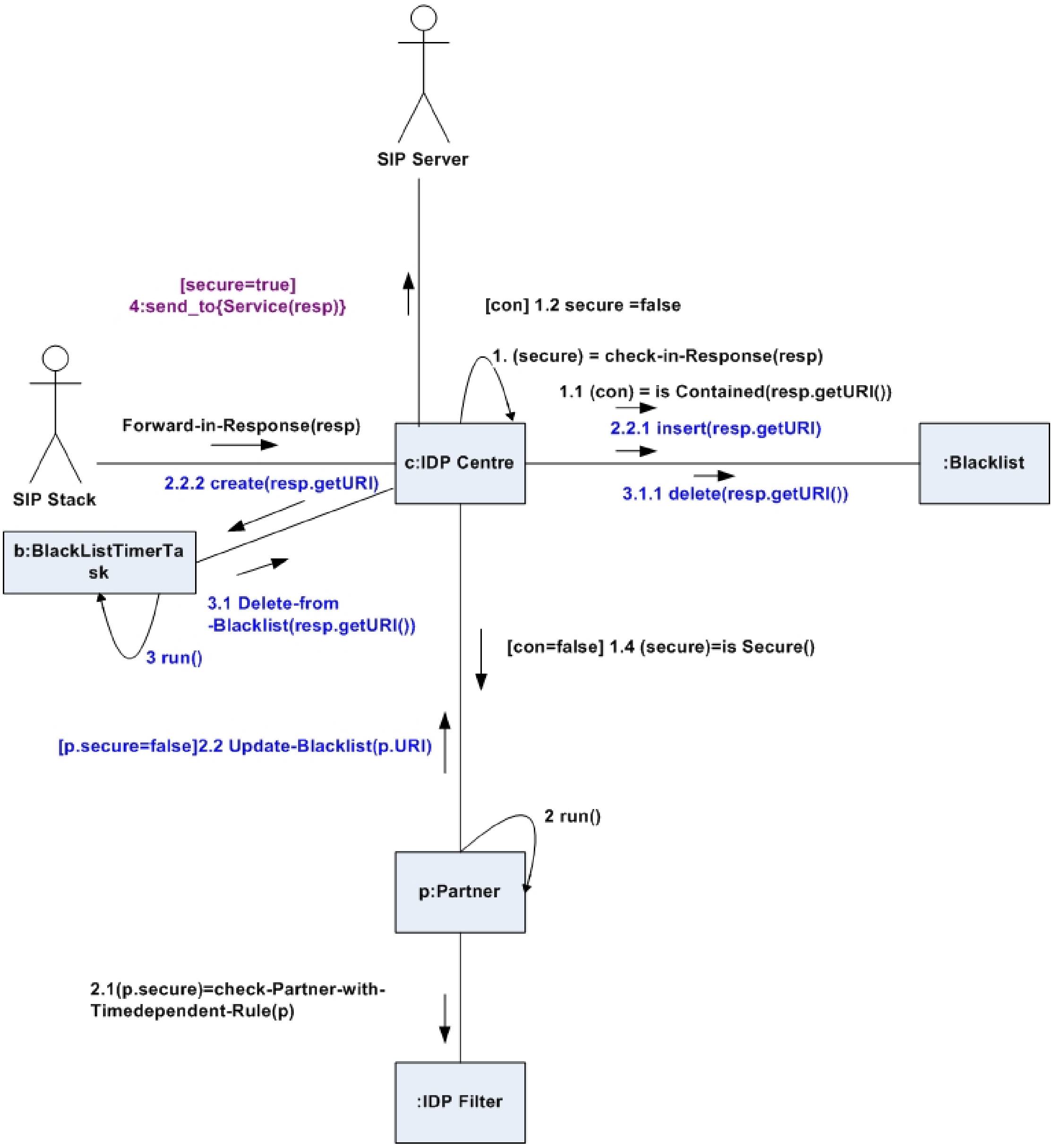

SIP Server
[secure=true]
4:send_to{Service(resp)}
[con] 1.2 secure =false
1. (secure) = check-in-Response(resp)
1.1 (con) = is Contained(resp.getURI())
2.2.1 insert(resp.getURI)
Forward-in-Response(resp)
SIP Stack
2.2.2 create(resp.getURI)
c:IDP Centre
:Blacklist
3.1.1 delete(resp.getURI())
b:BlackListTimerTask
3.1 Delete-from
-Blacklist(resp.getURI())
3 run()
[con=false] 1.4 (secure)=is Secure()
[p.secure=false]2.2 Update-Blacklist(p.URI)
2 run()
p:Partner
2.1(p.secure)=check-Partner-with-
Timedependent-Rule(p)
:IDP Filter

Figure 12.12 Incoming Response Object-Interaction Graph

12.7.3 Outgoing SIP Request Scenario

In the third scenario, the IDP-AS checks the outgoing SIP requests received from SIP Server. These outgoing SIP requests may be the result of any previously incoming request or response. Therefore, it is necessary to check these requests against any attack. If any attack is detected, the SIP server is informed about the attack, and SIP server will cease to process the request.

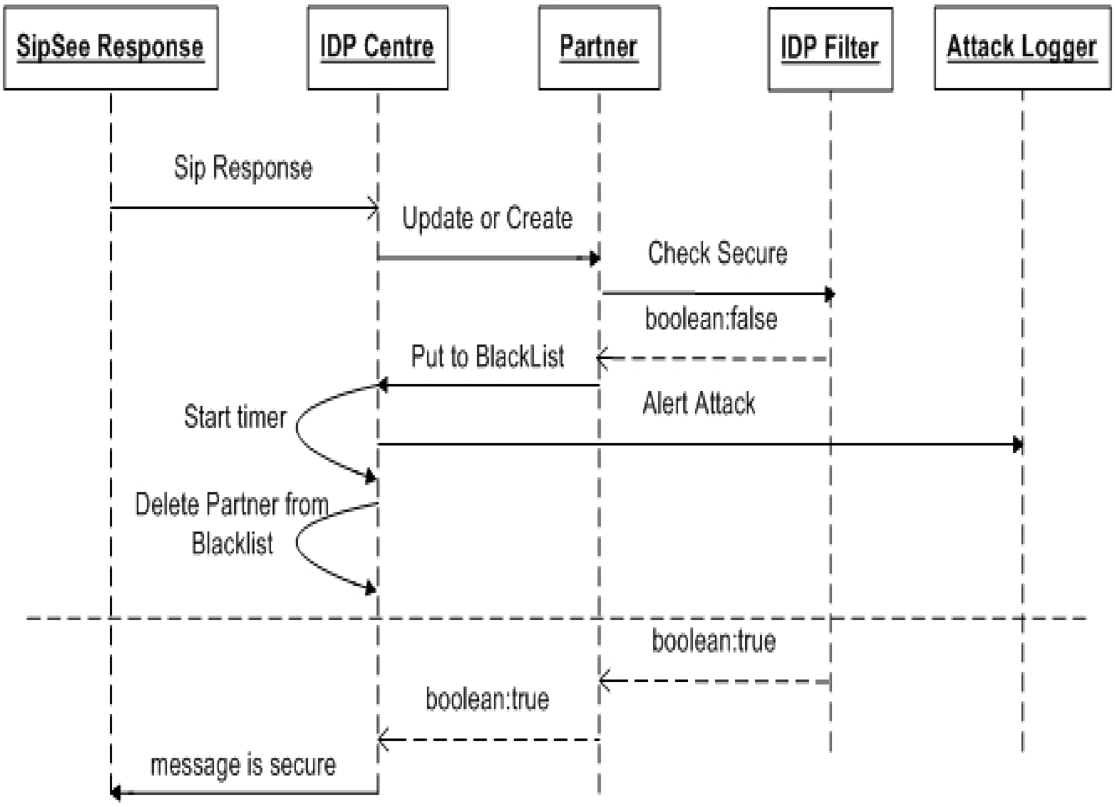


Figure 12.13 Outgoing SIP Request Scenario

Similar to the previous graphs it is always verified whether the URI of the response has been already contained in the Blacklist. If yes, the SIP server is informed about the outgoing response is from the attacker. Otherwise, IDP Centre updates the state of corresponding partner and IDP Filter compares the response with the defined rules of time-independent attack, in order to detect any time-independent attack. The time line diagram and object-interaction model is shown in *figure 12.13 & 12.14* respectively.

The partner is scheduled to repeatedly compare with the rules of time-dependent attack in order to detect time-dependent attacks. If it matches, in both cases IDP Centre is trigged to update the Blacklist, namely to insert the URI of the partner into the Blacklist. The IDP Centre creates the corresponding Blacklist timer task for the new insertion into the Blacklist. Finally, in the fifth and sixth operations, IDP Centre will inform the SIP server with the checking results.

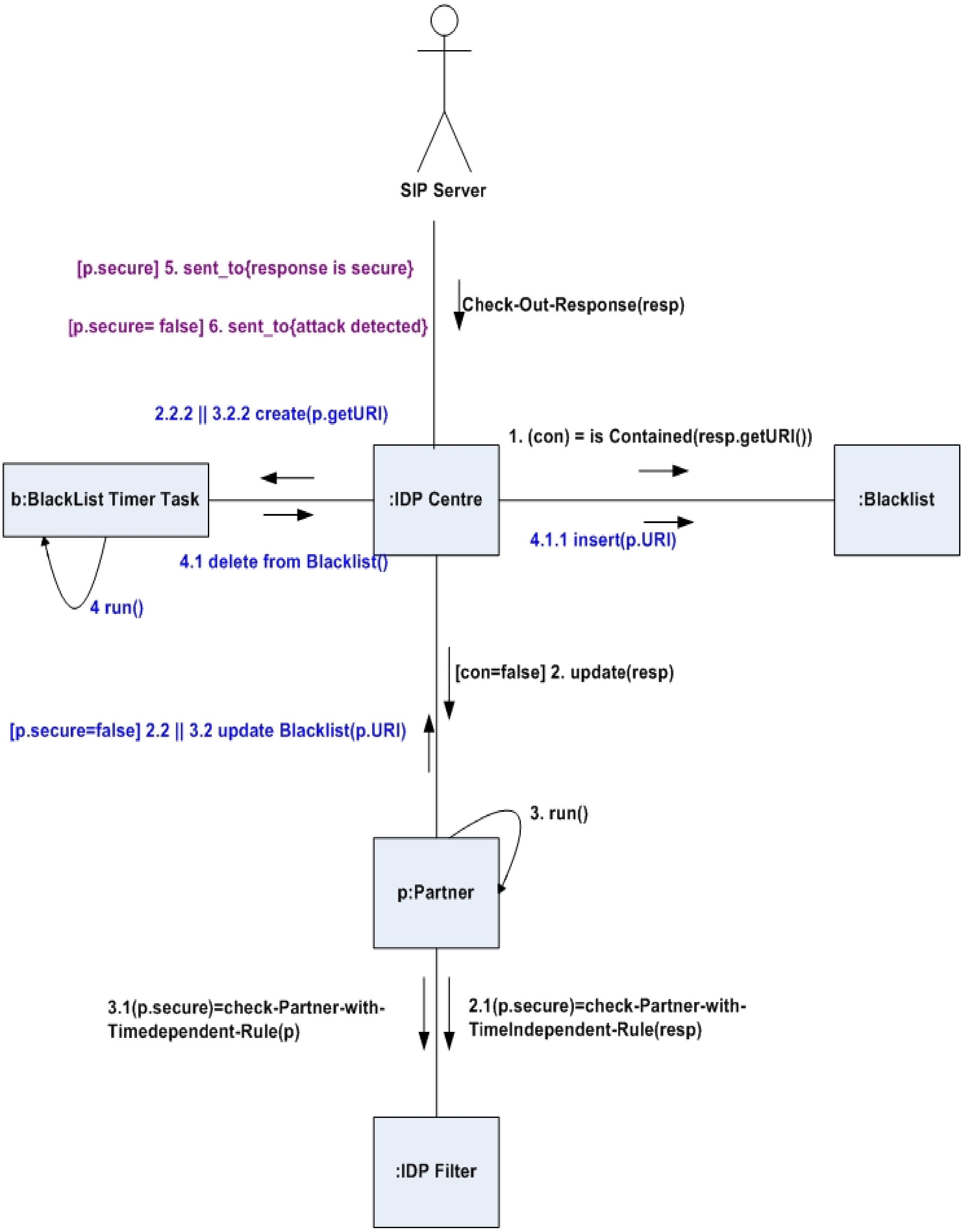

SIP Server
[p.secure] 5. sent_to{response is secure}
[p.secure= false] 6. sent_to{attack detected}
Check-Out-Response(resp)
2.2.2 || 3.2.2 create(p.getURI)
1. (con) = is Contained(resp.getURI())
b:BlackList Timer Task
:IDP Centre
:Blacklist
4.1.1 insert(p.URI)
4.1 delete from Blacklist()
4 run()
[con=false] 2. update(resp)
[p.secure=false] 2.2 || 3.2 update Blacklist(p.URI)
3. run()
p:Partner
3.1(p.secure)=check-Partner-with-Timedependent-Rule(p)
2.1(p.secure)=check-Partner-with-TimeIndependent-Rule(resp)
:IDP Filter

Figure 12.14 Outgoing Request Object-Interaction Graph

12.7.4 Outgoing SIP Response Scenario

In the last scenario, the IDP-AS checks the outgoing SIP responses against any attack. If attack is detected, it informs the Application Server about the attack. Only secure SIP responses are sent to SIP stack. In this case no attack has been identified; therefore all the outgoing SIP responses are treated as secure. The sequence diagram of this scenario is shown in *figure 12.15*.

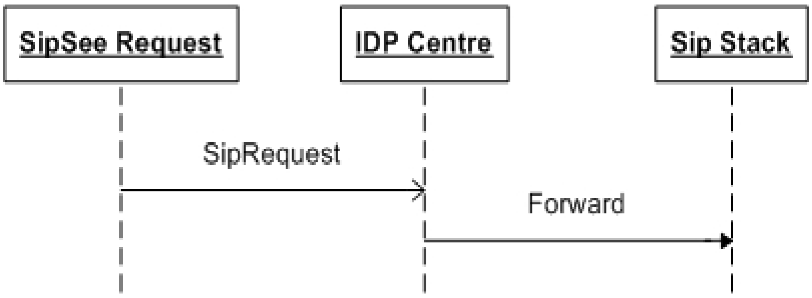


Figure 12.15 Outgoing SIP Response Scenario

12.8 Summary

In this chapter, the functionality and architectural design of Intrusion Detection and Prevention (IDP-AS) system for IMS Application Servers are presented. All the communication messages between IMS core and Application Server are processed by the IDP-AS. Four types of design scenarios are explained with time-line diagrams and object-interaction models.

Chapter 13 IDP-AS Implementation

13.1 Introduction

The SIP Servlet Execution Environment (SIPSEE) - IMS Application Server-is developed in Java, within Open IMS FOKUS Testbed. The Intrusion Detection and Prevention (IDP-AS) system is deployed within SIPSEE and implemented in Java. The signalling flow for secure IMS Application Server is provided in *figure 13.1*.

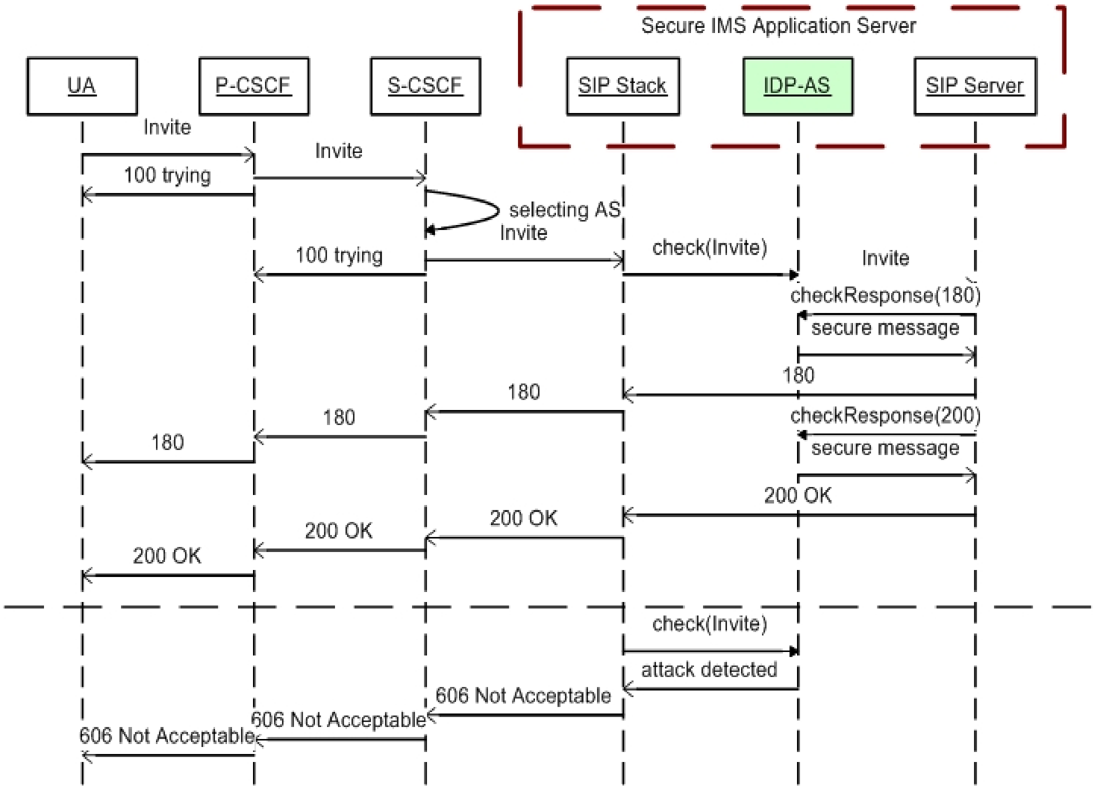


Figure 13.1 Secure IMS Application Server

The implementation of IDP-AS is divided into three parts:

(i) IDP Centre implementation

(ii) Partner, IDP Filter and Rules Collection implementation

(iii) Rules Parser and IDP Configuration implementation

These parts are briefly explained in this chapter.

