Risk Management for Spam over IP Telephony using Combined Countermeasures

R. Jabeur Ben Chikha
University of Carthage
Digital Security RU, Sup'Com
Tunis, Tunisia
randa.jabeur@supcom.tn

Tarek Abbes
University of Carthage
Digital Security RU, Sup'Com
Tunis, Tunisia
abbes.tarek@gmail.com

Adel Bouhoula
University of Carthage
Digital Security RU, Sup'Com
Tunis, Tunisia
bouhoula@gmail.com

ABSTRACT

Voice over IP (VoIP) is a very attractive technology. It is increasingly adopted by enterprises and consumers. VoIP inherits adjacent security issues to IP networks to which are added new specific problems. Spam over IP telephony (SPIT) is expected to become one of the VoIP problems. To resolve it, many anti-SPIT mechanisms are proposed but there are still limited in some cases. Indeed, these mechanisms can deteriorate the performances of the telephony service in terms of availability and quality of service. Thus, Risk management offers new perspectives regarding this dilemma. We adopt in this paper a risk management strategy to protect a VoIP infrastructure. To treat the risk, we employ in the first phase a set of combined countermeasures. In addition, we apply a known metric called "Return On Response Investment" (RORI) to provide the most optimal combination that reduces the risk without sacrificing the functionality of the system. The efficacy of our solution is demonstrated through a set of experimental results.

CCS Concepts

•**Software and its engineering** → **Risk management;**
•**Security and privacy** → *Intrusion detection systems;*

Keywords

VoIP, SPIT, Risk Management, RORI metric, Combined Countermeasures.

1. INTRODUCTION

Voice over IP (VoIP) offers several features and high flexibility to enterprises and consumers compared to traditional telephony. Indeed, it is a technology that allows both voice communication and multimedia sessions over internet protocol (IP) networks. In VoIP communications, Session Initiation Protocol (SIP) is adopted in signaling protocol while Real Time Transport Protocol (RTP) is used in media transmission. SIP aims to establish, modify and terminate multimedia sessions. It also handles the authentication of participants and the media type.

In SIP signaling environment, it is very easy for an attacker to transmit an abnormal number of calls solicitations (SIP INVITE) to the server. Spam over IP telephony (SPIT) is a Deny of Service attack which aims to exploit the weaknesses of SIP protocol. An attacker uses SPIT calls because of its low cost and high efficiency. Thus, he annoys VoIP users and overloads the network with a huge amount of messages.

In light of this, a large number of SPIT-mitigation methods have been introduced to detect and counter SPITters. The suggested methods include list-based filtering [23], fingerprinting [31], reputation systems [21], turing tests [28], call-frequency based [29] and the use of sophisticated machine learning [25, 26].

However, detection methods quickly reach their limits in terms of sensitivity and specificity. Moreover, the protection mechanisms can have a negative impact on the performances of the telephony service in terms of operational continuity and quality of service. Risk management offers new perspectives regarding this problematic. Indeed, it allows managing the trade-off between security and quality of service, which are both crucial for VoIP.

This paper deals with the implementation of a risk management solution in VoIP infrastructure. To apply our risk management process, we have to follow these steps: identify, estimate and treat the risk. The main contributions of our approach are as follows: (1) the use of combined countermeasures to counter complex SPIT attacks, (2) the application of return on response investment (RORI) index that guarantee the choice of the most appropriate combined solution to reduce the risk without sacrificing the functionality of system.

The rest of the paper is organized as follows. In Section 2, we introduce the concept of risk management. A combination of countermeasures is mathematically described in Section 3. In Section 4, we explain the use of the RORI index. We introduce our proposed risk management model in Section 5 then we present our experimental results in Section 6. Section 7 describes some related works about risk management in VoIP environment. Finally, Section 8 summarizes this work and enumerates some future works.

2. RELATED WORKS

To support risk management, three main models have been suggested: quantitative models, qualitative models and mixed models. The quantitative models provide a quantita-

INFOS '16, May 09-11, 2016, Giza, Egypt
 ISBN 978-1-4503-4062-5/16/05…$15.00
DOI: http://dx.doi.org/10.1145/2908446.2908486

tive value of risk. Thus qualitative models present the risk as a qualitative level. Finally, the mixed models represent a combination of the two previous [24]. Risk management is typically defined as the management process, which consists in assessing the risk and treating it [8].

