Automated Runtime Risk Management for Voice over IP Networks and Services

Oussema Dabbebi, Rémi Badonnel, Olivier Festor

Automated Runtime Risk Management for Voice over IP Networks and Services

Oussema Dabbebi [2], Rémi Badonnel[1] , Olivier Festor[2]
[1] LORIA - Nancy University
[2] LORIA - INRIA Nancy Grand Est
Campus Scientifique - BP 239
Technopôle de Nancy Brabois
54506 Vandœuvre-lès-Nancy, France
{dabbebi, badonnel, festor}@loria.fr

***Abstract*—Voice over IP (VoIP) has become a major paradigm for providing telephony services at a lower cost and with a higher flexibility. VoIP infrastructures are however exposed to multiple security issues both inherited from the IP layer and specific to the application layer. In the meantime, protection mechanisms are available but may seriously impact on the continuity and quality of such critical services. We propose in this paper an automated risk management schema for continuously adapting VoIP equipment exposure by activating security safeguards in a dynamic and progressive manner. We describe the architecture supporting our solution, the considered risk model taking into account VoIP properties and the algorithms for restricting and relaxing the risk level of the VoIP service at runtime. The benefits and limits of our solution are evaluated through an implementation prototype and an extensive set of experimental results in the case scenario of SPIT attacks.**

I. Introduction

The large-scale deployment of VoIP infrastructures has been leveraged by high-speed broadband access. This access provides the network performance required for such latency-sensitive services. Voice over IP includes a large variety of methods and techniques enabling the transmission of voice directly through the Internet and other packet-switched networks. It has rapidly been perceived by both research communities and service providers, as a potential solution for reducing infrastructure and maintenance costs. It also facilitates the integration of extended services that would be more difficult to deploy in traditional networks. The deployment has also been significantly supported by the standardization of dedicated signaling protocols for establishing, maintaining and terminating call sessions amongst VoIP devices.

VoIP services are however facing with multiple security issues due to the transmission of telephony calls on IP networks that are by nature less confined than traditional telephony networks and are usually shared with multiple other applications and services. In that context, security is one of the most important challenges in VoIP infrastructures, in comparison with traditional telephony where the security of conversations is guaranteed by the physical layer. Telephony over IP is concerned with attacks specific to VoIP protocols but also with attacks inherited from the IP layer. These VoIP attacks can typically be classified into four main categories [1]: (a) service disruption and annoyance such as SPIT[1] attacks, (b) eavesdropping and traffic analysis, (c) masquerading and impersonation such as spoofing attacks, (d) unauthorized access and fraud such as vishing[2] attacks. They can have significant consequences on the telephony service, such as the impossibility for a client of making an urgent phone call. These consequences are all the more important since the marketing strategies around VoIP technologies have generated a number of errors, false beliefs and high expectations of clients with respect to the adoption of telephony over IP.

A large variety of detection and protection mechanisms have been developed for identifying and blocking VoIP security attacks. However, detection methods rapidly show their limits in terms of sensitivity and specificity. The potentiality of an attack is often difficult to estimate and the time duration to precisely detect an attack can be important in comparison to the timescale of this attack. In the meantime, protections mechanisms are often harsh and may have a significant impact on the performance of the telephony service with respect to its operational continuity and its quality of service.

In that context, we propose a new approach for applying and automating risk management in VoIP networks and services at runtime. Risk management is required by VoIP infrastructures for dealing with the trade-off between security and quality of service, which are both crucial to the VoIP service. The objective is to continuously adapt the exposure of VoIP equipment by activating or deactivating security checks in the network in a progressive and fine-grained manner. Risk models such as Rheostat [2] must be extended to take into account VoIP properties. They complete detection techniques by integrating their performance limits and permit a fine-grained coupling of the detection phase with the treatment phase.

The main contributions of our approach are centered on: (a) the design of an architecture for supporting automated runtime risk management in VoIP networks, (b) the extension of the Rheostat formal model in order to take into account

[1]Spam over IP
[2]Voice over IP phishing

the properties of VoIP infrastructures, (c) the implementation of restriction and relaxation algorithms for progressively and continuously adapting the exposure of VoIP equipment, (d) the evaluation of our risk management schema based on an implementation prototype and a set of experimental results.

The paper is consequently organized as follows. Section II presents our automated runtime strategy for managing risks in a continuous and fine-grained manner in VoIP networks. Section III describes the underlying architecture, its components and how they interact in order to strengthen the coupling between an intrusion detection system and a configuration management system responsible for activating security safeguards. Section IV details further the risk manager component, the extension of the Rheostat formal model and the algorithms for mitigating risks in a dynamic manner. Section V discusses a set of experimental results obtained in the case scenario of SPIT attacks. Related work are presented in Section VI, and Section VII concludes the paper and presents future research efforts.

