1

Introduction

Such a thing could never be more than a scientific toy (Casson 1910). This sentence did not describe Intel's surf board with embedded tablet PC,[1] but was written in the late nineteenth century and described the telephone built by Graham Bell. If anything, this shows how difficult it is to anticipate the success or failure of a technology and even more the desires and needs of users. More than a hundred years later, telephones are a practical necessity, as well as an occasional annoyance. We all have at least two phones and even children of elementary school age firmly believe that a mobile phone is one of the most important gadgets they need to survive everyday life.

The vast majority of the telephony services used today are still broadly based on the system envisioned by Graham Bell and use the concept of circuit switching. In circuit-switched networks, also known as public-switched telephone network (PSTN), the communicating parties are connected through a circuit or channel with fixed bandwidth for the entire duration of the call. The first experiments with transmitting voice over IP networks were conducted in the early 1970s (Cohen 1977). The first commercial applications and devices appeared in the mid 1990s based on proprietary protocols. H.323 (ITU-T Rec. H.323 2006) was first published in 1996 and was the first widely deployed Voice over Internet Protocol (VoIP) standard. The Session Initiation Protocol (SIP) was first published in 1999 (Handley *et al*. 1999) and then updated in 2002 (Rosenberg *et al*. 2002b). In recent years, SIP has increasingly gained in popularity and has become the de-facto standard for public VoIP offerings. It was adopted under the name of IP Multimedia Subsystem (IMS) by the mobile telephony networks as the signaling protocol for next-generation networks.

When compared with the PSTN, the VoIP market is still small in terms of number of subscribers and revenue. However, with more than 25 million subscribers and a revenue of US$3 billion in 2007,[2] the VoIP market now has considerable size. To ensure that the VoIP market can continue to grow, VoIP cannot compete only on the basis of price and features offered. For VoIP to succeed in the long term, VoIP services must offer similar security and protection levels to what is available today in the PSTN. A headline in the newspapers about the telephony service of a VoIP provider not being reachable for

[1] http://www.intel.com/cd/corporate/pressroom/emea/eng/150308.htm
[2] http://www.telegeography.com/products/euro_voip

SIP Security Dorgham Sisalem, John Floroiu, Jiri Kuthan, Ulrich Abend and Henning Schulzrinne

a couple of hours due to a denial of service will certainly make a lot of people think whether they should really replace their current PSTN phone with a VoIP one. Rumors spread in blogs and Internet forums that VoIP services do not provide the same level of privacy protection as PSTN or about their vulnerability to fraud and identity theft can have tremendously negative effects on the reputation of VoIP. Finally, the proliferation of spam calls over VoIP services to levels similar to what we see today with email spam could further contribute to users yearning for the closed and protected PSTN service.

Security threats on VoIP services can be roughly categorized as follows (VoIPSA 2005):

- Social threats–because of the similarity to email services, VoIP services are expected to have the same social threats as email. This might include unsolicited calls, intrusion on the user's privacy, fraud, identity theft and misrepresentation of identity or content. To overcome these threats, we discuss in Chapter 6 various approaches for providing authenticated identities and combating identity theft and fraud as well as for ensuring the user's privacy. Chapter 9 presents different technologies that can be used for reducing the threats of unsolicited calls.
- Eavesdropping–by monitoring signaling and media information sent and received by a user, an attacker can collect various pieces of information about the user such as her identity, the identities of her communication partners and the content exchanged by the user. To reduce the possibility of eavesdropping on the user's audio or video calls, Chapter 7 describes different protocols used for securing the media communication. The security of the signaling data is discussed in Chapters 3, 5 and 6.
- Interception and modification–by intercepting exchanged signaling and media information or by getting access to the components providing the VoIP service, an intruder can reroute calls to malicious destinations, block calls from or to certain users or degrade the quality of the calls. Chapter 8 discusses possible attack scenarios that can be used for intercepting and modifying VoIP calls and approaches for defending against these attacks. Chapter 7 presents different protocols for supporting the encryption of media data and exchanging the necessary keys for encrypting and decrypting the media traffic.
- Service abuse–service abuse describes improper use of services by bypassing a provider's authentication mechanisms, stealing the service of other users or misusing the service provider's components for launching attacks on other users or service providers. Abuse scenarios and defense strategies are described in Chapters 6 and 8.
- Interruption of service–attackers launch denial of service attacks with the goal of interrupting a service and making it unavailable to legitimate users. In Chapter 8, different threats and attack scenarios and possible defense mechanisms are described.

In this book, we explore the security aspects of SIP and IMS services, with the goal of providing the reader with an insight into possible scenarios for launching denial of service attacks on SIP-based services, conducting fraud and identity theft and misusing the SIP service for distributing spam, as well as defending against such threats.

Chapter 2 lays out the basic technologies and mechanisms used for securing and encrypting traffic. Chapter 3 is an overview of SIP. In this context, the different usage scenarios of SIP and the different methods and authentication schemes supported by SIP are described. Further we touch on different deployment issues. Chapter 4 describes the usage of SIP in mobile and next-generation networks. The differences from the basic SIP specifications are highlighted and the call model in these networks is explained. Security aspects of user authentication and internetwork communication in next-generation

networks are described in Chapter 5. Chapter 6 presents an overview of the different mechanisms suggested for securing the user identity in SIP and preventing fraud. The mechanisms used for securing the media traffic in VoIP environments are described in Chapter 7. Chapter 8 presents the different possibilities for launching denial of service attacks on SIP-based services as well as the possible solutions for reducing the risks of attacks. Finally, possible misuse of spam services for distributing spam is described in Chapter 9, along with the legal aspects of SIP and the different measures for protecting against such misuse.

The SIP specifications especially in the security related areas are still evolving. Further, even after an extensive reviewing process we still suspect that there are a number of errors that we could not catch and would appreciate if our readers would point us to. For a central place listing the latest updates to the SIP specifications and security related issues as well as collecting reader feedback and keeping an up-to-date errata please visit the www.sipsecurity.org web site.