Regarding risk assessment in VoIP network, many previous works have proposed. Benini et al. present in [4] a model of risk attached to the interception of VoIP calls. The scenario is perceived as a major threat for companies that decide to migrate from traditional telephony to VoIP services. Thus, the authors use an attack tree to model the threat and vulnerabilities dependency graphs to consider related vulnerabilities. The method estimates the exploitability of each vulnerability and identifies the risk factors related to the interception of VoIP calls. However, it omits the potentiality of the attack, which is an important parameter.

In [9], Dantu et al. consider that the sequence of actions that an attacker performs in a VoIP network depends on its social status (for example his skills level, tenacity and financial capacity). Thus, they conceive a security mechanism to evaluate the risk level of critical resources that could be compromised. This evaluation is performed using attacks behavior graphs that represent all possible attacks paths on critical resources. The level of risk is calculated using these graphs and a quantification of vulnerabilities. The risk for a host is the sum of risks that it faces on its assets. Thus, the risk level provides an effective basis to make the appropriate changes to network configuration. This approach allows only a partial modeling of risk in the VoIP infrastructure. Indeed, the risk model does not quantify the consequences incurred in the case of successful attack, although this is an important element of such model [2].

Dabbebi et al. present in [7] 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. The model relies on VoIP properties and the algorithms for restricting and relaxing of the risk level. The model contributes to reduce attacks (in this case, SPIT attack) while maintaining the quality and availability of such critical service.

Other previous works related to risk treatment, study how to reduce and mitigate the risk by applying adequate protection and prevention systems [17]. They also try to eliminate the risk (risk avoidance) by applying standard's recommendations and best practices, to shift it (risk transfer) by subscribing to insurances or simply to accept it (risk retention) in some cases [2].

The closest work to us is that of Dabbebi et al. [7] since we adopt their risk management model. However, we treat differently the risk. Indeed, to reduce the impact of SPIT attack without sacrificing the functionality of the system, we search for the best combined countermeasures solution. This combination is selected depending on the RORI index which guarantees the most appropriate reaction.

3. CONCEPTS OF RISK MANAGEMENT

3.1 Terminology

In order to use the concept of security risk management, we must first establish a baseline of related terms. In the following, we give some important definitions.

Assets

According to ISO / IEC 27005 [2], an asset is anything that has a value or a technical challenge for infrastructure and services. In the context of VoIP, the concept of asset applies to register, User Agent (UA), database location and call history. In addition, assets include all that is in direct relation with the operation process, such as UA registration, establishment of the session, user location and routing call.

Threat

A threat is a source of attack that can cause a deterioration of the asset.

Vulnerability

A vulnerability is a weakness that allows the threat to make an attack on the service.

Attack

A security attack is defined as the intersection of three elements [10] namely: a set of exploitable vulnerabilities in the service, an attacker that can access to vulnerabilities (motivated by financial reasons such as free calls) and the ability of the attacker to exploit the flaw.

Risk

According to [2, 30], the risk is the possibility that a given threat exploits vulnerabilities of an asset to generate a malfunction or deterioration of the concerned service.

Risk Management

Risk management is the process of identifying the risk, assessing and evaluating it, and taking steps (security safeguards) to reduce it to an acceptable level [2]. According to ISO 27000, risk management refers to a coordinated set of activities, methods, and techniques that organizations use to deal with the risk and uncertainty that influences how well they achieves their objectives.

3.2 Risk Management Process

The risk management process includes three steps: risk identification, risk assessment and risk treatment. The purpose of risk identification is to identify critical assets, potential threats and vulnerabilities of the concerned service.

The risk assessment includes estimating the potentiality of the attacks and their impacts. The first term relates to the probability of occurrence of risk and the second one represents the induced consequences if the attack succeeded in achieving its goal.

Finally, the risk treatment includes a set of methods aimed to reduce the risk to an acceptable level. There are several ways to treat the risk. The first is to accept the risk without any treatment. The second is to avoid the risk by eliminating the cause (i.e., all vulnerabilities exploited by the threat). The third is to reducing the risk by applying a set of countermeasures. Finally, the last is to transfer the risk to a third party such as insurance that covers induced damage.

In the proposed system, we will either accept the risk or reduce it by applying a set of countermeasures. In this context, we suggest to employ multiple countermeasures as a single treatment to counter the consequence of complex attacks.

In the following, we will mathematically detail the concept of a "combination of countermeasures" as a single treatment.

