User-Profile Framework against a Spit Attack on VoIP Systems

Marialisa Scatá, Aurelio La Corte
Department of Electrical, Electronics and Computer Science
Engineering Faculty of Engineering, University of Catania
via le A.Doria 6, 95125 Catania, Italy

Abstract

Spam over Internet Telephony is becoming a large problem of the Voice over IP Architectures. Voice over IP has become a valid alternative to the Public Switched Telephone Network and it has a new paradigm for providing telephony services at a lower cost and higher flexibility. In the meantime, with Voice over IP the privacy becomes so hard and the benefits introduced are as strong as the security problems, like Spam over Internet Telephony. People have more attention on the spam voice issue, because of the great danger of this threat. Thus, in this paper we want to propose and introduce a new protection model against Spam over Internet Telephony attack, through a user-profile framework. This framework allows to identify the optimal countermeasures to be taken against this threat, according to the user assessment, that receives a certain number of calls during an observation period. We define general profiles based on certain parameters, and with a user-profile matching we can identifies the best security path which must be applied.

1. Introduction

The communication is the driving force of the society through a network and the information is the most important asset [1][2]. The meaning of communication is always the same but over the years, information has always changed in form. The need to communicate quickly and in real-time increases everyday, and, to be able to access any type of resource from anywhere and share information as safely as possible has become very important. Meanwhile, the next future requires a revolution of communications in the integration of services,through convergence of technologies to be closer to the user, simplifying the plurality of resources, thus offering convergence embedded in quick and easy sharing. There is a global and highly competitive environment, and ICT can provide a real advantage for competitive decisions. The evolution of ICT has been characterised by several evolving trends that support today's information and communication society, with multidisciplinary coordination and cooperation. One scenario in particular necessitates further investigation: ICT in communications. Information and Communication Technology pervaded all critical infrastructure and it is applied in various fields and it allows innovative solutions for emerging technologies, to support strategical decisions, management processes and security.Thus, the design of an information system must address issues related to planning an ICT infrastructure. In this context, telephony, internet, wired and wireless access and convergence are the new items of interest because each of them plays a key role in our lives. These technologies drive the economy and mostly business processes, and the daily lives.A telecommunication network capable of providing multimedia, convergence, mobility and personalisation, must face technological challenges not only to try to introduce more specialised networks, but also efficient networks. Meanwhile, in any network that allows the dynamic exchange of information the problem of security is as strong as its weakest link. Despite the growing interest in the research regarding communication security concerns, the target has always been to protect the computer world and, a consolidated study of the degree of security of an ICT system is still lacking. Voice over IP (VoIP) technology has a key role in the development of convergence in the near future, but with VoIP, to ensure privacy is extremely difficult [3][4][5]. In this paper, we investigate about the security issues of communication systems and about VoIP. We identify Assets, Threats and Vulnerabilities, and we investigate about Spam over Internet Telephony (Spit) attack. Then, we propose a user-profile framework to evalute the appropriate countermeasure which has to be used.

2 Communication Security Issues

Since the invention of the first telephone by Alexander Graham Bell in 1869, network telephony technology did not stop evolving: from circuit switching to packet switching, from fixed network to wireless network. However the functionality of the telephone system has not improved because the basic operation is always the same, but over the years several new architectures were created. These combine the transport of voice, data and images in the same data network to obtain the total convergence step-by-step. Voice over IP (VoIP) is one of the most emerging technologies, it has become an essential paradigm for providing telephony services because it introduces many benefits. This technology includes a large variety of methods and tools,enabling the transmission of voice through packet-switched network. The benefits of Voip are lower costs, centralized management, rapid deployment, higher flexibility,reducing infrastructure,convergence of voice and data, higher voice quality, seamless integration with the existing IP network, no need expensive end-terminal, computer-based soft-phones, etc. This technology will represent an advantage for the business and private networks with greater flexibility. The nature of these technologies has a serious impact on the voice in terms of security despite the huge amount of benefits. Attackers tipically target the most popular applications and VoIP has become one such application. By exploiting vulnerabilities, the probability that a threat will successfully attack a system is increasingly high. This probability increases with the value of the information. Therefore, the importance of security is directly proportional to the value of information in any communication system. A security analysis of communication systems is lacking because these systems, starting from PSTNs(Public Switched Telephone Networks) have never suffered from serious security problems. VoIP, which has become a valid alternative to the traditional telephone network is a technology that is being rapidly deployed but with many security problems. It is an economically viable, so care should be taken to ensure its security. The technology adds a third dimension to the voice communication. It exceeds and communicates with the PSTN and cellular networks. Security is one of the most important challenges in VoIP architectures, in comparison with traditional telephony where the safety is guaranteed by the physical layer. PSTN is a network, that interconnect elements over dedicated circuit-switched, based on closed infrastructure and so, the access is limited. It requires very high cost to access to the core network. The IP network has many kinds of weaknesses, related to the core of the infrastructure. The process of evolution of telecommunications systems towards the convergence is coming out through the development of the next generation network or NGN [6]. Convergence is the process of evolution of telecommunications networks[6]. The combination of multimedia and information and communication technologies, the growing digital traffic, the growing use of Internet and multimedia services and the need to converge networks and the existing fixed and mobile services will allow in the near future the total convergence of the triple play services (voice,video,data), quadruple play (voice, video, data and mobile communications) and transport over IP (All IP). Nowadays, when we talk about this we could refer to the idea of next generation network or NGN [6]. In accordance with the definition of ITU, a Next Generation Network is a packet-based network able to provide Telecommunication Services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users. In other words, if today, for each type of service, we use different infrastructures, a single NGN transport network will support all types of service. The service will become independent from the network: there will be no differences between fixed and mobile networks. Voice, internet, email and video will be available whether we are outdoors or indoors.Among the basic requirements of NGN we can mention the following:

- supply of each type of service: multimedia, data, video, telephone, mobile
- functions dedicated to service separate from those dedicated to transmission
- interworking with existing networks
- support to mobile users
- independence from a variety of network access

To achieve this we need a simplification of the protocols, while ensuring the unification of the treatment of different access mechanisms currently in use. NGN has been developed to take into account of new challenges of the telecommunication world. The NGN and the future New Generation Network (NWGN) want to become a network capable of providing multimedia, pervasiveness, mobility and personalization. The convergence allows to combine the benefits but also several issues. The NGN will be designed to add the benefits of all the technologies and services that will be provided. At the same time the vulnerabilities will increase and it gives space to new threats, unknown today. This will result in a limit for the future of converged networks, and a constraint on economic investments conveyed in this development. Accordingly, the telecommunications have to face technological challenges not only to try to introduce

the optimal convergence, but also more efficient security networks. VoIP technology has a key role in the development of convergence in the near future, because is the first step towards the future converged networks. However, the convergence contradicts one of the fundamental principle of security, to have different and redundant systems. The concept of convergence has been developed to take account of new challenges, new realities and the growing of digital traffic and multimedia services. Thus, the research interest pays more attention to the detection of the security problems, because of the probably great danger of a successfully attack.

3 Related Work

A large variety of detection and protection mechanisms have been developed for identifying and blocking VoIP security threats. Despite the growing interest of the research about security issues of communication systems, detection methods have many limits in terms of efficiency. About VoIP security we surveyed many research papers, such us [3][4][5]. We have identified the general tendency that protection mechanisms are often harsh and may have impact on the performance and quality of service of the systems. The VoIP attacks can tipically be classified into four main categories[3]. Among the most dangerous VoIP-specific attacks, social threats, like Spit, are becoming reality. Social Threats are attacks, which disturbs for the users through unsolicited communications. In recent years, with the rise of Internet Telephony, many sponsors use VoIP for many reasons like low-cost calls, ID-disguised, untraceable. Thus, they frequently send several automatic calls for advertisement, or even frauds sensitive informations of the users, sometimes leading to denial of service. About Spit Detection there are some valuable research results and detection methods [7][8][9][11], which in general can be divided into three types, signaling-based, content-based and voice-activity based[8][10][12]. Most of the spam-callers use anonymous and multiple agents, so in signaling-based detection is difficult to determine the true identity. In the content-based detection there are some legal obstacles because of this method requires the analysis of the speech. The detection method based on voice activity, needs to some features of the spam-call to determine the difference between human-human dialogue and human-computer dialogue. In this case the process of analysis could affects the speed and the quality of the service. We propose in this paper, a new approach for appliyng in VoIP against Spit, for dealing with the trade-off between security and quality of service.

4 VoIP Security Assessment

The large-scale deployment of VoIP infrastructures has been determined by high-speed broadband access. this technology of communication includes a large variety of methods enabling the transmission of voice directly through the Internet and other packet-switched networks.VoIP appears to be an attractive alternative compared to traditional telephony for several reasons, such as seamless integration with the existing IP networks, low cost phone calls not expensive end-users, etc. VoIP is a technology that allow users to make calls using a broadband internet connection. The interest in IP telephony for years has been renewed continuously, due to both the dissemination and use of the Internet that the significant changes and brought real benefits in the business and beyond. Voice Over IP, is an alternative to traditional telephone communications infrastructure, allowing the transport of audio information in real time through the IP network. The VoIP system can be implemented on any network infrastructure which is based on IP, such as Internet, Intranet and local area networks (LAN). The interest in the use of this technology, that has allowed to migrate telephony services to IP networks, is linked to the possibility of developing new services resulting from the transport of audio information, video and data, all on a single network. In general, VoIP infrastructure consists of endpoints (telephones), control nodes, gateway nodes, and IP-based network, and it can utilize various media including Ethernet, fiber, and wireless. The PSTN allows a reliable telecommunications network in some aspects, that makes it fairly safe, but also moderately expensive. This architecture is based on a fixed and constant relation between the number and location of the user. This is not suitable to support services requiring mobility and portability. In a circuit-switched network like PSTN, when two parties establish a communication, the path is established between them and for the duration of the call only these two parts, can use this particular route. In a packet-switched network, like the Internet, any kind of data is sent in IP packets and each packet travels on a road across the network. Eventually all the packets are reassembled at the destination. These are some of the many differences that make the VOIP system, a very cheap flexible system . However, the rapid adoption of VoIP introduced new weaknesses and more attacks, whilst new threats of networks have been recorded which have not be reported in traditional telephony. One such example is the Spit. One of the limitations of VoIP technology is the variety of architectural structures and this makes more difficult to design a general antiSpit systems. The VoIP infrastructure is characterised by three different parts such as:

- End-users Equipment (hard phones and soft phones).
- Network Component (routers, switches,firewall).