13.2 The IDP Centre

The implementation procedure is explained with the properties and the operations of IDP Centre.

13.2.1 Properties of IDP Centre

The IDP Centre is composed of four properties Blacklist, SIP server, list of partner and timer as depicted in *figure 13.2*. If SIP server property is set with null, then IMS AS works without IDP-AS. Therefore it is feasible to mount or demount the IDP-AS. The blacklist property is a hash set which stores URI of the malicious communication partners. In start, both the blacklist and list of partner are empty. On the reception of SIP request or SIP response from new UE, IDP Centre creates new partner and inserts into the list of partner. The timer property is responsible for scheduling timer tasks created for elements in the blacklist.

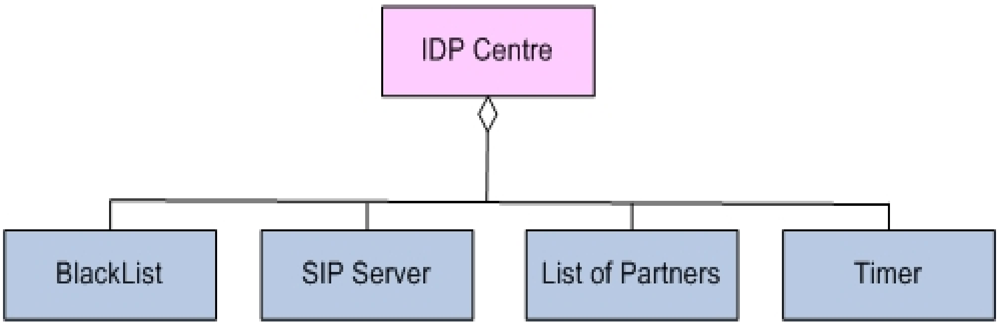


Figure 13.2 Property Structure of IDP Centre

13.2.2 Operations of IDP Centre

The property structure provides the static features but the dynamic features of IDP Centre are described with the operation structure as depicted in *figure 13.3*. The methods forward-in-request(), forward-in-response(), check-out-request() and check-out-response() are the interfaces of IDP centre for exchanging messages. The "in" and "out" represent the direction of messages. The method forward-in-request() forwards the request to the method check-in-request(), in order to verify whether the incoming request is secure. On the basis of the result of method check-in-request(), the method forward-in-request() decides to forward the request to the SIP server or blocks the request. The method forward-in-response() checks the incoming response.

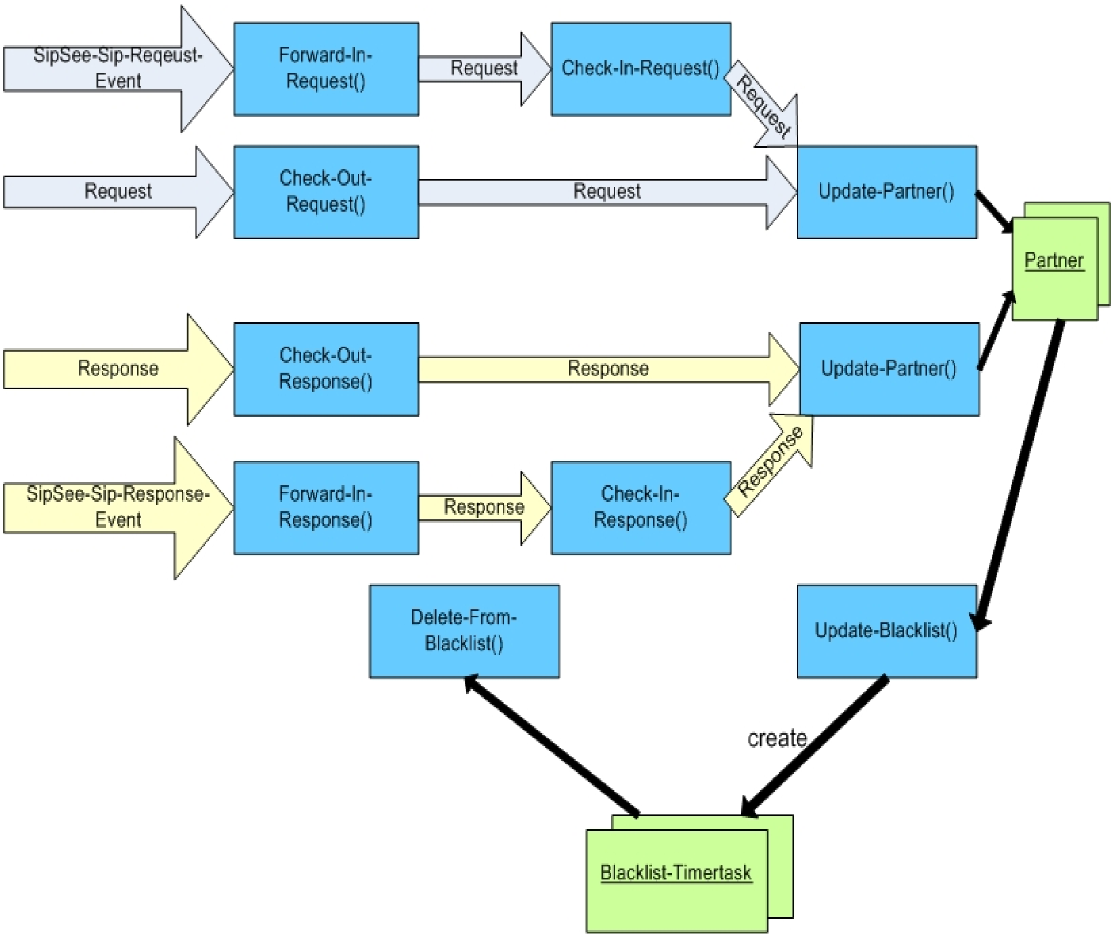


Figure 13.3 Operation Structure of IDP Centre

We have assumed that the outgoing request initiated by the SIP server never contains any attack, the method check-out-request() in the current implementation always returns true. The check-out-response() is similar to the check-in-response(). Both utilize the update-partner() to create new instance of the partner or to update the existed instance. The method update-blacklist() can be invoked by a partner to insert the URI of the partner into the blacklist, if the partner noticed that the partner itself is no more secure. Simultaneously this method update-blacklist() creates a new instance of the blacklist timer task for the new inserted record in the blacklist. In the preconfigured time interval, the new created instance of blacklist timer task calls method delete-from-blacklist() to delete the URI from the blacklist. It is also noticeable that the IDP Centre is a singleton.

In order to understand the check-XXX() operation in more detail, a control flow graph of check-out-response() is provided as an example. As shown in *figure 13.4*, the method at first initiate the private method get-originator() to obtain the URI of the response. Then it verifies whether the URI was contained in the blacklist check-in-response(). If it contained, it means that the target of the outgoing response is a malicious UE, and the method returns a false and terminates. Otherwise the update-partner() is invoked to create a new partner or to update the existed partner. Finally, the partner should be reviewed for its state of security.

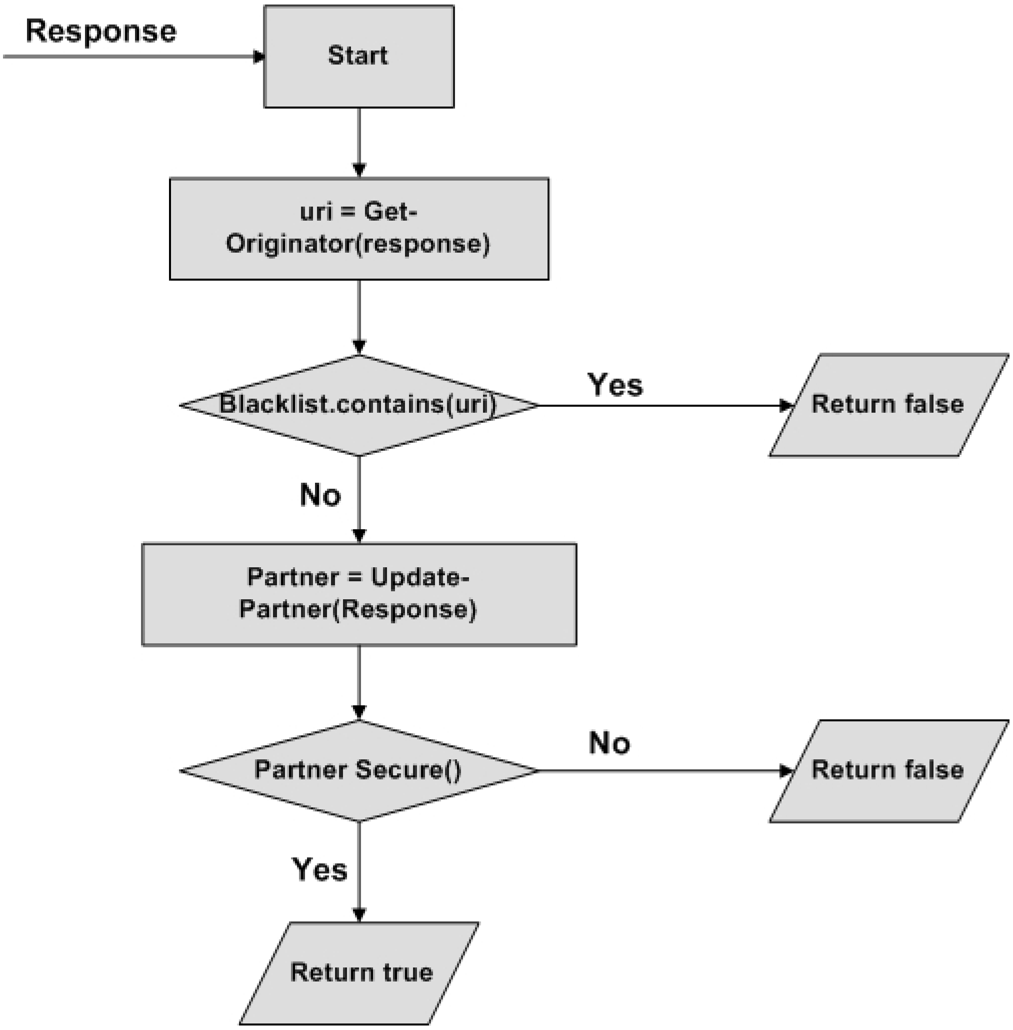


Figure 13.4 Control Flow Graph of Check-Out-Response() Operation

13.3 Partner, IDP Filter and Rule Collection

The relationships among the Partner, IDP Filter and Rule Collection are explained in design section. The task of IDP Filter is to compare the partner or message with the rules stored in Rule Collection.

13.3.1 The Partner

The primary objective of development of partner is how to represent the state of a communication entity. The class partner contains a counter for each SIP method, num-INVITE counts how much INVITE messages are received. In addition, the class partner has counters for 401-Response and 407-Response, namely num-status 401 and num-status 407 as depicted in *figure 13.5*. The flooding attack is time based; the state of a partner must be evaluated with regard to time interval. The attributes duration and time recorder serve for the time interval. The partner is a timer task and each time interval is defined in the duration, the partner checks its state to detect time-dependent attack. If no attack is detected and value of the time recorder is equal to or greater than the pre-defined time interval, the state of the partner will return back to the initialized state.

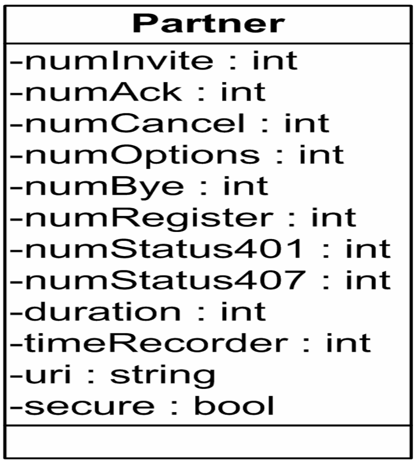


Figure 13.5 The Class Model of Partner

The state chart provided in *figure 13.6* describes the states of partner for INVITE request [4]. The life cycle of a partner begins when the first SIP message is received from a new UE. The partner is removed from system, if it has not been updated since a pre-defined time interval.

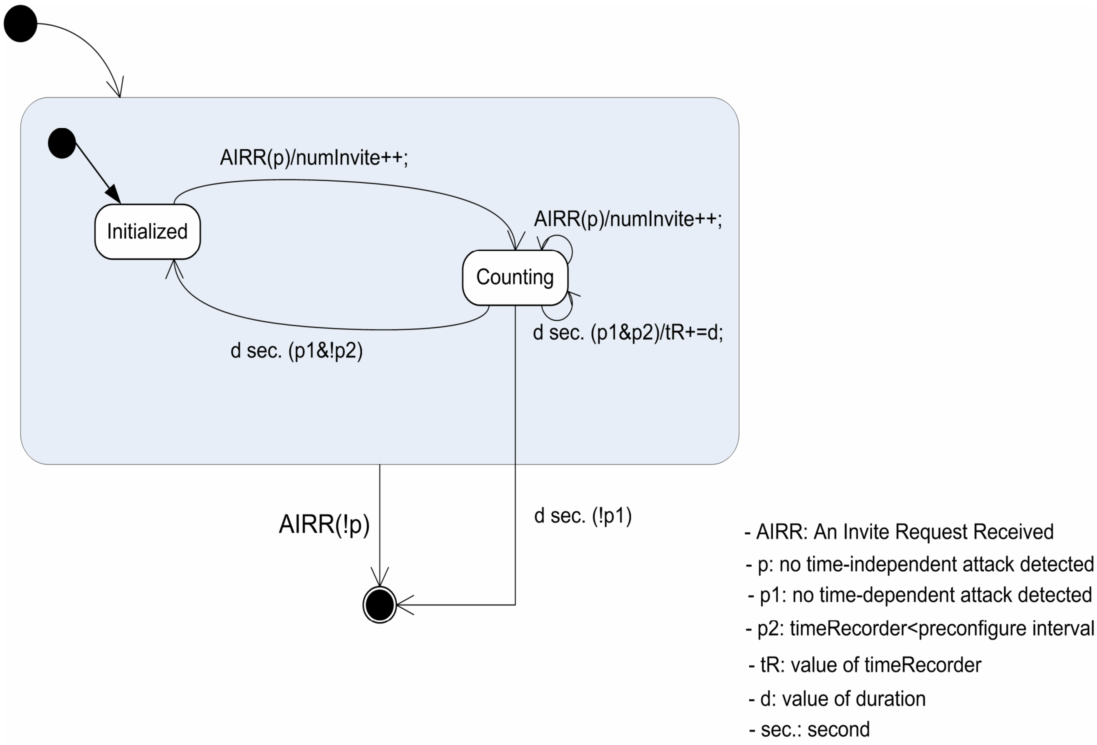

AIRR(p)/numInvite++;
Initialized
AIRR(p)/numInvite++;
Counting
d sec. (p1&p2)/tR+=d;
d sec. (p1&!p2)
AIRR(!p)
d sec. (!p1)
- AIRR: An Invite Request Received
- p: no time-independent attack detected
- p1: no time-dependent attack detected
- p2: timeRecorder<preconfigure interval
- tR: value of timeRecorder
- d: value of duration
- sec.: second

Figure 13.6 Partner State Chart for INVITE Request

13.3.2 The IDP Filter

The IDP Filter performs the comparison with two methods: first check-PWithoutRTTime() which compares the message with time-independent attack rules. A private method check-SQL-Injection() is invoked by check-PWithoutRTTime() operation to detect any SQL-injection contained in the message. The tasks of check-SQL-Injection() are parsing the message to get the username and compare it with the attack rules describing SQL-injection. For example username is “bob; drop table subscriber”, a statement of a rule is “drop”; that matches with username. The second check-PWithRTTime() which checks partner to detect time-dependent attacks by comparing the corresponding states of the partner with the number defined in the rules as given in *figure 13.7*. The corresponding state of partner is num-status 407 whose value is compared with element Number. If the value of the num-status 407 exceeds 50 and the partner's URI is not included in the element white-list, an INVITE response flooding is detected.