II. VoIP Runtime Risk Management

Our risk management approach aims at determining to what extent risk management can be applied and automated in VoIP networks and services. Risk is typically defined as the combination of the probability that a given threat exercises a vulnerability and the resulting impact of that adverse events on the VoIP infrastructure [3]. The exercise by a threat of a vulnerability corresponds to a security attack. Risk management is the process consisting of identifying risks, assessing and evaluating them, and taking steps (security safeguards) to reduce risks to an acceptable level [4]. Traditional risk management strategies have to be extended to take into account the dynamics and criticality properties of VoIP environments. In particular, if we refer to our definition of risk, the reduction of risks could be obtained by eliminating all the vulnerabilities of the VoIP service by deploying protection mechanisms. The absence of vulnerability makes the probability that a given threat exercises a vulnerability converging to zero, and reduces the risk level to zero. However, some vulnerabilities are intrinsic to the VoIP service. For instance, blocking all the paying calls can prevent the VoIP service from toll fraud attacks, but this treatment significantly degrades the IP telephony service.

One of the main challenges in the application of risk management in these services is to provide an efficient response to the trade-off between security and quality of service. Indeed, the execution of protection mechanisms may significantly impact on the operational continuity of IP telephony. VoIP applications are real-time, the alteration of their quality of service by protection mechanisms may make their use inconvenient. Typically, a VoIP call becomes incomprehensible under a 150 milliseconds delay or a 5% packet loss, even when efficient codecs are used. Protection mechanisms have to be executed in a dynamic and efficient manner with respect to the potentiality of the security attack. It is necessary for that purpose to improve the coupling between the different steps of risk management from the detection of attacks to the execution of treatments. Risk management have to be performed dynamically at runtime in order to give a fine-grained and progressive response to risks in the VoIP infrastructure.

In that context, we propose an automated runtime risk management solution for VoIP networks and services. Our schema relies on the extension to VoIP environments of the Rheostat risk model which provides support for dynamically altering the exposure of an host. This alteration is driven by a cost-benefit analysis at runtime in order to provide a systematic response with respect to the probability of a security attack. The exposure of the VoIP equipment is controlled by auxiliary security safeguards/checks applied in a progressive manner. The activation of a security check permits to reduce the exposure when the potentiality of an attack increases, while the deactivation permits to reduce security costs and to improve the quality and operational continuity of the VoIP service. The solution does not require the attack potentiality to be high in order to execute auxiliary checks. The checks are activated progressively as the attack potentiality increases. We have specified the architecture supporting our risk management schema through the integration of an intrusion detection system with a configuration management tool. We have extended the Rheostat risk model and its algorithms for automatically restricting and relaxing VoIP risks at runtime. We have evaluated the performance and benefits of our strategy through an extensive set of experiments. In the following of this paper, we will further focus on the case scenario of SPIT attacks, but our fine-grained solution is generic and can be extended to other VoIP threats.

III. Functional architecture

The architecture that supports our runtime risk management solution aims at strengthening the coupling between the detection of risks and the application of treatments. The objective is to take into account at an early stage the results of the detection system in order to provide a graduated and continuous treatment of risks. The architecture of our solution is depicted on Figure 1 and is composed of the three following main components:

- Intrusion detection system: this first component is responsible for measuring the potentiality of an attack. Its role consists in monitoring critical network elements and identifying attack scenarios. We consider a network-based intrusion detection system in order to control the VoIP elements at the network scale. The performance of an intrusion detection system are necessary limited in terms of sensitivity and specificity. Typically, a threshold value permits to determine when an attack is considered as effective. The risk management schema permits to deal with the intrinsic limits of the detection system. The results of the intrusion detection system are transmitted to the risk manager at an early stage, even if these results are partial and the attack potentiality is not high. They are progressively integrated into the risk model in order to activate safeguards in continuous and adaptive manner.

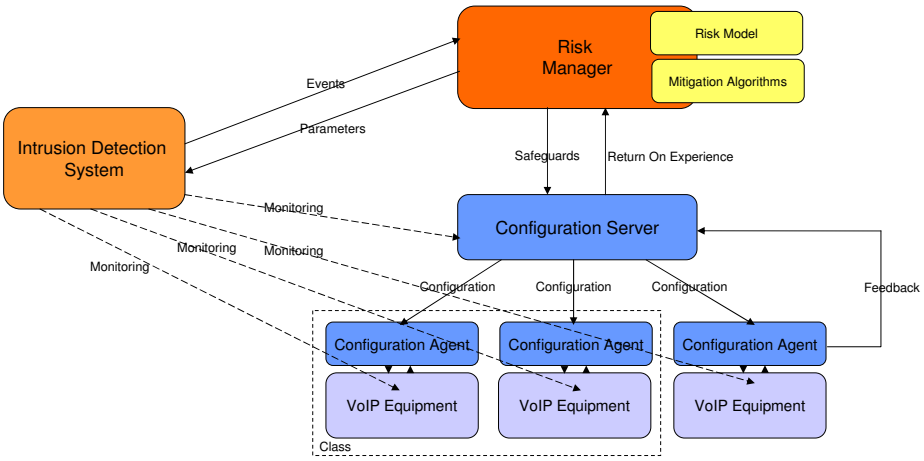

Fig. 1. Functional architecture, its components and their interactions supporting our automated runtime risk management schema

