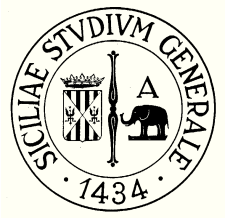
Security Analysis of ICT Systems based on Bio-Inspired Models



Ing. Marialisa Scatá

Department of Electrical, Electronics and Computer Science Engineering

Faculty of Engineering, University of Catania
Supervisor: Chiar.mo Prof. Ing. Aurelio La Corte

A thesis submitted for the degree of

Dottorato di Ricerca in
Ingegneria Informatica e delle Telecomunicazioni

XXIV CICLO

There comes a moment in the evolution of every field or discipline when central intellectual issues come into focus as the field and the discipline on which it rests shift from a rough, ambiguous territory to an arena of reasoned inquiry. At such a time, scholars, scientists, researchers, and their students begin to focus articulate attention on such issues as research methods, methodology (the comparative study of methods), philosophy, philosophy of science, and related issues in the metanarrative through which a research field takes shape.

Ken Friedman. Theory Construction in Design Research

Abstract

In recent years, information and communication technology (ICT) has been characterized by several evolving trends and new challenges. The design and management of each information system must address issues related to planning an ICT infrastructure. The design of an ICT infrastructure can not ignore the technological and social analysis, to be also linked to the economic aspects, and now also linked to the sustainability.

Communication tecnologies are evolving very fast following the current trend of the time where everything is becoming digitized and the demand for ubiquitous and opportunistic network and services is growing. Communication, over the years, is the driving force of the society through the networks. The next future requires a revolution in the integration of services, convergence of technologies, sharing of resources and processes optimization. The aim is to be closer to the user, simplifying the plurality of resources and communicating with interfaces, thus offering convergence, ubiquity and dinamicity in quick and easy sharing, from the workplace to everyday life. What is becoming increasingly important is the need to communicate quickly and in real time, to be able to access any type of resource and information from anywhere and to be able to access and share data and knowledge at the same time as safely as possibile.

Most of the ICT systems have emerged without clear global strategy to project information and communication security. Historically, security decisions are taken outside of the context and after the damage occurs, with false perception to obtain high security and efficiency

at reasonable cost.The systems are not born confident, but they nust be deliberately designed for this. A security mamagement strategy implies a complex dynamic risk analysis of the system without unnecessary additional cost, computational and redundant resources. Thus, dwawing inspiration from biology that has led to useful approaches to problem solving, this Ph.D. dissertation propose and develop a risk analysis model and security analysis and management model.

The risk analysis proposed aims to address technical, human and economic aspects of the security to strategically guide security investments through a bio-inspired approach. This is a global analysis that sets the stage to manage the security of an ICT system. This analysis require a step-by-step approach, the knowledge of the survivor and failure analysis, the assessment of the threats taxonomy and the existing countermeasures, policy and control strategies. An economic investment can not ignore the technical evaluation of the system, vulnerabilities and threats analysis, and the estimate of expected risk, in order to ensure proper countermeasures to limit the technological and economic damage over time.

Risk analysis involves these aspects to guide strategy of investment.The aim is to estimate the risk degree and the security degree, to mimize the losses and successfully applies security investments, with positive expected benefits. With this Ph.D. thesis I want to propose and show a new kind of research topic, Bio-Inspired Telecommunication Security. Thus, I showed that it is possible to inspire the risk and security analysis from biological systems, because in examing some of the most common structures used today in ICT environment we can find striking similarities with biological environments and we can discover and adapt these mechanisms to ICT technical solutions. It will be key to reach efficiency of the future networks and to obtaine a sustainable ICT infrastructure in terms of energy consumption, economic investment and in terms of privacy and security.

Contents

List of Figures

Chapter 1

Introduction

Overview:

|This Chapter introduces the research topic of Security Analysis of ICT Systems, and sets out the vision and the need for a model to estimate the risk degree. It explains the principal benefits and discusses the challenges, both technical and social, involved in realising such a project on a global scale. It outlines a strategy for tackling these problems and states the research questions addressed in the remainder of this dissertation.

1.1 Security Analysis of ICT Systems

Information is defined as an important asset of an ICT system, and it can exist in many forms. Information can be managed, manipulate, to be availabe to the users at any time. ICT links two components, the information technology (IT) and the Communication Technology (CT). ICT pervaded all critical infrastructures and it is applied in various areas and it allows innovative solution for emerging technologies. This process allows to support strategically decisions, processes of management, security, quality and energy consumption awareness. The future of ICT is the real support to the future sustainability.

