Managing Risks at Runtime in VoIP Networks and Services

O. Dabbebi, R. Badonnel and O. Festor

INRIA Nancy Grand Est - LORIA
Campus Scientifique - BP 239
Technopôle de Nancy Brabois
54506 Vandœuvre-lès-Nancy, France

Abstract. IP telephony is less confined than traditional PSTN telephony. As a consequence, it is more exposed to security attacks. These attacks are specific to VoIP protocols such as SPIT, or are inherited from the IP layer such as ARP poisoning. Protection mechanisms are often available, but they may seriously impact on the quality of service of such critical environments. We propose to exploit and automate risk management methods and techniques for VoIP infrastructures. Our objective is to dynamically adapt the exposure of a VoIP network with regard to the attack potentiality while minimizing the impact for the service. This paper describes the challenges of risk management for VoIP, our runtime strategy for assessing and treating risks, preliminary results and future work.

1 Introduction and challenges

Voice over IP (VoIP) defines a new paradigm for telephony services. It permits to transmit telephony communications directly over IP networks at a low cost and with a higher flexibility than traditional PSTN[1] telephony. It relies on an infrastructure composed of VoIP phones, IPBX servers for establishing and managing call sessions, and VoIP gateways for interconnecting with the PSTN. It exploits dedicated protocols including signaling protocols such as SIP[2] or H.323, and transport protocols such as RTP or RTCP. However, VoIP communications are less confined, and then are more exposed to security attacks. They are concerned by security attacks inherited from the IP layer such as poisoning and flooding attacks, and also by VoIP-specific attacks such as SIP spoofing and SPIT[3] [1]. Moreover, security mechanisms may significantly deteriorate the quality and usability of these services. Typically, the application of encryption, filtering and authentication techniques may seriously increase delays and loads of VoIP communications.

Risk management provides new opportunities for dealing with these security issues in such critical environments. It can be defined as a process which consists

[1] Public Switch Telephony Network
[2] Session Initiation Protocol
[3] Spam Over IP Telephony

in assessing risks and treating them, i.e. taking steps in order to minimize them to an acceptable level [2]. Existing work related to risk assessment in VoIP infrastructures includes approaches for assessing threats (defender viewpoint) such as honeypot architectures and intrusion detection systems based on signatures, or based on anomalies [3, 4]. They also include approaches for assessing vulnerabilities (attacker side) such as fuzzing-based discovery and auditing/benchmarking tools [5]. Risk models supporting this assessment may be qualitative (based on linguistic scales), quantitative (based on probabilities) or mixed (based on aggregations of qualitative parameters) [6]. Existing work on risk treatments permit to eliminate risks (risk avoidance) by applying best practices, to reduce and mitigate them (risk optimization) by deploying protection and prevention systems [7], to ensure against them (risk transfert) by subscribing an insurance contract or to accept them (risk retention) [8].

When we look further at these approaches proposed for VoIP networks and services, we can clearly observe that most of them do not really address risk management. They usually do not integrate any risk model, or at least not explicitly, and they only cover partially the risk management process. There is therefore a serious need for applying risk management in these environments in order to protect them efficiently, while maintaining their quality of service.

2 Runtime risk management for VoIP

We propose to investigate risk management methods and techniques for VoIP infrastructures. In particular, we are interested in automating risk management at runtime: the objective is to dynamically adapt the exposure of the VoIP network and its components with respect to the potentiality of attacks. This automation aims at reinforcing the coupling between the risk assessment phase and the risk treatment phase. The exposure is continuously controlled based on the activation and the deactivation of countermeasures (or safeguards). A countermeasure permits to reduce the performance of a security attack, but it may also deteriorate the service by introducing additional delays or reducing the access to some specific features. In that context, we have extended the rheostat runtime risk model [9] to VoIP environments. Let consider a security attack noted $a \in A$ with A defining the set of potential VoIP attacks. Risk is typically defined as the combination of the potentiality $P(a)$ of the related threat, the exposure $E(a)$ of the VoIP infrastructure, and the consequence $C(a)$ on that infrastructure if the attack succeeds (see Equation 1).

$$\mathcal{R} = \sum_{a \in A} P(a) \times E(a) \times C(a) \tag{1}$$

Rheostat exploits a risk reduction algorithm and a risk relaxation algorithm. The risk reduction algorithm permits to reduce the risk level when the potentiality $P(a)$ of the threat is high, by activating security safeguards (such as passwords

and turing tests). This activation reduces the exposure $E(a)$ of the infrastructure, and then permits to decrease the risk level to an acceptable value. The risk relaxation algorithm permits to minimize the impact on the infrastructure by deactivating security safeguards when the risk level is low. We have evaluated this risk model and specified several safeguards for specific VoIP attacks in [10]. We are generalizing this work to multiple VoIP security attacks.