- Risk manager: this component plays an important role in our risk management solution because it integrates the risk model and the risk mitigation algorithms. The risk manager controls risks by estimating the risk level and by evaluating the status of each VoIP component. The risk calculation (assessment phase) is based on the exposure of the VoIP equipment, the potentiality of an attack and its consequences on the VoIP infrastructure. Based on the risk level, the risk manager determines (evaluation phase) if the risk level is acceptable or not. Consequently, it selects if necessary the treatments to be applied on the VoIP infrastructure. This task typically consists in activating or deactivating the auxiliary security checks in order to optimize the trade-off between security and quality of the VoIP service.
- Configuration management system: this third component is responsible for executing the treatments in the VoIP infrastructure through a set of configuration operations. The configuration management system is typically composed of a configuration server and a set of configuration agents deployed on VoIP equipment. The application of a same risk treatment may vary depending on the class of VoIP equipment. Treatments concern all the network elements that may impact on the exposure of the VoIP infrastructure to risks. These elements include VoIP phones and VoIP servers, but also the signaling and media transport protocols, the supporting services such as DNS, TFTP and RADIUS, the integrated services such as instant messaging services, and the security equipment such as network and applicative firewalls.

As previously mentioned, we focus in our work on the case scenario of SPIT attacks in a VoIP infrastructure. One of the key motivations is that many detection techniques already exist and can be improved and integrated together by considering risk models. A SPIT attack typically targets the phones part of a given VoIP infrastructure. It generates VoIP calls to a large number of phones, which may impact on the network performance and may significantly alter the VoIP service availability. The load on network resources and the level of annoyance of users is much more important than traditional email spamming. In order to measure the potentiality of a SPIT attack, we considered a set of six common detection criteria of the DEVS[3]-based modeling of spitter behavior proposed in [5] and detailed below:

- Call rejection rate (noted $Rejection_{rate}$): this first parameter represents the normalized number of rejected calls for a given caller. This rate is usually low for a regular caller while it may significantly increase in the case of a SPIT caller.
- Call recipient rate (noted $Recipient_{rate}$): it corresponds to the normalized number of call recipients for one established call. In a similar manner as email spamming, this rate is usually more important for a SPIT caller.
- Call duration rate (noted $Duration_{rate}$): the duration of calls is also an important parameter to detect SPIT callers. It is usually very short and rarely very long in the case of SPIT attacks.
- Call traffic rate (noted $Traffic_{rate}$): it takes into account the traffic generated during call conversations. The conversation during a SPIT call is usually one-sided and contains less pauses than that of a regular caller.
- Call rate (noted $Call_{rate}$): this parameter evaluates the number of calls generated during a given time period and compares the distribution of the caller with respect to the normal distribution in the VoIP network.
- Call inter-arrival time (noted $Inter_{rate}$): the inter-arrival times for VoIP calls generated by a spitter are usually much more regular in comparison with a regular caller.

During the risk management process, these parameters are continuously and finely measured by the intrusion detection system. They are then exploited at an early stage by the risk manager to assess/evaluate the risk level and to select the proper risk treatments to be executed by the configuration management system.

[3]Discrete Event System Specification

IV. Risk Manager Component

The risk manager is the main component of our runtime risk management solution. It ensures the strong and fine-grained coupling of detection and treatment phases, and implements the supporting risk model and the mitigation algorithms (restriction and relaxation of the risk level by activating or deactivating safeguards).

A. Extension of the Rheostat risk model

The first activity of the risk manager is to assess and evaluate the risk level in the network. We considered the Rheostat risk model which has been specifically designed to manage risks at runtime. We extended it to take into account the properties of our VoIP infrastructure. The risk level is calculated based on Equation 1 with t_α corresponding to the signature of the attack, $\mathcal{T}(t_\alpha)$ the potentiality of this attack, $\mathcal{V}(t_\alpha)$ the host exposure to the threat depending on safeguards, and $\mathcal{C}(t_\alpha)$ the consequences of the attack on the VoIP infrastructure. Each element of this equation is assessed in a quantitative manner.

$$\mathcal{R} = \sum_{t_\alpha \in T} \mathcal{T}(t_\alpha) \times \mathcal{V}(t_\alpha) \times \mathcal{C}(t_\alpha) \quad (1)$$

The potentiality of an attack is based on the parameters transmitted by the intrusion detection system. In the Rheostat model, when a signature is partially detected, the sequence of events necessary to complete it is used as an indicator for this assessment. Rheostat uses a function μ to calculate the probability of a given threat $\mathcal{T}$ with μ depending on the historical events in the system. In our case scenario, we considered the VoIP parameters that characterize a SPIT attack. We therefore define mathematically the $\mathcal{T}(t_\alpha)$ potentiality as the SPIT level given by Equation 2 with $\{\beta, \gamma, \delta, \varepsilon, \zeta, \eta\}$ the set of factors weighting the detection parameters previously mentioned.

$$\begin{aligned} \mathcal{T}(t_\alpha) &= \beta \times Duration_{Rate} \\ &+ \gamma \times Traffic_{Rate} \\ &+ \delta \times Rejection_{Rate} \\ &+ \varepsilon \times Inter_{Rate} \\ &+ \zeta \times Call_{Rate} \\ &+ \eta \times Recipient_{Rate} \end{aligned} \quad (2)$$

These weighting factors are specified based on the study described in [5]. The risk management permits to take into account the limits (sensitivity and specificity) of these criteria during the detection of attacks.