In the process towards convergence, along with many positive benefits there are several security concerns and ensuring privacy is extremely difficult. The need for security is linked to the value of information that is transmitted, and with the new development of converged networks, the information also aquires an impor-

tant shared communication value. Therefore, in an ICT system is important to understand, first of all, why we must protect information, than figure out what kind of risks are there, and the safety requirements, suitable to the system, even before to design an analysis of the assets and evaluate what to do. A Bio-Inspired approach allows to focus on identification of mechanisms and models applicable to biological technical solution for ICT systems. A step-by-step preventive approach to the issues could allows analysis of the information assets, processes, vulnerabilities and not only a simple taxonomy of the old and new threats. At the same time we can assess risk and quality of service (QoS) and energy consumption giving an appropriate analysis method regarding certain parameters and requirements evaluating factors of influence and general incidence of certain features of the Next Generation Network(NGN).

Inside this we found integration and convergence of technologies, protocols, services to create a single IP-based network technology. The reason that lead to the creation of next generation networks is not unique to the integration and convergence of network technologies and protocols, but also it is to create a single IP-based network technology that converges the entire service offering high and very high speed fixed and mobile, traditional and innovative, and accessible from different networks.

The drive towards this direction has been given by the growth of Internet traffic due to the use of customized content especially for video, the growth of peer to peer and social networking applications and istant messaging, the growth of IP-based services and applications such as VoIP(Voice Over IP). With VoIP the privacy becomes so hard and the benefits introduced are as strong as the security problems. VoIP has become a valid alternative to the PSTN (Public Switched Telephone Network) and it has a new paradigm for providing telephony services at lower cost and higher flexibility. The rapid adoption of VoIP introduced new weaknesses and more attacks, whilst new threats of networks has been recorded which there are not in the traditional telephony network. From the perspective of the study of threats and resistence to their attacks, a VoIP system can be studied following the models and principles of Survivor Analysis, which is the widespread

in the study of the effectiveness of clinical therapies for population that suffers from certain diseases. For this reason it is possible to characterize a VoIP system through its survival function, failure and hazard function trend. Thus, through a Bio-Inspired Approach.

1.2 Potential Benefits and Drawbacks

In this Ph.D. thesis, starting from some considerations about security, we propose a model for analyzing and managing security for an ICT system. The aim is to focus on attention to a problem that in most cases is considered as a protection action after the damage occurs. This may reduce the risk that a threat may act through an attack exploiting a vulnerability of the system, but only temporarily, giving the false perception of security of the system itself. A priori design to evaluate and analyze the system and put preventive measures, is useful to decide strategies of control and monitoring, and application of countermeasures. A general analysis system can guarantee the security requirements of various entities, estimating the expected risk and possible benefits that might have from security investments. The analysis model for an ICT system at the same time, is very complex to apply because of the plurality of systems and assets involved.

The risk itself is subjected to many influences and changes due to factors not only technological, but human and social. Ultimately, the factors that could confuse and undermine are difficult to categorize, both for individual assets, and for the entire system. The analysis must be done considering "sure and certain" the unpredictability of certain events, failures, ranging from natural disasters to malicious events. A security management strategy implies a complex dynamic risk analysis of the system, of information exchanged and of communication and cooperation with other systems. Introducing robustness inevitatable requires additional cost, computational and reduntant resources on making network tollerant to failures, but this is not cost-effective in the short term. Drawing inspiration from biology has led to useful approaches to problem solving, this Ph.D. thesis is a proposals and a development to find solutions in biology that can be applied to security issues of informtaion systems to have a biologically inspired model for

dynamic, adptive converged information and communication systems to estimate a quantitative measure of risk.

1.3 Research Questions

This dissertation tackles the issue of security and how the bio-inspired approch can improve the analysis models about this and addresses seven main research questions:

- Most of ICT systems pervaded all critical infrastructures and have emerged without a clear global strategy for security. This is due to changes in technology, human, social and economic aspects. ***Can security of an ICT system be analyzed and managed trying to provide at least the requirements of confidentiality, integrity and availability?***

- 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 hard, because the benefits introduced are as strong as the security problems, like Spam over Internet Telephony. ***How we can identify Assets, Threats and Vulnerabilities? How we can investigate and use these information to estimate the risk? Can Spam on VoIP be identified and can Spit calls be minimized maximizing the security degree of the system?***

- In the Next Generation Network there are many factors that affects the Quality of Service (QoS), such as encoders, delay, jitter, packet loss and echo. At the same time, the quality is linked to the safety. The security requirements, if breached, worse the parameters affecting privacy and also quality of service. ***To what extent can quality and security of the next generation network be considered improved in comparison with not-converged solutions?***

