Faculty of Economic Sciences, Communication and IT
Computer Science

Ge Zhang

Towards Secure SIP Signalling Service for VoIP applications

Performance-related Attacks and Preventions

Karlstad University Studies
2009:27

Ge Zhang

Towards Secure SIP Signalling Service for VoIP applications

Performance-related Attacks and Preventions

Karlstad University Studies
2009:27

Ge Zhang. *Towards Secure SIP Signalling Service for VoIP applications - Performance-related Attacks and Preventions*

Licentiate thesis

Karlstad University Studies 2009:27
ISSN 1403-8099
ISBN 978-91-7063-250-1

Distribution:
Faculty of Economic Sciences, Communication and IT
Computer Science
SE-651 88 Karlstad
+46 54 700 10 00

www.kau.se

Printed at: Universitetstryckeriet, Karlstad 2009

“Know your enemy, know yourself and you can
fight a hundred battles without disaster...“

“All warfare is based on deception...“

The Art of War
Sun Tzŭ

Towards Secure SIP Signalling Service for VoIP applications

Performance-related Attacks and Preventions

GE ZHANG
D*epartment of Computer Science, Karlstad University*

Abstract

Current Voice over IP (VoIP) services are regarded less secure than the traditional public switched telephone network (PSTN). This is due to the fact that VoIP services are frequently deployed in an relatively open environment, so that VoIP infrastructures can be easily accessed by potential attackers. Furthermore, current VoIP services heavily rely on other public Internet infrastructures shared with other applications. Thus, the vulnerabilities of these Internet infrastructures can affect VoIP applications as well. Nevertheless, deployed in a closed environment with independent protocols, PSTN has never faced similar risks.

The main goal of this licentiate thesis is the discussion of security issues of the Session Initiation Protocol (SIP), which serves as a signalling protocol for VoIP services. This work especially concentrates on the security risks of SIP related to performance. These risks can be exploited by attackers in two ways: either actively or passively. The throughput of a SIP proxy can be actively manipulated by attackers to reduce the availability of services. These attacks are defined as Denial of Service (DoS) attacks. On the other hand, attackers can also profile confidential information of services (e.g., the calling history) by passively observing the performance of a SIP proxy. This is defined as a timing attack. In this thesis, we carefully studied four concrete vulnerabilities existing in current SIP services, among which, three of them can lead to DoS attacks and one can be exploited by timing attacks. The results of our experiments demonstrate that these attacks can be launched easily in real applications.

Moreover, this thesis discusses different countermeasure solutions for the attacks respectively. The defending solutions have all in common that they are influencing the performance, by either enhancing the performance of the victim during a DoS attack, or abating the performance to obscure the time characteristic for a timing attack. Finally, we carefully evaluated these solutions with theoretical analyses and concrete experiments.

Keywords: Signalling attacks, Voice over IP, Session Initiation Protocol, network security, Denial of Service.

Acknowledgments

First of all, I would like to express my sincere gratitude to my supervisor, Prof. Simone Fischer-Hübner, for her advice, attention and encouragement during my research studies. I am also very grateful for the valuable research network shared by Prof. Fischer-Hübner. It is an honor to work under the direction of her.

I believe that a nice work environment makes the greater part of a research experience and for this I would like to thank my colleagues in Computer Science Department at Karlstad University. Further, special appreciation is given to all members of the Privacy and Security Group (PRISEC). They are Prof. Simone Fischer-Hübner, Prof. Stefan Lindskog, Prof. Thijs J. Holleboom, Leonardo A. Martucci, Hans Hedbom, Reine Lundin and my co-advisor, Prof. Andreas J. Kassler. Also, thanks to the C-BIC project that funded part of my research work.

I have had the good opportunities to work with several other research institutes before. My stay in Berlin at Fraunhofer FOKUS institute is a valuable experience because I started my first step of doing research work at there. My sincere thanks must go to Prof. Thomas Magedanz and Sven Ehlert for their offer and advice.

My family have been always generous with their encouragement to me despite the long geographical distance between us. My deepest appreciation goes to my parents, Jinyi Zhang and Ming Qian. I am forever indebted to them for their endless love and support. Finally, I thank with love to my dear wife, Hui Xie. Without her love and understanding, it is impossible for me to accomplish this work.

Karlstad, March 2009 Ge Zhang

List of Appended Papers

This thesis is comprised of the following four peer-reviewed papers. References to the papers will be made using the Roman numbers associated with the papers such as Paper I.

I. **Ge Zhang**, Sven Ehlert, Thomas Magedanz, and Dorgham Sisalem. Denial of service attack and prevention on SIP VoIP infrastructures using DNS flooding. In *Proceedings of the 1st international Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM 2007)*. New York, NY, USA, 24–27 July 2007. ACM Press. Part of this paper summarizes results reported in:

- Sven Ehlert, **Ge Zhang**, Dimitris Geneiatakis, Georgios Kambourakis , Tasos Dagiuklas, Jiří Markl, and Dorgham Sisalem. Two layer Denial of Service prevention on SIP VoIP infrastructures. In *Computer Communications*, Elsevier, Vol. 31, Issue 10, June 2008, Pages 2443-2456.

II. **Ge Zhang**, Simone Fischer-Hübner, and Sven Ehlert. Blocking attacks on SIP VoIP proxies caused by external processing. In *Special Issue on Secure Multimedia Services, Journal of Telecommunication Systems*, Springer, to be published in 2009.

III. Sven Ehlert, **Ge Zhang**, and Thomas Magedanz. Increasing SIP firewall performance by ruleset size limitation. In *Proceedings of the IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*. Cannes, France, 15–18 September 2008. IEEE Press.

IV. **Ge Zhang**, Simone Fischer-Hübner, Leonardo A. Martucci, and Sven Ehlert. Revealing the calling history on SIP VoIP systems by timing attacks. In *Proceedings of the 4th International Conference on Availability, Reliability and Security (ARES 2009)*. Fukuoka, Japan, 16–19 March 2009. IEEE Press.

Some of the papers have been subjected to some minor editorial changes.

Comments on my Participation

For paper I, my major contributions include the testbed configuration, solution implementation, carrying out experiments and most of the written work of this paper. Sven Ehlert, Prof. Thomas Magedanz and Dr. Dorgham Sisalem provided this research topic with original ideas, revised my written material and supervised this work.

Concerning paper II, Sven Ehlert proposed basic requirements of the VoIP firewall optimization. The detailed algorithm was a result of discussion between him and me. Further, I developed the proof-of-concept program and performed experiments to evaluate this algorithm. The first version of this paper was accomplished by me. Sven Ehlert also contributed his comments and revised this paper. This work was supervised by Prof. Magedanz as well.

The main idea in Paper III, a timing attack aiming to disclose calling history of SIP domains, stems from the discussion from Prof. Simone Fischer-Hübner, Leonardo A. Martucci and me. In addition, I am responsible for design of the testbed, implementation of the prototypes and experiments. Finally, most parts of the written material was finished by me. Prof. Fischer-Hübner, Leonardo A. Martucci and Sven Ehlert contributed comments and suggestions.