4. COMBINATION OF COUNTERMEASURES

A combination of countermeasures is the result of applying simultaneously two or more safeguards to counter attack. Mathematically, to combine multiple countermeasures, we need to calculate their union and intersection area. In the following, the countermeasure is considered as an event. The probability of an event corresponds to the likelihood of its occurrence. We distinguish two cases to define the occurrence of multiple events: mutually exclusive and non-mutually exclusive events.

4.1 Mutually Exclusive Events

In this case, events are mutually exclusive if they cannot occur simultaneously. Let's consider $A_1, ..., A_n$ a sequence of n events, the probability of union of multiple events is shown as [27]:

$$P(\bigcup_{i=1}^{n} A_i) = \sum_{i=1}^{n} P(A_i) \tag{1}$$

and the intersection is represented as:

$$P(\bigcap_{i=1}^{n} A_i) = 0. \tag{2}$$

4.2 Non-Mutually Exclusive Events

In this case, all events can occur in the same time. For that, let's consider $A_1, ..., A_n$ a sequence of n events, then union of multiple events is shown as [27]:

$$\begin{aligned} P\left(\bigcup_{i=1}^{n} A_i\right) \simeq & \sum_{k=1}^{n} P\left(A_k\right) - \sum_{i<j} P\left(A_i \cap A_j\right) + \\ & \sum_{i<j<k} P\left(A_i \cap A_j \cap A_k\right) + ... + \\ & (-1)^{n+1} P\left(A_1 \cap A_2 \cap ... \cap A_n\right) \end{aligned} \tag{3}$$

and the intersection is represented as:

$$P\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} P\left(A_i\right) \tag{4}$$

A combination of countermeasures can be chosen based on cost-sensitive metrics. In our proposal, we will use the Return On Response Investment (RORI) index to select the most appropriate combination.

5. RETURN ON RESPONSE INVESTMENT (RORI)

Cost sensitive metrics are widely proposed as a viable approach to find an optimal balance between intrusion damages and response costs, and to guarantee the choice of the most appropriate response without sacrificing the system functionalities [13]. In the following, we will describe in detail the RORI (Return On Response Investment) cost-sensitive metric.

5.1 Definition of RORI

RORI is a service dependency model for cost sensitive response based on financial comparison of the response alternatives [18, 19]. RORI provides a qualitative comparison of response against an intrusion. It is an adaptation of the ROSI (Return On Security Investment) index. The RORI index was firstly introduced by Kheir et al. [18, 19]. [14] proposes an improvement of the RORI index by taking into account the expected losses that may occur as a consequence of an attack and the infrastructure value. The improved RORI index can be written as

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100, \tag{5}$$

where ALE is the Annual Loss Expectancy and refers to the impact cost obtained in the absence of security measures, RM refers to the Risk Mitigation level associated to a particular solution, ARC is the Annual Response Cost that is incurred by implementing a new security action and AIV is the Annual Infrastructure Value that is expected from the system, regardless of the implemented countermeasures. Here, ALE depends directly on the attack's severity and likelihood.

5.2 Specification of RORI parameters

The RORI metric is considered as a quantitative approach to evaluate and select the best countermeasure that mitigates the effects of a given attack. The calculation of RORI parameters follows the approaches proposed by Kheir et al. [18] for the RORI model as well as Kosutic [22] and Lockstep Consulting [1] for the ROSI model. The rest of this subsection details each parameter in the case of individual countermeasure and a combination of countermeasures.

5.2.1 Case of individual countermeasure

Annual Loss Expectancy (ALE): ALE refers to the Impact Cost that is produced in the absence of countermeasures. The ALE can be expressed as

$$ALE = SLE \times ARO. \tag{6}$$

where SLE (Single Loss Expectancy) represents all expected losses (assets, data, etc.) and ARO is the annual rate of occurrence.

To estimate ALE, we adopt the approach proposed by Lockstep [1]. This solution converts qualitative estimations of severity (SLE) into quantitative values of costs. In the same way, it transforms the likelihood of an incident into *ARO* parameter.

According to [1], TABLE 1 and TABLE 2 show respectively the Severity transformed to probabilistic Costs and the Likelihood transformed to Probabilistic *ARO* .