- The future convergence of the networks and the evolution of the communication systems is a process highly complex. Our networks are increasingly

facing new challenges and they grow larger in size, and we want to continue to be able to achieve the same robustness, availability and safety. Biological systems have been evolving over billions of years, adapting to a continuous changing of environment. If we consider information systems and biological systems, they share several properties such as complexity and interactions between individuals of a population (asset of the information system). ***To what extent can analytical models and biological processes inspire the analysis and management of the trend of risk, useful in decision making strategies of countermeasures and safety policy?***

- The measure of risk will be useful to evaluate the most appropriate security countermeasures, the expected benefits from an investment, and then it allows to manage the security degree, balancing costs and efficiency of the systems. An optimal strategy considers the economic tradeoff between the timing of investment, its value and cost-effective. ***What kind of strategy and investments can be applied to an ICT system to produce a positive expected benefits. Can Survivor Analysis be useful to give a realistic measure of risk and to evaluate the impact on security requirements?***

- The emerging information society is widely expected to experience massive embedding of both fixed and portable devices into our local physical spaces, with more and more devices having the capacity to initiate, store and communicate information and content in all aspect of life. This will result in significant challenges for communication and information provision, based on required scalability, efficiency in forwarding, heterogeneity re-configurability, security and dynamicity.***How dinamically chooses routing and find an optimal routing mechanism according to dynamic network condition in wireless ad hoc networks, to obtain improvement in terms of energy consumption in a mobile ad hoc network?***

- If a threat, exploiting a vulnerability, attacks a node, this being connected to the domain, will be able to spread the malicious code to adjacent nodes, in a certain time interval t. If we introduce the concept of bio-diversity, through phylogenetic algorithms we can calculate the extent of diversity among the nodes for each topology, and we can build different paths to safe the network. ***How to generate the bio-diversity in terms of single node and in terms of network domain? How to use the diversity and heterogeneity among nodes and between domains to bring out the best path to identify the points of the network more secure?***

1.4 Methodology

My research topic is based on the concept that the best ideas born always from interdisciplinarity. This involves the combining of two or more academic fields into one more, that crosses traditional boundaries between areas of research apparently disconnected. This method gave me the advatage of covering many research topics and obviously facing with many interesting issues. The aim is to discover and evaluate all the topics, which are related to issues of safety and risk analysis and management for information and communication technology systems. To improve my knowledge about nature of the security subject, I searched many related work and studied numerous scientific contributions to find new approaches, new methodologies to develop analysis model, tools and frameworks applicable in different areas. I summarize below the issues of interest that I studied in the Ph.D. period and which I'm going to improve in the next future. The following list of keywords of my research represents also the macroareas of this dissertation.

- Information and Communication Techonology and Information Security
- Voice over IP Security Assessment
- Spit Prevention Models
- Failure Time Distributions and Survival Analysis

- Bio-Inspired Communication Security and Bio-diversity
- Risk Analysis and Management
- Energy Awareness and Sustainability ICT

My research work has been articulated over the years in different phases, logically linked. I show the logical link among the different areas in the next section using a mind map.