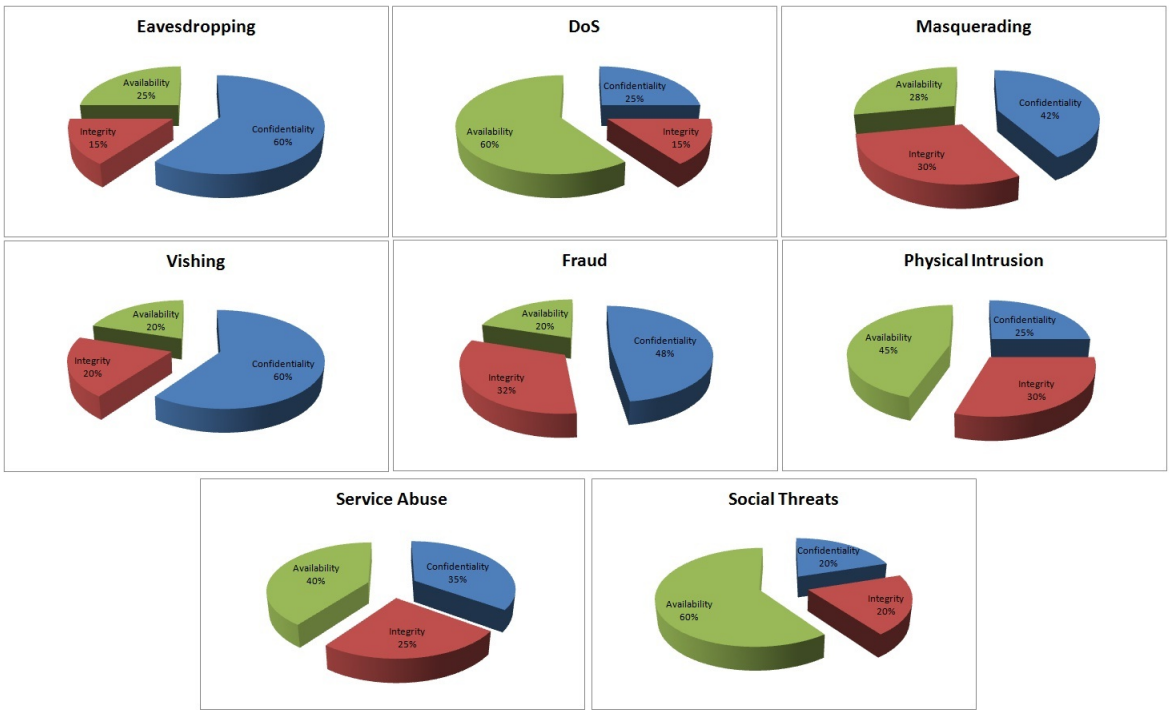


Figure 1. Impact on CIA requirements

- VoIP Gateway.

and several assets:

- Network and Service Access.
- Protocols.
- Processes.
- Service Infrastructure.
- Physical Component Architectures.
- APIs and Network Peering.
- Business Areas.

giving signaling, encoding, transport, and management of the infrastructure. There are different protocols which defines different types of VoIP network.

- Signaling Protocols.
- Media Transport Protocols.

The signaling protocols are handle detection, recording and reporting of call-exchange parameters for the transmission of streaming media, and also management, establishment, setup negotiation and teardown of sessions. They are:

- SIP [13][14]: it is a IETF standard and it is responsible to establish, modify or terminate a call between two or more users. A client sends a request to which the recipient has to reply.It is based therefore on the principle of request-response. This protocol has security mechanisms as end-to-end and hop-by-hop.
- H.323 [15]: it is ITU-T standard and it is a set of multiple protocols for multimedia communications systems based on IP networks.H.323 borrows from traditional PSTN protocols, eg, Q.931, and is well suited for PSTN integration. However, H.323 does not employ the PSTN's circuit-switched technology like SIP, H.323 is completely packet-switched.It addresses many security issues and can use SSL for transport-layer security.
- SCCP: the Skinny Client Control Protocol is a Cisco proprietary product. It uses a TCP connection rather than the UDP and encrypts call control information.

The media transport protocols control digitizing, encoding, decoding, and ordening of voice samples for real-time communications:

- RTP [16]: it is the real time transport protocol according to RFC1889. The basic function of RTP is to perform the multiplexing of real time data streams in a

single stream of UDP packets. It defines a standardised packet format for delivering audio e video over the internet.It include services such as payload-type-identification, sequence numbering and time stamping.

- RTCP [17]: this protocol realt-time transport control protocol. It provides out of band control for an RTP stream. Its main task is to collect statistics about the quality of the RTP protocol through feedback.