Table 1: Severity transformed to probabilistic Costs

Severity	Cost
Insignificant	0€
Minor	1,000€
Significant	10,000€
Damaging	100,000€
Serious	1,000,000€
Grave	10,000,000€

Table 2: Likelihood transformed to *ARO*

Likelihood	*ARO*
Negligible	0.05
Very Low Likely	0.50
Low Likely	1.00
Medium Likely	2.00
High Likely	12.00
Very High Likely	50.00
Extreme Likely	500.00

Risk Mitigation (RM): RM refers to the risk mitigation associated with a given countermeasure. The RM is given by

$$RM = SC \times EF. \tag{7}$$

where SC (Surface Coverage) is the percentage of the attack surface that is covered and controlled by a given countermeasure and EF (Effectiveness Factor) represents the percentage of reduction of the total incident cost that is given from the enforcement of a security measure.

To ensure the calculation of RM, we need to compute the countermeasure surface coverage and then, its level of effectiveness.

According to Microsoft SDL Team [3], the surface coverage represents the percentage of assets and threats that are controlled by a given countermeasure. In the proposed system, the surface coverage is considered as the percentage of attack detection.

We follow the rheostat [11] approach in order to quantify the Effectiveness Factor (EF). This approach defines the risk of an attack (R) as the product of its Exposure (E), Potentiality (P), and consequence (C), (i.e., $R = E \times P \times C$). Therefore, the Effectiveness Factor (EF) is considered as the risk reduction percentage resulting from the applying a given countermeasure. For instance, let's assume that $R_{before} = 0.25$ as the risk of a given attack before application of countermeasures and $R_{after} = 0.11$ as the risk resulting after the application of a given countermeasure. The Effectiveness is then given by: $EF = 100 - \frac{(R_{after} \times 100)}{R_{before}} = 56\%$.

Annual Response Cost (ARC): ARC refers to the all costs associated to a given countermeasure (cost of implementation, cost of maintenance and cost of damage). To estimate the Annual Response Cost (ARC) parameter, we identify direct and indirect costs. Based on educated expert knowledge and statistical data, it is possible to determine each element composing the ARC.

Annual Infrastructure Value (AIV): AIV represents the sum of security tools costs (i.e. Equipment cost, Personnel cost, Service cost) that are expected on the system regardless of the implemented countermeasure. It is calculated as the total of the annual value of all preliminary security equipments (i.e. Policy Enforcement Points (PEP)). These equipements ensure an acceptable level of security in the first phase of the system architecture. The AIV includes the cost of purchasing, licensing, and/or leasing the security equipments in a given organization.

5.2.2 Case of combined countermeasures

In this case, the values of ALE and AIV remain unchanged. Indeed, these two parameters depend on the considered attack. However, the combination of two or more countermeasures affects the values of RM and ARC. In the following, based on [13], we assess RM and ARC in the context of countermeasures combination.

Combined ARC: The cost of a combined countermeasure is defined as the sum of all individual countermeasure's cost. It can be expressed as:

$$ARC\left(\bigcup_{i=1}^{n} C_i\right) = \sum_{i=1}^{n} ARC\left(C_i\right), \tag{8}$$

where C_i is the individual countermeasure.

Combined RM: The combination of RM is only allowed when the countermeasures are not mutually exclusive and the surface of one countermeasure is not totally covered by another countermeasure. In this case, the risk mitigation is calculated by referring to (1) and given by

$$\begin{aligned} RM\left(\bigcup_{i=1}^{n} C_i\right) &= \sum_{k=1}^{n} RM\left(C_k\right) - \sum_{i<j} RM\left(C_i \cap C_j\right) + \\ &\sum_{i<j<k} RM\left(C_i \cap C_j \cap C_k\right) + ... + \\ &(-1)^{n+1} RM\left(C_1 \cap C_2 \cap .... \cap C_n\right) \end{aligned} \tag{9}$$

RM are replaced by their expressions, the equation becomes

$$\begin{aligned} &RM\left(\bigcup_{i=1}^{n} C_i\right) = \sum_{k=1}^{n} SC\left(C_k\right) \times EF\left(C_k\right) - \\ &\sum_{i<j} SC\left(C_i \cap C_j\right) \times EF\left(C_i \cap C_j\right) + \\ &\sum_{i<j<k} SC\left(C_i \cap C_j \cap C_k\right) \times EF\left(C_i \cap C_j \cap C_k\right) + .. + \\ &(-1)^{n+1} SC\left(C_1 \cap ... \cap C_n\right) \times EF\left(C_1 \cap ... \cap C_n\right). \end{aligned} \tag{10}$$