13.3.3 The Rule Collection

The task of Rule Collection is to store rules defined in the rules.xml as provided in *figure 13.7*. In order to accelerate the processing of the IDP, the Rule Collection contains two searching lists: first “rules-time-based” stores only the time-dependent attack rules and the second list “rules-no-time-based” stores the time-independent attack rules. It must be noted that the Rule Collection loads the rules at the start of the IDP-AS. If any rule is inserted into or deleted from the “rules.xml” during the runtime, it is recommended to start the IDP-AS system to load the current rule. These rules contain four types of SIP flooding and four types of SQL injection attacks.

```
<?xml version="1.0" encoding="UTF-8"?>
<Rules>
 <Rule type="flood">
     <Name>INVITE flooding</Name>
     <Method>INVITE</Method>
     <Status></Status>
     <Number>100</Number>
     <Interval>60</Interval>
     <Alert>INVITE message flood</Alert>
     <Whitelist>158.88.0.1</Whitelist>
  </Rule>
  <Rule type="flood">
        <Name>REGISTER flooding</Name>
        <Method>REGISTER</Method>
        <Status></Status>
        <Number>100</Number>
        <Interval>60</Interval>
        <Alert>REGISTER message flood</Alert>
        <Whitelist>158.88.0.1</Whitelist>
   </Rule>
   <Rule type="flood">
```

```
      <Name>INVITE response flooding</Name>
      <Method></Method>
      <Status>407</Status>
      <Number>100</Number>
      <Interval>60</Interval>
      <Alert>SIP/2.0 407 unauthenticated</Alert>
      <Whitelist>158.88.0.1</Whitelist>
    </Rule>
    <Rule type="flood">
          <Name>REGISTER response flooding</Name>
          <Method></Method>
          <Status>401</Status>
          <Number>50</Number>
          <Interval>60</Interval>
          <Alert>SIP/2.0 401 unauthenticated</Alert>
          <Whitelist>158.88.0.1</Whitelist>
     </Rule>
     <Rule type="sqlinject">
          <Name>Drop statement</Name>
          <Statement>drop</Statement>
          <Alert>a drop injection attack launched</Alert>
     </Rule>
     <Rule type="sqlinject">
          <Name>Delete statement</Name>
          <Statement>delete</Statement>
          <Alert>a delete injection attack launched</Alert>
      </Rule>
      <Rule type="sqlinject">
          <Name>Insert statement</Name>
          <Statement>insert</Statement>
          <Alert>a insert injection attack launched</Alert>
      </Rule>
      <Rule type="sqlinject">
          <Name>Update statement</Name>
          <Statement>update</Statement>
          <Alert>a update injection attack launched</Alert>
      </Rule>
      <Rule type="sqlinject">
          <Name>Union statement</Name>
          <Statement>union</Statement>
          <Alert>a union injection attack launched</Alert>
      </Rule>
</Rules>
```

Figure 13.7 IDP-AS Attacks Rules

13.4 The Rule Parser and IDP Configuration

The implementations of these two modules are explained below:

13.4.1 The Rule Parser

The Rule Parser is a XML parser which utilizes the Document Object Model (DOM) which is a standard API for XML parsers. The exploited parser is *Xerces* which supports XML 1.0 recommendation and contains advanced parser functionality, such as support for W3C's XML Schema recommendation version 1.0, DOM Level 2 version 1.0, and SAX Version2, in addition to supporting the industry standard DOM Level 1 and SAX version 1 APIs. In brief, the task of Rule Parser is to read the file "rules.xml" into a Document and extract a list of Rule from the Document. The code fragment of Rule Parser is given in *figure 13.8*

```
public Hashtable<String,Rule> getRules(){
    Hashtable<String,Rule> rules = null;
    Document docu = parseXMLFile(IDSConstant.RULEFILE);
    rules = parseDocument(docu);
    return rules;
 }
 ...
 private Document parseXMLFile(String xmlFile){
     Document dom = null;
     DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
     try {
        //Using factory get an instance of document builder
        DocumentBuilder db = dbf.newDocumentBuilder();
         URL url = RulesParser.class.getClassLoader().getResource(xmlFile);
        //parse using builder to get DOM representation of the XML file
        dom = db.parse(new File(url.getFile()));
     }catch(ParserConfigurationException pce) {
        pce.printStackTrace();
     }catch(SAXException se) {
        se.printStackTrace();
     }catch(IOException ioe) {
        ioe.printStackTrace();
     }
     return dom;
  }
  ...
```

```
private Hashtable<String,Rule> parseDocument(Document dom){
   //get the root elememt
    Element docEle = dom.getDocumentElement();
    Hashtable<String,Rule> rules = new Hashtable<String,Rule>();
    //get a nodelist of <employee> elements
   NodeList nl = docEle.getElementsByTagName("Rule");
   if(nl != null && nl.getLength() > 0) {
      for(int i = 0 ; i < nl.getLength();i++) {
         //get the employee element
         Element el = (Element)nl.item(i);
         //get the Employee object
         Rule e = getRule(el);
         //add it to list
         rules.put(e.getName(),e);
      }
   }
   return rules;
}
```

Figure 13.8 Rule Parser Code Fragment

13.4.2 IDS-Configuration

The IDSConfig is used to read the properties configured in the file “ids.config”. We utilized Java 1.5 enum to realize the IDSConfig. The Java 1.5 enums are references to a fixed set of objects to represent various possible choices. Enum and the enum constants are just classes. In our implementation, there is always a constant corresponding to each property in the “ids.config”. The code fragment of the IDSConfig is provided in *figure 13.9.*

```
public enum IDSConfig {
                          ATTACKTYPE_TIME,
                          ATTACKTYPE_WITHOUTTIME,
                          BLACKLIST_UPDATE_TIME,
                          MOUNT_IPTABLE,
                          IPTABLE,
                          TIME_INTERVAL;
                          ... ...
}
```

The file “ids.config” is:

```
attacktype.time=flood
attacktype.withouttime=sqlinject
#########################################################
#the life cycle of a IP Address in the blacklist. The unit is hour  #
########################################################
blacklist.update.time=1
##########################################################
# Time interval for time dependent attack. The unit is second      #
#########################################################
time.interval=60
###############################################################
#if the IP table was mounted, the IDS will filter only the messages      #
# which are proxied or sent by the IPs or URI specified in the IP table  #
###############################################################
mount.iptable=false
iptable=10.0.1.100,198.32.22.111
```

Figure 13.9 IDSConfig Code Fragment

13.5 Summary

This chapter presented the implementation of stateful misuse Intrusion Detection and Prevention (IDP-AS) system for IMS Application Servers. The implementation is based on SIPSEE developed within Open IMS FOKUS Testbed. The attacks rules are developed in XML and are loaded during runtime. The implementation work is performed in three phases (a) IDP Centre implementation; (b) Partner, IDP Filter and Rules Collection implementation; (c) Rules Parser and IDP Configuration implementation.

Chapter 14 IDP-AS Testing and Evaluation

14.1 Introduction

In this chapter, we present test execution and performance results of developed IDP-AS prototype. First we focus on testing environment and tool, and then describe the test cases and performance evaluation. The performance results should help to deploy the IDP-AS in real world environment at the Open IMS Fraunhofer Testbed. They also facilitate to further improve the developed prototype. The testing environment is comprised of SIPSEE (SIP Servlet Execution Environment) IMS Application Server integrated with IDP-AS and SIP Forum Test Framework (SFTF) [90] acts as a client to launch the attacks as depicted in *figure 14.1*.

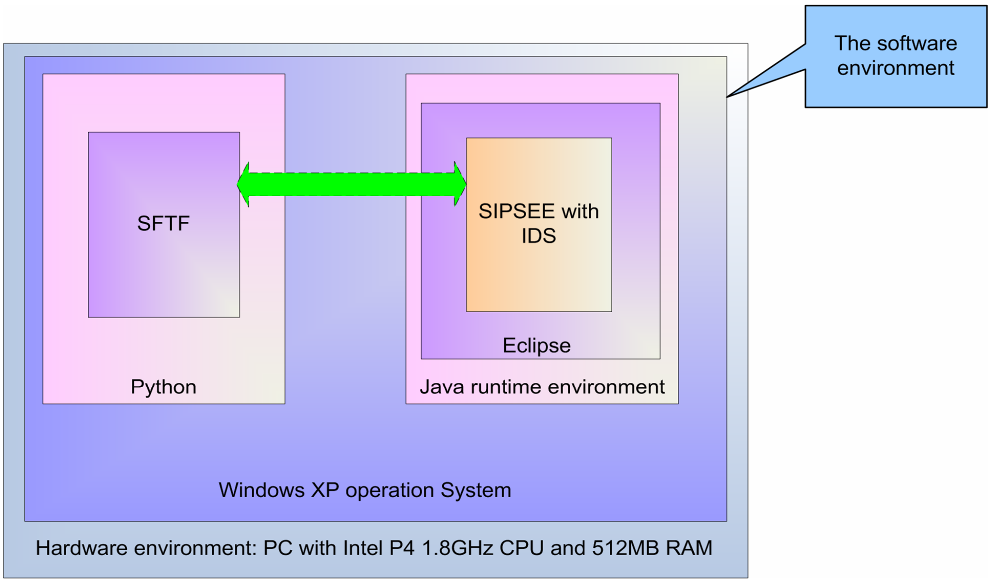

The software environment
SFTF
Python
SIPSEE with IDS
Eclipse
Java runtime environment
Windows XP operation System
Hardware environment: PC with Intel P4 1.8GHz CPU and 512MB RAM

Figure 14.1 IDP-AS Testing Environment

The approach for executing functional tests is to launch simulated attacks against the IMS AS. Each attack pattern defined by IDP-AS in Rule Collection should be checked with the corresponding attack simulated by a test case of SFTF. If IDP-AS detects all of simulated attacks, it fulfils the functionality requirements. The tests procedure is illustrated in *figure 14.2*. In each test the malicious client (SFTF) sends multiple SIP messages. The IDP-AS should detect the simulated attacks and should stop the further messages sent by the SFTF.

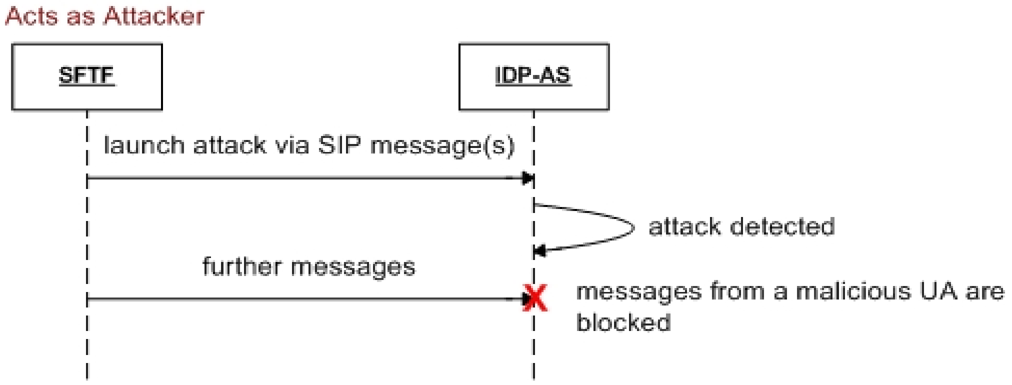

Acts as Attacker
SFTF
IDP-AS
launch attack via SIP message(s)
attack detected
further messages
messages from a malicious UA are blocked

Figure 14.2 Test Procedure

14.2 Test Case for INVITE Flooding – "caseinviteflood"

In order to test the INVITE flooding rule, this test case generates 200 INVITE Request and then sends to IMS AS with is equipped Intrusion Detection and Prevention (IDP-AS) system. The code fragment of the test case is given as:

```
class caseinviteflood (TestCase):
def config(self):
    self.name = "Case invite flood"
    self.description = "Testcase for IDS"
    self.isClient = True
    self.transport = "UDP"
def run(self):
   self.neh = NEH.NetworkEventHandler(self.transport)
  #generate an Invite Request
   inv = self.createRequest("INVITE")
                                                              inv.rUri.params.append("unknownparam")
inv.setHeaderValue("NewFangledHeader     ",  "    newfangled  value\r\n  continued     newfangled
value\r\n")
                                   fo = inv.getParsedHeaderValue("From")
                                  fo.params.append("   unknownparam  =   unknowvalue  ")
    fo.displayname = "SIP Cert \\\\\\"   "
    inv.setHeaderValue("From", fo.create())
    via = inv.getParsedHeaderValue("Via")
   via.host = via.host + "\r\n   "
        ... ...
   #send the Request for 200 times
   for i in range(200):
          self.writeMessageToNetwork(self.neh, inv)
  self.neh.closeSock()
```

Figure 14.3 Test Case for INVITE Flooding

The IDP-AS declared after 133rd INVITE Request that the attack is detected as depicted in *figure 14.4*. Why does the prototype not detect the attack after 100th INVITE request as defined in the attack rules? The reason is that the partner's state is verified up to 133rd Request and then declares it as a malicious user. Once the attack is detected, the IP address 127.0.0.1 is inserted into the blacklist and further messages from 127.0.0.1 are blocked. The test result of INVITE flooding is presented in *figure 14.5*.

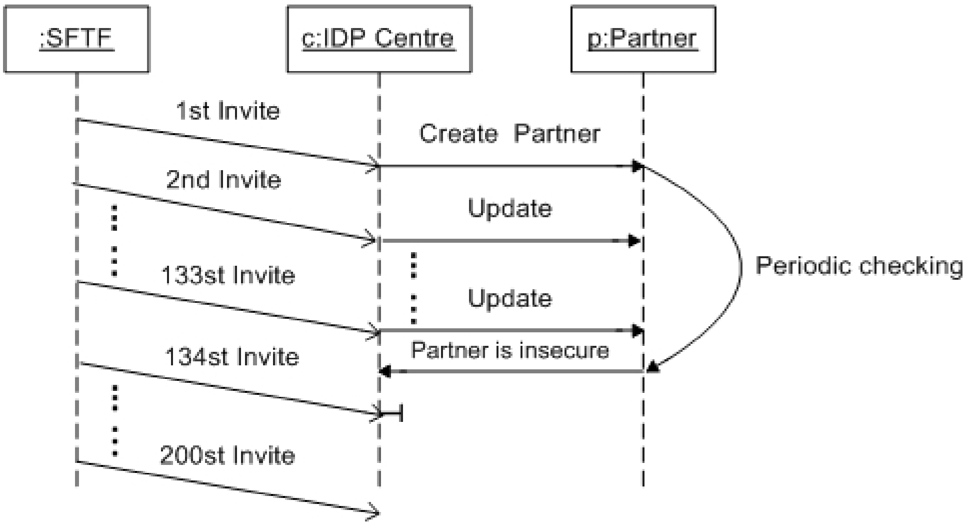
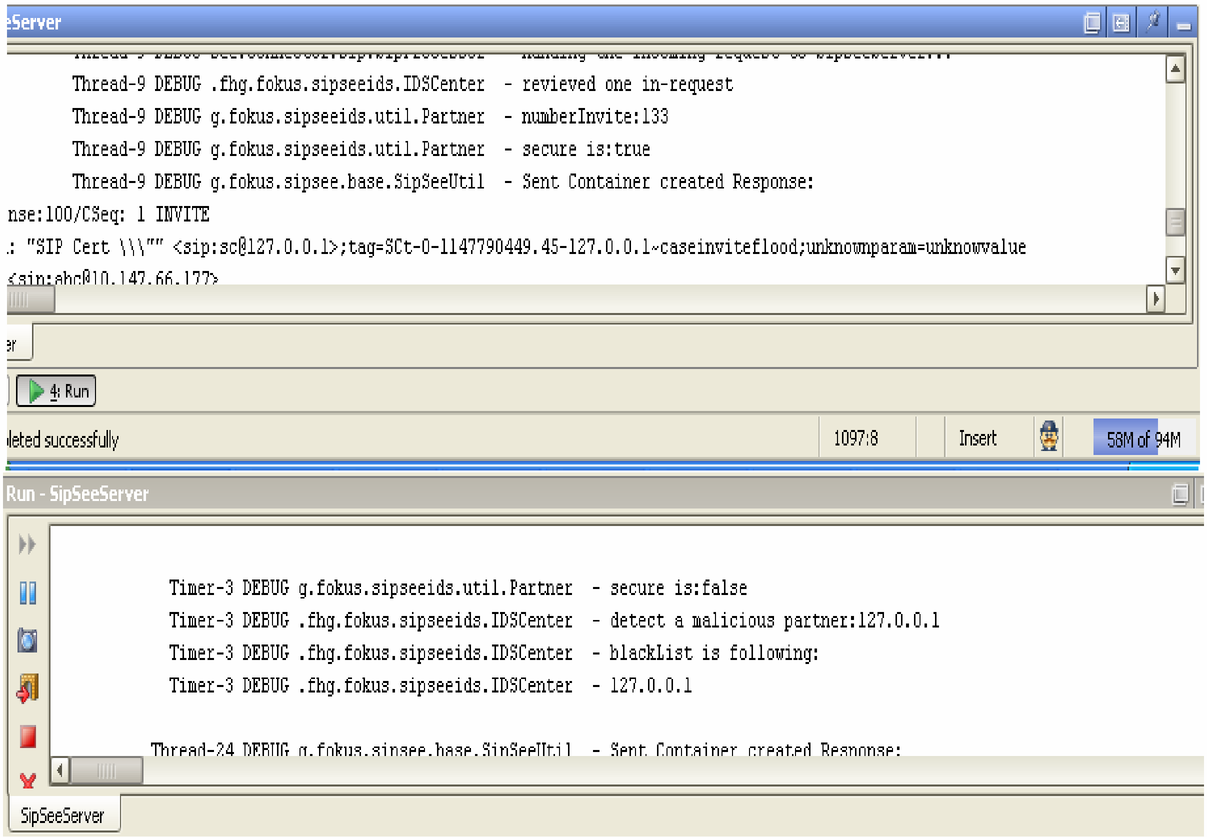


Figure 14.4 Process of INVITE Flooding Test



```
        Thread-9 DEBUG .fhg.fokus.sipseeids.IDSCenter  - revieved one in-request
        Thread-9 DEBUG g.fokus.sipseeids.util.Partner  - numberInvite:133
        Thread-9 DEBUG g.fokus.sipseeids.util.Partner  - secure is:true
        Thread-9 DEBUG g.fokus.sipsee.base.SipSeeUtil  - Sent Container created Response:
nse:100/CSeq: 1 INVITE
: "SIP Cert \\\"" <sip:sc@127.0.0.1>;tag=SCt-0-1147790449.45-127.0.0.1~caseinviteflood;unknownparam=unknowvalue
<sip:abc@10.147.66.177>
```

```
        Timer-3 DEBUG g.fokus.sipseeids.util.Partner  - secure is:false
        Timer-3 DEBUG .fhg.fokus.sipseeids.IDSCenter  - detect a malicious partner:127.0.0.1
        Timer-3 DEBUG .fhg.fokus.sipseeids.IDSCenter  - blacklist is following:
        Timer-3 DEBUG .fhg.fokus.sipseeids.IDSCenter  - 127.0.0.1

       Thread-24 DEBUG g.fokus.sipsee.base.SipSeeUtil  - Sent Container created Response:
```