4.1 Threats Taxonomy and Impact on CIA Security Requirements

The new trends of the communication is the move towards the transmission of voice over traditional packet switched IP network, voice over IP. VoIP is the first step for the future convergence. Although it is a technology that is being rapidly deployed, there are many security challenges and the benefits of VoIP are as strong as security issues.Each threat could compromises the security requirements of confidentiality, integrity and availability, also called CIA requirements. The confidentiality, if compromised, involves access to information by those who have not right to access, and they could use sensitive information of users attached to commit other types of attacks such as fraud. The integrity, if compromised, results in the destruction or modification of sensitive data. The availability, if compromised, leads to the denial of access to the system and interrupt the processes that regulate it. The attack is successful if the threat uses the correct system vulnerabilities. We briefly listed the main threats[3][4][5] associated with this technology, giving a concise description for each of them:

- Eavesdropping: when an attacker eavesdrops on private communication. It describes a method by which an attacker is able to monitor the entire signaling and/or data stream between two or more VoIP endpoints, but cannot or does not alter the data itself.

- DoS: it is the denial of service threat. It consists in interruptions of service which are classified into Specific Denial of Service,General DoS, Physical Intrusion, Loss of External Power, Resource Exhaustion and Performance Latency.

- Vishing: it is a a combination of VoIP and caller ID spoofing. Vishing attacks are often hidden behind false financial companies which asking for confidential information such as credit card numbers. Unlike most phishing scheme that direct the recipient to a fraudolent site, this scam instructed victims to call a phone number, where they were asked to divulgue accoutn information .

- Fraud: or Toll Fraud means to access a VoIP network and to make unauthorized calls (usually international or intercontinental). Hackers exploit weak passwords and user names. The toll fraud is one of the most frequent attacks to VoIP.

- Masquerading: when a perpetrator is able to impersonate a VoIP Server and trick the victim to send requests to the masqueraded server, the victim will not be able to receive any services from the server that has been masqueraded.

- Physical Intrusion: this threat could compromise of lock and key entry systems, alarm systems, surveillance systems, and security guards can seriously impact VoIP Service.A number of possible interruptions of service arise when physical access is gain to components within the VoIP Network, such as ARP spoofing/poisoning and IP spoofing, Unauthorized configuration changes and Intentional loss of power.

- Service Abuse: is a large category of improper use of services and of communication processes to defraud or to commit other types of network attacks through unauthorized use of the network.

- Social Threats:Security and privacy are important social needs that planners balance against other vital needs such as return on investment and convenience.This type of threat includes Misrepresentation of Identity, Authority, Rights and Content, and also Theft of Services and Unwanted Contact such as Spit, which is discussed in the next section.

In Figure 1 we evaluate the impact on CIA requirements of the most important threats.

5 Spam Over Internet Telephony Overview

Spam is defined as the transmission of unsolicited email and in general it is considered one of the biggest problems of the Internet because of there are no solutions readily available when the problem arose. Thus, often we have more spam emails than regular emails. Nowadays, there are methods available that are able to counteract this problem using different approaches, but none of these methods constitutes a definitive solution. Spit indicates a common variant of spam for email. Spit is a social threat. The social threats are attacks ranging from the generation of unsolicited communications. These kinds of communications disturb the users with unwanted calls and advertisements unsolicited. Spit calls can be telemarketing calls used for influencing callees to sell products, for example. There have been disclosed many real Spit attacks and it was pointed out since 2004 a substantial increase of sending Spit

that within a few years could lead to considerable discomfort.Meanwhile, it's important to prevent and protect the infrastructure. Spit is defined as the transmission of unsolicited calls over Internet telephony, it is expected to become a serious threat inhibiting the delivery of voice services over the Internet in the near future both because of its technical and economical features. It will be difficult to detect with a single detection method a Spit call. We have to remember that unsolicited calls already exist in the traditional public switched telephone network (PSTN), where such calls are mostly initiated by telemarketers but are limited in number because of the relatively high cost of a PSTN. Spit is three orders of magnitude cheaper to send than traditional telemarketing calls [19]. Taking into account this threat could seriously impair communication systems, triggering other types of attacks, such as vishing, service abuse, fraud and denial of service. The reak problem is that VoIP is different from email in the sense that it is in real-time while email is an ofine medium and therefore not time- critical. Emails can be scanned before deciding if it is spam or not.VoIP communications cannot be accessed before the call is actually answered. It's very difficult to identify spit calls in advance. This also because the factors affecting the undesirability of a call are many, and they could be subjective. There are no effective methods against the Spit but there are a number of countermeasures, some of which stem directly from spam on email and have been converted to the VoIP case. So taking into account the difficulty of detection models, in this paper we propose a different way to assess the problem of the Spit with a different point of view. We propose a detection strategy based on the behaviour of the users, during an observation period. This allows us to evaluate in a more efficient way the probability that a call is spam or not. The assessment comes from the consideration that, learning the habits of users, we can find anomalies in the system under these consideration. Thus, for example, if a user rarely receives phone calls during the night, then the probability is high that it is as spam call. In the proposed model we classify users according to certain parameters in order to associate to each the most appropriate countermeasure. This paper presents a framework for Spit prevention designed to be easily manageable and extensible and based on the users and their habits. Additionally, the framework makes use of different countermeasures in order to exploit the knowledge about this and to highlight the extent to which priority is given to effectiveness, speed and not-intrusive. A Spit prevention system has to meet some basic requirements [19]:

- minimize the probability of blocking legiti- mate calls.
- maximize the probability of blocking Spit calls.
- minimize the interactions with the callee to determine whether a call is Spit.
- limit the inconvenience caused to the caller that tries to place a legitimate call.
- applicable to different types of environments, different cultures, languages, and so on.