Regarding paper IV, I have contributed with ideas, implementations, experiments and most parts of the written material. Prof. Fischer-Hübner and Sven Ehlert offered their help on revising this paper.

Other Papers

Apart from the papers included in this thesis, I have also authored the following papers.

1. **Ge Zhang**, Feng Cheng, and Christoph Meinel. Towards secure mobile payment based on SIP. In *Proceedings of the 15th Annual IEEE international Conference and Workshop on the Engineering of Computer Based Systems (ECBS 2008)*. Belfast, Northern Ireland, UK, March 31 - April 04, 2008. IEEE Press.

2. **Ge Zhang**, Feng Cheng, and Christoph Meinel. SIMPA: A SIP-based mobile payment architecture. In *Proceedings of the 7th IEEE/ACIS international Conference on Computer and information Science (ICIS 2008)*. Portland, Oregon, USA, 14–16 May 2008. IEEE Press.

Contents

Introductory Summary

1 Introduction

Voice has been transmitted over a long distance using the Public Switched Telephone Network (PSTN) for more than 100 years. However, with the rapid evolution of packet-switched network technology, consumers show substantial interests in transmitting voice over IP networks (VoIP) instead of PSTN in recent years. According to a marketing investigation in 2007 [1], there is already around 50% of all global telecommunication traffic is done over IP networks, and this will increase to 75% in a few years time. Another report [2] predicts that VoIP revenues are expected to double and to reach over $6bn by 2012. Sales of VoIP equipments are forecast to grow 25% a year over the same period. People are optimistic about the prospects of VoIP applications because the benefits of using VoIP, especially, low-cost and flexibility, are difficult to be achieved in PSTN [3]. Nevertheless, with existing weaknesses (e.g., security risks), it is unlikely for current VoIP to totally replace PSTN. Therefore, improving its security for VoIP is an important task and many research projects on VoIP security have been proposed [4–8].

Securing VoIP is not an easy task, as it needs efforts in several stages. One of the essential issues in VoIP security is protecting the signalling messages being exchanged between VoIP infrastructures. Signalling does not transfer voice packets, but is designed for establishing, controlling, modifying and terminating communications. The protection of signalling includes integrity and confidentiality of signalling messages as well as availability and confidentiality of signalling services [9]. Another core issue in VoIP security is protecting multimedia communications between endpoints, which is a separate topic from signalling security. It consists confidentiality, integrity and availability of multimedia communications. *In this thesis, the scope of our research ONLY focuses on the security issues of SIP [10], a signalling protocol.*

The reasons that we are motivated to choose SIP security as our research field are represented as follows. Firstly, signalling plays a vital role in VoIP services. Threats posing in signalling services can lead to serious results (e.g., making the services unavailable [11], causing financial loss of the users [12] and disclosing the users' private information [13]). Moreover, signalling also can help to establish a secure multimedia communication (e.g., voice) by assisting in the media key exchange [9]. It means that the security of multimedia communication depends on signalling as well. Secondly, SIP, regulated by the Internet Engineering Task Force (IETF) [14], has been selected as the signalling protocol in the Internet and next generation networks. It is also employed as a standard protocol for the IP Multimedia Subsystem (IMS) [15]. Last but not least, although a lot of security solutions and mechanisms were proposed for SIP recently, whether these solutions can be adopted by SIP service providers in the real world is questionable. However at least, there are a lot of open source software-based SIP components available for both SIP services and endpoints. Therefore, it has been feasible for us to implement the test environment to evaluate our ideas and hypothesis in practice.

The objective of this thesis is to define and elaborate unexplored security risks in SIP

networks, especially under the scenarios in which attackers can either actively manipulate or passively observe the performance of SIP proxies. We are also interested in finding out how easily these risks can be exploited by attackers in the real world, and in consequence, how high the risks are for SIP users. We furthermore aim at contributing several defending solutions to eliminate or minimize the impact caused by the risks. Finally, we would like to know which solution is the most practical and efficient.

This licentiate thesis presents an introductory summary and a collection of four peer-reviewed papers in the area of security in SIP signalling service that were either authored or co-authored by the writer of this thesis. The rest of the introductory summary is organized as follows. Section 2 presents the general background of current VoIP applications and SIP signalling protocol. Section 3 presents some general security considerations for SIP services. Further, Section 4 outlines the research questions of this thesis and the research methodologies that we applied. Related work to this research is outlined in Section 5, followed by a summary of our contributions in Section 6. Section 7 summarizes the contents of the four papers included in this thesis. Finally, Section 8 concludes the introductory summary with an outlook to future work in this direction.

2 Background

The fundamental background of this thesis is represented in two parts: (1) the general concept of VoIP with its pros and cons; (2) SIP, a signalling protocol which is designed for VoIP applications.

2.1 VoIP

VoIP is an innovative technology which enables its users to make calls through the existing packet-switched networks (e.g., the Internet)[1] instead of traditional PSTN networks. The concept of VoIP is based on the factor that packets running over an IP network can deliver different kinds of multimedia contents including text, pictures, audio and video. However, different to transferring packets for text and pictures, transferring audio packets poses a high requirements on the performance of networks. Suffered from performance issues (e.g., packet loss and jitter), the Internet in early stage cannot afford the VoIP applications. That is why although the concept of using computer networks to make cheap long-distance calls has been proposed for decades [16], commercial VoIP solutions were not widely accepted by users until the recent appearance of broad-bandwidth technologies.

VoIP can be regarded as an alternative of PSTN to achieve the same function: making voice calls. Nevertheless, VoIP has its own advantages and disadvantages compared with PSTN. The advantages of VoIP can be summarized as follows:

[1] VoIP can be deployed over the Internet, but the environment of VoIP is not limited only to the Internet.

1. **Low cost:** The most distinctive advantages of VoIP is its low-cost. By allowing voice to be converted into packets and transported over existing packet-switched networks (e.g., Internet), the cost for building and operating telephony services is reduced considerably. Another reason for low-cost is due to the factor that VoIP terminals and servers can be software-based. Especially, there are a number of open source software products (e.g., kphone [17], kcall [18], X-Lite [19], SER [20], OpenSIPS [21], etc) developed for VoIP applications. Deploying these free software products on computers, instead of buying expensive PSTN equipment, saves money for both users and service providers.

2. **More features:** VoIP is based on data communication and the services are digital. Therefore it can provide more features than traditional PSTN services. For example, it is easy to integrate audio, video and email applications together on VoIP platforms. Also, presence [22], a method to convey the ability and willingness of a user to communicate, has been already implemented in most commercial VoIP protocols. More features are still under development. However, as most PSTN infrastructures are implemented for specific purposes, it is difficult to realize flexible features in PSTN services.