Figure 14.5 Test Result for INVITE Flooding

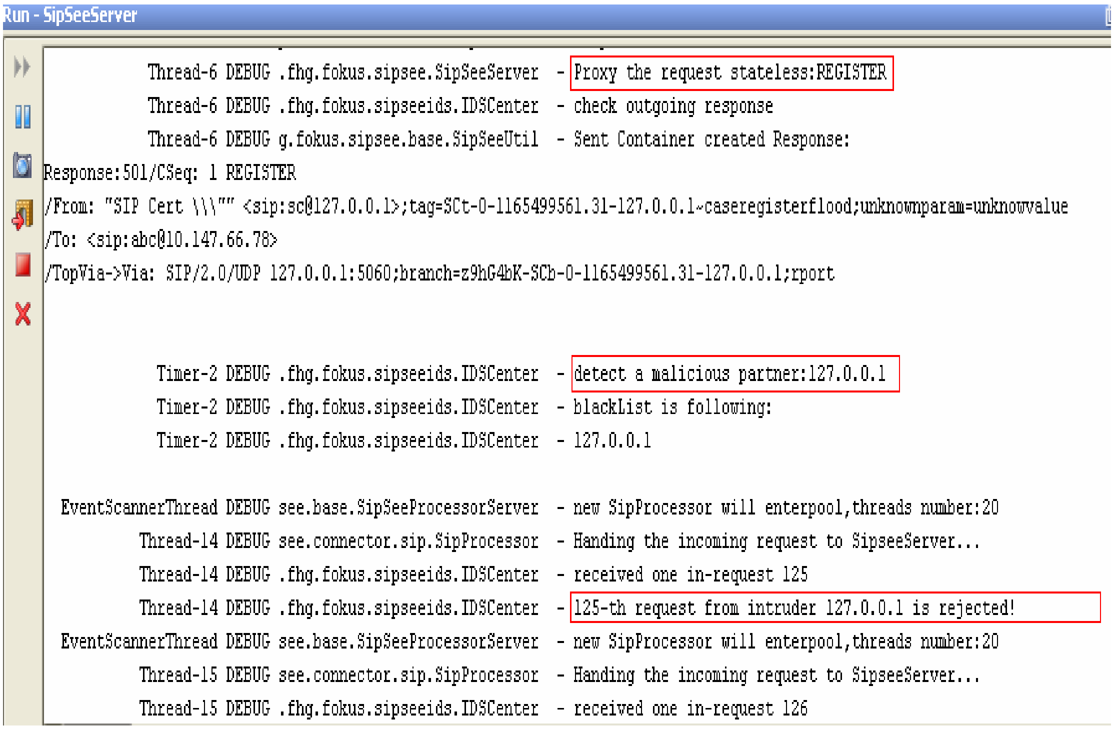
14.3 Test Case for REGISTER Flooding – "caseregisterflood"

Similar to the previous test case, the REGISTER flooding test case "*caseregisterflood*" also generates 200 REGISTER SIP Requests in 60 seconds and then sends to secure IMS Application Server as provided in the following code:

```
class caseregisterflood (TestCase):
    def config(self):
        self.name = "Case register flood"
        self.description = "simulation of register flood"
        self.isClient = True
        self.transport = "UDP"
    def run(self):
        self.neh = NEH.NetworkEventHandler(self.transport)
        reg = self.createRequest("REGISTER")
        reg.rUri.params.append("unknownparam")
        reg.setHeaderValue("NewFangledHeader      ", "    newfangled value\r\n continued
newfangled value\r\n")
        fo = reg.getParsedHeaderValue("From")
        fo.params.append("   unknownparam  =  unknowvalue  ")
        fo.displayname = "SIP Cert \\\\\\\"   "
        reg.setHeaderValue("From", fo.create())
        via = reg.getParsedHeaderValue("Via")
        #via.host = via.host + "\r\n   "
     via.host = "pc33.here.com\r\n "
        reg.setHeaderValue("Via", via.create())
        co = reg.getParsedHeaderValue("Contact")
        co.displayname = "Quoted String \\\"\\\""
        co.params.append("newparam =\r\n  newvalue")
     # set value for Expire header
        #ex = reg.getParsedHeaderValue("Expire")
        #reg.setHeaderValue("Expire", 7200)
        reg.setHeaderValue("Contact", co.create())
        reg.removeHeaderField("Contact")
        #Note: explicitly removed Contact because the m with the spaces below
        # will not replace the original Contact header
        reg.setHeaderValue("m    ", co.create())
     for i in range(200):
          self.writeMessageToNetwork(self.neh, reg)
        self.neh.closeSock()
```

Figure 14.6 Test Case for REGISTER Flooding

The IDP-AS detected the REGISTER flooding attack and it blocked the IP address of malicious user to stop further communication from this user for defined time period. The test result of REGISTER flooding attack as dipected in *figure 14.7*.



```
            Thread-6 DEBUG .fhg.fokus.sipsee.SipSeeServer  - Proxy the request stateless:REGISTER
            Thread-6 DEBUG .fhg.fokus.sipseeids.IDSCenter  - check outgoing response
            Thread-6 DEBUG g.fokus.sipsee.base.SipSeeUtil  - Sent Container created Response:
Response:501/CSeq: 1 REGISTER
/From: "SIP Cert \\\"" <sip:sc@127.0.0.1>;tag=SCt-0-1165499561.31-127.0.0.1~caseregisterflood;unknownparam=unknowvalue
/To: <sip:abc@10.147.66.78>
/TopVia->Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK-SCb-0-1165499561.31-127.0.0.1;rport


             Timer-2 DEBUG .fhg.fokus.sipseeids.IDSCenter  - detect a malicious partner:127.0.0.1
             Timer-2 DEBUG .fhg.fokus.sipseeids.IDSCenter  - blackList is following:
             Timer-2 DEBUG .fhg.fokus.sipseeids.IDSCenter  - 127.0.0.1

  EventScannerThread DEBUG see.base.SipSeeProcessorServer  - new SipProcessor will enterpool,threads number:20
           Thread-14 DEBUG see.connector.sip.SipProcessor  - Handing the incoming request to SipseeServer...
           Thread-14 DEBUG .fhg.fokus.sipseeids.IDSCenter  - received one in-request 125
           Thread-14 DEBUG .fhg.fokus.sipseeids.IDSCenter  - 125-th request from intruder 127.0.0.1 is rejected!
  EventScannerThread DEBUG see.base.SipSeeProcessorServer  - new SipProcessor will enterpool,threads number:20
           Thread-15 DEBUG see.connector.sip.SipProcessor  - Handing the incoming request to SipseeServer...
           Thread-15 DEBUG .fhg.fokus.sipseeids.IDSCenter  - received one in-request 126
```

Figure 14.7 Test Result for REGISTER Flooding

14.4 Test Cases for INVITE Response and REGISTER Response Flooding

The objective of these two attacks is that the malicious user or attacker continuously sends SIP Requests with random username and password until the network authenticate the attacker. To detect these attacks we have to compare 401 and 407 SIP Responses [7] with the attacks rules. In order to generate 407 or 401 Response we perform a mandatory modification of status-code on every outgoing Response, namely the status-code of outgoing Response being always set with 401 or 407. For example, to test the INVITE Response flooding, the mandatory modification locating in the method *send-Container-Response()* of class *SIPSee-Util* is as follows:

```
public void sendContainerResponse(Request req, int status, ServerTransaction strans,String reason){
    if(!req.getMethod().equalsIgnoreCase(Request.ACK)) {
      try {
        Response resp = _server.getMessageFactory().createResponse(status,req);
        /* for testing password guessing*/
        if(resp.getStatusCode()!=407)
           resp.setStatusCode(407);
        if(!SIPSeeUtil.isStringNull(reason)) {
           resp.setReasonPhrase(reason);
        }
        boolean secure = IDSCenter.getInstance().checkOutResponse(resp);
        if(strans!=null) {
          // Response not sent yet
          if(strans.getState().getValue()<=TransactionState.PROCEEDING.getValue()) {
            if(secure){
             strans.sendResponse(resp);
            }
          }
        } else {
          // send response statlessly
         if(secure) {
          _server.getSIPConnector().sendStatelessResponse(resp);
         }
        }
        LOGGER.debug("Sent Container created Response:"+responseToShortString(resp));
      } catch (Throwable e) {
        LOGGER.error("SIPSee Exception -> ", e);
      }
    }
}
```

Figure 14.8 Test Cases for INVITE/REGISTER Responses

To test the REGISTER response flooding, we need to modify the status-code of outgoing Responses with 401 instead of 407.

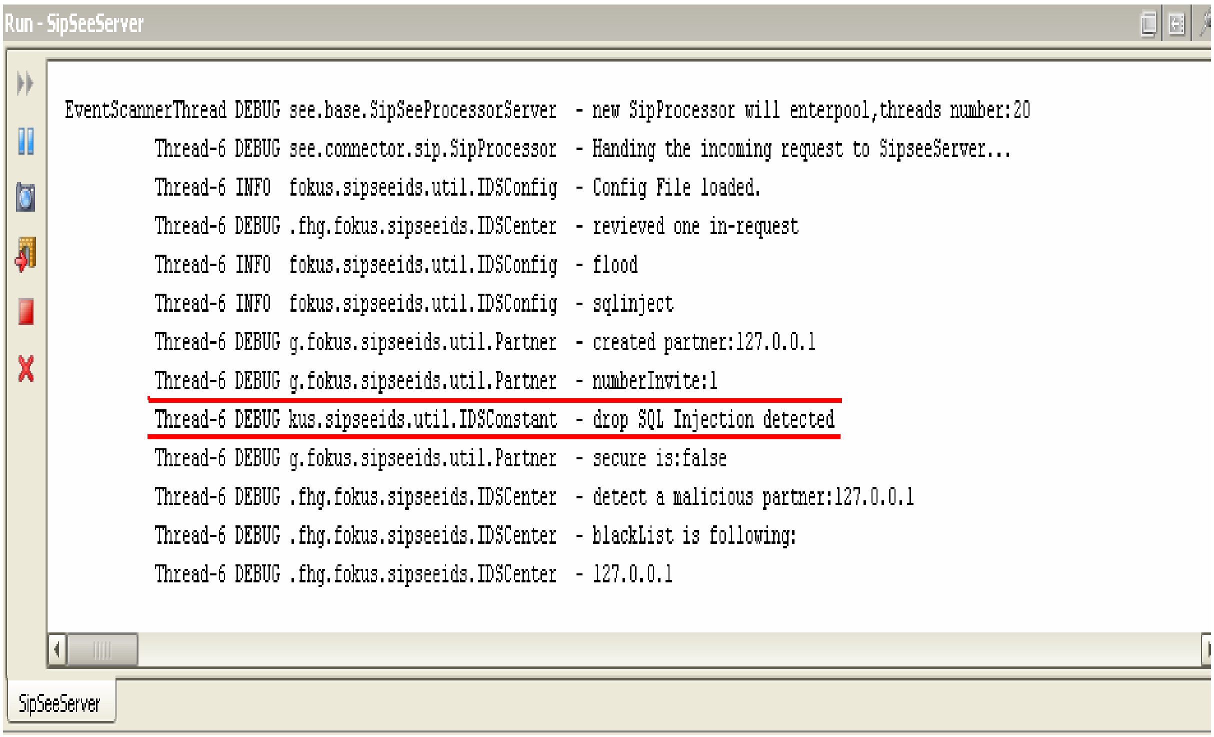
14.5 Test Cases for SQL Injection

The task of test cases for the SQL Injection attacks are to build such Requests which contain an Authorization header injected with SQL, and then send it to IMS Application Server. The position of SIP Request, where the SQL commands could be injected, is the username in “Authorization” header. The feature of injected username is that it always contains a semicolon followed by the SQL commands. The test case for the SQL “drop” Injection is given as an example with following code fragment:

```
class casesqldrop (TestCase):
        def config(self):
                        self.name = "Case sql injection drop"
                        self.description = "simulation of drop sqlinjection attack"
                        self.isClient = True
                        self.transport = "UDP"
                def run(self):
                        self.neh = NEH.NetworkEventHandler(self.transport)
                        inv = self.createRequest("INVITE")
                        ...
                        inv.setHeaderValue("Authorization","Digest username=\"bob';drop table subscriber\" ")
                        ...
                        self.writeMessageToNetwork(self.neh, inv)
                        self.neh.closeSock()
```

Figure 14.9 Test Case for SQL Injection

This test case dropped the table called subscriber via setting the username with *"bob'; drop table subscriber"*. The Request sent by the test case is matched with the rule "Drop statement". The result depicted in *figure 14.10* shows that IDP-AS is capable to detect the SQL Injection attack.



```
EventScannerThread DEBUG see.base.SipSeeProcessorServer  - new SipProcessor will enterpool,threads number:20
          Thread-6 DEBUG see.connector.sip.SipProcessor  - Handing the incoming request to SipseeServer...
          Thread-6 INFO  fokus.sipseeids.util.IDSConfig  - Config File loaded.
          Thread-6 DEBUG .fhg.fokus.sipseeids.IDSCenter  - revieved one in-request
          Thread-6 INFO  fokus.sipseeids.util.IDSConfig  - flood
          Thread-6 INFO  fokus.sipseeids.util.IDSConfig  - sqlinject
          Thread-6 DEBUG g.fokus.sipseeids.util.Partner  - created partner:127.0.0.1
          Thread-6 DEBUG g.fokus.sipseeids.util.Partner  - numberInvite:1
          Thread-6 DEBUG kus.sipseeids.util.IDSConstant  - drop SQL Injection detected
          Thread-6 DEBUG g.fokus.sipseeids.util.Partner  - secure is:false
          Thread-6 DEBUG .fhg.fokus.sipseeids.IDSCenter  - detect a malicious partner:127.0.0.1
          Thread-6 DEBUG .fhg.fokus.sipseeids.IDSCenter  - blackList is following:
          Thread-6 DEBUG .fhg.fokus.sipseeids.IDSCenter  - 127.0.0.1
```

Figure 14.10 Test Result for Drop SQL Injection

Test cases for other SQL Injection are similar to the drop SQL Injection. The only modification in these test cases is the username of the Authorization header should be replaced by other corresponding SQL statements. To test the delete SQL Injection, for example, we could set the username with "bob'; Delete From subscriber where username='bob"". Thus from this test it is proved that the prototype is able to detect the SQL Injection attacks.

14.6 Performance Evaluation

The performance matrix of developed IDP-AS based on measuring system signalling cost and processing delay for attacks detection. We have utilized SIP Forum Test Framework (SFTF) [90] to perform the evaluation and performance tests. In the development process, it has been considered that the IDP-AS should meet the requirements of processing delay as mentioned in RFC3261 [4]. The state machine for SIP INVITE client transaction is provided in *figure 14.11*. As mentioned in the specification, the timer A is set with a value of T1 with default value 500 ms. When timer A expires, the client transaction must retransmit the request, and must reset the timer with value of 2xT1. When timer A expires again from 2*T1 seconds, the request must be retransmitted again. This process must continue to retransmit the request with intervals that double after each transmission. These retransmissions should only be done while the client transaction is in the "*calling*" state [4].

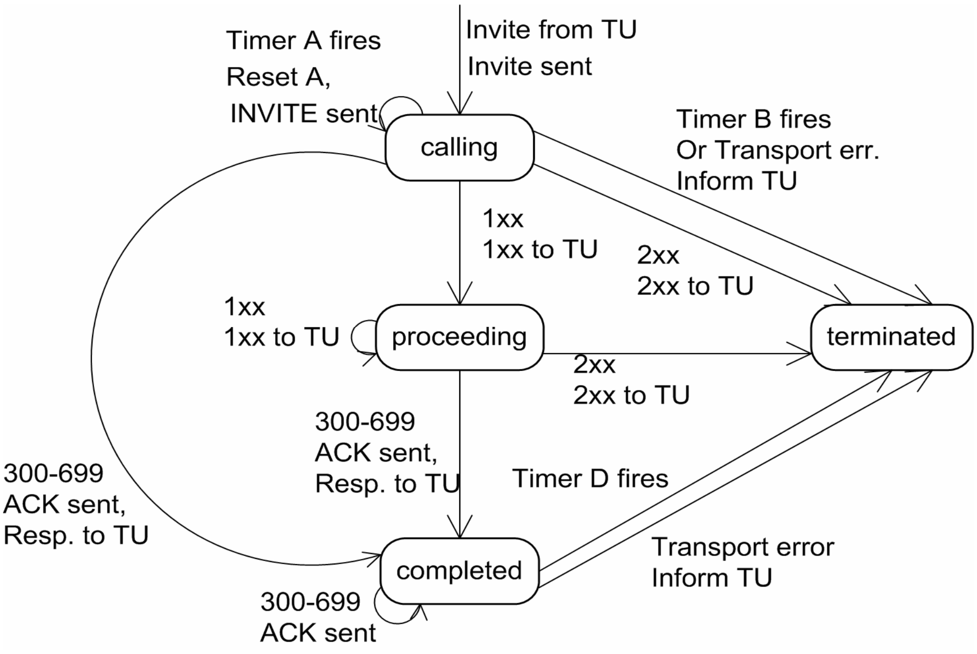


Figure 14.11 SIP INVITE Client Transaction State Diagram

To avoid this retransmission of INVITE Request, it is required that the processing delay time or overhead of IDP-AS should be minimum. It means that the delay in "INVITE client transaction" introduced by the prototype should be very small as compared to the initial value of timer A (T1 = 500ms). The total delay (D_t) shown in *figure 14.12* consists of the request processing delay (D_{Rq}) and response processing (D_{Res}) i.e.

$$D_t = D_{Rq} + D_{\mathrm{Re}\,s} \qquad (14.1)$$

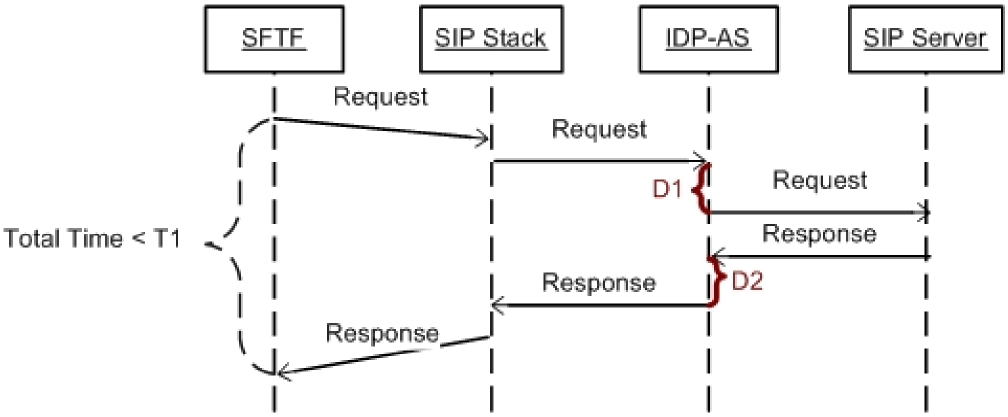


Figure 14.12 IDP-AS Processing Delay

Now we present the performance of test cases for INVITE, REGISTER, INVITE Response and REGISTER Response flooding and SQL Injection within IMS Testbed to evaluate the practical performance of IDP-AS.