The surface coverage of the intersection is calculated as the average of the lower and upper bounds:

$$SC\left(\bigcap_{i=1}^{n} C_i\right) = \frac{SC\left(\bigcap_{i=1}^{n} C_i\right)_{low} + SC\left(\bigcap_{i=1}^{n} C_i\right)_{up}}{2}, \tag{11}$$

where

$$SC\left(\bigcap_{i=1}^{n} C_i\right)_{low} = \begin{cases} 0 & if \sum_{i=1}^{n} SC\left(C_i\right) \leq n-1 \\ \sum_{i=1}^{n} SC(C_i) - (n-1) & if \sum_{i=1}^{n} SC\left(C_i\right) > n-1 \end{cases} \tag{12}$$

and

$$SC\left(\bigcap_{i=1}^{n} C_i\right)_{up} = min\left\{SC\left(C_1\right), .., SC\left(C_n\right)\right\}. \tag{13}$$

The Effectiveness of the intersection is calculated by con-

sidering the upper bounds and is given by

$$EF\left(\bigcap_{i=1}^{n} C_i\right) = EF\left(\bigcap_{i=1}^{n} C_i\right)_{up} = min\left\{EF\left(C_1\right), .., EF\left(C_n\right)\right\} \quad (14)$$

6. PROPOSED RISK MANAGEMENT

In this section, we propose a new concept of risk management in VoIP networks and services. To evaluate the effectiveness and feasibility of our approach, we consider the SPIT attacks scenario (see Figure 1). Our purpose is to perform a set of combined countermeasures that reduces the risk with a reasonable cost. To achieve the proposed risk management process, we should apply three main steps, namely the risk identification, the risk estimation and the risk treatment. For the identification of risk, an intrusion detection system is essential. After that, the implementation of the last two steps requires several elements that are a risk model, mitigation algorithms and a set of countermeasures.

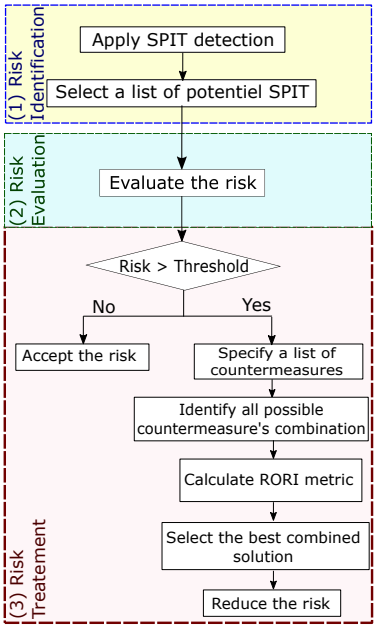

Figure 1: Proposed Risk management

6.1 Identification step

In this step, we apply the SPIT detection method introduced in [5, 6]. According to this method, we collect network traces of signaling and voice activities. These traces are useful to extract the identification criteria of SPIT attacks such as Call rejection rate, Call recipient rate, Call duration rate, Call traffic rate, Call rate and Call inter-arrival time. After that, we use the AdaBoostM1 classifier (which gave the best detection rate in [6]) to reveal suspect activities identified as SPIT attacks.

6.2 Evaluation step

We choose a quantitative risk model to evaluate. This model is more significant for a critical and interactive service such as VoIP. Thus, it will allow us to have a clear idea about the risk level, and to automate the risk management processes. To develop our risk model, we rely on the formalism introduced by Rheostat [11]. We develop it to consider the properties of our VoIP infrastructure. The risk level can be expressed as:

$$R = \sum_{t_\alpha} P(t_\alpha) \times E(t_\alpha) \times C(t_\alpha), \quad (15)$$

where t_α is the signature of attack, $P(t_\alpha)$ is the potentiality of attack, $E(t_\alpha)$ is the host exposure to the threat depending on countermeasure and $C(t_\alpha)$ is the consequence of the attack on the VoIP infrastructure.

The attack potentiality is calculated using our SPIT detection system, which evaluates several parameters to decide the nature of a VoIP activity. The expression of the potentiality $P(t_\alpha)$ is defined as follow:

$$\begin{aligned} P(t_\alpha) &= \beta \times CallDuration_{Rate} + \gamma \times CallRejection_{Rate} \\ &+ \delta \times Callrecipient_{Rate} + \varepsilon \times Call_{Rate} \\ &+ \zeta \times Callinter_{Rate} + \eta \times Traffic_{Rate}, \end{aligned} \quad (16)$$

where $\{\beta, \gamma, \delta, \varepsilon, \zeta, \eta\}$ is a set of weighting factors specified based on the study described in [20].