Still, there are several disadvantages when it comes to VoIP:

1. **Security threats:** VoIP infrastructures are deployed in an open network environment (e.g., the Internet) and sometimes, VoIP applications need support from external Internet infrastructures shared with other applications (e.g., DNS servers). Thus, it is easy for unauthorized users to access VoIP infrastructures over the Internet. Furthermore, the vulnerabilities of external Internet infrastructures can affect VoIP services as well. In comparison, within a closed network environment and independent infrastructures, the cost on intruding PSTN networks is higher than the cost on intruding VoIP networks.

2. **Quality loss:** There are many QoS issues experienced by VoIP that do not affect PSTN. Since PSTN infrastructures are independent and reserved for specific application, acceptable quality can be guaranteed for PSTN. Nevertheless, packet-switched networks (e.g., Internet) are designed for multiple purposes. Then the Internet traffic may surge from time to time. As a result, the QoS of VoIP cannot be assured, which leads to variable latencies and dropped packets occurring. As telephony services are time-sensitive, these quality problems become the most essential barrier for VoIP applications. This drawback will remain a major restraint until a successful QoS management mechanism can be available.

Current standards for VoIP protocols and services are regulated by the Internet Engineering Task Force (IETF) [14]. There are three core protocols for VoIP: Session Initiation

Protocol (SIP) [10], which is a signaling protocol aiming to establish or terminate a session between users; Session Description Protocol (SDP) [23], which is used to negotiate the types of media sessions that are going to be established; and also the Real-time Transport Protocol (RTP) [24], which is used to transmit media packets based on an established session between users. Readers please bear in mind that this thesis mostly focuses on the security and performance issues of SIP protocol, and not SDP or RTP protocols. Therefore, SIP will be generally introduced in the following section.

2.2 SIP

SIP, developed by IETF, is a text-encoded protocol based on elements from the HTTP [25] and SMTP [26] protocols. The primary function of SIP is to establish or terminate a session between two or more endpoints, but it also contains other important functions such as notification for presence and short messaging services. Similar to email users, SIP users are represented by means of Uniform Resource Identifier (URI) [27], a universal name with a pair of domain name and a user name registered for this domain, e.g., (sip:ge.zhang@kau.se). Most current SIP applications in the real world employ a client/server transaction model similar to HTTP. A SIP client generates SIP request messages and a SIP server responds by generating response messages.

Six basic SIP request types are defined in RFC 3261 [10]:

- **INVITE:** Initiate a SIP transaction to setup a session.
- **ACK:** Acknowledgement of final response to INVITE.
- **BYE:** Terminate an undergoing session.
- **CANCEL:** Cancel an unfinished SIP transaction.
- **REGISTER:** Register a user to a SIP domain.
- **OPTIONS:** Query capabilities of SIP infrastructures.

There are a lot of SIP response types, many of which are oriented from HTTP protocol. SIP response codes are divided into six classes, identified by the first digit of the code:

- **1xx:** Provisional – the request has been received but the processing is unfinished.
- **2xx:** Success – the request has been received and accepted.
- **3xx:** Redirection – the request should be delivered to another place.
- **4xx:** Client error – the request cannot be processed due to error in the request.

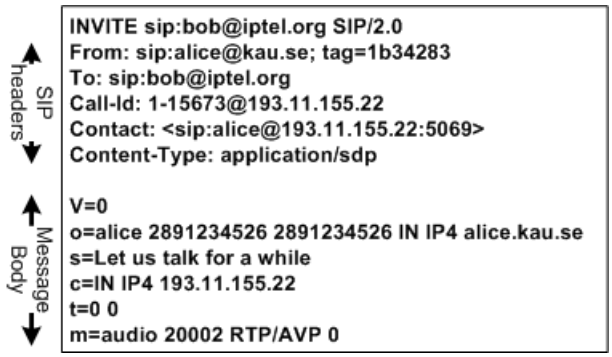

Figure 1: An example of SIP INVITE request

- **5xx:** Server error – the request cannot be processed due to server's failure.
- **6xx:** Global failure – the request cannot be processed at any server.

Both SIP requests and responses are following the message format with three elements: the *first line*, containing either a request method or a response code; *headers*, containing a list of message headers with values for SIP transaction; *message payload*, can be text-based content for different purpose (e.g., SDP payload). An example message for the SIP INVITE request is shown in Figure 2, indicating that a caller with URI "sip:alice@kau.se" wants to reach a callee "sip:bob@iptel.org". Several message headers dedicated to routing purposes are explained as follows:

- *To:* indicates the URI of the message recipient.
- *From:* indicates the URI of the message originator.
- *Via:* indicates a list of all intermediate SIP hosts that this message has passed. Any host that forwards the message adds its own address to the *Via* field. It is used for routing purpose.
- *Contact:* indicates one or more SIP URIs of the originator by which the recipient can contact with the originator directly. They can be different from the one in the *From* header.

Regarding the architecture, various network elements compose a SIP network, such as User Agents (UA), SIP servers and location servers.

- **SIP UA:** UA can be any device (e.g., computer, smart phone, etc) which connects to network to generate and receive SIP requests or responses.

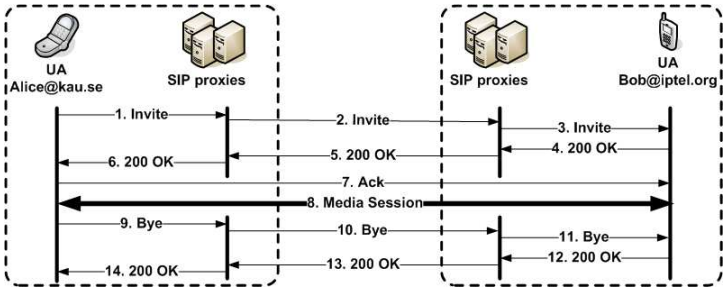

Figure 2: A general overview of SIP components and the working procedure

- **SIP servers:** There are three kinds of SIP servers including a SIP proxy, a redirect server and a register server. A SIP proxy forwards SIP requests and responses to UA or other servers. A redirect server receives a request and makes a redirection response message (3xx), indicating that this message should be delivered to another location. A registrar server receives REGISTER requests from SIP users and updates the users' location information to location servers.

- **Location servers:** The location server is a database storing the users' URIs linked with their uptodate IP addresses, presence, and other related information. The information is constantly updated or required by SIP servers using non-SIP protocol.

The procedure of SIP-based telephony calling setup is shown in Figure 1. There are two SIP users located in different domains in this scenario: Alice, a caller, is located in the domain kau.se and Bob, a callee, is located in iptel.org. Initially, Alice sends an INVITE request to one of the local proxies. This INVITE request indicates that she wants to talk with Bob at iptel.org. Then, the local proxy forwards this INVITE request to the remote proxy at iptel.org. The request is finally delivered to the UA of Bob. If Bob wants to accept the call, his UA will reply with a 200 OK response back through the proxies. After Alice has sent an ACK message to confirm the request, the signaling handshaking is accomplished. Thus, Alice and Bob will build a peer-to-peer media session in which they can talk with each other by means of exchanging voice packets. When Alice wants to tear down the conversation, her UA will send a BYE request to Bob, and Bob's UA will reply with a 200 OK response. Then the call is terminated.