14.6.1 Performance Test for INVITE Flooding

To calculate the INVITE flooding detection performance, the client sends number of requests to IMS Application Server. We start the test from 10 INVITE Requests and increase the number by 10 up to 150 INVITE messages. We note the time interval for every incoming request when it arrives to the IDP-AS and is forwarded to the SIP Server. Similarly we record the time interval for each outgoing response when it arrives to IDP-AS and is forwarded to the SIP Stack.

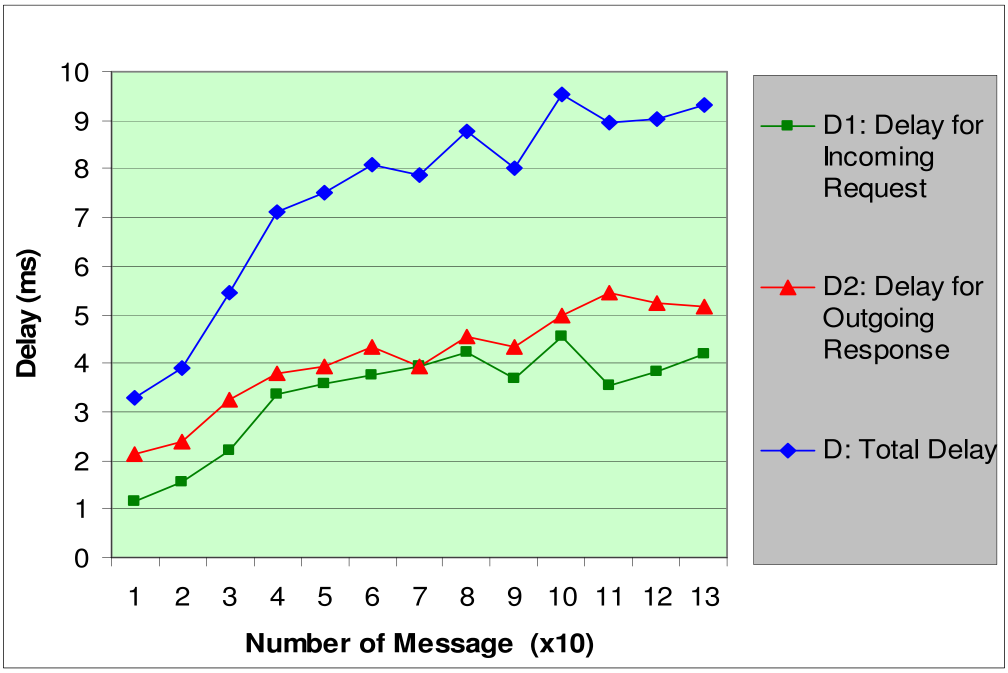


Figure 14.13 Performance Test for INVITE Flooding

The average processing delay for each INVITE Request is given equation 14.2:

$$D_{Invite}^{Av} = \frac{D_{Rq} + D_{\mathrm{Re}\,s}}{n} = \frac{\sum_{k=1}^{n} T_k}{n} \qquad (14.2)$$

Where, T_k is the time interval for both incoming request and outgoing response, K is the index of message, and n is the sum of messages received by IDP-AS. The maximum value of n should be less than the Number Value (200) defined in the rule of INVITE Request flooding, so that no message will be blocked.

From performance test, we have obtained the chart shown in *figure 14.13*. The curve marked (□) represents the total delay (D) which varies from 3.28 ms to 9.32 ms. This delay is very small as compared to round-trip time (T1) and the placement of IDP-AS within IMS AS does not cause the retransmission of SIP messages.

14.6.2 Performance Test for REGISTER Flooding

Similar to the INVITE flooding, the performance for REGISTER flooding is depicted in *figure 14.14*. The processing overhead varies 1.88 ms to 9.12 ms for maximum of 150 REGISTER requests. The total delay is calculated using the equation 14.3.

$$D_{\mathrm{Re}\,gister}^{Av} = \frac{D_{\mathrm{Re}\,q} + D_{\mathrm{Re}\,s}}{n} = \frac{\sum_{k=1}^{n} T_k}{n} \qquad (14.3)$$

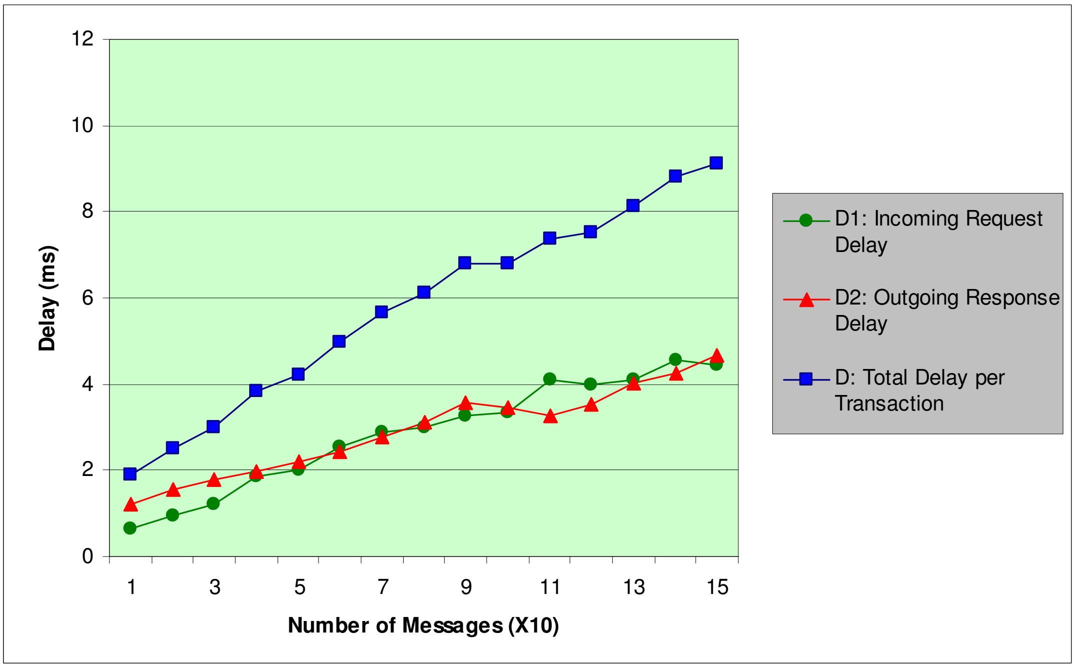


Figure 14.14 Performance Tests for REGISTER Flooding

14.6.3 Performance Test for INVITE Response Flooding

The performance results for detecting INVITE Response flooding are provided in *figure 14.15*. The curve marked (□) represents the total delay (D) as calculated from equation 14.4, varies in the range of 1.97 to 8.98 ms.

$$D^{Av}_{Invite-\mathrm{Re}\,sponse} = \frac{D_{\mathrm{Re}\,q} + D_{\mathrm{Re}\,s}}{n} = \frac{\sum_{k=1}^{n} T_k}{n} \qquad (14.4)$$

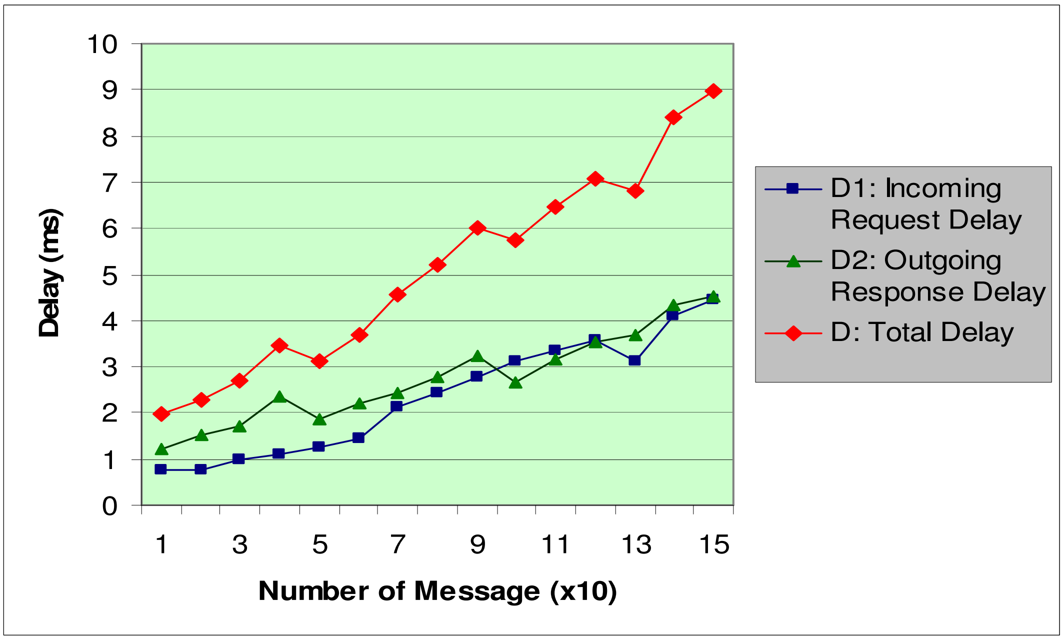


Figure 14.15 Performance Tests for INVITE Response Flooding

14.6.4 Performance Test for SQL Injection

The practical performance results for the drop SQL injection are provided in *figure 14.16*. The delay is between 2.63 ms and 10.34 ms for 10 to 150 SIP requests and responses. The total delay is expressed with equation 14.5.

$$D^{Av}_{SQL-Injection} = \frac{D_{\mathrm{Re}\,q} + D_{\mathrm{Re}\,s}}{n} = \frac{\sum_{k=1}^{n} T_k}{n} \qquad (14.5)$$

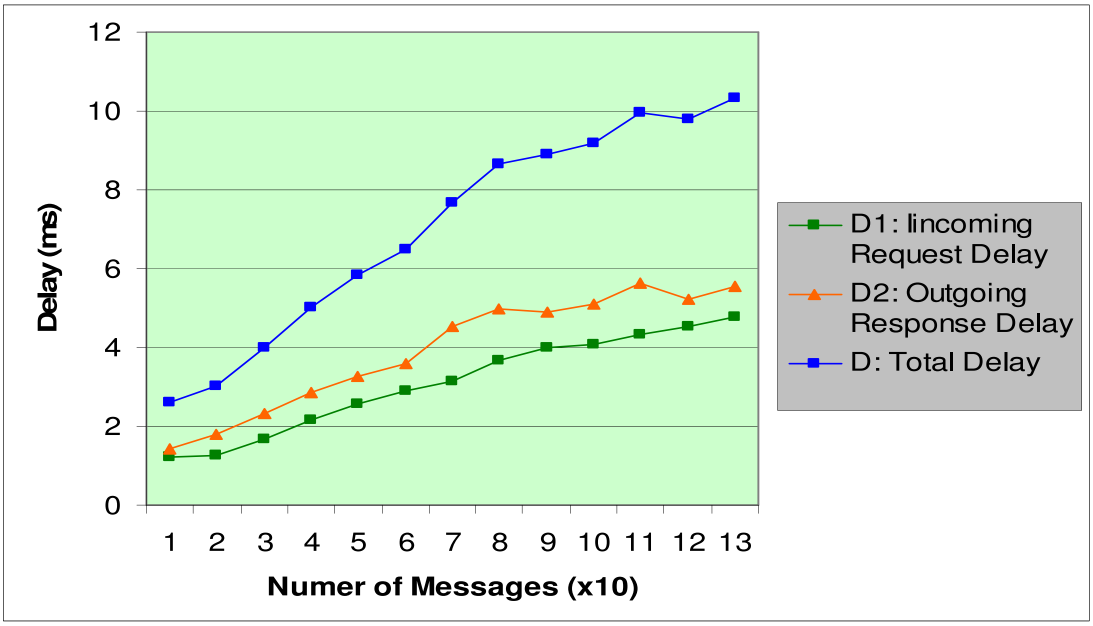


Figure 14.16 Performance Test for SQL Injection

14.7 Summary

In this chapter, the testing and performance results of Intrusion Detection and Prevention (IDP-AS) system for IMS Application Servers are presented. The performance evaluation is performed at Open IMS Testbed. The attacks detection procedure is on-line and real-time. Therefore, the IDP-AS performance is very critical and should not affect the communication flow between client and IMS Application Server. The performance results showed that the total delay introduced by IDP-AS to process the SIP messages is about 10 ms.

Part-F

Comparison with Related Work

&

Conclusion

Chapter 15 Comparison with Related Work

15.1 Introduction

The IP Multimedia Subsystem (IMS) is new and emerging technology providing Fixed-Mobile Convergence (FMC) platform. It is passing through evolutionary and development phase. The 3GPP and TISPAN have not provided any solution for Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS) attacks and abuse of IMS-based applications from malicious and legitimate users. The research community has concerns about the emerging security threats facing to emerging IP-based IP Multimedia Subsystem (IMS), Web 2.0, VoIP technologies. For example some of the comments and concerns are summarized as follows:

- The 3GPP in TSG SA WG3 Security meeting [91] in 2003 have discussed and considered that Denial-of-Service (DoS) attacks are serious threats to IMS Core and IMS Application Servers.

- The University of Southern California and VeriSign has published a white paper “Building a Security Framework for Delivery of Next Generation Network Services” in 2005 [92]. This report explores that the emerging security challenge are identity theft, services vulnerability and Internet based flooding attacks for NGN/IMS networks.

- The INRIA Nancy Universités Centre de Recherché Grand Est., France, has published “New Frontier in VoIP Security, 2007” [93]. This study says that most of the VoIP Devices (e.g. Cisco IP/SIP Phone 7940/7960 & ASTERISK) are vulnerable to DoS and SQL-Injection. The research work is conducted in Madynes project.

- The Georgia Technology Information Security Center (GTISC), USA, has published “Emerging Cyber Threats Report for 2008” in October 2007 [94]. This report explores the alarming and emerging threats like Denial-of-Service (DoS), flooding attacks, SQL-Injection for emerging technologies e.g. IMS, VoIP, Web2.0 and Mobile Converged Networks.

- The Sipera VIPER™ (Voice over IP Exploitation Research) Lab [95]has identified over 90 major classes of unique vulnerabilities and over 20 000 attacks in the last 3 years that can be launched against IMS networks. These threats includes IMS framework-related vulnerabilities, SIP protocol vulnerabilities, VoIP, video, PoC, Messaging, Presence, Conferencing applications vulnerabilities and voice spam**.**

Only few researchers and communications organisations are working for the development on Intrusion Detection and Prevention (IDP) for IMS. The well known research organizations working for the protection of IMS against Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS) Attacks includes Verizon Advance IMS (A-IMS), Juniper Networks IDP, Acme Packet DoS Protector, Fokus Fraunhofer VoIP Defender and Sipera IPCS (Internet Protocol Communications Security) etc. Their brief description of their work is as follows:

15.2 Verizon –Advance IMS (A-IMS) Solution

The Verizon is working on the Advances to IP Multimedia Subsystem (A-IMS) with its partners Cisco Systems, Lucent Technologies, Motorola, Nortel and QuelComm. The A-IMS is being developed to improve the shortcoming and deficiencies with the existing 3GPP2 MMD (Mobile Multimedia Domain) [3] standards. This new architecture has many new features like support of SIP and non SIP services, packet flow optimization and integrated end-to-end security etc [96].

The security enhancements that A-IMS provides are substantial. The A-IMS integrates intrusion detection/prevention (IDS/IPS) and anti-malware into the network, and provides a separate Security Operations Center (SOC) [96] for real-time response to security threats.

The development of IDP for IP Multimedia Subsystem is yet in proposal phase and it will be developed for 3GPP 2 IMS Architecture. It provides protection against DoS/DDoS attacks. Our solution is developed for 3GPP IMS Architecture and it focus on protecting against DoS/DDoS attacks as well as securing IMS services and applications from malicious and non-malicious users.

15.3 Juniper IMS-IDP Solution

Juniper Networks has developed T-Series, M-Series and E-Series routers and Integrated Security Gateways (ISGs). Theses routers and security gateways provide Intrusion Detection and Prevention (IDP) solutions and resource and admission control policy to extend capabilities to further meet the needs of service providers while conforming to 3GPP and TISPAN standards [97].

From security point of view, Juniper claims that their security gateways protect IMS services and applications by the Intrusion Detection and Prevention (IDP) system. They claim that their products protect SIP-based application servers and users from attacks, including SIP anomaly protection for zero-day attacks.