1.5 Mind Map of Keywords

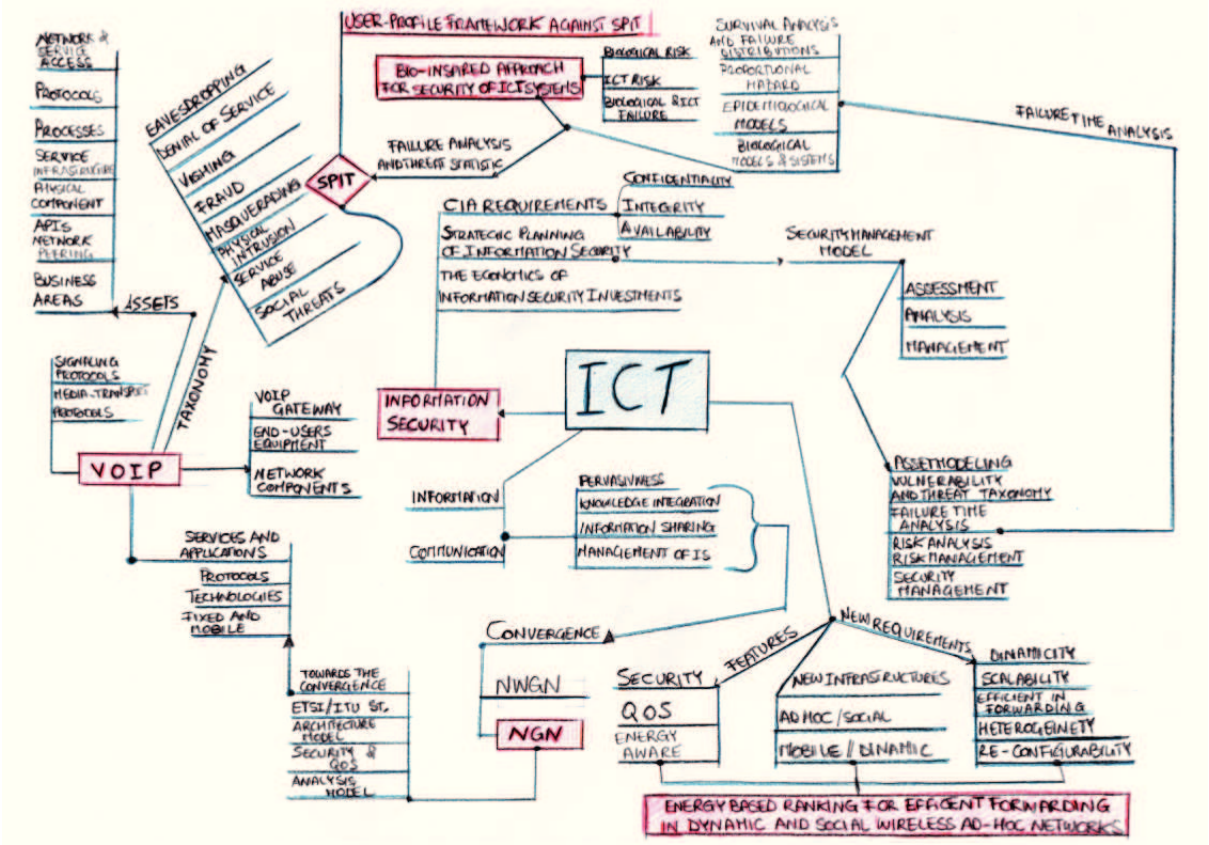


Figure 1.1: Mind Map of Dissertation Research Keywords

1.6 Dissertation Outline

The structure of the remainder of this dissertation is as follows:

- **Chapter 2** reviews related work in relevant areas of research. Existing techniques for influencing behaviour, security issue about ICT systems, VoIP Security and Spam over Internet Telephony, QoS and Security of NGN, Bio-Inspired Models are described and showed.

- **Chapter 3** presents the results of two studies to motivate the remainder of this dissertation. It describes the importance of ICT systems in the

future of the networks and evaluates information security definition. This Chapter presents a step-by-step preventive approach, a range of strategies to evaluate the information security and an architecture that provides an all-encompassing framework to analyze the security.

- **Chapter 4** investigates how VoIP has become a valid alternative to the traditional Public Switched Telephone Networks (PSTN) and about the benefits introduced. It presents a technique to evaluate assets, vulnerabilities, threats and countermeasures of VoIP. Finally, it describes a novel framework that allow to identify the optimal countermeasures to be taken against the Spam over Internet Telephony (Spit), according to the user behavioural features.

- **Chapter 5** identifies the key characteristics to assess quality of service (QoS) and security of Next Generation Network. It proposes and presents a novel analysis model that has the potential to provide a comparison between converged and not-converged networks.

- **Chapter 6** examines the bio-inspired models, the analytical models of Survivor and Failure Analysis. It identifies and shows all the similarities between biological population and ICT systems. It shows a model to estimate the trend of the risk, with a bio-inspired approach and applies this to the systems described in previous chapters.

- **Chapter 7** investigate about the economic investment and the expected benefits in security. Following a step of the framework proposed in the previous chapter, introduces the importance of the economic aspect and contextualizes this identifing different possible investiments cases.

- **Chapter 8** concludes by revisiting the research questions posed in Section 1.4, outlining possible avenues for future research and summarising the main contributions of this dissertation. In this Chapter is also presented further work about two open problems of the last year of the Ph.D. period. about deleay tolerant network, social network and energy consumption, in order to

obtain a sustainable ICT, not only efficient and secure. It evaluate also the possibility to apply the bio-diversity to realize a secure network, assessing the degree of heterogeneity of the networks nodes.

1.7 Publications

- **La Corte, A. and Scatá, M.**;*"A Process Approach to Manage the Security of the Communication Systems with Risk Analysis Based on Epidemiological Model"*, Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on , vol., no., pp.166-171, 22-27 Aug. 2010, Nice (France), doi: 10.1109/ICSNC.2010.32, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5634998&isnumber=5634631.

- **Scatá, M. and La Corte, A.**;*"Security analysis and countermeasures assessment against spit attacks on VoIP systems"*, Internet Security (WorldCIS), 2011 World Congress on , vol., no., pp.177-183, 21-23 Feb. 2011, London (UK), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5749907&isnumber=5749844.