3 Security requirements and mechanisms on SIP services

Compared with the SS7 signalling protocol [28] used in PSTN network, SIP is applied in an open and insecure environment. Therefore, additional security enhancements for SIP

are necessary. This section introduces basic security requirements and threats to SIP with its security mechanisms.

3.1 Security requirements on SIP

The security requirements on SIP services are examined according to basic security components (confidentiality, integrity, availability) defined in [29].

- **Confidentiality:** "Confidentiality is the concealment of information or resources [29]". Confidentiality should be taken into account for both SIP messages and SIP services. When it comes to SIP messages, it requires that not only the SIP message payload (e.g., SDP content), but also related information in message headers (e.g., To and From headers) should be kept as a secret from unauthorized network intermediaries. Further, SIP service providers often wish to conceal their network configurations as well as stored information about users (e.g., calling history).

- **Integrity:** "Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized changes [29]". There are two kinds of integrity: *data integrity* and *origin integrity*. Regarding SIP services, data integrity means that the content of SIP messages should not be modified by unauthorized intermediaries. Origin integrity means that the source of SIP messages should not be spoofed to be another one.

- **Availability:** "Availability refers to the ability to use the information or resource as desired [29]". Considering the cost on infrastructures, it is unlikely for a SIP service provider to offer services with unlimited capacity. Similar to other online applications, SIP service providers deploy SIP servers by assuming a statistic model for the perspective usage. However, sophisticated attackers may manipulate their use to break the assumed statistic model on purpose. In this way, legal users may be unable to access the service which they should get. Availability aims at preventing that the statistical model is broken.

3.2 Classic attacks on SIP

Classic attacks on SIP can be summarized as follows.

- **Eavesdropping:** Eavesdropping is a passive attack launched by network intermediaries to disclose the communication content of other users. It can be easily realized by using some packet capture tools (e.g., wireshark [30]). An attacker may eavesdrop signalling traffic for multiple purposes (e.g., getting credential of users).

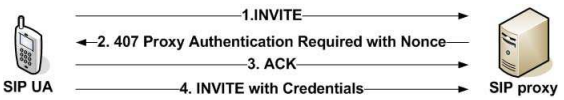

Figure 3: The HTTP Digest authentication adapted in SIP

- **Replay:** A replay attack refers to capturing one or more SIP messages and re-sending them again after a period of time. In consequence, it may enable unauthorized users to access SIP services by using identities or credentials of other users. A replay attack can also lead to financial loss of legal users, so called billing attack [12].

- **Message tampering:** Message tampering indicates that an unauthorized intermediary alters relayed SIP messages during transmission. For example, given that Alice sends an INVITE request to call Bob, an intermediary can alter the first line and *To* header in the request to make Alice talk with another person instead of Bob.

- **Identity spoofing:** Spammers and attackers frequently use faked SIP identities in order to be untraceable. However, it is unlikely to deploy a global centralized accounting database for all SIP users from different domains. Thus, it is difficult for the callee's domain to authenticate the originator of a SIP message in an inter-domain context since the callee's domain may do not have the account information of the originator. In this way, spammers and attackers can easily send SIP messages with spoofed identities.

- **Denial of Service:** Denial of Service (DoS) aims at preventing legal users to access SIP services or at making the services temporarily unavailable. An attacker can mount DoS attacks on SIP services by depleting resources (e.g., CPU, memory and bandwidth) of corresponding SIP proxies [11]. As VoIP is time-sensitive, SIP services can be suffer more from DoS than other non-realtime services (e.g., email).

3.3 Security mechanisms in SIP-related RFC

In RFC 3261 [10], RFC 3329 [31] and RFC 4474 [32], several security mechanisms are recommended to secure SIP services. These security mechanisms are summarized as follows:

- **HTTP Digest authentication:** HTTP Digest [33], a stateless, challenge-based mechanism, provides source authentication and anti-replay protection. It can be used for both proxy-to-user authentication and user-to-user authentication. An example of this mechanism is illustrated in Figure 3. The user first sends a INVITE request to a proxy. Then, the proxy responses with a "407" message containing a unique

nonce (a random number). The user receives this message and generates a hash digest for the combination of the nonce and owned password. Thus, the user sends the INVITE request again including the generated hash digest. Since the secret knowledge (the nonce and user's password) is shared with the proxy, the hash digest can be re-generated by the proxy to authenticate the source of this request. It is difficult for an eavesdropper to capture the plain text of a password since only a hash digest is transmitted over the network. Furthermore, by hashing a password with a nonce, replay attack can be efficiently prevented.

- **S/MIME:** Both message integrity and confidentiality can be ensured by carrying S/MIME [34] bodies. A signature for part of the message will be generated and attached in order to ensure that the content is not modified during the transmission. Moreover, the message payload and some headers can be encrypted to protect against eavesdropping attacks. However, the integrity of some header fields, which are allowed to be modified by intermediaries (e.g., *Via*), cannot be protected by the signature. Similarly, the fields of some message headers for routing purpose (e.g., *To*, *Via*) must be keeping in plain text during transmission.

- **TLS:** Transport Layer Security (TLS) [35], working at the transportation layer, provides source authentication, message authentication and message confidentiality, based on a Public Key Infrastructure (PKI). There are three phrases to build a TLS connection between two end-points: First, two end-points negotiate for supported cryptographic algorithms. Second, two end-points exchange a symmetric key and authenticate each other. Finally, they communicate with each other using the symmetric key for encrypting messages.

- **IPSec:** IPSec [36] stands for IP Security, which is designed by IETF to provide security at the network layer using a collections of techniques (authentication header (AH), encryption security protocol (ESP) and internet key exchange (IKE)). AH provides cryptographic authentication to IP packets, while ESP offers security services including both authentication and confidentiality. IKE is employed for session key management. However, IPsec can only authenticate machines instead of SIP users.