The exposure of the VoIP infrastructure to a threat depends on the countermeasure that are activated or deactivated in the network. These safeguards are used to reduce the vulnerabilities of the VoIP service. The exposure $E(t_\alpha)$ is defined by

$$E(t_\alpha) = \sum_{o_\lambda \in \hat{P}(t_\alpha)} \frac{e\left(o_\lambda\right) \times i\left(o_\lambda\right)}{\left|\hat{P}\left(t_\alpha\right)\right|} \quad (17)$$

where $\hat{P}(t_\alpha)$ denotes the set of operations that are necessary to conduct an attack t_α, $e\left(o_\lambda\right)$ represents the initial exposure of a given operation $o_\lambda$and $i\left(o_\lambda\right)$ is the weight factor that quantify the impact of the activation or the deactivation of countermeasure. It takes the value of 1.0 if no countermeasure is activated and 0.0 if the operation is under control.

Finally, the consequence $C(t_\alpha)$ of the considered attack represents a normalized value that is important when multiple threats are in competition.

6.3 Treatement step

After evaluating the risk, we compare its current value with a threshold value $R_{threshold}$. If this value is less than $R_{threshold}$, the risk is accepted. Otherwise, a set of countermeasures were defined to reduce the risk. Some of these countermeasure are selected to be combined. This selection depends on the nature of countermeasure. Indeed, only non-restrictive countermeasures (can be perfectly combined) are choosed to be combined. After specifying the different possible combinations. We compute the RORI of each combination to select the optimal one. *Indeed, the most optimal combinaison corresponds to the most important value of RORI.*

7. EXPERIMENTAL RESULTS

In order to evaluate the performance of our solution, we take as an input the results of the SPIT detection system introduced in [6]. According to this study, 333 SPITters has been detected. We discover a SPITter with $\text{Spit}_{Level} = 0,48$ and $Impact = 0.4$. These SPIT attacks may be generated by

two different types of entities: humans that make calls for marketing purposes and bots that initiate sessions using a set of addresses.

Upon the SPIT attacks detection, we evaluate the risk level as follow: $R1 = P \times E \times C = 0.48 \times 1 \times 0.4 = 0.19$. We assume that the $R_{threshold} = 0.15$. Thus, we do not have to accept the risk but we need to select some candidate countermeasures to reduce it. To counter the SPIT attacks, we experiment five different countermeasures that are illustrated in TABLE 3. These countermeasures are firstly defined in [7].

Table 3: Countermeasures supporting our risk management in the case of SPIT attacks

Countermeasures	Exposure	Impact	EF
Sending a busy message to the caller	0.9	0.1	0.27
Asking the caller to put a particular code	0.7	0,4	0,70
Asking the caller to answer a specific question	0.6	0.5	0.82
Putting the caller on a waiting queue	0.3	0.8	0.98
Blocking the caller	0.1	0.9	0.99

In the first step, we compute the RORI index of each countermeasure to can select possible combination. The RORI parameters (ALE, AIV, RM, ARC) are evaluated as follows:

- The selected SPITter has an estimated "Medium" likelihood ($0.2 < Spit_{Level} < 0.5$) and a "Minor" severity level [7] (equivalent to 1000€) . Thus, the ARO correspond to 2 and the Annual Loss Expectancy (ALE) for this attack is expected to be 2000€.
- The Annual Infrastructure Value (AIV) is calculated as the total value of all the Policy Enforcement Points (PEP). These equipements are required to be deployed in the preliminary phase of the system architecture. We choose Snort as Network Intrusion Detection System with AIV=400€ and Cisco SA 500 Series as Intrusion Prevention System with AIV=1000€[12]. The AIV is therefore estimated as 1400€ (the cost of all the selected solutions).
- The Annual Response Cost ARC of each countermeasure is estimated based on its impact on the performance of the VoIP service. Thus, we use the Monte Carlo simulation approach as a solution of estimation. This approach uses a random sequence of numbers to construct a sample of the population, from which statistical estimates of the parameter are obtained [16]. After 250 iterations, we obtain the value of ARC of each countermeasure.