- **La Corte, A., Scatá M., and Giacchi, E.**;*"A Bio-Inspired Approach for Risk Analysis of ICT Systems"*, Book Chapter in Computational Science and Its Applications - ICCSA 2011, Lecture Notes in Computer Science,Springer Berlin (Heidelberg), Santander (Spain), Isbn: 978-3-642-21927-6, vol.6782, pp. 652-666, doi: 10.1007/978-3-642-21928-3-48, http://dx.doi.org/10.1007/978-3-642-21928-3_48.

- **La Corte, A. and Scatá, M.**;*"Security and QoS analysis for Next Generation Networks"*, Information Society (i-Society), 2011 International Conference on , vol., no., pp.248-253, 27-29 June 2011, London (UK), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978445&isnumber=5978433.

- **La Corte, A. and Scatá, M.**;*"Failure Analysis and Threats Statistic to Assess Risk and Security Strategy in a Communication System"*, Systems and Networks Communications (ICSNC), 2011 Sixth International Conference on, Oct. 2011, Barcelona (Spain), ISBN: 978-1-61208-166-3.

- **Scatá, M. and La Corte, A.**;*"User-Profile Framework against a Spit Attack on VoIP Systems"*, International Journal for Information Security Research (IJISR), Volume 1, Issue 4, ISSN: 2042-4639 (Online), http://www.infonomics-society.org/IJISR/ (accepted).

- **La Corte, A. and Scatá, M.**;*"Convergence, Security and Quality in the NGN"*, International Journal for Internet Technology and Secured Transactions (IJITST), ISSN 1748-569X (Print), ISSN: 1748 - 5703 (Online), http://www.inderscience.com/sample.php?id=190 (accepted).

- **La Corte, A. and Scatá, M.**;*"Information Security Management with a Process-Oriented Architecture"*, The International Journal of Information Systems Applications, Information and Management, Elsevier. (submitted)

Chapter 2

Related Works

Overview:

|This chapter provides a detailed survey of related work, about the topics of this disseratation thesis. The idea is to cuts across a broad range of research areas, from information and communication technology (ICT) and information security issues, through Voice over IP (VoIP), Next Generation Network (NGN) and New Generation Network (NWGN) to Bio-Inspired approach to risk. This chapter first motivates and places in context the security issues , risk analysis topic, bio-inspired models, through a review of studies showing the scientific contributions, the existing theoreticla models and technologies designed. It surveys strategies about risk analysis and security management in ICT context, and the problems with requirementsfor extensive additional infrastructure and reviews potential solutions drawing inspiration from biological mechanisms, focussing on the essential properties of futuristic ICT systems, that will have quality, security and energy consumnption awareness. This chapter therefore identifies where further research is needed and guides the remainder of this Ph.D. dissertation thesis.

2.1 What about Information and Commmunication Security

Information and communication technology is the study of design, implementation, support and management of information systems.

> *"In a society based on knowledge, culture of sharing, information is the lifeblood, and the nervous system is the network of communication that allows the worldwide dissemination and the spread of the positive aspect to be linked everytime, everywhere, anyway and the negative aspect to expose own weaknesses." (Marialisa Scatá)*

> *"Information is an asset that,like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this incresing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Privacy isn't something that occurs naturally online, it must be deliberately architected. (Bruce Shneier).*

The idea of security cut across a broad range of research areas. From the time when information began to transmitted, stored and processed, it required protection. The security is protection of secrecy of hand written messages, it is protection of telegrams, telephone conversations and about world of computing. For a long time organizations would not recognize the importance of securing information and network that holds and transmits their strategic data. In general during the years the innovations in technologies introduces benefits and at the same time weaknesses.

> *Information security has been treated as a by-product, if not a "necessary evil that hinders productivity" (Conray-Murray)*

Information Security is not about looking at the past in anger of an attack once faced; neither it is about looking at the present in fear of being attacked; nor

about looking at the future with uncertainty about what might befall us. Security experts must be alert at all times. The aim is not to scare people but to make them aware of how information security has evolved over the past five decades. Information Security come into existence even before the invention of a computer. Information security is as old as information itself. From the time when information began to be transmitted, stored and processed, it required protection [Dlamini et al., 2009] [Veiga and Eloff, 2010]. The speed of innovation involves continuous evolution and changes, in terms of social, economic and technological aspect. The scientific value of the innovation in this context is directly proportional to the social sharing. Data shared becames lifeblood and the network becomes the highway to sort, share information, knowledge and collective culture with other users. Therefore the interest must primarily be to preserve historical memory, which through the years changes media, and appears inclined to support change, to achieve sustainability in terms of energy consumption and good management of economic resources with a certain strategy.