The conclusion of these considerations is a strong need for Spit prevention systems to be expected in the near future.Thus, we present the framework in the next section to suggest solutions to these issues, combining the capabilities offered by different countermeasures methods and the user-behavioural assessment model, that we propose, to efficiently block Spit calls while requiring the least possible interaction with caller and called, in some cases, a faster resolution in other cases, or a high effectiveness.

5.1 Countermeasures

We describe briefly the existing countermeasures [18][19][20] against the Spit attack.

- Blacklist filtering: blacklist filtering is a simple mechanism where the identity of a caller is compared to a set of stored identities to decide whether to accept or reject a call. There are two different kinds of lists, white and black. If a user enters a caller to be blacklisted by identifier (URI User Resource Identification), the call will be blocked by the VSP (VoIP Service Provider).The method is highly not-intrusive, but its effectiveness is limited.
- Greylisting: it is used for email spam. If a user calls for the first time he is inserted into a "gray" list and the system asks him to call back. If the caller calls again is put in the white list, otherwise it is blacklisted.Greylisting is a very efficient method for blocking email spam using a built-in feature of the Simple Mail Transfer Protocol (SMTP).For Spit, greylisting would require user interaction.
- SIPFW: this method uses the fingerprinting model. This implement a Spit firewall involving the use of SIP. There are two type of this, active and passive. The active fingerprinting is more robust than the passive method and it uses SIP messages manually created to obtain specific answers. The passive fingerprinting is based on exchanges managed by existing protocols without additional messages.
- Sender Check: the caller brings references from its domain. This method does not exist yet but it is real applicability. However, its implementation is quite complex. The level of not Intrusiveness was rated medium-high.

- Content Filtering: the original method is based on studying the content of the email. In the VoIP applications it is based on speech recognition. It requires great computational effort and waiting the user must start talking.
- Consent Based: the callee shall authorize the caller. So it is a slow method and highly intrusive. It is being standardized by IETF for SIP.
- User reputation: this method is applied by the provider, so, the callee is not involved in the analysis of the type of call. Each VSP (VoIP Service Provider) collects CDR (Call Detail Record)data of the users, analyse information and it associates a spam index. If the index of some users is high, the VSP classifies the call as a call spam. In cases where a call is highly suspect, but without any statistical evidence, it will be forwarded to the recipient.
- Correlation IP/Domain: this method records the SIP identifier and IP address of the calls. When the callee receives a new call the system checks whether the information for the SIP domain and IP address match with those previously saved.
- Pattern Anomaly Detection: it is based on the models of the probability of arrival of the call and the module decides whether the incoming call might be Spit or not.It uses the knowledge of statistical and deterministic models.
- Circles of Trust: it introduces trusted interdomain connections. The domains control their users and they work to not send Spit each other. This method needs to be implemented on Sip by using Transport Layer Security (TLS) connections intradomains.
- Simultaneous Calls: this method checks if a caller , that is identified by a SIP identifier,actives multiple simultaneous calls. The method failes to detect simultaneity if the caller changes the SIP identifier for each call.
- Turing Test: the Turing test asks callers a question. In most cases, the spam caller is not a human being but an automated program. In this case it may happen that a recording message starts automatically (perhaps advertising) or that you do not receive any response. The Touring test measures the energy of the signal of the caller.The VSP may increase the spam index and route the call from the list gray to black.
- Call Rate: it can be applied to the prevention of Spit and Spam. The system could accept, for example, a user which tries to call someone else up to two times for minute, but no more. The developed module storse and checks the recent call made by a caller. This method sets a maximum limit for calls in a certain time interval TD. If we receive a call several times during TD, this call is classified as Spit.