This security solution is specific vendor based product and not open based. Our IDP is developed for research purpose as a part of Open IMS Playground [80].

15.4 Acme Packet Solution

The Acme Packet is working with IMS Enterprise (IMS-E) to develop IMS wirleline enterprise services. On security side, Acme Packet working on developing solution against Denial-of-service (DoS) and Distributed DoS (DDoS) protection from both malicious attacks and non-malicious users. The solution will provide IMS core DoS prevention [98]. It focuses on SIP flooding and RTP attacks.

This solution is like a firewall and deployed as session border control. It is not mentioned that the solution is real time. This security solution is also vendor specific and not available for open IMS research community. Our IMS Intrusion Detection and Prevention prototype is developed for IMS research and educational community to be extended for IMS security research work.

15.5 VoIP Defender

The VoIP Defender [99] is research project developed by Fraunhofer FOKUS Open Communication Institute Berlin [100] for VoIP infrastructure. It will officially release in 2007. This research work is the continuation of VoIP security project SNOCER (Low Cost Tool for Secure and Highly Available VoIP Communication Services). The VoIP Defender is generic security architecture to monitor, detect, analyze and counter attacks relevant for a SIP-based VoIP infrastructure. The architecture is scalable and can be easily extended with new detection algorithms. Analysis and traffic control can be performed from the SIP layer down to the transport, network and MAC layers. The VoIP Defender is designed to work fully transparent to clients and SIP servers. It performs attacks detection and analysis off-line.

The project is not designed for IMS but in future there is possibility that it could be used for IMS infrastructure for detecting unknown attacks by using anomaly detection approach. As compared to VoIP Defender, the IMS-IDP approach is stateless and state-full misuse detection and prevention.

15.6 Siemens Nokia IMS 5 Solution

Siemens has released IMS 5 commercial product in 2007 [101] providing efficient Voice over IP (VoIP) services. The IMS 5.0 system consisting of the CFX-5000 and the CMS-8200, is integrated as the controlling core element of the IMS 5.0 mobile voice over IP solution. Related to IMS DoS attacks protection and prevention, Siemens claims that the P-CSCF supports a mechanism to detect attacks from a specific terminal identified by its IP address and port number based on pre-configured observation data. When a terminal has been identified as malicious, it is blocked from communicating with the P-CSCF for a configurable period of time. All active sessions of this UE shall be terminated by a network initiated deregistration. When at least one terminal has been blocked, the security center generates an alarm notifying the actual number of blocked endpoints. The blocking and unblocking of a terminal is logged in a file. If it is a registered user, the IMPU is logged so that the operator can find out the identity of the malicious user [101]. This approach is applied at network layer but the performance results of adopted approach are yet not available. The provided solution is vendor specific and not available as open source for IMS research community as compared to our solution.

15.7 Sipera IPCS (Internet Protocol Comm Security)

The Sipera Voice over IP Exploitation Research (VIPER) Lab [95] is working over VoIP and IMS for the last three years to identify the new threats and to propose solutions to secure these technologies. They say "with the advent of new access technologies and devices, the probability of malicious attacks and service abuse of Voice over Internet Protocol (VoIP) and other real-time, IP communications applications has increased significantly together with the increase in attack sophistication. All these developments are creating a new level of security requirements for the operator that go beyond anything they have deployed thus far and well beyond standard authentication and encryption mechanisms". Their products are also Vendor Specified (IPCS 520 & IPCS 620).

15.8 Open Source SNORT Intrusion Detection System

Snort is open source, IP-based network IDS capable of performing packet logging and real-time traffic analysis. For intrusion prevention and detection, it utilizes rule-driven language, which combines signature, protocol and anomaly based inspection methods [102]. We have utilized Snort in IMS testbed environment but due to heavy weight protocol based architecture, it is not suitable for IMS.

Chapter 16 Conclusion and Outlook

16.1 Summary

This chapter summarizes the research domain, solution and the results of this thesis. The objective of this work is to develop a "Secure Service Provisioning (SSP) framework for IP Multimedia Subsystem (IMS)". The SSP framework comprises two security levels. The level 1 integrated all the security solutions developed and recommended by IETF, 3GPP and TISPAN for IMS and IMS based Service Delivery Platform (SDP). The level 2 security focused on IMS security extension for Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS) attacks and misuse of IMS services. The first module of level 2 security solution presented the design and implementation of Intrusion Detection and Prevention (IDP-Core) system for IMS core protection against DoS attacks. The second module of level 2 security solution presented the design, implementation and deployment of Intrusion Detection and Prevention (IDP-AS) system for IMS Application Server (AS) against misuses and fraud protection.

The challenging aspect of this work has been the study and solution for the protection and securing the emerging IP Multimedia Subsystem (IMS). The IMS is developed by 3GPP for mobile domain and extended by TISPAN for fixed networks with a motivation of seamless Service Delivery Platform (SDP) for Fixed-Mobile Convergence (FMC). The IMS is an overlay technology on top of different access networking and emerging as the All-IP Network. On one side, IMS is fascinating approach to merge the fixed and mobile communication as well as voice and data networks on single platform. But on the other hand side with integration of different protocols, access networks and technologies, there are new security threats and vulnerabilities. The potential IMS security threats and challenges are from application layers protocols like Session Initiation Protocol (SIP), IP and transport layers protocols, and access networks.

The IMS is SIP based architecture; therefore it is facing the same threats which any SIP based communication platform like Voice-over-IP (VoIP) has faced. The well-known threats are the denial-of-service attacks on IMS core networks. The SIP REGISTER and SIP INVITE methods could be used to launch flooding attacks in IMS. The objectives of these attacks are to fall-down the IMS core entities especially P-CSCF. The Part-B described the procedures to launch these flooding attacks in IMS.

The IMS Application Servers are service enabler providing value added services. These entities are loosely attached with IMS through ISC (IMS Service Control) interface. The IMS applications are managed and handled by these servers. Therefore, IMS AS security is a vital issue. The potential threats facing to IMS AS includes hacking of applications, accessing value added services without charges and launching of DoS attacks to crumple the IMS enablers. The IMS potential security challenges and threats are presented in requirement analysis of this thesis.

With the rapid development and innovation in IT filed, the new methods and techniques have been developed for easy development and efficient use of modern IT technologies. Now-a-days a person needs only know-how to use complex and sophisticated tools, devices and systems. Similarly most of the software and tools are available as open source for developing innovative and next generation applications. These easy and open based IT architectures are beneficial for hackers to launch complex nature of attacks even with limited knowledge of these technologies. The curves presented in figure *16.1* indicate that the new range of attacks and their complexities have increased with the passage of time and on the other side the attacker's acquired knowledge to launch these sophisticated attacks has decreased sharply.

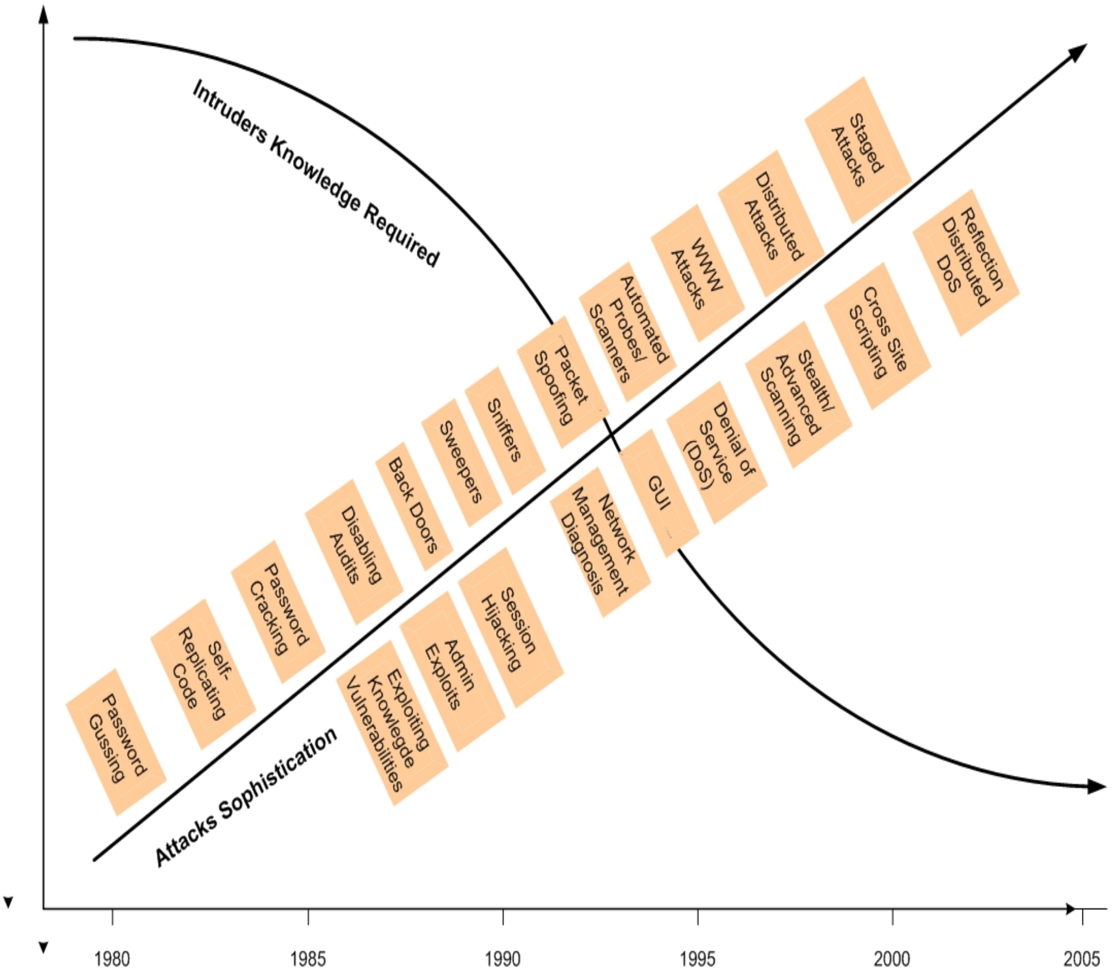


Figure 16.1 Attacks Complexities verses Attacker Knowledge

With increasing the complexity of these attacks, the old and existing security solutions are not enough to provide secure communication to users, protection of network resources and value added services. The research is going for developing new, efficient and reliable security mechanisms for the protection of data systems and information networks. Depending upon the nature of security attacks and vulnerabilities threats, the security protection solutions could be deployed at different layers as depicted in *figure 16.2.* The IMS security solutions has also been deployed at different layers and levels to provide secure signalling and data flow among users and in different IMS domains for roaming traffic protection.

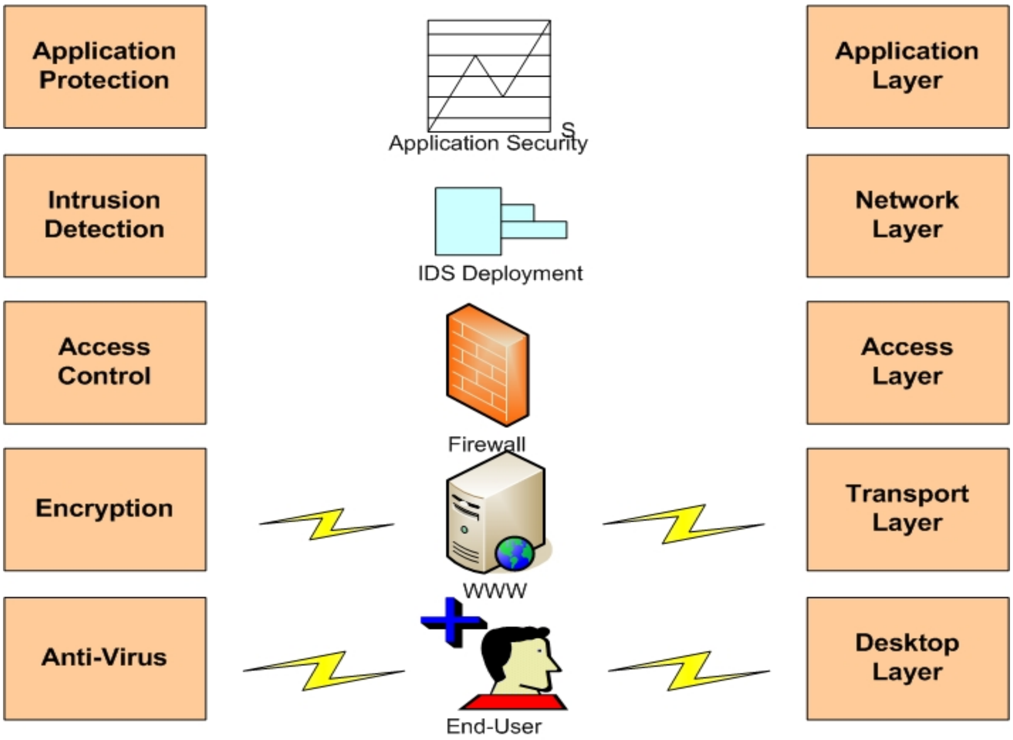


Figure 16.2 Deployment of Security Mechanisms

During the development and standardization of IMS, the 3GPP has challenged from different domains i.e. security, quality of service (QoS) and mobility management etc. For IMS security, the 3GPP focused to standardize the access security mechanisms and encryption algorithms. In this thesis our focus is to explore all possible IMS security mechanisms and propose a comprehensive security architecture that can be used to secure Open IMS Fraunhofer Testbed. This IMS level 1 security solutions focused on user's authentication before accessing the IMS resources, key generation and management, confidentiality and integrity protection which are achieved by utilizing IPsec ESP (IP Security – Encapsulated Security Payload). This procedure is explained in chapter 5.

The Network Domain Security (NDS) is the next objective of IMS security architecture. The NDS is achieved by security gateways which are responsible to implement PKI (Public Key Infrastructure) Authentication Framework (AF) as explained in chapter 6, to implement security when user is roaming.

The IMS HTTP-based applications are addressed by IMS Application Server (AS) through Ut interface. The Authentication Proxy (AP) is responsible to secure these services. This security is achieved by implementing Generic Bootstrapping Architecture (GBA) as an extension to Generic Authentication Architecture (GAA) to authorize users to access services and implementing TLS (Transport Layer Security) to provide secure communication channel. The use of GBA is explained in Part-C.

The major contribution of this thesis has been the IMS security extension as level 2 security solution. This level 2 security extension focused on the detection and mitigation of those threats and vulnerabilities which are not addressed by the standard bodies. These threats are the denial-of-service attacks and fraud control in IMS. The development of level 2 security extension has been divided into two modules; one is focusing the IMS core protection from flooding attacks and the second is protecting the IMS services against misuses.

The Part-D of the dissertation focused on the protection of IMS core entities from SIP REGISTER and SIP INVITE flooding attacks. The security solution based on the development of Intrusion Detection and Prevention (IDP-Core) system within P-CSCF to detect and mitigate the DoS flooding attacks. The prototype is implemented in C/C++ and the results are validated and verified at Open IMS FOKUS Testbed. The IDP-Core performs real time and online detection and prevention processing in two modes i.e. normal and overload. In normal mode, it checks the SIP message tampering attacks like SQL-injection, and in overload, it detects and mitigates the SIP flooding attacks. To block the address of an attacker for a defined time interval, the IPtable is utilized. The IDP-Core is a stateless module. The processing delay and overhead of developed prototype is very small (in the range of 1-2 ms). This proves that IDP-Core is light weight component and does not affect the communication flow. Therefore, it could be utilized and deployed in real world IMS scenarios. After the deployment of this module, the Open IMS core is considered a secure from DoS flooding attacks. The IDP-Core design, attacks detection algorithm, implementation and performance evaluation are presented in Part-D.

In the context of IMS security extension, the next module focused on the protection of misuses of IMS applications form legitimate as well as illegitimate users. These applications could be secured with the deployment of Intrusion Detection and Prevention (IDP-AS) system. The IDP-AS prototype based on SIPSEE (SIP Servlet Execution Environment); an IMS Application Server developed by Fraunhofer FOKUS Institute. The IDP-AS is developed in Java within IMS AS. It provides stateful misuses of IMS applications and services. It processes all SIP messages that flow between S-CSCF and IMS AS to secure ISC interface. It performs real time and online processing. The attacks rules are developed in XML and loaded runtime. The IDP-AS compares both the SIP messages and state of partner against defined attacks rules. The performance evaluations showed that the total delay introduced by IDP-AS is less than 10 ms.

This Secure Service Provisioning (SSP) framework is developed for IMS research community, working for the development of secure, reliable and efficient next generation applications and services. This work is validated at Open IMS Fraunhofer NGNI Testbed which is a well-know research activity platform for multi-national research community through out the world. The academia, scientists, engineers and IT industrial community could get benefit from this research work by developing new and innovative IMS based applications like IPTV, push-to-talk, conferencing and presence etc. in a secure and protected environment.

This research work could be justified with a successful track of publications that are achieved during the development of SSP framework for IMS. From the start to the last stage of this work different security issues and ideas are raised and a step wise state of the art approach is adopted. At every step in carrying this research, the state of the art solution is presented and justified in particular article or paper in a reputed and refereed journal and/or well-known IEEE/IFIP/ACM international IT security and communication conferences. The list of publications is attached at the end of this dissertation under “Own Related Publications”.

16.2 Outlook

This section explores those issues that have not been addressed in detail within this work and/or have been raised during this work. These issues have been declared to be out of the scope of this thesis, outlining the basis for future work. The significant contribution of Secure Service Provisioning (SSP) framework was the protection of IMS from SIP flooding attacks and fraud protection of misuses of IMS applications. For that purposes, two modules – IDP-Core and IDP-AS – have been developed. In the following the future enhancements and directions are explained separately for each module.