The exposure of the VoIP infrastructure to a threat is also assessed in a quantitative manner. It directly depends on the safeguards that are activated or deactivated in the network. These safeguards permit to reduce the vulnerabilities intrinsic to the VoIP service and related to its current configuration. The exposure $\mathcal{V}(t_\alpha)$ is mathematically defined by Equation 3 through the extension of the Rheostat model.

$$\mathcal{V}(t_\alpha) = \sum_{o_\lambda \in \hat{P}(t_\alpha)} \frac{v(o_\lambda) \times s(o_\lambda)}{|\hat{P}(t_\alpha)|} \quad (3)$$

In this equation, $\hat{P}(t_\alpha)$ represents the set of operations that are required for performing an attack t_α. The $\mathcal{V}(t_\alpha)$ value is calculated based on the initial exposure $v(o_\lambda)$ of a given operation o_λ. This exposure is weighted by the $s(o_\lambda)$ factor quantifying the impact on the exposure of the safeguards activated or deactivated for this operation. This factor is set to 1.0 if no safeguard is activated and is set to 0.0 if the operation is fully controlled. In that manner the exposure of the VoIP infrastructure directly depends on the presence and impact of security safeguards for protecting the operations serving as a support for performing attacks.

The risk level takes also into account a normalized value quantifying the consequences of the considered attack, as specified by the $C(t_\alpha)$ parameter in Equation 1. This value is important when several threats are in competition and permits to prioritize the safeguards to be activated. In our scenario, this value has a limited impact on the behavior of our runtime risk management schema, as we only focus on the case of SPIT attacks.

B. Graduated risk management algorithms

The risk manager exploits two different management algorithms derivated from Rheostat in order to address the trade-off between security and quality of service in VoIP infrastructures. The risk level is controlled event-by-event in a continuous manner based on results generated by the intrusion detection system. These two algorithms rely on a cost-to-benefit analysis of each safeguard addressing the considered attack. The risk manager determines the candidate safeguards based on the ratio of two opposite criteria: their capabilities to reduce risks and their impact on the VoIP service usability and quality.

On the one hand, the restriction algorithm permits to progressively activate auxiliary safeguards for altering the exposure of the VoIP infrastructure when the risk level increases. Each time the risk level increases up to a threshold value, the manager selects the set of proper safeguards permitting to reduce the risk to a lower value than the threshold and presenting the best cost-to-benefit ratio. As described in Equation 4, the choice of safeguards aims at minimizing the impact on performance and at the same time to maintain the risk level to a value below the considered threshold value $R_{threshold}$.

$$\begin{aligned} &minimize(\textstyle\sum_{o_\lambda \in \hat{P}(t_\alpha)} i(o_\lambda)) \\ &and\ R_{new} \leq R_{threshold} \end{aligned} \quad (4)$$

R_{new} corresponds to the new risk level calculated based on the previously described risk model and $i(o_\lambda)$ quantifies the impact on the service performance of the security safeguards activated for the operation o_λ.

On the other hand, the relaxation algorithm permits to deactivate auxiliary safeguards in order to optimize the VoIP service performance when the risk level is low. This risk level typically decreases when no event corresponding to the considered attack t_α has been observed during a given time period. At the expiration of a timer, the relaxation algorithm deactivates safeguards based on the same criteria mentioned in Equation 4. The impact on VoIP service can be minimized

Aux. safeguard	Functional description	System Exposure	Performance Impact
s1	Sending a busy signaling message to the caller	0.9	0.1
s2	Asking the typing of an antibot code	0.7	0.4
s3	Asking the answer to a specific question	0.6	0.5
s4	Putting the caller on a waiting queue	0.3	0.8
s5	Systematically blocking the caller	0.0	1.0

Fig. 2. *Auxiliary safeguards supporting our runtime risk management schema in the case scenario of SPIT attacks*

if and only if the risk level variation due to this relaxation algorithm maintains the new risk level below the threshold value $R_{threshold}$.

C. Progressive treatments based on auxiliary safeguards

The performance of our risk management schema is strongly dependent on the application of safeguards in adequation with the risk level. Indeed these auxiliary safeguards impact both on the exposure of the system and on their performance. In our case scenario of spam over telephony, the SPIT attacks may be generated by two different types of entities: bots that automatically initiate sessions to a set of addresses and humans that typically perform calls for marketing purposes. We designed in that context five different safeguards that are summarized on Table 2 with normalized values characterizing their impact on the exposure and their impact on the performance of the VoIP service. These safeguards are ordered according their capability to alter the exposure of the VoIP infrastructure:

- Safeguard s1 consists in sending a busy signaling message to the caller. Typically, the PBX server responds with a message indicating that the called party is busy. As a consequence, if the caller corresponds to a bot, there is a high probability that it abandons this recipient and initiates call sessions with other phones. We considered this safeguard as the solution that impacting the less on the exposure (10% of spitters are assumed to be blocked by this safeguard) but also impacting the less on the service performance.
- Safeguard s2 consists in asking the typing of a particular code to the caller. The SPIT caller is invited to enter a sequence of numbers. This sequence is not a password but aims at detecting if the caller is a SPIT bot or not. We consider this safeguard eliminates most of bot spitters, while speech recognition could be easily exploited to identify the sequence of numbers. This safeguard is inefficient to counter human spitters.
- Safeguard s3 asks the caller to answer to a specific question. It blocks most of bot spitters and perturbate human spitters because the SPIT caller has to answer a question each time it wants to establish a call session. This safeguard permits to significantly alter the exposure to risks but has also an important impact on the VoIP service performance.
- Safeguard s4 puts the caller into a waiting queue. This safeguard can be implemented using the hold signaling message. This safeguard progressively increases the waiting time for the considered caller. The more the SPIT caller initiates call sessions, the more it has to wait before establishing the call. This solution can be quite efficient against bot and human spitters depending on the chosen increasing factor.
- Safeguard s5 consists in blocking systematically all the calls initiated by the considered caller. This safeguard is applied to the VoIP infrastructure when the potentiality of this attack is high. The attacker is fully detected by the intrusion detection system. This solution is equivalent to putting the caller to a blacklist. The VoIP service becomes unavailable for the caller. As a consequence, the normalized value specifying the impact on the service for this caller is set to 1.0.

This set of safeguards is specific to our scenario of SPIT attacks, but the runtime risk management solution can easily integrate other auxiliary safeguards.

V. Experimental results

In order to evaluate the performance of our solution, we have developed an implementation prototype of the risk manager component and performed an extensive set of experiments. This prototype implements in C++ the proposed risk model and the restriction and relaxation algorithms. It takes as an input the results of the intrusion detection system and provides as an output the security safeguards to be activated or deactivated by the configuration system. We have emulated different attack scenarios in order to evaluate the behavior and the benefits of our runtime risk management solution in comparison with other traditional strategies.

A. Impact of the restriction algorithm

In a first series of experiments, we were interested in evaluating the restriction algorithm and in determining how it impacts on the risk level of the VoIP service. In our experiments, we varied the attack potentiality perceived by the risk manager. Figure 3 represents the potentiality of the attack, the risk level calculated by the risk manager and the exposure of the VoIP service over time. We can first observe on this figure that the potentiality of the attack is initially equal to zero. Consequently, the risk level $\mathcal{R}$ is null and the exposure $\mathcal{V}$ is maximal. As the potentiality increases over time, the risk level $\mathcal{R}$ increases as well. At the instant time $t = 9$, the risk level $\mathcal{R}$ reaches the threshold value $R_{threshold} = 0.25$. The risk manager activates the first auxiliary safeguard $s1$ which exploits busy signaling messages against the potential spitter.

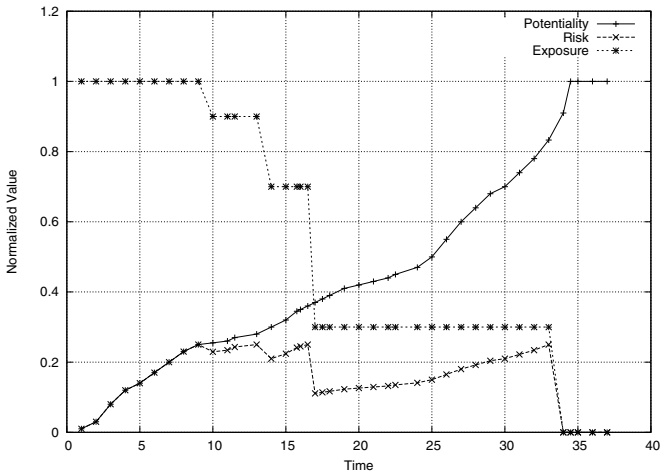

Fig. 3. Impact of the restriction algorithm on the VoIP service risk level

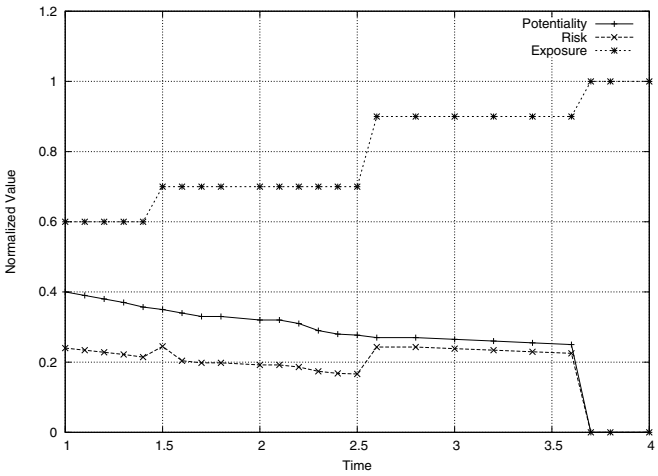

Fig. 4. Impact of the relaxation algorithm on the VoIP service risk level

This activation permits to reduce the exposure $\mathcal{V}$ to 0.9 and to mitigate the risk $\mathcal{R}$ to 0.225. While the first safeguard is activated, the potentiality of the attack (SPIT level) continues to grow until the risk level reaches again the threshold value $R_{threshold}$ at the instant time $t = 13$. The risk manager activates the second safeguard $s2$ which consists in asking for a particular code. The exposure converges to 0.7 and the risk level $\mathcal{R}$ is reduced to 0.21. We can observe on this Figure 3 how the risk manager succeeds in maintaining the risk level at a lower value: the safeguards are successively activated as long as the potentiality increases.