Countermeasures	nI	Sp	Eff
Black List	H	M	ML
Call Rate	H	M	ML
Circle of Trust	H	M	M
Consent Based	M	L	H
Content Filtering	ML	L	MH
Greylisting	H	L	M
IP/Domain Correlation	H	H	ML
Pattern/Anomaly Detection	H	M	M
Sender Check	H	H	L
Simultaneous Calls	H	ML	L
Sipfw	H	MH	M
Turing Test	MH	L	MH
User Reputation	L	M	ML

Table 1. Spit Countermeasures Assessment

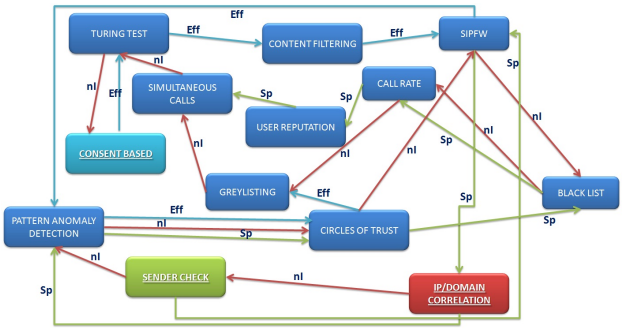


Figure 2. AntiSpit Methods Assessment

We group the countermeasures described above in a conceptual map where the nodes are the antispit methods. We assess each of them, as in Figure 2. Each method is characterised by a different value, High (H), Low (L), Medium (M), Medium Low (ML) , Medium High (MH), of three parameters as in Table I, not Intrusive (nI), Speed (Sp) and Effectiveness(Eff). The parameter not Intrusive refers to the extent of noise and feedback, required to the users, to evaluate the call and classify it as Spit or not. The prevention methods could act invisible to the caller and called or they could intercat with the users terminal. They could requires feedback from the callee before the call is actually established,or feedback from the called occurs after the call has been terminated and contributes to blocking Spit in the future. At the same time we could instead give priority to other types of parameters such as Speed. There are methods that have a higher rate of resolution and analysis of the

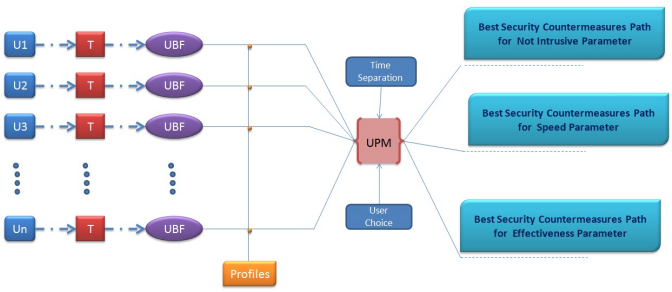


Figure 3. User-Profile Framework

call, to block unwanted calls. All this is at the expense of effectiveness. Finally, we could give greater priority to the Effectiveness of a detection method against Spit call. A user may choose voluntarily to contribute with the aim of the analysis to determine the nature of the call before the call is actually established and for the future if a call is Spit or not. This is at the expense of speed and therefore of the degree of intrusion detection. In the map in Figure 2, we show the relationship of the various methods on the basis of the variation of these parameters. The indicator shows the transition from a countermeasure with the highest value of parameter to the countermeasure with the lower value of the same parameter. When two countermeasures have the same value for a parameter, we consider the values of the other two parameters, giving priority to the highest of these. In this way, the choice of countermeasures to be applied will be optimal for the called.

6 User-Profile Framework

The framework presented in this paper, allows you to evaluate a set of users, profiles and countermeasures against Spit Calls. The aim of this framework is to assess the habits of a user, based on certain observations in a given period T. Then we associate the user to a profile to identify the best countermeasure, which is the best suited for that user, against a Spit attack. The framework is described in Figure 3. We can identify the following parties:

- Un=Users;
- T=Observation Period;
- UBF=User Behavioral Features;
- Profiles;
- UPM=User-Profile Matching;
- Time Separation;
- User Choice;
- Best Security Countermeasures Path, for not Intrusive, Speed and Effectiveness parameter;

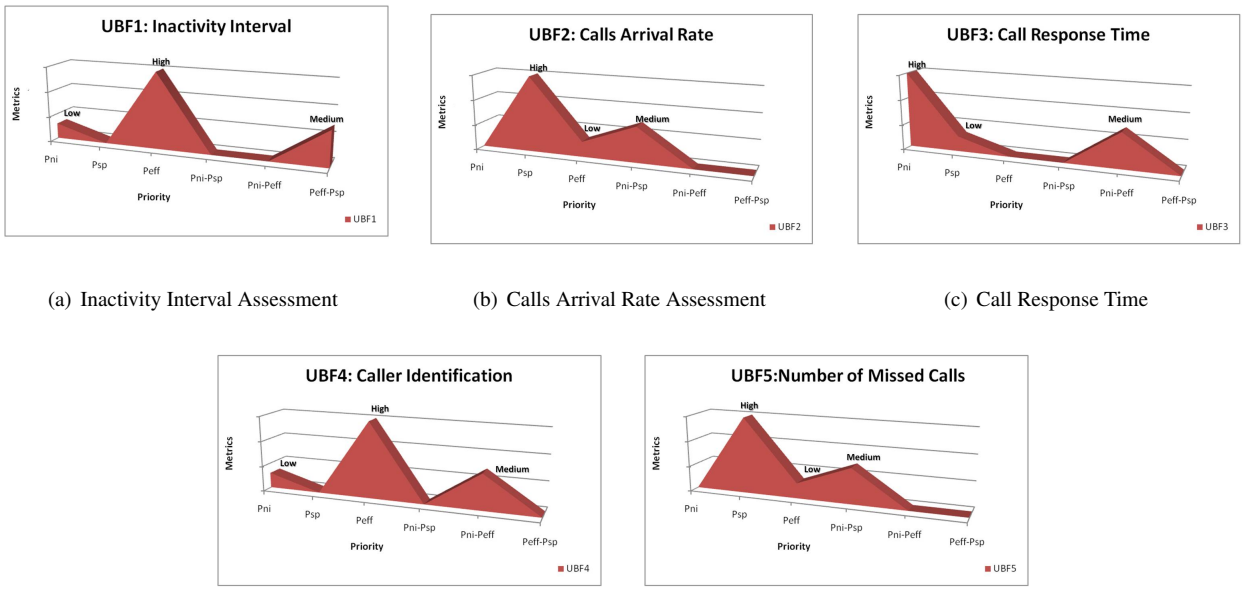
In order to describe the features of the framework, the following definitions have to be given:

- Users Behavioral Features: are features of each user, which is observed during the observation period T.
- Profiles: definition of three general profiles, based on the variation of the three parameters (nI,Sp,Eff).
- User-Profile Matching: matching between profiles and users features, to associate each user to the best security path.
- Time Separation: matching function is evaluated on the basis of a period T of observation and on the basis of the different parts of the day, that influences users behavior and hence also the incoming calls.
- User Choice:represents the subjective choice of the user. Each user could decide to give priority to a parameter rather than another. This choice influences the association of the best countermeasure. For example we can have a best path for a part of the day and another best path for the rest of the day.

Each user will receive a certain number of calls during the observation period T, and will be analyzed according to certain parameters, Users Behavioral Features. These features include some characteristics of the calls, so, the following definition are given:

- Inactivity Interval (UBF1): the time interval between the end of a call and the arrival of the next.
- Calls Arrival Rate(UBF2): the calls arrival rate during the observation period.
- Call Response Time(UBF3): the time interval between the arrival of the call and response of the called.
- Caller Identification(UBF4): the number of different callers during the observation period.
- Number of Missed Calls(UBF5): the number of missed calls by the called, during the observation period.

Each UBF is a parameter of observation and its value influences the choice of the optimal path. From these parameters we can understand, learn and evaluate everything relating to the calling habits of a user. Leaving for assumption the User Choice and Separation Time, we associate a qualitative measure (High, Medium and Low) to each UBF



(a) Inactivity Interval Assessment (b) Calls Arrival Rate Assessment (c) Call Response Time

(d) Caller Identification (e) Number of Missed Calls

Figure 4. User-Behavioral Features Assessment

observed during the observation period T.Each measure of UBFs, matches a priority of parameters among not Intrusive,Speed and Effectiveness,as in Figure 4:

- Pni= not Intrusive Priority
- Psp= Speed Priority
- Peff= Effectiveness Priority
- Pni-Psp= intermediate priority value among not Intrusive and Speed
- Pni-Peff= intermediate priority value among not Intrusive and Effectiveness
- Peff-Psp= intermediate priority value among Effectiveness and Speed

From this evaluation we can define the three profiles basing on the values of UBF and the values assigned to each priority.

- Profile 1: Low Inactivity Interval,High Call Response Time and Low Caller Identification.
- Profile 2: High Calls Arrival Rate, High Number of Missed Calls and Low Call Response Time.
- Profile 3: High Caller Identification, Low Number of Missed Calls and High Inactivity Interval.

Each profile will match one and only one best path securiy countermeasures. Thus, each user will receive the best security path suited to its specific features. Then, the three profiles identify a path of security countermeasures against spit calls. The Profile 1 identify the Best Security Countermeasures Path for not Intrusive parameter. The Profile 2 identify the Best Security Countermeasures Path for Speed parameter. The Profile 3 identify the Best Security Countermeasures Path for Effectiveness parameter. Each security countermeasures path, as in Figure 5 has a starting point that identifies the best countermeasure for the specific parameter (Non-intrusive, Speed, Efficiency) of the corresponding profile (Profile1, Profile 2, Profile 3) and the subsequent countermeasure,and so on, is based on the variation of the same parameter, according to the conceptual map of the preceding section. About the intermediate priorities value identified by UBFs, in these cases the subjective choice of user is involved, which may also changes in terms of time interval on the basis of their habits.

7 Conclusions

In this paper we want to propose and to introduce a new framework to protect against Spit attacks in a VoIP infrastructure. We outlines the security issues in communication system which characterise ICT environments, such us VoIP infrastructures and in the next future the NGN networks.