- **Inter-domain authentication:** To prevent identity fraud problems, an inter-domain authentication has been proposed in RFC 4474 [32]. Its purpose is to authenticate the originator of an inter-domain SIP message. The method is shown in Figure 7. For each outgoing message to other domains, the SIP proxy in the caller's domain generates a hash digest for this message. The digest is signed by the caller's proxy with its private key. The generated signature is encoded in a new header field *Identity* added to the original SIP message. Furthermore, the SIP proxy attaches another new header field *Identity-info*, which contains the Uniform Resource Locator (URL) [37] where the certificate can be fetched from. Then, this SIP request is forwarded to the callee's domain. It is regulated that each certificate must be provided by its domain itself. That is, in a SIP message, the URL indicated in the *Identity-info* field and the

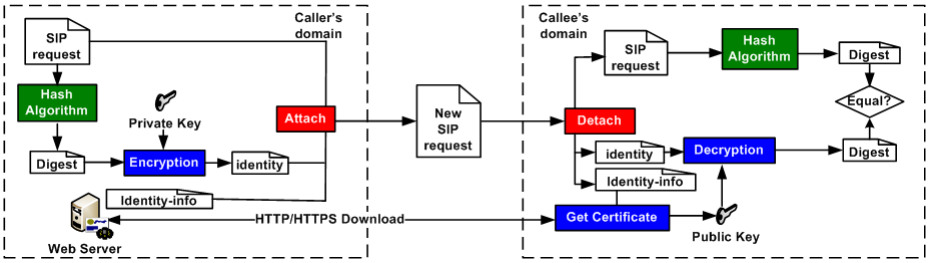

Figure 4: The mechanism of inter-domain authentication for message source

originator domain indicated in the *From* field should be matched. For each incoming message from other domains, the SIP proxy in the callee's domain first downloads the certificate according to the URL given in the *Identity-info* field. The public key extracted from the certificate is used to decrypt the signature contained in the *Identity* field. Then, a hash digest will be recomputed for the request. The result is used to be compared to the newly generated hash digest. The proxy will continue to process the message only if the two values are equal. This mechanism is recommended to be deployed in future SIP services to prevent SPAM [38].

4 Research Issues

In this section, three underlying research questions of this thesis are outlined. Corresponding methodologies applied to address these questions are listed as well.

4.1 Research questions

- **Question 1:** *How can a potential attacker launch DoS attacks to actively decrease the performance of a SIP proxy by exploiting the vulnerabilities of VoIP deployment?*

  This question is discussed in Paper I, II and III. These papers demonstrate three different methods which enable attackers to decrease the performance of a SIP proxy. These attacks have been explored both in theory and practice. The papers also address the serious consequences to which the vulnerabilities can lead.

- **Question 2:** *How can an attacker passively observe the performance of a SIP proxy by a timing attack to profile confidential information of services (e.g., calling history)?*

  This question is investigated in Paper IV, which introduces an attacking method to profile the calling history between two domains. This attacking method is a kind of

timing attacks in which attackers retrieve confidential information by observing and comparing the Round Trip Time (RTT) of their requests. The method in detail is discussed in Paper IV.

- **Question 3:** *How can the consequences caused by these threats be minimized or prevented in practice?*

  In this thesis, our goal is to help SIP service providers to offer SIP services in a more secure way. Therefore, it is necessary to provide practical solutions to eliminate the threats proposed in Question 1 and 2. To realize this goal, we design, discuss and evaluate solutions for each vulnerability in Paper I, II, III and IV respectively.

4.2 Research methodology

The research conducted in this thesis follows the steps as suggested in [39]: *ideas development*, *quantitative experiments* and *data analysis*. And these steps are performed twice in each paper, once for evaluating the feasibility of the attacking methods and once for exploring effective countermeasure solutions. Below, we describe the research methodologies in detail to address the questions above.

First research question: We investigated three unexplored vulnerabilities, which enable an attacker to manipulate the performance of a SIP proxy, to answer the first question. The three attacking methods are demonstrated in Paper I, II and III respectively. Firstly, we reviewed literatures including SIP specifications and other related papers (*literature review*). After discussion, we found several vulnerabilities that may enable an attacker to control the performance of a SIP proxy (*hypothesis formulation*). To validate our hypothesis, we adopted different designs to collect data. In paper I, we implemented an attacking tool with a testbed and performed experiments. The experiments are designed to compare the performance of a victim SIP proxy when it is under attack and without attack. We built the testbed for the experiments. The core of the testbed, a victim SIP proxy, is a real implementation connecting to the Internet. This method is defined in [40] as a *measurement* [1]. Finally, we analyzed the measurement results and demonstrated the correlation between attacking and performance reducing (*data analysis*). In Paper II, we also followed the same research process in Paper I. In addition, we also employed *inductive approach* to propose a formalized model from two concrete attacking methods. According to [40], this method is defined as *analytical modeling*. We adopted both of them because using both *measurement* and *analytical modeling* is helpful to enhance the validation of results [40]. The vulnerability addressed in Paper III was found from the real SIP service running, then we collected the data measured from the SIP service providers directly.

Second research question: In Paper IV, we firstly reviewed literatures including RFC 4474 [32] and papers about the timing attack [41, 42] (*literature review*). Then, we found

[1] According to [40], there are mainly three evaluation techniques: Analytical modeling, simulation and measurement.

out a vulnerability which can be used to mount the timing attack in SIP environment as well (*hypothesis formulation*). We proposed a mathematical model describing this attack (*analytical modeling*). Furthermore, we built a testbed in the laboratory environment and performed a *measurement* to collect data. Finally, we analyzed the measurement results and made a conclusion (*data analysis*).

Third research question: We applied *evaluation research method* [39] for this question. Firstly, we enumerated possible defending solutions for the aforementioned threats. Secondly, we analyzed advantages and disadvantages of each solution theoretically. Then, we eliminated the solutions which were obviously inefficient or might cause further problems. Thirdly, the prototypes of the remaining solutions were developed and we deployed these solutions in the test environments. With these solution prototypes, we did *measurements* in Paper I, II and IV to evaluate their effectiveness. However, due to some constrains (e.g., to simulate attackers using different IP addresses), we only applied *analytical modeling* in Paper III to evaluate the solution at this moment. Finally, we compared these solutions based on the evaluation results.

For legal and ethical considerations, we built our own SIP services as the attacking target instead of attacking the ones in the real world during all the experiments. Therefore, the damage and effect caused by attacks could be confined only in our laboratory environment. However, the SIP services built by us are based on the real implementations. In this way, our tests still have a high accuracy.

5 Related work

There are many issues which can affect the performance of a SIP network. Nahum et al. [43] published their measurements on the throughput of a SIP proxy under different configurations (e.g., stateful or stateless, using TCP or UDP, with or without authentication). The result demonstrates that the throughput can be reduced more than 94% from the best case (stateless, using UDP, without authentication) to the worst case (stateful, using TCP, with authentication). Their result also shows that the request time increases with the raising of the calling rate on a SIP proxy. Kuthan [44] and Cortes et al. [45] investigated the performance of SIP proxies by introducing more variables. Kuthan proposed that identities parsing, memory management and thread contention are main factors impacting SIP proxy performance. Cortes et al. found that string handing and synchronous DNS requests also impact the performance of SIP proxies. Some research works have been done aiming to evaluate the performance impact of deploying security mechanism on SIP networks. Rebahi et al. [46] did a performance analysis of inter-domain authentication mechanism in SIP. They argued that RSA, the default cryptographic algorithm recommended in RFC 4474, brings too much overload to SIP proxies. Instead, their testing result shows that using Elliptic Curve algorithm can achieve a better performance. Similarly, Ranganathan et al. [47] investigated the performance overhead of deploying IPSec in SIP networks based

on simulation. They found that the most predominant effect on VoIP network performance is caused by the dynamic public key exchanging. Furthermore, Salsano et al. [48] explored the performance overhead by introducing HTTP digest authentication and TLS in SIP services (The performance can be decreased by around 30% by introducing authentication and TLS). In summary, their measure results revealed that the performance of a SIP proxy can be reduced considerably depending on different security parameters. However, their works are focused on performance only, and not on security. For instance, their work did not represent how a potential attacker can take advantage of the parameters to launch DoS attacks on SIP servers. Differently, our work aims to find the correlation between performance and security of SIP services. Furthermore, our work demonstrates how an attacker can exploit the performance overhead on SIP proxies to mount attacks in detail.