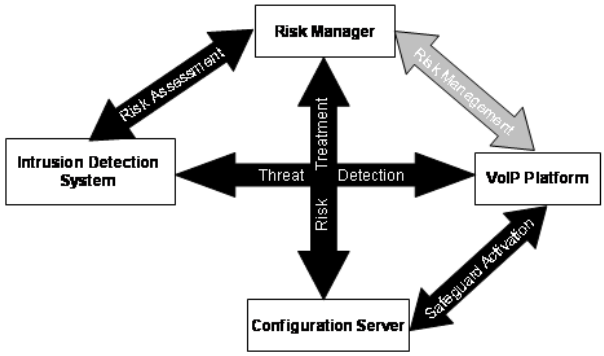

Fig. 1. Runtime risk management for VoIP environments

We have also specified a functional architecture for supporting runtime risk management in these environments, as depicted on Figure 1. This architecture is composed of an intrusion detection system responsible for detecting threats in the VoIP platform, a risk manager for managing risks and selecting security safeguards with respect to a given context, and a configuration server for dynamically activating or deactivating the security safeguards. We are determining several strategies for deploying this architecture on a VoIP infrastructure.

3 Preliminary results

We have developed a first implementation of the risk manager component and have evaluated its behavior based on a set of experiments. We have focused on SPIT attacks and have considered two main scenarios: a first one corresponding to the case when the threat potentiality increases over time (risk reduction algorithm), and a second one corresponding to the case when the potentiality decreases (risk relaxation algorithm). We have shown the capability of the risk manager to reduce risks due to VoIP attacks and to minimize costs induced by safeguards. We have also shown the benefits and limits of our approach in comparison with traditional strategies. Our runtime solution permits to mitigate the risk level (benefits of up to 41%) and to maintain the continuity of the VoIP service in an dynamic manner. The benefits are limited in the case of instantaneous VoIP attacks. We are performing additional and complementary experiments of this schema based on Monte-Carlo simulations.

4 Conclusions and perspectives

Telephony over IP has known a large-scale deployment. VoIP communications are less confined than in traditional telephony, and are exposed to multiple attacks. Security mechanisms are required for protecting these communications. Their application may however seriously deteriorate the performances of such a critical service: a VoIP communication becomes incomprehensible as soon as the delay is more than 150 ms, or the packet loss is more than 5%. In that context, we propose to exploit and automate risk management methods and techniques at runtime in VoIP networks and services. Our aim is to dynamically adapt the exposure of the VoIP infrastructure based on a set of security safeguards in order to provide a graduated and progressive answer to risks. We have exploited the rheostat risk management model, specified a functional architecture, and evaluated the case scenario of SPIT attacks. We are extending this approach to multiple VoIP attacks, and are quantifying the impact of parameters based on Monte-Carlo simulations. For future work we are planning to evaluate several configurations for deploying our functional architecture, and will investigate return-on-experience mechanisms for automatically configuring and refining the risk model parameters.

References

1. Thermos, P., Takanen, A.: Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures. Addison-Wesley Professional (2007)
2. Kuhn, D.R., Walsh, T.J., Fries, S.: Security Considerations for Voice Over IP Systems. National Institute of Standards and Technology, http://csrc.nist.gov/publications/ (2005)
3. Dantu, R., Kolan, P., Cangussu, J.W.: Network Risk Management using Attacker Profiling. Security and Communication Networks **2**(1) (2009) 83–96
4. Shin, D., Shim, C.: Progressive Multi Gray-Leveling: A Voice Spam Protection Algorithm. IEEE Network Magazine **20** (September 2006)
5. Bunini, M., Sicari, S.: Assessing the Risk of Intercepting VoIP Calls. Elsevier Journal on Computer Networks (May 2008)
6. Bedford, T., Cooke, R.: Probabilistic Risk Analysis: Foundations and Methods. Cambridge University Press (April 2001)
7. D'Heureuse, N., Seedorf, J., Niccolini, S., Ewald, T.: Protecting SIP-based Networks and Services from Unwanted Communications. In: Proc. of IEEE/Global Telecommunications Conference (GLOBECOM'08). (December 2008)
8. ISO/IEC 27005: Information Security Risk Management, International Organization for Standardization, http://www.iso.org (June 2008)
9. Gehani, A., Kedem, G.: RheoStat: Real Time Risk Management. In: Proc. of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004). (2004)
10. Dabbebi, O., Badonnel, R., Festor, O.: Automated Runtime Risk Management for Voice over IP Networks and Services. In: Proc. of the 12th IEEE/IFIP Network Operations and Management Symposium (NOMS 2010). (April 2010)