In the second step, we identify all possible countermeasures combinations. According to the first five ligne of table 4, C1 has a low value of RORI. Thus, C1 is excluded from combination. In addition, C5 is considered as restrictive countermeasure (can not be combined with other one). Thereby, we select C2, C3 and C4 as the candidates for combination. The set of all possible combination is evaluated as the sum of the n^{th} row of the binomial coefficients [15] that is expressed as: $\sum_{0<k<n} \binom{n}{k} = 2^n - 1 - n$ where n is the number of elements to be combined. For instance, for a group of 3 countermeasures (C2, C3 and C4), the maximum number of possible combinations are: $2^3 - 1 - 3 = 4$.

Table 4 gives a summary of parameters that build RORI index.

Table 4: Countermeasure Evaluation with ALE=2000€and AIV=1400€

Countermeasures	ARC	SC	EF	RM	RORI
C1	50€	0.1	0.27	0.027	0,29
C2	100€	0.3	0,70	0.221	21,57
C3	140€	0.4	0.82	0.328	33,50
C4	300€	0.7	0.98	0.687	63,22
C5	550€	0.9	0.99	0.891	63,17
C2+C3	240€	0,15	0,70	0,433	38,28
C2+C4	400€	0,15	0,70	0,793	65,92
C3+C4	440€	0,25	0.82	0,810	58,73
C2+C3+C4	540€	0,15	0,70	0,916	66,62

From the list of proposed combined countermeasures, the first alternative (C2+C3) has a minor effect on reduction of risk. As a result, the RORI value remains insignificant. Both combined solution C2+C4 and C2+C3+C4 provide a great reduction of the risk (79-91%). The RORI of C2+C4 and C2+C3+C4 is 65,92% and 66,62% respectively. We can show that the cost of implementation (ARC) of C2+C3+C4 is very high. However, its effect to reduce the risk is very important. For this reason, the RORI of C2+C3+C4 is the best.

As a conclusion, we can assume that the combination C2+C3+ C4 is the optimal solution that can be selected to counter the SPITter.

Conclusion

In this work, we proposed a new VoIP risk management process. We applied SPIT, as a scenario attack to evaluate the effectiveness and feasibility of the proposed approach. Our risk model included tree steps: the risk identification, the risk estimation and the risk treatment. In the first step, we employ an intrusion detection model based on AdaBoost classifier to detect SPIT attacks and evaluate their identification parameters. In the second step, we adopt the Rheostat model to evaluate the risk. Finally, we selected a combination of countermeasures as a solution to counter complex attack. For that, we employed the RORI metric in order to well choose the best combined solution and hence reduce the risk. The best combination of countermeasures is the one with the highest RORI. This solution appears to be a trade-off between security and cost. In our experiment, we show that the combination of three countermeasures represents the best solution against SPIT attack.

In a future work, we study the combination of countermeasures in multiple attack scenarios.

8. REFERENCES

[1] LOCKSTEP Consulting. A Guide for Government Agencies Calculating ROSI. Technical report, http://lockstep.com.au/library/return_on_investment.

[2] ISO/IEC 27005 Information technology – Security techniques – Information security risk management. Tech. rep., 2008.

[3] SDL Team Microsoft. Attack Surface Analyzer 1.0, http://blogs.msdn.com/b/sdl/archive/2012/08/02/attack-surface-analyzer-1-0-released.aspx.

[4] Benini, M., and Sicari, S. Assessing the risk of intercepting voip calls. *Computer Networks 52*, 12 (2008), 2432–2446.

[5] Chikha, B., Jabeur, R., Abbes, T., and Bouhoula, A. A spit detection algorithm based on user's call behavior. In *Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on* (2013), IEEE, pp. 1–5.

[6] Chikha, R. J. B., Abbes, T., Chikha, W. B., and Bouhoula, A. Behavior-based approach to detect spam over ip telephony attacks. *to appear in International Journal of Information Security* (2015), 1–13.

[7] Dabbebi, O., Badonnel, R., and Festor, O. Automated runtime risk management for voice over ip networks and services. In *Network Operations and Management Symposium (NOMS), 2010 IEEE* (2010), IEEE, pp. 57–64.

[8] Dabbebi, O., Badonnel, R., and Festor, O. Econometric feedback for runtime risk management in voip architectures. In *Managing the Dynamics of Networks and Services*. Springer, 2011, pp. 26–37.