Some research work of investigating DoS attacks on SIP VoIP are summarized in this paragraph. Sisalem et al. [11] investigated the issues of DoS attacks targeting SIP infrastructures. They developed a taxonomy of attacks by different exploitable resources, including CPU, memory and bandwidth, to reduce the performance of a victim SIP proxy. A stateful SIP proxy has to consume memory resources to keep the transaction states of unfinished SIP transactions. Therefore, stateful SIP proxies are especially vulnerable to INVITE flooding attack, in which an attacker floods SIP proxies with only INVITE messages to create a large number of broken transactions. Sengar et al. [49] proposed a machine learning method to distinguish legal against INVITE flooding attacks. Based on this method, they firstly characterized legal SIP traffic behavior by summarizing the normalize frequency of INVITE, 200 OK, ACK and BYE messages. Based on this benchmark, they can later detect the attacks by the abnormal frequency of the messages. Moreover, [50–52] proposed specification-based detection methods using SIP state machine models to counter INVITE flooding attacks. Conner et al. [53] proposed a ringing-based DoS attack to consume memory resources of stateful SIP proxies. Different to INVITE flooding, this attack exploits the potential long time 180 Ringing state. They also designed an algorithm to optimize the system. Our work is similar to theirs. However, we investigated the different DoS attacks on SIP proxies. We focus on the threats to SIP proxies caused by external infrastructures (e.g., DNS server, HTTP server, and firewall). Moreover, we proposed our countermeasure solutions that aim at enhancing the performance of a SIP proxy, and not at detecting the attacker. It means that our solutions are based on *prevention*, instead of *detection*. One of the benefits of *prevention* is that *prevention* can minimize the attacking impacts during the attacks. Therefore, the damage caused by attacks has been eliminated from the beginning, whereas, in most cases, *detection* works only after the damage actually happens. It is too late as the damage already occurs.

To the best of our knowledge, the previous work on VoIP timing attacks, which enable attackers to disclose confidential information by observing the performance of services, is only proposed by Wang [54] and Chen [55] so far. Their papers proposed a method to reveal the identity of two parties of a specified communication. The attacker actively adds timing characteristics into a VoIP flow by altering the time intervals between voice

packets and observing the characteristics on the other side of the communication. In this way, the attacker can profile who has called whom. In contrast, the timing attack proposed in our paper is much easier to be realized. There is no need for an attacker to manipulate the timing characteristic of voice packets. Instead, the attackers can just simply send SIP signalling requests and observe the response time of them. Moreover, we also addressed a countermeasure solution to eliminate the timing characteristic based on response delaying.

6 Contributions

As VoIP is an emerging Internet application, security evaluation and enhancement of VoIP are necessary before it should be widely deployed in the real world. In contrast to previous work, we investigated some security risks related to the performance of SIP VoIP which have not been studied before. Furthermore, we found that the performance issues affect not only the availability, but also the confidentiality of SIP services. We also proposed novel countermeasure solutions. Below follows a summary of the main contributions of this thesis:

- We have investigated several threats in which an attacker can arbitrary affect the performance of a SIP proxy. Firstly, a sophisticated attacker can take advantage of the communication latency between a SIP proxy and other external infrastructures (e.g., DNS servers, Web servers) to decrease the throughput of the proxy (in Paper I and II). We named this type of attacks as blocking attacks and a formalized model of such blocking attacks was given in our work (in Paper II). Secondly, firewalls, which are generally deployed in front of SIP proxies, also have the possibility to be exploited to decrease the performance of SIP services (in Paper III). These threats on SIP have not been studied before.

- We have identified and analyzed a timing attack aiming at extracting the calling history between domains. An attacker can send to a victim proxy spoofed SIP requests and observe the Round Trip Time (RTT) between the request and its response. With caches widely deployed, the RTTs for recently contacted domain should be relatively lower. Thus, the calling history of a domain can be profiled by a comparison of RTTs. We named this a SIP timing attack in Paper IV, which has not been studied before.

- We proposed and discussed different countermeasure solutions for each vulnerability in Paper I, II, III and IV. To efficiently minimize the impact of attacks, our solutions are mostly based on *prevention*, instead of *detection*. The defending solutions prevent the threats by influencing the performance of a victim SIP proxy, either by enhancing the performance of the proxy during a DoS attack, or by abating the performance to obscure the time characteristic for a timing attack. The solutions are first compared with each other in a theoretical way. We also implemented prototypes of each solution and evaluated them in the testbeds.

7 Summary of Papers

This section contains short summaries of the papers included in this thesis.

Paper I – Denial of service attack and prevention on SIP VoIP infrastructures using DNS flooding

A simple yet effective DoS attack on SIP servers is to flood the server with requests including hard-to-resolve domain names. In this paper, we evaluate different possibilities to mitigate these effects and show that over-provisioning is not sufficient to handle such attacks. As a more effective approach we present a solution called unblocking cache. Based on various measurements conducted over the Internet we investigate the efficiency of the unblocking cache and compare its performance with different cache replacement policies applied.

Paper II – Blocking attacks on SIP VoIP proxies caused by external processing

As VoIP applications become increasingly popular, they are more and more facing security challenges that have not been present in the traditional PSTN. One of the reasons is that VoIP applications rely heavily on external Internet-based infrastructures (e.g., DNS server, web server), so that vulnerabilities of these external infrastructures have an impact on the security of VoIP systems as well. This article presents a Denial of Service (DoS) attack on VoIP systems by exploiting long response times of external infrastructures. This attack can lead the whole VoIP system in a blocked state thus reducing the availability of its provided signalling services. The results of our experiments prove the feasibility of blocking attacks. Finally, we also discuss several defending methods and present an improved protection mechanism against blocking attacks.