In a context in which is possible to invests often on semantic search, and digitizing dematerialiazation,mobile communications, multimedia and pervasive technologies, cloud computing and social networking, we risk to trust the network more than we should do and we can lose control of the data for lack of knowledge of the tools that are possible to use. On the one hand we have the information of the common user, in most cases not very interesting for professionals hackers, on the other hand we have to face with the needs of the business organizzations that have an abnormal amount of sensitive information, fully shared and accessible over the network. A lot of people lack a strategy to control and monitoring, but above all a culture of safety design in advance, that could gives an estimate of damage impact in terms of economic, technological and social aspect that you can have when a threat affects the vulnerabilities in the system. A strategic approach would evaluate each part of the system, the type of users, the habits of them, the environment and the context, tha possible links, the assets involved, the processes, the presence of any social network that would change the dynamics of virus spread, which would become very uncontrollable.

The need for security is closely tied to the value of information: this is much higher, the more we are willing to spend to protect it. Security management is a matter purely managerial and not only as a technology issue how is often understood, or even restricted to a single asset. For this, bringing together of different aspects, is possible to introduce in the ICT world a methodology for strategic analysis and risk management socio-economic and technological global system, as an indispensable tool for planning of a complex model of security management.

Despite the growing interest of the research and standardization communities about security issues of computer science and of communication systems, a general consolidated study on security degree of an Information and Communication Technology (ICT) sytstem is still missing. Ongoing standardization activities attempt to solve the security problems of ICT systems by promoting use of many different models of study and analysis. The evolution of ICT has been characterized over the years by several trends to support information society. More paper [Lenz and Reichert, 2005][L. Willcocks and Jackson, 1997][M. Buckley and Braswell, 2004][Heeks, 2008] investigate about ICT applications in various fields. ICT technologies have pervaded all critical infrastructures. Thus, in many processes, the security risk has recently gained in significance. How to apply ICT in various fields has become essential to understanding how to protect what led to its introduction. The adoption of ICT by enterprises is a phenomenon that grows continuosly and that allows implementation of innovative solutions, exploiting emerging technologies and supporting decisions and management processes that are otherwise enormously complex. Innovation in ICT thus bring countless benefits to enterprises in different areas of interest, and it ultimately enables the design of security solutions in many areas of study [Leveque, 2006][Shneier, 2009].

2.2 A Survey about attitudes to Security and Privacy

> *Miscreants are continuing to find new and creative ways to exploit network, system, and even human vulnerabilities to steal information or do damage. The challenge is that we need to block their exploits 100 percent of the time if we are to protect our networks and information. They can be right once; we have to be right all of the time. We need to be ever-vigilant in our efforts to protect our assets, information, and ourselves online. (John N. Stewart, vice president and chief security officer, Cisco)*

There are some scientific reports that show interesting results about the spread of threats and attacks of the networks. One case is VOME (Visualisation and Other Methods of Expression), that is collaborative research project made from researchers from the Information Security Group (ISG), Royal Holloway, University of London, the School of English, Sociology, Politics and Contemporary History (ESPaCH), Salford University and Department of Informatics and Sensors at Cranfield Defence and Security, Cranfield University are working together with privacy and consent practitioners from Consult Hyperion and Sunderland City Council in order to develop new ways to engage service users and service providers in privacy and consent dialogues within and related to on-line services. About Internet use and attitudes of users, they found some results on common activities on the Internet, Experience/Knowledge of Pirvacy Invasion, attitude towards privacy and internet mechanisms, as shows in Figure 2.1 and Figure 2.2 The majority of respondents agree that control and autonomy over the use of their data is important. However, 13.6% of respondents hardly ever and 5% never read user agreements and privacy statements before disclosing personal information for registration to use an online site. Of the technical measures explored, 86.2% of the participants watch for ways to control what people send them online, while only 10.4% fail to engage in such safeguards. There also appears to be a slight tendency for both more experienced and more educated users to read user agree-