16.2.1 IDP-Core Future Recommendations

The future recommendations for Intrusion Detection and Prevention (IDP-Core) for IMS core are the following:

- In the development process of IDP-Core, the blacklist approach is used to block the attacker for launching the SIP flooding attacks. This approach is suitable for preventing DoS attacks. The use of blacklist approach is not considered an efficient approach for the protection of distributed DoS attacks due to increase of fake and spoofed addresses list. The future enhancement of this module is to extend the blocking procedure with additional approach for efficient protection of distributed DoS and reflected distributed DoS attacks.

- The IDP-Core does not provide protection against flooding attack at normal CPU load. In normal CPU load, it only checks the SIP message flow attacks like SQL-injection. The flooding attacks prevention in normal load condition could be extended in future. But this problem is not very serious because at normal load there are no serious threats of DoS.

- At present, the flooding detection algorithm of IDP-Core based on CPU load monitoring of P-CSCF. The other flooding resources are not addressed. In future, the detection procedure could be extended to monitor flooding other IMS resources like memory, buffers and bandwidth.

- The IDP-Core has been deployed as a module of P-CSCF, but in future, it could be separated from P-CSCF and could be developed as independent and stand alone IMS component with new interface with P-CSCF.

16.2.2 IDP-AS Future Recommendations

The future recommendations and enhancements of Intrusion Detection and Prevention (IDP-AS) for IMS Application Server are the following:

- The IDP-AS compares each SIP message (from and to the Application Server) and state of the partner with attacks rules contained in Rule Collection. At present, only SQL-injection attacks are developed in the category of time-independent attacks. In future, more attacks patterns and rules could be developed to cover SIP message flow attacks and complex fraud scenarios.

- If there is any change in the definition of rule or new rule is developed, this leads to change the source code of IDP-AS. The future enhancement of IDP-AS in this context is that the system should adapt the new attacks description without modifying the source code.

- The current IDP-AS is not portable. It is developed within IMS Application Server. The final goal is to make the IDP-AS separate from the source code of AS to make it portable.

- The developed prototype only maintains and monitors communication partner's states. The relationships or dependencies among partners are not developed, therefore the IDP-AS may not be able to effectively detect the distributed DoS attacks. The future extension of IDP-AS could be the implementation of dependencies among partners for effective control of distributed DoS attacks.

The Secure Service Provisioning (SSP) framework for IMS is a first initiative and state-of-the-art solution to provide secure and protected IMS environment against SIP REGISTER and INVITE flooding attacks and fraud control. This work is an initiative for the standardization of DoS attacks protection in IP Multimedia Subsystem. This developed prototype is available as open source as a part of Open Source IMS FOKUS Testbed for IMS research community for the development of fancy and innovative next generation IMS secure applications.

Acronyms

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorisation, and Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
A-IMS	Advances in IP Multimedia Subsystem
AIN	Advanced Intelligent Network
AKA	Authentication and Key Agreement
ANSI	American National Standards Institute
AP	Authentication Proxy
APIs	Application Programming Interfaces
AS	Application Server
AuC	Authentication Centre
AUTN	Authentication Token
AV	Authentication Function
B2BUAs	Back To Back User Agents
BGCF	Border Gateway Control Function
BSF	Bootstrapping Server Function
B-TID	Bootstrapping Transaction Identifier
CA	Certification Authority
CAMEL	Customized Applications for Mobile Enhanced Logic
CAP	CAMEL Application Protocol
CBC	Cipher Block Code
CGI	Common Gateway Interface
CK	Cipher Key
COPS	Common Open Policy Service
CORBA	Common Object Request Broker Architecture
CPL	Call Programming Language
CPU	Central Processing Unit
CRLs	Certificate Revocation Lists
CS	Circuit Switched
CSCFs	Call State Control Functions

CSE	CAMEL Support Environment
DCA	Domain Certificate Authority
DDoS	Distributed Denial-of-Service Attacks
DES	Data Encryption Standard
DNS	Domain Name Server
DOM	Document Object Model
DoS	Denial of Service
DSS1	Digital Subscriber Signalling #1
EAI	Enterprise Application Integration
ESP	Encapsulating Security Payload
FMC	Fixed Mobile Convergence
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GGSN	GPRS Serving Node
GPRS	General Packet Radio System
GSM	Global System for Mobile
GUSS	GBA User Security Settings
HE	Home Environment
HLR	Home Location Register
HMAC	Hash Message Authentication Code
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP – Secure (HTTP over TLS)
ICMP	Internet Control Message Protocol
ICSCF	Interrogating Call State Control Function
I-CSCF	Interrogating Call State Control Function
ICV	Integrity Check Value
ID	Identity
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IK	Integrity Key
IKE	Internet Key Exchange
IM	Instant Messaging/IP Multimedia

IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
INAP	IN Application Protocol
IP	Internet Protocol
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISC	IP Multimedia Service Control
ISG	Integrated Security Gateway
ISIM	IP Multimedia Services Identity Module
ISIM	IM Service Identity Module
ISPs	Internet Service Providers
ISUP	ISDN User Part
IT	Information Technology
ITU-T	International Telecommunications Union
J2EE	Java 2 Enterprise Edition
JAIN	Java APIs for Integrated Networks
JCP	Java Community Process
Ks	Session Key
LAI	Location Area Identification
LCA	Local Certificate Authority
MAP	Mobile Application Protocol
MCSF	Microsoft Connected Service Framework
MD	Message Digest
ME	Mobile Equipment
MG	Media Gate
MMD	Mobile Multimedia Domain
MRF	Media Resource Function
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
NAF	Network Authentication Function
NDS/AF	Network Domain Security / Authentication Framework
NDS/IP	Network Domain Security / IP network layer security

NGN	Next Generation Network
NGNI	Next Generation Network Integration
OMA	Open Mobile Alliance
OSA	Open Service Access
OSE	Open Service Environment
P-CSCF	Proxy Call State Control Function
PDP	Packet Data Protocol
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
PoC	PPT over Cellular
POTS	Plain Old Telephony Service
PS	Packet Switched
PSK	Pre-Shared Key
PTT	Push To Talk
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RAND	Random number
RDDOS	Reflected Distributed Denial-of-Service
RES	Response
RFC	Request For Comments
RNC	Radio Network Controller
RPC	Remote Procedure Call
RTP	Real-time Transport Protocol
RTP	Real-time Transport Protocol
SA	Security Association
SAD	Security Associations Database
SBLP	Service Based Local Policy
SCPs	Service Control Points
S-CSCF	Serving Call State Control Function
SDP	Service Delivery Platform
SEG	Security Gateway
SER	SIP Express Router
SFTF	SIP Forum Test Framework

SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm
SIBs	Service Building Blocks
SIP	Session Initiation Protocol
SIP-Sec-Agree	SIP Security Agreement
SIPSEE	SIP Servlet Execution Environment
SLEE	Service Logic Execution Environment
SOAP	Simple Object Access Protocol
SOC	Security Operation Centre
SPA	Service Provider Access
SPAN	Service Provider Access Networks
SPD	Security Policy Database
SPI	Security Parameter Index
SS7	Signalling System Number 7
SSP	Secure Service Provisioning
TCP	Transmission Control Protocol
TD	Time Dependent
TI	Time Independent
TINA	Telecommunications Information Networking Architecture
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
UAC	User Agent Client
UAs	User Agents
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication Standard
URI	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
VHE	Virtual Home Environment
VLR	Visited Location Register
VoIP	Voice over Internet Protocol

WAP	Wireless Application Protocol
WIN	Wireless Intelligent Networks
WLAN	Wireless Local Area Network
WSDL	Web Service Description Language
XML	eXtensible Markup Language
XRES	Expected Response

References and Bibliography

[1] Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3GPP, TS 23.228 V6.7.0 (2004-09), "IP Multimedia Subsystems (IMS)".

[2] Third Generation Partnership Project (3GPP). www.3gpp.org/

[3] Third Generation Partnership Project 2 (3GPP2). www.3gpp2.org/

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", IETF RFC 3261 (June 2002).

[5] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", IETF RFC 3588 (Sep. 2003).

[6] Angelo Morelli, "The Role of a Service Delivery Platform in the Battle for New Communication Revenues", Outlook Point of View, March 2006.

[7] M. Poikselkae, G. Mayer, H. Khartabil, A. Niemi, "The IMS, IP Multimedia Concepts and Services in the Mobile Domain" ISBN 0-470-87133-X, John Willey & Sons Ltd. West Sussex, England, 2004.

[8] M. Sher, F. Gouveia, T. Magedanz, "IP Multimedia Subsystem (IMS) for Emerging All-IP Networks", Encyclopaedia of Internet Technologies and Applications" Pub. IGI Global, formerly Idea Group Inc. 701 East Chocolate Avenue, Suite 100, Hershey, PA 17033-1240, USA, 2007.

[9] ETSI TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) WG. http://portal.etsi.org/tispan/

[10] UMTS Forum, http://www.umts-forum.org/

[11] DSL Forum, http://www.dslforum.org/

[12] Fixed-Mobile Convergence (FMC) Alliance, http://www.thefmca.com/

[13] ETSI Mobile Competence Centre, "Overview of 3GPP Release 5, Summary of all Release 5 Features", 2003. http://www.3gpp.org/specs/releases-contents.htm#3GRelease5

[14] ETSI Mobile Competence Centre, "Overview of 3GPP Release 6, Summary of all Release 6 Features", 2006. http://www.3gpp.org/specs/releases-contents.htm#3GRelease6.

[15] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambbrinoudakis, S. Gritizalis, S. Ehlert, D. Sisalem, "Survey of Security Vulnerabilities in SIP Protocol", IEEE Communication Surveys Volume 8, No.3 ISBN 1553-877X, pp 68-81, 2006.

[16] T. Magedanz, K. Knüttel, D. Witszek: "The IMS Playground @ Fokus – an Open Testbed for Next Generation Network Multimedia Services", 1st Int. IFIP Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (Tridentcom), Trento, Italian, February 23 - 25, 2005, Proceedings pp. 2 – 11, IBSN 0-7695-2219-x, IEEE Computer Society Press, Los Alamitos, California.

[17] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RFC 3550 RTP -A Transport Protocol for Real-Time Applications", July 2003.

[18] E. Rescorla, "HTTP over TLS, IEFT RFC 2818" May 2000.

[19] J. Klensin, Ed., "Simple Mail Transfer Protocol, IETF RFC 2821", April 2001.

[20] IETF AAA Working Group, "IETF Authentication, Authorization and Accounting (AAA) Working Group", (Accessed 2007), http://ch.tudelft.nl/~arthur/aaa/links.html.

[21] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS), IETF RFC 2865, June 2000.

[22] J. Loughney - "Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5", RFC 3589, September 2003.

[23] S. Bellovin, J. Ioannidis, A. Keromytis, R. Stewart, "On the Use of Stream Control Transmission Protocol (SCTP) with IPSec", IETF, RFC 3554, July 2003.

[24] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax, IETF RFC 3986" January 2005.

[25] Third Generation Partnership Project, Technical Specification, "3GPP, TS 29.208, End-to-end Quality of Service (QoS) Signalling Flows", March 2006.

[26] Gonzalo Camarillo, Miguel A. Garcia-Martin, "The 3G IP Multimedia Subsystem (IMS) – Merging the Internet and the Cellular Worlds", 2nd Edition, John Wiley & Sons Ltd. ISBN-13: 978-0-470-01818-7, The Atrium, Southern Gate, Chichester, West Sussex, England, 2006.

[27] T. Magedanz, M. Sher, "IT-based Open Service Delivery Platforms for Mobile Networks -From CAMEL to the IP Multimedia System", chapter of "Mobile Middleware" book, ISBN: 0849338336, edited by P. Bellavista and A. Corradi published by Chapman & Hall/CRC Press, 2006.

[28] OSA/Parlay "Parlay Open Service Architecture", http://www.parlay.org/en/index.asp.

[29] Magedanz, T., Popescu-Zeletin, R., "Intelligent Networks - Basic Technology, Standards and Evolution", International Thomson Computer Press, ISBN: 1-85032-293-7, London, UK, June 1996.

[30] Open Mobile Alliance "OMA the leading industry forum for developing market driven, interoperable mobile service enablers", http://www.openmobilealliance.org/

[31] Third Generation Partnership Project, "Presence Service, Architecture and Functional Description (Release 6)", 3GPP TR 23.841, V6.0.0. (2002-07).

[32] N. Blum, T. Magedanz: "'Push-To-Video as a platform for NGN Services", 11th European Wireless 2005 - "Next Generation Wireless and Mobile Communications and Services", Nicosia, Cyprus, April 10-13, 2005.

[33] K. Knuettel, T. Magedanz, L. Xie, "SIP Servlet Execution Environment (SIPSEE) - An IMS / NGN SIP AS for Converged Applications″, ICIN07 Conference, Bordeaux, France, 2006.

[34] Thomas Magedanz, "Tutorial IEEE ISCC, IEEE Symposium on Computer and Communications", Spain, 27 June 2005.

[35] Ravi Jain, John-Luc Bakker, Farooq Anjum, "Programming Converged Networks – Call Control in Java, XML, and Parlay/OSA", ISBN 0-471-26801-1, John Wiley & Sons, Inc. 111 River Street, Hoboken, NJ 07030, USA, 2005.

[36] R. Bonica, D. Gan, D. Tappan, C. Pignataro, "Extended ICMP to Support Multi-Part Messages, IETF RFC 4884", 2007.

[37] Yu-Sung Wu, Saurabh Bagchi, Schin Garg, Navjot Singh, Tim Tsai, SCIDIVE: A

Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments, 2004.

[38] M. Zhang, Y. Fang, "Security Analysis and Enhancement of 3GPP Authentication and Key Agreement Protocol", IEEE Transactions on Wireless Communication Vol. 4, No. 2, ISBN 1536-1276, March 2005.

[39] "Low Cost Tools for Secure and Highly Available VoIP Communication Services (SNOCER)", A research project supported within the Sixth Framework Programme of the EU Commission" 2005, http://www.snocer.org.

[40] A. Niemi, J. Arkko, V. Torvinen, "HTTP Digest Authentication Using AKA", IETF RFC 3310 (2002).

[41] Chen, E.Y., "Detecting DoS attacks on SIP systems," IEEE Workshop on VoIP Management and Security, Page(s):53 – 58, April 2006.

[42] M. Sher, S. Wu, T. Magedanz, "Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS)", IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation. MonAM06 Proc. IEEE/IST, ISBN: 3-937201-02-5, ISSN: 1862-7803, Diadem Firewall Project (FP6 IST-2002-002154), pp 38-44, Tuebingen, Germany, September 28-29, 2006. http://www.diadem-firewall.org/workshop06/

[43] R. Sparks, "The Session Initiation Protocol (SIP) Referred-By Mechanism", IETF RFC 3892, September 2004.

[44] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 6); 3GPP, TS 33.102 V6 (2004).

[45] V. Gurbani, A. Jeffrey, draft-gurbani-sip-tls-use-00: The Use of Transport Layer Security (TLS) in the Session Initiation Protocol (SIP), February 2006.

[46] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, (Nov 1998).

[47] M. Sher, T. Magedanz, "Development of IMS Privacy & Security Management Framework for FOKUS Open IMS Testbed", Journal of Mobile Multimedia, Vol. 2, No.3 (2006) 225-258, ISSN: 1550-4646 © Rinton Press. http://www.rintonpress.com/journals/jmm/

[48] Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3GPP, TS 33.210, Network Domain Security (NDS); IP Network Layer Security V6.5.0 (2004-06).

[49] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 7), 3GPP TS 33.220 V7 (2005).

[50] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to Network Application Functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (Release 7), 3GPP TS 33.222 V7 (2005).

[51] Vignal Giovanni et al, A Stateful Intrusion Detection System for World-Wide Web Servers (WEBSTAT), 2003.

[52] SIPSEE (SIP Servlet Execution Environment) is the FOKUS development of a SIP Application Server (SIP AS) based on SIP Servlet Technology, 2006, http://www.fokus.fraunhofer.de/bereichsseiten/testbeds/ims_playground/components/sipsee.php

[53] Jetty, an Open Source, Standards-based, Full-featured Web Server, http://jetty.mortbay.org/jetty/index.html.

[54] Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3G Security; "Access Security for IP-based services (Release 6)", 3GPP, TS 33.203 V6.4.0 (2004-09).

[55] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", IETF RFC 4301, December 2005.

[56] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", IETF RFC 3329, January 2003.

[57] S. Kent, "IP Encapsulating Security Payload (ESP)", IETF RFC 4303, December 2005.

[58] C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", IETF RFC 2403 (1998).

[59] C. Madson, R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", IETF RFC 2404 (1998).

[60] V. Niemi, K. Nyberg, "UMTS Security" ISBN 0-470-85314-X, John Willey & Sons Ltd. West Sussex, England, 2003.

[61] R. Pereira, R. Adams, "The ESP CBC-Mode Cipher Algorithms" IETF RFC 2451, November, 1998.

[62] S. Frankel, R. Glenn, S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPSec" IETF RFC 3602, September, 2003.

[63] Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3GPP, TS 33.210, Network Domain Security (NDS); IP Network Layer Security V6.5.0 (2004-06).

[64] M. Sher, T. Magedanz, W.T. Walter, "Inter-Domains Security Management (IDSM) Model for IP Multimedia Subsystem (IMS)", IEEE 1st Int. Conference on Availability, Reliability & Security, Vienna, Austria, 20th-22nd April 2006. IEEE/ARES2006 Proceeding ISBN 978-0-7695-2567-9, pp. 502-509, April 2006.

[65] C. Kaufman, Ed. "Internet Key Exchange (IKEv2) Protocol, IETF, RFC 4306", December 2005.

[66] D. Maughan, M. Schertler, M. Schneider, J. Turner, IETF, RFC 2408, "ISAKMP: Internet Security Associations and Key Management Protocol".