B. Impact of the relaxation algorithm

In a second series of experiments, we analyzed the capability of the risk management solution to relax the risk level when the potentiality of an attack decreases. The objective is to optimize the performance and usability of the VoIP service when the potentiality of an attack is low. Figure 4 describes the behaviours of the same parameters (potentiality, risk level and exposure) as Figure 3 but in that case the potentiality decreases over time. At the instant time $t = 1$, the safeguard $s3$ is running. The risk level is equal to $\mathcal{R} = 0.24$ and the exposure $\mathcal{V}$ is equal to 0.6. We emulated the decreasing of the attack potentiality. At the instant time $t = 1.5$, the manager deactivates the current safeguard $s3$ and activates the safeguard $s2$. It reduces the impact on the network performance but maintains the risk level to a value lower to the threshold $R_{threshold}$. The exposure $\mathcal{V}$ increases and reaches the normalized value of 0.7. The potentiality $\mathcal{T}$ continues to decrease over time and reaches the value of 0.27. In the meantime, the risk level decreases by a third and reaches 0.16. At the instant time $t = 2.6$, the risk manager relaxes once again the risk level in order to optimize the usability of the VoIP service. Finally at the instant time $t = 3.7$ it deactivates all the auxiliary safeguards as the risk level can be maintained to a value lower than $R_{threshold}$.

The two figures 3 and 4 show clearly how the exposure of the VoIP service can be altered or improved by the risk manager based on the activation or the deactivation of auxiliary safeguards. The set of experimental results confirms that the solution is capable of managing the risk level in a graduated manner. The manager selects the most appropriate safeguards in order to optimize the trade-off between the risk that an attack occurs and the impact of the safeguards on the service performance.

C. Comparison with traditional strategies

In a third series of experiments, we were interested in comparing our solution with traditional schemas and in quantifying the benefits and limits of integrating risk models to intrusion detection systems. Figure 5 describes the risk level of our solution noted A as well as the risk level of three alternative strategies noted $B1$, $B2$ and $B3$. These strategies correspond to the case of a detection system without an explicit risk model: the risk level is only based on the potentiality of the attack. They differ from their sensitivity and specificity with respect to the detection of attacks. The first strategy $B1$ provides a high true positive rate (high sensitivity) and consists in blocking VoIP communications of a given caller as soon as the potentiality exceeds a value of 0.3. The second strategy $B2$ consists in blocking communications when the potentiality reaches 0.5. This solution provides an average sensitivity and specificity and is considered by [5] as a baseline detection approach. The last strategy $B3$ reduces the false positive rate (high specificity) and blocks communications of the caller only when the potentiality of the attack is higher than 0.7.

The comparison of our solution A with the first strategy $B1$ shows the benefit in terms of risk level is low. Indeed the strategy $B1$ rapidly rejects the communications of the caller, and the risk level is reduced to zero. We can observe it on Figure 5 at the instant time $t = 15$. However the benefit in terms of service availability is quite high. Our risk management solution permits to maintain the VoIP service during a longer time period, as the safeguard $s5$ blocking the caller only takes effect at the instant time $t = 34$ on our graph.

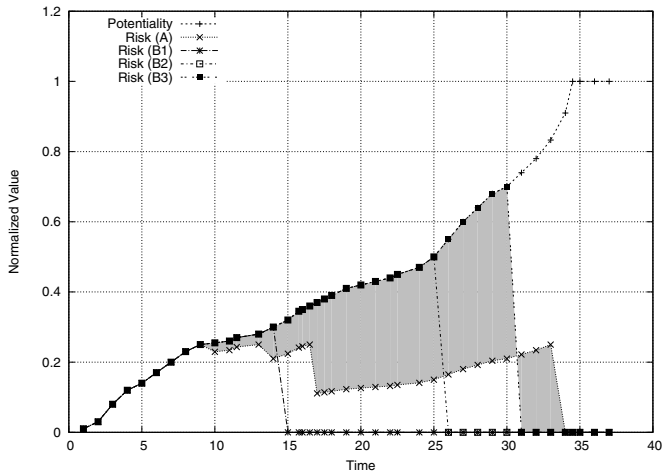

Fig. 5. Comparison of our solution with traditional strategies

When we compare our solution with the strategy $B3$, we expected a significant benefit in terms of risk, which was the case. We clearly observe the benefit of our risk management solution which is represented by the gray area over the curve of A on Figure 5. During experiments we quantified an average benefit of 32%. The major drawback of the strategy $B3$ is that the risk level can reach a high value before the caller is considered as a spitter by the detection system. In particular the maximum risk level generated by our solution is relatively low ($R_{threshold}$ set to 0.25) while it can be significantly higher with the strategy $B3$ (0.7 on Figure 5). In terms of service availability the two approaches A and $B3$ provide similar performance but the service is progressively restricted with our risk management approach.