Paper III – Increasing SIP firewall performance by ruleset size limitation

To protect SIP communication networks from attacks, especially flooding attacks like DoS or message spam, Intrusion Detection Systems (IDS) are deployed at the ingress point of the network to filter potential malicious traffic. A key issue of IDS performance is the operation of its firewall to block malicious user requests. Depending on the complexity of the firewall ruleset, filtering performance of the IDS can decrease considerably during high-load flooding situations. In this paper we propose a scheme to increase IDS firewall performance by merging several similar rules into more general ones and ignoring lesser relevant rules to limit the number of firewall rules. We formalize a mathematical model to

compute new firewall rules and show exemplary with traffic from SIP VoIP communication networks how the calculation can be performed. If applied to a VoIP IDS, the scheme can increase firewall throughput considerably, while retaining most of its effectiveness.

Paper IV – Revealing the calling history of SIP VoIP systems by timing attacks

To provide high-level security assurance to SIP VoIP services, an inter-domain authentication mechanism is defined in RFC 4474. However, this mechanism introduces another vulnerability: a timing attack which can be used for effectively revealing the calling history of a group of VoIP users. The idea here is to exploit the certificate cache mechanisms supported by SIP VoIP infrastructures, in which the certificate from a caller's domain will be cached by the callee's proxy to accelerate subsequent requests. Therefore, SIP processing time varies depending whether the two domains had been into contact beforehand or not. The attacker can thus profile the calling history of a SIP domain by sending probing requests and observing the time required for processing. The result of our experiments demonstrates that this attack can be easily launched. We also discuss countermeasures to prevent such attacks.

8 Conclusions and Outlook

In this thesis, we have elaborated some security risks for SIP services, particularly, raised by the performance of SIP proxies. Some of the main conclusions of this thesis are:

- *Achieving security in VoIP is much more difficult than in traditional PSTN.* VoIP infrastructures are deployed in a relatively open environment (e.g., the Internet). It is easy for potential attackers to access these infrastructures for launching attacks. In contrast, PSTN, a closed network using independent communication protocols, requires more cost for attackers to access. Moreover, since VoIP services heavily rely on assistance from external servers (e.g., DNS server, web server), the communication between VoIP servers and these external servers can be exploited to impact the confidentiality and availability of VoIP users. Such risks have never been reported in PSTN since it does not employs shared infrastructures.

- *Cache-based solution for VoIP is a two-edged weapon.* It is obvious that caching external information (DNS mapping, certificates) is helpful to enhance the performance of SIP services. In this way, solutions based on cache are designed to defend against Denial of Service attacks. Unfortunately, however, the performance unbalance caused by using caches can also be exploited by potential attackers to launch timing attacks to impact the confidentiality of services.

- *Security products for VoIP should be designed taking efficiency into account.* In contrast to other services (e.g., email, web), VoIP is time-sensitive. Therefore, complicated and time consuming security mechanisms are not suitable to apply for VoIP. If a designer fails to consider efficiency, attackers can easily manipulate the performance of SIP services to lauch a Denial of Service attack.

We have contributed with several countermeasures for the threats that had been explored. One of our future work will be the integration of these separated solutions into a single product. The challenge is that some solutions may conflict with others. For example, a SIP proxy equipped with a cache can achieve a better performance, but the cache may leak secret information. The problem of how to handle this paradox should be solved before integrating these solutions. Moreover, the solutions we investigated in this thesis are performance related, that is, the solutions for defending against attacks either by enhancing the performance of SIP proxies (for Denial of Service attack), or by reducing the performance of SIP proxies (for timing attack). These performance related solutions are however not capable to trace back the attackers. In the future work, we will also explore other defending alternatives, which enable SIP service providers to trace back the attacking source based on previous research in Intrusion Detection System (IDS).

References

[1] 2007 Global NGN IP VoIP - Analyses Statistics and Forecasts. http://www.marketresearch.com/product/display.asp?productid=1513239&g=1, visited at 16th-Feb-2009.

[2] IP phone revenues forecast to reach $6bn by 2012. http://www.voip-news.co.uk/2008/01/29/ip-phone-revenues-forecast-to-reach-6bn-by-2012/, visited at 16th-Feb-2009.

[3] U. Varshney, A. Snow, M. McGivern, and C. Howard. Voice over IP. *Commun. ACM*, 45(1):89–96, 2002.

[4] D. Butcher, X. Li, and J. Guo. Security challenge and defense in VoIP infrastructures. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 37(6):1152–1162, 2007.

[5] T.J. Walsh and D.R. Kuhn. Challenges in securing Voice over IP. *Security & Privacy, IEEE*, 3(3):44–49, 2005.

[6] S. M. Bellovin, M. Blaze, and S. Landau. The real national-security needs for VoIP. *Commun. ACM*, 48(11):120, 2005.

[7] D. C. Sicker and T. Lookabaugh. VoIP security: Not an afterthought. *Queue*, 2(6):56–64, 2004.

[8] E. A. Blake. Network security: VoIP security on data network–a guide. In *InfoSecCD '07: Proceedings of the 4th annual conference on Information security curriculum development*, pages 1–7, New York, NY, USA, 2007. ACM.

[9] H. Sinnreich. *Internet communications using SIP*. Wiley, 2006.

[10] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol, 2002. RFC 3261.

[11] D. Sisalem, J. Kuthan, and S. Ehlert. Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms. *IEEE Network*, 20(5):26–31, 2006.

[12] R. Zhang, X. Wang, X. Yang, and X. Jiang. Billing attacks on SIP-based VoIP systems. In *WOOT '07: Proceedings of the first USENIX workshop on Offensive Technologies*, pages 1–8, Berkeley, CA, USA, 2007. USENIX Association.

[13] C. Shen and H. Schulzrinne. A VoIP privacy mechanism and its application in VoIP peering for voice service provider topology and identity hiding. *ArXiv e-prints*, July 2008.

[14] IETF. http://www.ietf.org/, visited at 16th-Feb-2009.

[15] G. Camarillo and M.A. García-Martín. *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the cellular worlds eBook*. John Wiley & Sons, 2004.

[16] W. Remmele. Voice over IP: Potential - status - trends. In *Interaktion im Web - Innovative Kommunikationsformen, Fachtagung und Kongreßdes German Chapter of the ACM, der Gesellschaft für Informatik (GI) sowie Fachbereich Mathematik und Informatik der Philipps-Universität Marburg/Lahn am*, pages 215–220. Teubner, 1988.

[17] Kphone. http://sourceforge.net/projects/kphone, visited at 16th-Feb-2009.

[18] Kcall. http://www.basyskom.de/index.pl/kcall, visited at 16th-Feb-2009.

[19] X-Lite. http://www.counterpath.net/x-lite.html, visited at 16th-Feb-2009.

[20] SIP Express Router. http://www.iptel.org, visited at 16th-Sep-2008.

[21] OpenSIPS. http://www.opensips.org/, visited at 16th-Feb-2009.

[22] J. Rosenberg. A presence event package for the Session Initiation Protocol (SIP), 2004. RFC 3856.

[23] M. Handley and V. Jacobson. SDP: Session Description Protocol, 1998. RFC 2327.

[24] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A transport protocol for real-time applications, 2003. RFC 3550.