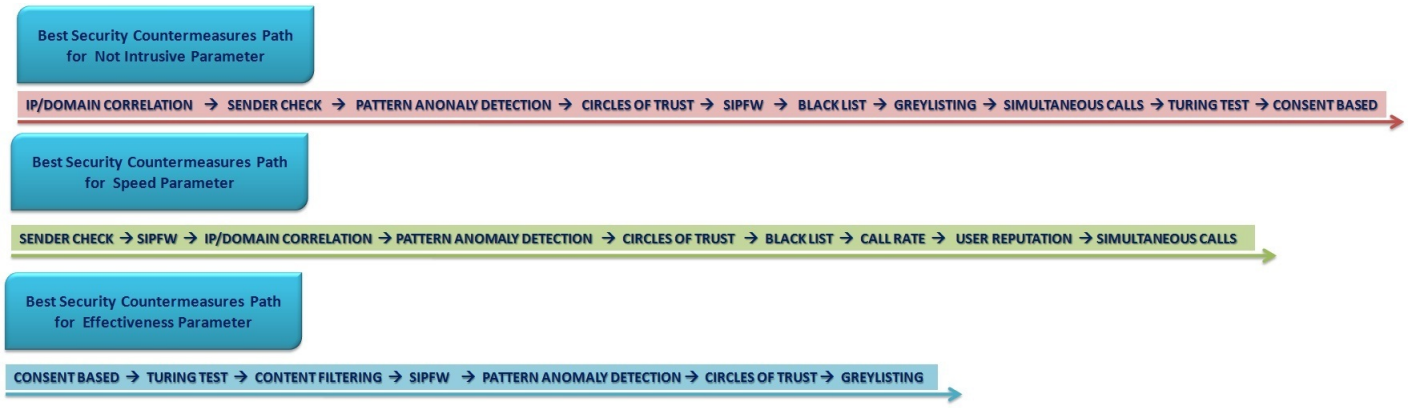


Figure 5. Security Countermeasures Path

We have considered the principals assets of a general architecture and we have assessed each part of these, giving a briefly overview of the communication system on IP. Then, we have analysed several coutermeasures to understand the level of applicability and real implementation of each of them. Finally, we propose the user profile framework, and in the next future we want to improve, to extend and to test it. We have proposed an analysis procedure that allows to observe certain characteristics of a predefined number of users receiving a number of calls every day. This framework allows to understand the habits of each users and what respect its and what a user wants to prioritize among the three evaluation parameters (nI,Sp,Eff). This method also allows to identify the optimal countermeasures to be taken against the spit calls, according to the user behavioral features. Each user receives a certain number of calls during an observation period. We define general profiles with some features, based on certain parameters, and with a user-profile matching we can identifies the best security path which must be applied. The aim is to learn from the habits of every user, to understand and identify the fault, which is the successfully Spit attack.

References

[1] R. Heeks, *Ict4d 2.0: The next phase of applying ict for interna- tional development*, Computer (2008)

[2] V. Leveque, *Information Security. A Strategic Approach* IEEE Computer Society, J.Wiley and Sons, 2006.

[3] VoIP Security Alliance, *VoIP Security Threat Taxonomy*, Technical Report, 2005.

[4] A. Keromytis, *Voice over ip security: Research and practice*,IEEE Computer and Reliability Society, Secure Systems,2010.

[5] *Voice over IP: Risk, Threats and Vulnerabilities*, Proc. Cyber Infrastructure Protection (CIP) Conference, 2009.

[6] T. Ayoama, *A New Generation Network: Beyond the Internet and NGN*, Keio University and National institute of Information and Communications Technology, ITU-T KALEIDOSCOPE, IEEE Communications Magazine,2009.

[7] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald, *Detecting SPIT Calls by Checking Human Communication Patterns*, in ICC, 2007.

[8] R. MacIntosh and D. Vinokurov, *Detection and mitigation of spam in IP telephony networks using signaling protocol analysis*, in IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, 2005.

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

[10] Ram Dantu and Prakash Kolan. *Detecting Spam in VoIP Networks. In Proceedings of the Steps to Reducing Unwanted Traffic on the Internet Workshop*,Cambridge,MA, 2005

[11] M. Sasaki and H. Shinnou,*Spam Detection Using Text Clustering*, in International Conference on Cyberworlds,2005.

[12] HUANG Hai, YU Hong-Tao, FENG Xiao-Lei, *A SPIT Detection Method Using Voice Activity Analysis*, International Conference on Multimedia Information Networking and Security,2009

[13] J. Rosenberg, et al., *SIP: Session Initiation Protocol* IETF RFC 3261, June 2004.

[14] C. J. J. Rosenberg, *RFC 5039 : The Session Initiation Protocol (SIP) and Spam*, 2008.

[15] Goode B. *Voice over Internet Protocol (VoIP)* Proc IEEE Sept. 2002.

[16] Schulzrinne H, Casner S, Frederick R and Jacobson V. , *RTP a transport protocol for real-time applications*,RFC 1889,Jan. 1996.

[17] Baugher M, Carrara E. *The use of timed efcient stream loss- tolerant authentication (TESLA) in the secure real-time transport protocol (SRTP)*, RFC 4383, Feb. 2006.

[18] TaiJin Lee1,et al. *User Reputation based VoIP Spam Defense Architecture* Korea Information Security Agency, Seoul Womens University

[19] Juergen Quittek, Saverio Niccolini, Sandra Tartarelli, and Roman Schlegel, NEC Europe Ltd., *On Spam over Internet Telephony (SPIT) Prevention* IEEE Communications Magazine, August 2008.

[20] G.F.Marias, et al. *SIP Vulnerabilities and Anti-SPIT Mechanisms Assessment*, Information Security and Critical Infrastructure Protection Research Group, IEEE, 2007.