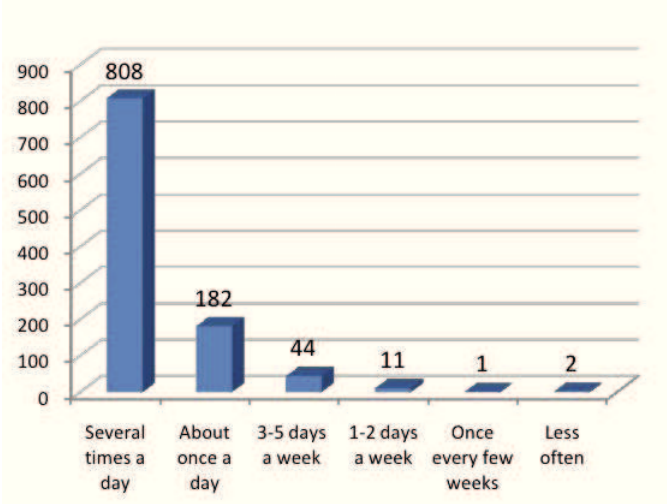


Figure 2.1: Internet use statistics

ments and privacy statements. Almost all the respondents (97.3%) have used the Internet to send/read an email. 85.3% have used the Internet to read news online or search for information. 84.4% have utilised the Internet to purchase something. Web blogs are not so prevalent in the Internet activities of our respondents. Only 28% of the respondents have read blogs on the Internet and only 12.7% have created/written blogs of their own. Gender, length of Internet experience and education levels all contribute to affecting the level of general concern. The survey contains some interesting pointers as to the nature of this effect: for example female respondents appear to have a higher level of general caution than male respondents; the more years someone has used the Internet the lower the general level of caution and education levels affect the nature of the concern [Coles-Kemp and Lai, 2010]. The future of information security remains clouded with numerous uncertainties. However, two things remain certain IT infrastructures are vulnerable and motivated attackers are always ready to exploit these vulnerabilities. It is therefore critical that securing information and infrastructures should not be considered in fear of inevitable attacks, but in preparation for the uncertain future [Dlamini et al., 2009]. From statistical reports of 2010 there are worrying data under so many points of view [Coles-Kemp and Lai, 2010] [Microsoft, 2010] [Cisco, 2010] [Namestnikov, 2010]:

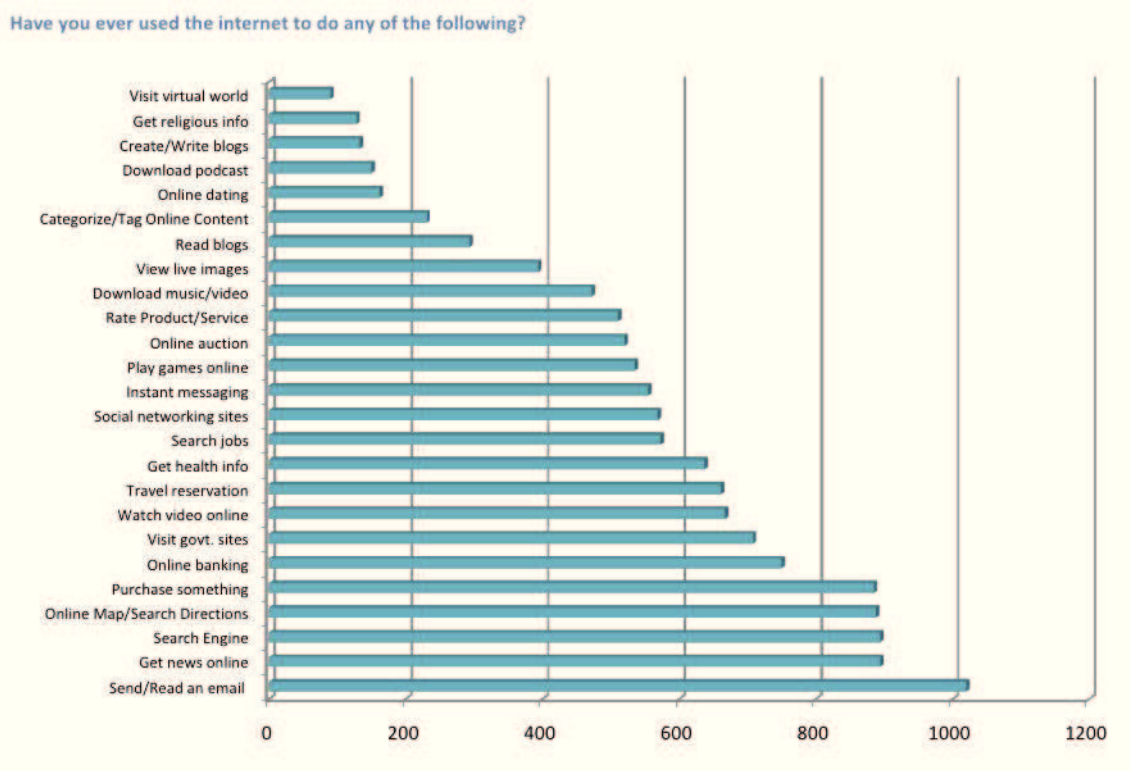


Figure 2.2: Internet use habits

- A total of 327,598,028 attempts to infect users computers in different countries around the world were recorded that's 26.8% more than in the previous quarter.
- The vector of attack employed by the cybercriminals is changing: the percentage of attacks that targeted Chinese users dropped by 13%.
- The most dominant malware family on the Internet utilizes HTML code or scripts that the cybercriminals primarily use to infect legitimate sites.
- A total of 119,674,973 malicious host servers were identified. The US and Russia were both ahead of China in terms of the number of malicious hosting servers.
- Detected vulnerabilities increased by 6.9% from the previous quarter. Six of the ten most common vulnerabilities found were in Microsoft products.
- The number of exploits increased 21.3%. Roughly fifty percent of all exploits take advantage of vulnerabilities in Adobe programs due to the fact that Adobes programs are widespread and can be run on a number of different platforms.
- Almost any device that synchronizes with a computer is used by the cybercriminals as a carrier of malware these days. The most unusual of which has so far been a USB charger for Energizer batteries.