The comparison with the strategy $B2$ also generates interesting results. The benefit in terms of service availability is important. The strategy $B2$ therefore blocks the VoIP communications of the caller at the instant time $t = 26$ while our solution A maintains the VoIP service until the instant time $t = 34$ on Figure 5. We quantified a benefit of up to 14% during our set of experiments. The averaged risk level is similar with the two approaches A and $B2$. However the maximum risk level is of 0.25 with our solution A and is of 0.5 with the $B2$ strategy. This phenomenon is similar to the one observed with $B3$ and is due to the progressive application of auxiliary safeguards.

D. Comparison with other attack temporal behaviors

We performed a last series of experiments in order to compare further the performance of our solution with other temporal behaviors of SPIT attacks. We considered four different types of temporal behaviors and evaluated the benefit of our approach in comparison with the strategy $B2$ (trade-off between sensitivity and specificity). We experimented a first behavioral type $C1$ consisting in increasing the potentiality of the attack (SPIT level) on a short time period. This corresponds to a scenario where the detection system can easily identify the attacker. A second behavioral type $C2$ increases the potentiality until half of the experiment duration and then decreases it. This illustrates the case of an attack that is not maintained over time. A third type $C3$ aims at increasing the potentiality until the threshold of $B2$ is reached and then reducing it afterwards. This reduces the benefits of the risk management schema after the threshold value. In the fourth type we reduced the potentiality just before the threshold of $B2$ is reached. As expected, the behavioral type $C1$ generated the worst performance while the third other types $C2$, $C3$ and $C4$ provided a benefit of up to 41% in terms of risk during the experiments. The functional architecture can typically be deployed on an IPBX server: the scalability of our solution directly depends on the scalability of VoIP servers.

VI. Related work

Risk management is a major challenge in computer science and networking. The standardization of the supporting process contributes to its deployment at a larger scale [6], [7]. Risk management plays an important role in service management platforms for determining the operations to be executed and their impact on the infrastructure. Typically in [8] the authors propose a formal model for evaluating the risk exposure associated to a change. The system is then capable of automatically assigning priorities to changes based on this exposure metric and on financial constraints. In [9], the CHAMPS system reduces the complexity of change management by analyzing the dependencies amongst the infrastructure components and determining the most performant change plans in an automatic manner. In security, risk management permits to assess the probability of a threat and to reduce the probability of vulnerabilities to be exercised by this threat. For instance, intrusion detection systems identify attacks or abnormal activities and generate alerts. In [10], a fuzzy-logic based technique permits to score and prioritize these alerts. In the meantime, standardized languages such as OVAL (Open Vulnerability Assessment Language) serve as a support for specifying, identifying and treating vulnerable configurations in systems and networks [11].

A few of approaches address risk management in VoIP networks and services. In [12], the authors propose to estimate the risk of interceptions in VoIP infrastructures. This risk assessment is performed before the deployment of the network. It models the possible threats to the system based on attack tree and the vulnerabilities are identified based on dependency graphs. It estimates based on this model the exploitability of each vulnerability and determines the main risk factors related to the interception of VoIP calls. This assessment is performed in a static manner. A large variety of methods and techniques permit to determine the potentiality of an attack at runtime, but they do not integrate explicitly a risk model. Typically intrusion detection and prevention systems have been proposed to deal with SPIT attacks. In [13], the approach is capable of controlling SPIT attacks based on multi-gray leveling technique applied to the number of calls per time unit. This solution only focuses on the assessment of VoIP users, their classification based on a greyscale and the determination

of when they have to be blocked. The objective is limited to the detection of users. The approach does not discuss how to apply a progressive treatment based on this detection, does not integrate a risk model and relies on a single detection criterion.

Other approaches have been designed to prevent SPIT attacks. For instance, [14] describes a solution for managing communications based on consent. The caller asks first to be added to the list of authorized contacts. This schema has an important impact on the service usability as the users may receive many consent requests. In order to deal with SPIT, the IETF Sipping group suggests defining two new SIP headers [15]: an identity header to provide a certificate of identity and an identity-info header to indicate the authority which signed this certificate. Another schema consists in building circles of trust by using TLS connections. This approach is very useful in a proxy-to-proxy scenario, but poses many scalability issues. In [16] and [17], a socio-technical defense strategy consists in applying a multi-step adaptive filter based on the presence, the trust and the reputation of callers. It relies on the intuitive human behavior of accepting or rejecting a call based on its direct and indirect relations with the caller. In [18] the authors propose an holistic framework for countering SPIT attacks. Detection and protection modules are applied in a dynamic manner at different stages i.e. before, during and after the call. These solutions do not explicitly integrate risk models. They can be seen as possible safeguards to be activated based on our risk management solution. For instance, communications established by consent (list of authorised contacts) could only be activated when the risk level is important in the network.