[67] M. Sher, T. Magedanz, "Developing Network Domain Security (NDS) Model for IP Multimedia Subsystem (IMS)", Journal of Networks, Vol.1, No.6, November/December 2006, pp.10-17, ISSN: 1796-2056 © Academy Publisher, Oulu, Finland, 2006.

[68] Third Generation Partnership Project Technical Specification, "Network Domain Security (NDS); Authentication Framework (AF) Release 7" TS 33.310 V7.1.0 (2006-09).

[69] P. Karn, P. Metzger, W. Simpson, "The ESP Triple DES (3DES) Transform, IETF, RFC 1851", 1995.

[70] William Stallings, "Cryptography and Network Security", 4th Edition, ISBN 0131873164, Prentice Hall, 2005.

[71] R. Rivest, IETF RFC 1321, "MD5: Message Digest Algorithm", April 1992.

[72] D. Piper, IETF RFC 2407, "The Internet IP Security Domain of Interpretation for

ISAKMP" November 1998.

[73] S. Kiran, P. Lareau, S. Lloyad, "PKI Basics – A Technical Perspective", November 2002. http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf.

[74] S. Santesson, R. Housley, IETF RFC 4325, "Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension" 2005.

[75] R. Housley, W. Polk, W. Ford, D. Solo, IETF RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.

[76] Third Generation Partnership Project Technical Specification, "Generic Authentication Architecture (GAA); Early Implementation of HTTPS Connection between a Universal Integrated Circuit Card (UICC) and Network Application Function (NAF) (Release 7)", 3GPP TR 33.918 V7 (2005).

[77] Third Generation Partnership Project Technical Specification, "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (Release 7)", 3GPP TS 31.111 V7 (2005).

[78] Third Generation Partnership Project; Technical Specification, "3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification", 3GPP TS 35.206 V 6.0.0, 2004.

[79] Open Source IP Multimedia Subsystem (IMS) Core, official released in 2006. http://www.fokus.fraunhofer.de/ngni/topics/ims_core.php

[80] Open IP Multimedia Subsystem (IMS) Playground, 2003-2007, http://www.fokus.fraunhofer.de/ims/index.php?lang=en

[81] SIP Express Router (SER), 2001-2007, http://www.iptel.org/ser/

[82] Linux Overall System Resources Utilization, http://www.linuxjournal.com/

[83] Firewall Protection Using IPtables, "The Netfilter Webmaster", 1999-2007. http://www.netfilter.org/

[84] IMS Client Developed by UCT/FOKUS, 2006, http://uctimsclient.berlios.de/

[85] Open Source SIP Test Tool, http://sipp.sourceforge.net/

[86] Third Generation Partnership Project Technical Specification, "Sh Interface based on the Diameter Protocol (Release 7)", 3GPP TS 29.329 V 7.3.0. (2006-09).

[87] 3Gb National Host "Third Generation and beyond Testbed", 2003. http://www.fokus.fraunhofer.de/bereichsseiten/testbeds/national_host/testbed/testbed.php?lang=en

[88] K. Knuttel, T. Magedanz, L. Xie, "SIP Servlet Execution Environment (SIPSEE) – An IMS / NGN SIP AS for Converged Application", International Conference on Intelligence in Networks, ICIN, Bordeaux, France, 2006.

[89] Yu-Sung Wu, Saurabh Bagchi, Schin Garg, Navjot Singh, Tim Tsai, SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments, 2004.

[90] SIP Forum Test Framework (SFTF), "A Testing Software for SIP", January 2007. http://www.sipfoundry.org/sip-forum-test-framework/sip-forum-test-framework-sftf.html

[91] The 3GPP TSG SA WG3 Security, "Proposed Confidentiality for IMS" Sophia-Antipolis, France, 2003.

http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_27_Sophia_Antipolis/Docs/PDF/S3-030149.pdf

[92] The University of Southern California and VeriSign "Building a Security Framework for Delivery of Next Generation Network Services" 2005. http://www.verisign.com/static/035478.pdf

[93] Radu State, "New Frontier in VoIP Security" and "Building Management and Security Solutions of Tomorrow's Internet" Madynes Research Project, INRIA Nancy Universités Centre de Recherché Grand Est., France, 2007. http://madynes.loria.fr/

[94] The Georgia Technology Information Security Center (GTISC), "Emerging Cyber Threats Report for 2008" USA, October 2007. http://www.gtisc.gatech.edu/pdf/GTISC%20Cyber%20Threats%20Report.pdf

[95] Sipera Technical Security Report, "Protecting IMS Netwroks from Attacks: Operators Need More than Encryption and Authentication" 2007. http://www.sipera.com.

[96] Verizon and Cisco, "Advances to IP Multimedia Subsystem (A-IMS) Architecture, White Paper", June 2006. http://www.voip-magazine.com/content/view/4212/

[97] Juniper Networks, " Solution Brief – How Juniper Networks Enables Intelligent, Secure, and Open IMS-FMC Networks", September 2006, http://www.juniper.net/solutions/literature/solutionbriefs/351218.pdf

[98] Aceme Packet, "DoS/DDoS Protection for IMS Core Elements", June 2007. http://www.acmepacket.com/html/page.asp?PageID=%7B51CB22C4-7243-43D1-9847-6253984B1671%7D

[99] J. Fiedler, T. Kupka, S. Ehlert, T. Magedanz, D. Sisalem, "VoIP Defender: Highly Scalable SIP-based Security Architecture", IPComm, New York, USA, 2007. http://iptcomm.org/

[100] Fraunhofer FOKUS Open Research Communication Institute, Berlin, http://www.fokus.fraunhofer.de/home/index.php?lang=en

[101] Nokia Siemens Networks, "IMS Technical Description and Information" A50016-D3605-X20-1-7618, Id: 0900d80580129f8e, 2007.

[102] Open Source Network and IP Based Intrusion Detection System, SNORT 2005-2006**.** www.snort.org

Own Related Publications

A. Books Chapters and Encyclopedia Contribution

[1] M. Sher, T. Magedanz "IMS – A Secure Architecture for All IP Networks", *IMS Handbook: Concepts, Technologies, and Services* (Chapter 1), Editors: Syed Ahson, iDEN Mobile Devices and Emerging Standards Motorola Inc. Plantation, Florida, 33322 and Mohammad Ilyas, College of Engineering & Computer Science, Florida Atlantic University Boca Rato, Florida 33431, © Taylor & Francis CRC Press, NW, FL 33487, USA, (Accepted) 2008.

[2] M. Sher, F. C. Gouveia, T. Magedanz, "IP Multimedia Subsystem (IMS) for Emerging All-IP Networks", *Encyclopedia of Internet Technologies and Applications*, ISBN: 978-1-59140-993-9, pp 249-256, Mário Freire and Manuela Pereira (editors), IGI Global - Information Science Reference (publisher), Hershey, New York, USA, August 2007. http://www.igi-global.com/reference/details.asp?id=6925

[3] T. Magedanz, M. Sher, "IT-Based Open Service Delivery Platforms for Mobile Networks: From CAMEL to the IP Multimedia System", *The Handbook of Mobile Middleware* (chapter 37), Paolo Bellavista and Antonio Corradi (editors), Cat. # AU3833, ISBN: 0849338336, pp 1001-1037, October 2006, © Taylor & Francis CRC Press, NW, FL 33487, USA, 2006. http://www.crcpress.com/shopping_cart/products/product_detail.asp?id=&parent_id=&sku=AU3833&pc=

A. Journals Publications

[4] M. Sher, T. Magedanz, "Developing Intrusion Detection and Prevention (IDP) System for IP Multimedia Subsystem (IMS) Application Servers", *Journal of Information Assurance and Security (JIAS),* ISSN: 1554-1010, © Dynamic Publisher Inc. Atlanta, GA 30362-0654, USA (Accepted), 2008. http://www.softcomputing.net/jias/

[5] M. Sher, T. Magedanz, "A Vulnerabilities Analysis and Corresponding Middleware Security Extensions for Securing NGN Applications", *Elsevier Journal of Computer Network, Special Issue on (1) Innovation in Web Communication Infrastructure; (2) Middleware Challenges for Next Generation Networks and Services*, ISSN: 1389-1286, Volume 51, Issue 16, pp 4697-4709, Science Direct and Elsevier Publishers, 14 November 2007. http://dx.doi.org/10.1016/j.comnet.2007.06.011

[6] M. Sher, T. Magedanz, "Secure Access to IMS Services Based on Generic Bootstrapping Architecture (GBA) for Next Generation Networks", *International Engineering Consortium (IEC) Comprehensive Technical Report on "Business Models and Drivers for Next Generation IMS Services"*, ISBN: 978-1-931695-55-8, pp 249-260, Senior editor: André Sulluchuco, @ IEC, Chicago, USA, May 2007. http://www.iec.org/pubs/

[7] M. Sher, T. Magedanz: "Security Associations Management (SAM) Model for IP Multimedia System", in *IFIP International Federation for Information Processing*, Volume 229, Network Control and Engineering for QoS, Security and Mobility, IV, ed. D. Gaiti, ISSN: 1571-5736 / 1861-2288 (Internet), ISBN: 10: 0-387-49689-0, ISBN: 13: 978-0-387-49689-4, pp. 311-325, Springer-Boston, March 2007. http://www.springerlink.com/content/pm825g412684pg85/

[8] M. Sher, T. Magedanz, “Developing Network Domain Security (NDS) Model for IP Multimedia Subsystem (IMS)”, *Journal of Networks*, ISSN: 1796-2056, Vol.1, No.6, pp.10-17, © Academy Publisher, Oulu, Finland, November/December 2006. http://www.academypublisher.com/jnw/index.html

[9] M. Sher, T. Magedanz, “Development of IMS Privacy & Security Management Framework for FOKUS Open IMS Testbed”, *Journal of Mobile Multimedia, IP Multimedia Subsystem (IMS)*, Vol. 2, No.3, 225-258, ISSN: 1550-4646 © Rinton Press, Inc., New Jersey, USA, September 2006. http://www.rintonpress.com/journals/jmm/

B. International Conferences, Symposiums and Workshops Proceedings

[10] M. Sher, T. Magedanz, “SQL Injection and Password Guessing Detection and Mitigation for Next Generation IMS”, *IEEE Workshop on Monitoring, Attack Detection and Mitigation,* MonAM07 Proc. IEEE, ISBN: 978-1-4244-1842-8, ISSN: 1862-7803, pp 59-64, LAAS-CNRS, Toulouse, France, 5-6 November 2007. http://www.laas.fr/MonAM2007/

[11] M. Sher, T. Magedanz, “Mobile Multimedia Broadcasting Vulnerability Threats, Attacks and Security Solutions”, *IFIP/IEEE 9th International Conference on Mobile and Wireless Communications Networks*, MWCN07 Proc. IEEE, ISBN: 978-1-4244-1719-3, pp 56-60, Cork, Ireland, 19-21 September 2007. http://www.mwcn2007.org/

[12] M. Sher, T. Magedanz, “Protecting IP Multimedia Subsystem Service Delivery Platform from Time Independent Attacks”, *IEEE Third International Symposium on Information Assurance and Security*, IAS 2007 Proc. IEEE, ISBN: 0-7695-2876-7, pp 171-176, Manchester, United Kingdom, 29-31 August 2007. http://www.ias07.org/

[13] M. Sher, T. Magedanz, "3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Management Model”, *IEEE/International Conference on Availability, Reliability & Security* organized by Dexa Association & ENISA (European Network and Information Security). ARES 2007 Proc. IEEE, ISBN: 0-7695-2775-2, pp 198-205, Vienna, Austria, April 10-13, 2007. http://www.ares-conf.org.

[14] M. Sher, T. Magedanz, “Secure Access to IP Multimedia Services Using Generic Bootstrapping Architecture (GBA) for 3G & Beyond Mobile Networks”, *2nd ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2006)*, in conjunction with 9th ACM/IEEE International Symposium on Modeling, Analysis, Simulation of Wireless and Mobile System. Q2SWinet06 Proc. ACM, ISBN: 1-59593-486-3 pp 17-24, Torremolinos, Malaga, Spain, October 2-6, 2006. http://www.cs.unibo.it/mswim2006/

[15] M. Sher, S. Wu, T. Magedanz, “Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS)”, *IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation.* MonAM06 Proc. IEEE/IST, ISBN: 3-937201-02-5, ISSN: 1862-7803, Diadem Firewall Project (FP6 IST-2002-002154), pp 38-44, Tuebingen, Germany, September 28-29, 2006. http://www.diadem-firewall.org/workshop06/

[16] M. Sher, T. Magedanz, W.T. Walter, "Enhanced SIP Security for Air Interface (Gm) between IMS Core and Client", *IST/IEEE-Africa 2006 Conference (Information Society Technologies in Africa)* supported by the European Commission under IST Program of FP6. IST-Africa Proc. ISBN: 1-905 824-01-7, Proc. on CD, Pretoria, South Africa, 03 - 05 May 2006. http://www.ist-africa.org/Conference2006.

[17] M. Sher, T. Magedanz, W.T. Walter, "Inter-Domains Security Management (IDSM) Model for IP Multimedia Subsystem (IMS)", *IEEE/International Symposium on Frontiers in Availability, Reliability & Security (FARES 2006)* in conjunction with 1st International Conference on Availability, Reliability & Security. ARES06 Proc. IEEE,

ISBN: 978-0-7695-2567-9, pp. 502-509, Vienna, Austria, April 20-22, 2006. http://www.ares-conf.org.

[18] M. Sher, T. Magedanz: "Security Management Model for IP Multimedia System (IMS)", *IFIP TC6 International Conference on Network Control and Engineering for QoS, Security and Mobility (NetCon05)*, Working Groups WG6.2, WG6.6, WG6.7 & WG6.8 and France Telecom, Conference Proc. on CD, Lannion, France, November 14-18, 2005.

[19] M. Sher, T. Magedanz: "Network Access Security Management (NASM) Model for Next Generation Mobile Telecommunication Networks", *IFIP/IEEE 2nd Workshop on Mobility Aware Technologies and Applications - Service Delivery Platforms for Next Generation Networks.* MATA05 Proc. Springer-Verlag, Berlin Heidelberg, LNCS 3744-0263, ISSN 0302-9743, ISBN: 3-540-29410-4 (pp. 263-272), Montreal, Canada, October 17-19, 2005. http://www.congresbcu.com/mata2005

[20] F. C. Gouveia, T. Magedanz, M. Sher, “Understanding the Issues of Providing IMS Capabilities on Different Access Networks – The Use of Policies for QoS Provision”, *Proc. 9th WSEAS International Conference on Communications*, ISBN: 960-8457-29-7, WSEAS Press, July 2005.

[21] M. Sher, T. Magedanz, "Secure Service Provisioning Framework (SSPF) for Multimedia Systems and Next Generation Mobile Networks", *3rd International Workshop in Wireless Security Technologies 2005* organized by Wireless Information Technology Research Centre(WITRC). IWWST05 Proc. ISSN: 1746-904X, (pp. 101-106), London, UK April 4-5, 2005.

Annex A

Installation Guide for IDP-Core

The following instructions and guidelines are important to run the IDP-Core:

1. Check whether the DNS runs correctly. Test the DNS with command:

   “ping pcscf.open-ims.test”

   If it is not running, then check the file “/etc/bind/open-ims.dnszone”, which is the configuration file for the DNS server (bind9). How to do this?

   Use command: *“ifconfig”* to get the current IP address.

   Use the current IP address to replace the old one in the file open-ims.dnszone.

   In order to edit this file, you should require the super user privilege.

   Command: *“sudo vi open-ims.dnszone”*

2. Check the /etc/resolv.conf file

   Command: *“sudo cp resolv.conf.ims resolv.conf”*

3. Restart the DNS server

   Commands: *“sudo bind”* then *“sudo rndc reload”*

4. Now “ping pcscf.open-ims.test” should work.

5. Check the configuration file of the PCSCF (/opt/OpenIMSCore/pcscf.cfg).

   In the line for listening “listen=10.147.66.182”, this IP address must be the current IP of the system.

6. Start the open ims core with super user in the folder /opt/OpenIMSCore.

   To start the pcscf using command *“sudo ./pcscf.sh”;*

   Start the scscf *“sudo ./scscf.sh”* ;

   Start the icscf *“sudo ./icscf.sh”*.

   Change the current folder to /opt/OpenIMSCore/FHoSS/deploy,

   Run the HSS using *“./startup.sh”*

7. On the client computer, use the SIPp to simulate the flooding attack.

   The test client is under c:\temp\sipp

   a. Use a low rate to test the IDP, the command is *“sipp 10.147.66.182:4060 -r 10 -rp 10s -sf bob_register.xml”*

   b. Use a high rate to test the IDP, command is *“sipp 10.147.66.182:4060 -r 10 -rp 10 -sf bob_register.xml”*

8. To start the UCT client, change the folder /home/swu/downloads/uctimsclient1.0.3.tar.gz_FILES/src

   Use command *“sudo./uctimsclient”*.

Annex B

User Guide for IDP-AS

The following instructions are important to use IDP-AS:

1. The prerequisite to start IDP-AS, the "rules.xml" and "ids.con_g" should be under the directory "etc" of the IMS AS.

2. The IDP-AS is integrated with IMS AS. Therefore it starts automatically, when IMS AS is started.

3. Note that the IDP Centre must have the reference of the started SIPSeeServer in order to protect the IMS AS. The following main method of the SIPSeeServer shows the action.

```
public static void main(String[] arg) {

// Create Server with properties file

SIPSeeServer server = new SIPSeeServer((arg.length>0)?arg[0]:null,false);

IDSCenter.getInstance().set_server(server);

try {

// start server

server.start();

} catch (Exception e) {

LOGGER.debug("SIPSee Exception -> ", e);

}

}
```