[9] Dantu, R., Kolan, P., and Cangussu, J. Network risk management using attacker profiling. *Security and Communication Networks 2*, 1 (2009), 83–96.

[10] Dwivedi, H. *Hacking VoIP: protocols, attacks, and countermeasures*. No Starch Press, 2009.

[11] Gehani, A., and Kedem, G. Rheostat: Real-time risk management. In *Recent Advances in Intrusion Detection* (2004), Springer, pp. 296–314.

[12] Gonzalez-Granadillo, G., Garcia-Alfaro, J., Alvarez, E., El-Barbori, M., and Debar, H. Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the rori index. *Computers & Electrical Engineering 47* (2015), 13–34.

[13] Granadillo, G. D. G. *Optimization of cost-based threat response for Security Information and Event Management (SIEM) systems*. PhD thesis, Institut National des Télécommunications, 2013.

[14] Granadillo, G. G., Débar, H., Jacob, G., Gaber, C., and Achemlal, M. Individual countermeasure selection based on the return on response investment index. In *Computer Network Security*. Springer, 2012, pp. 156–170.

[15] Grimaldi, R. P. *Discrete and Combinatoral Mathematics: An Applied Introduction 2nd Ed.* Addison-Wesley Longman Publishing Co., Inc., 1989.

[16] Halton, J. H. A retrospective and prospective survey of the monte carlo method. *Siam review 12*, 1 (1970), 1–63.

[17] Heureuse, N. D., Seedorf, J., Niccolini, S., and Ewald, T. Protecting sip-based networks and services from unwanted communications. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (2008), IEEE, pp. 1–5.

[18] Kheir, N. *Response policies and countermeasures: Management of service dependencies and intrusion and reaction impacts*. PhD thesis, PhD thesis, Ecole Nationale Supérieure des Télécommunications de Bretagne, 2010.

[19] Kheir, N., Cuppens-Boulahia, N., Cuppens, F., and Debar, H. A service dependency model for cost-sensitive intrusion response. In *Computer Security–ESORICS 2010*. Springer, 2010, pp. 626–642.

[20] Kim, H.-J., Kim, M. J., Kim, Y., and Jeong, H. C. Devs-based modeling of voip spam callers' behavior for spit level calculation. *Simulation Modelling Practice and Theory 17*, 4 (2009), 569–584.

[21] Kolan, P., and Dantu, R. Socio-technical defense against voice spamming. *ACM Transactions on Autonomous and Adaptive Systems (TAAS) 2*, 1 (2007), 2.

[22] Kosutic, D. Is it possible to calculate the return on security investment (rosi),in http://blog.iso27001standard.com/2011/06/13/is-it-possible-to-calculate-the-return-on-security-investment-rosi/, 2011.

[23] Mathieu, B., Niccolini, S., and Sisalem, D. Sdrs: a voice-over-ip spam detection and reaction system. *Security & Privacy, IEEE 6*, 6 (2008), 52–59.

[24] Modarres, M. *Risk analysis in engineering: techniques, tools, and trends*. CRC press, 2006.

[25] Nassar, M., Dabbebi, O., Badonnel, R., and Festor, O. Risk management in voip infrastructures using support vector machines. In *Network and Service Management (CNSM), 2010 International Conference on* (2010), IEEE, pp. 48–55.

[26] Nassar, M., Festor, O., et al. Monitoring sip traffic using support vector machines. In *Recent Advances in Intrusion Detection* (2008), Springer, pp. 311–330.

[27] Olofsson, P., and Andersson, M. *Probability, statistics, and stochastic processes*. John Wiley & Sons, 2012.

[28] Schlegel, R., Niccolini, S., Tartarelli, S., and Brunner, M. Ise03-2: Spam over internet telephony (spit) prevention framework. In *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE* (2006), IEEE, pp. 1–6.

[29] Shin, D., Ahn, J., and Shim, C. Progressive multi gray-leveling: a voice spam protection algorithm. *Network, IEEE 20*, 5 (2006), 18–24.

[30] Stoneburner, G., Goguen, A., and Feringa, A. Risk management guide for information technology systems: Recommendations of the national institute of standards and technology, retrieved november 25, 2009, 2002.

[31] Yan, H., Sripanidkulchai, K., Zhang, H., Shae, Z.-Y., and Saha, D. Incorporating active fingerprinting into spit prevention systems. In *Third annual security workshop (VSW'06)* (2006), Citeseer.