VII. Conclusions and Future Work

Telephony over IP is a critical service exposed to multiple security threats. Protection mechanisms exist but may seriously deteriorate the service performance. Applying risk management methods and techniques to VoIP infrastructures provide new opportunities for addressing the trade-off between security and quality of such sensitive services. In that context, we have designed a runtime risk management solution for automatically and continuously adapting the exposure of VoIP equipment to the network risk level. This exposure is controlled by the activation and deactivation of safeguards in a graduated manner based on a dedicated risk model. This permits to prevent potential risks while maintaining the quality of the VoIP service. We have specified the architecture composed of an intrusion detection system, a risk manager and a configuration platform. This architecture improves the coupling between the detection of attacks and the application of treatments. We have extended the Rheostat formal risk model to VoIP networks and services and have identified a subset of safeguards. We have shown how the restriction and relaxation algorithms permit to provide an adequate and progressive response to risks by exploiting safeguards at runtime. The activation of a safeguard reduces the exposure when the potentiality of an attack increases, while the deactivation reduces the impact of protection mechanisms on the quality of service. We have evaluated the performance of our solution through an implementation prototype and a set of experimental results obtained in the case scenario of SPIT attacks. We have determined the impact of the two algorithms on the risk level and have quantified the benefits of our solution in comparison with traditional approaches. We have also experimented different temporal behaviors of SPIT attacks. The integration of risk models to detection and prevention systems clearly contributes to a more appropriate response to threats for these critical services. We observed a benefit of up to 41% in terms of risk in the best cases. In future work we are planning to apply and experiment our risk management solution to a larger scope of VoIP threats. We are also interested in investigating techniques for efficiently combining security safeguards, developing autonomic mechanisms for dynamically adapting the formal risk model and performing complementary experiments for refining the risk parameters.

References

[1] VOIPSA, Voice over IP Security Alliance, http://www.voipsa.org.

[2] A. Gehani and G. Kedem, "RheoStat: Real Time Risk Management," in *Proc. of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04)*, Springer, 2004.

[3] T. Bedford and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*, 2001.

[4] M. Modarres, *Risk Analysis in Engineering: Techniques, Trends, and Tools*. Taylor & Francis Editions, 2006.

[5] H.-J. Kim, M. J. Kim, Y. Kim, and H. C. Jeong, "DEVS-Based Modeling of VoIP Spam Callers' behavior for SPIT level Calculation," *Elsevier Journal on Simulation Modelling Practice and Theory*, Sep 2008.

[6] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems," National Institute of Standards and Technology, Tech. Rep., July 2002.

[7] ISO/IEC 27005, Information Security Risk Management, http://www.iso.org.

[8] J. Sauve, R. Santos, R. Reboucas, A. Moura, and C. Bartolini, "Change Priority Determination in IT Service Management Based on Risk Exposure," *IEEE Transactions on Network and Service Management*, vol. 5, no. 3, September 2008.

[9] A. Keller, J. Hellerstein, J. Wolf, K. Wu, and V. Krishnan, "The CHAMPS System: Change Management with Planning and Scheduling," in *Proc. of IEEE/IFIP Network Operations and Management Symposium (NOMS'04)*, April 2004.

[10] K. Alsubhi, E. Al-Shaer, and R. Boutaba, "Alert Prioritization in Intrusion Detection Systems," in *Proc. of IEEE/IFIP Network Operations and Management Symposium (NOMS'08)*, April 2008.

[11] OVAL, Open Vulnerability Assessment Language, Mitre Corporation, http://oval.mitre.org.

[12] M. Bunini and S. Sicari, "Assessing the Risk of Intercepting VoIP Calls," *Elsevier Journal on Computer Networks*, May 2008.

[13] D. Shin and C. Shim, "Progressive Multi Gray-Leveling: A Voice Spam Protection Algorithm," *IEEE Network Magazine*, vol. 20, p. 18.

[14] R. Macintosh and D. Vinokurov, "Detection and Mitigation of Spam in IP Telephony Networks using Signaling Protocol Analysis," in *Proc. of the IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication (SAWWC'05)*, April 2005.

[15] J. Peterson and C. Jennings, Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), IETF Request for Comments 4774, 2008.

[16] P. Kolan and R. Dantu, "Socio-Technical Defense against Voice Spamming," *ACM Transactions on Autononous and Adaptive Systems*, vol. 2, no. 1, 2007.

[17] T. Peng, M. Luo, and C. Leckie, "CPU-Based DoS Attacks against SIP Servers," in *Proc. of IEEE/IFIP Network Operations and Management Symposium (NOMS'08)*, April 2008.

[18] N. d'Heureuse, J. Seedorf, S. Niccolini, and T. Ewald, "Protecting SIP-based Networks and Services from Unwanted Communications," in *Proc. of IEEE Global Telecommunications Conference (GLOBECOM'08)*, Dec 2008.