[25] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1, 1999. RFC 2616.

[26] J. B. Postel. Simple Mail Transfer Protocol (SMTP), 1982. RFC 821.

[27] T. Berners-Lee, R. Fielding, and L. Masinter. Uniform Resource Identifier (URI): Generic syntax, 2005. RFC 3986.

[28] D. Lee and J. Hewitt. *Signalling System No. 7 (SS7/C7): Protocol, architecture, and services*. Cisco Press, 2004.

[29] M. Bishop. *Introduction to computer security*. Addison-Wesley, 2005.

[30] Wireshark. http://www.wireshark.org/, visited at 16th-Feb-2009.

[31] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, and T. Haukka. Security mechanism agreement for the Session Initiation Protocol (SIP), 2003. RFC 3329.

[32] J. Peterson and C. Jennings. Enhancements for authenticated identity management in the Session Initiation Protocol (SIP), 2006. RFC 4474.

[33] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart. HTTP authentication: Basic and digest access authentication, 1999. RFC 2616.

[34] B. Ramsdell. Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3.1 message specification, 2004. RFC 3851.

[35] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) protocol version 1.2, 2008. RFC 5246.

[36] S. Kent and R. Atkinson. Security architecture for the Internet Protocol, 1998. RFC 1825.

[37] T. Berners-Lee, L. Masinter, and M. McCahill. Uniform Resource Locators (URL), 1994. RFC 1738.

[38] J. Rosenberg and C. Jennings. The Session Initiation Protocol (SIP) and Spam, 2008. RFC 5039.

[39] C. Robson. *Real world research*. Blackwell Publishing, 2002.

[40] R. Jain. *The art of computer systems performance analysis: Techniques for experimental design, measurement, simulation, and modeling*. Wiley- Interscience, 1991.

[41] A. Bortz and D. Boneh. Exposing private information by timing web applications. In *WWW '07: Proceedings of the 16th international conference on World Wide Web*, pages 621–628, New York, NY, USA, 2007. ACM.

[42] E. W. Felten and M. A. Schneider. Timing attacks on web privacy. In *CCS '00: Proceedings of the 7th ACM conference on Computer and communications security*, pages 25–32, New York, NY, USA, 2000. ACM.

[43] E.M. Nahum, J. Tracey, and C.P. Wright. Evaluating SIP server performance. In *SIGMETRICS '07: Proceedings of the 2007 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, pages 349–350, New York, NY, USA, 2007. ACM.

[44] J. Kuthan. Accelerating SIP, http://phoenix.labri.fr/documentation/sip/Documentation/Papers/SIP/Presentation/kuthan-Server.pdf, visited at 16th-Sep-2008.

[45] M. Cortes, J. R. Ensor, and J. O. Esteban. On SIP performance. *Bell Labs Technical Journal, Special Issue: Session Initiation Protocol*, 9(3):155–172, 2004.

[46] Y. Rebahi, J.J. Pallares, T. M. Nguyen, S. Ehlert, G. Kovacs, and D. Sisalem. Performance analysis of identity management in the Session Initiation Protocol (SIP). In *IEEE/ACS International Conference on Computer Systems and Applications*, pages 711–717. IEEE, 2008.

[47] M. K. Ranganathan and L. Kilmartin. Performance analysis of secure session initiation protocol based VoIP networks . *Computer Communications*, 26(6), 2003.

[48] S. Salsano, L. Veltri, and D. Papalilo. SIP security issues: The SIP authentication procedure and its processing load. *IEEE Network*, 16:38–44, 2002.

[49] H. Sengar, D. Wijesekera, H. Wang, and S. Jajodia. Fast detection of denial of service attacks on IP telephone. In *14th IEEE International Workshop on Quality of Service*, New Haven, USA, June 2006. IEEE.

[50] E. Y. Chen. Detecting DoS attacks on SIP system. In *1st IEEE Workshop on VoIP Management and Security*, Vancouver, Canada, April 2006. IEEE.

[51] H. Sengar, D. Wijesekera, H. Wang, and S. Jajodia. VoIP intrusion detection through Interacting protocol state machines. In *DSN '06: the International Conference on Dependable Systems and Networks*, pages 393–402, Washington, USA, June 2006. IEEE Computer Society.

[52] S. Ehlert, C. Wang, T. Magedanz, and D. Sisalem. Specification-based denial-of-service detection for SIP Voice-over-IP networks. In *3rd International Conference on Internet Monitoring and Protection*, Bucharest, Hungary, July 2008. IEEE.

[53] W. Conner and K. Nahrstedt. Protecting SIP proxy servers from ringing-based denial-of-service attacks. In *the Tenth IEEE International Symposium on Multimedia (ISM)*, Berkeley, USA, December 2008. IEEE.

[54] X. Wang, S. Chen, and S. Jajodia. Tracking anonymous peer-to-peer VoIP calls on the Internet. In *CCS '05: Proceedings of the 12th ACM conference on Computer and communications security*, pages 81–91, New York, NY, USA, 2005. ACM.

[55] S. Chen, X. Wang, and S. Jajodia. On the anonymity and traceability of peer-to-peer VoIP calls. *IEEE Network*, 20(5):32–37, 2006.

Towards Secure SIP Signalling Service for VoIP applications

Current Voice over IP (VoIP) services are regarded less secure than the traditional public switched telephone network (PSTN). This is due to the fact that VoIP services are frequently deployed in an relatively open environment so that VoIP infrastructures can be easily accessed by potential attackers. Furthermore, current VoIP services heavily rely on other public Internet infrastructures shared with other applications. Thus, the vulnerabilities of these Internet infrastructures can affect VoIP applications as well. Nevertheless, deployed in a closed environment with independent protocols, PSTN has never faced similar risks.

The main goal of this licentiate thesis is the discussion of security issues of the Session Initiation Protocol (SIP), which serves as a signalling protocol for VoIP services. This work especially concentrates on the security risks of SIP related to performance. These risks can be exploited by attackers in two ways: either actively or passively. The throughput of a SIP proxy can be actively manipulated by attackers to reduce the availability of services. It is defined as Denial of Service (DoS) attacks. On the other hand, attackers can also profile confidential information of services (e.g., calling history) by passively observing the performance of a SIP proxy. It is defined as a timing attack. In this thesis, we carefully studied four concrete vulnerabilities existing in current SIP services, among which, three of them can lead to DoS attacks and one can be exploited for timing attacks. The results of our experiments demonstrate that these attacks can be launched easily in the real applications.

Moreover, this thesis discusses different countermeasure solutions for the attacks respectively. The defending solutions have all in common that they are influencing the performance, by either enhancing the performance of the victim during a DoS attack, or abating the performance to obscure the time characteristic for a timing attack. Finally, we carefully evaluated these solutions with theoretical analyses and concrete experiments.

Karlstad University Studies
ISSN 1403-8099
ISBN 978-91-7063-250-1