From statisical report of Microsoft Security Intelligence [Microsoft, 2010] and Consumer Report online the Figure 2.3 and Figure 2.4 shows information about threats spread. There are significant differences in the types of threats that affect users in different parts of the world. The spread of malware and its effectiveness are highly dependent on language and cultural factors, in addition to the methods used for distribution. Some threats are spread using techniques that target people who speak a particular language or who use online services that are local to a specific geographic region. Other threats target vulnerabilities or operating system configurations and applications that are unequally distributed around

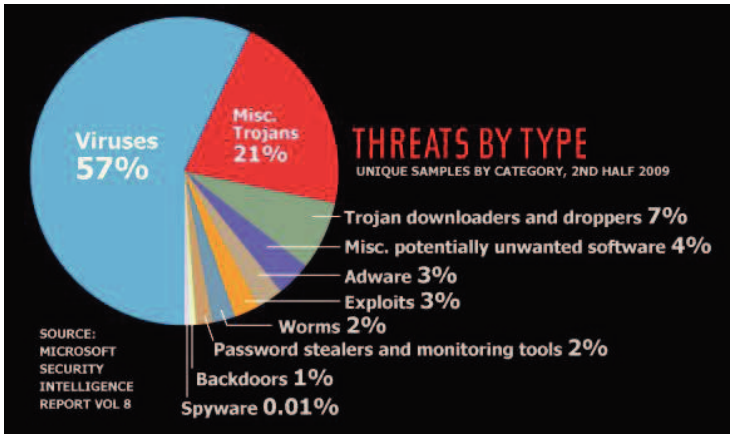


Figure 2.3: Threats by Type statistics

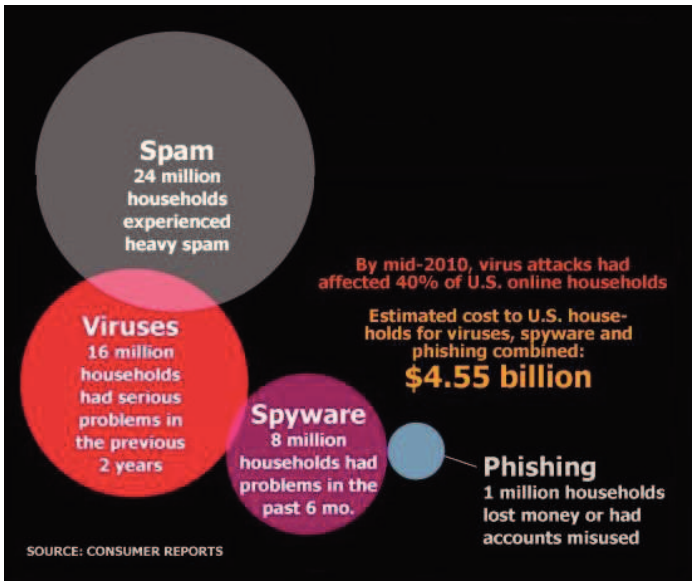


Figure 2.4: Consumer Report about Threats

Category	World	US	Brazil	Fr.	UK	China	Ger.	Russ.	Italy	Can.	Tur.
Adware	37.0%	39.7%	26.1%	72.4%	49.1%	5.3%	44.1%	9.7%	60.0%	45.8%	37.7%
Misc. Potentially Unwanted Software	30.6%	22.1%	35.2%	27.7%	27.9%	48.8%	26.5%	60.3%	26.1%	26.7%	34.7%
Misc. Trojans	28.9%	38.9%	22.6%	12.1%	31.9%	36.6%	25.4%	34.1%	15.5%	36.2%	41.9%
Worms	17.2%	6.3%	24.2%	7.3%	5.9%	14.0%	8.6%	19.9%	11.9%	5.0%	31.3%
Trojan Downloaders & Droppers	14.7%	17.8%	21.0%	7.0%	13.8%	20.4%	13.4%	9.7%	9.1%	17.4%	13.5%
Exploits	10.0%	14.4%	16.3%	2.7%	10.5%	15.0%	7.9%	7.1%	4.0%	13.1%	3.4%
Viruses	6.7%	2.0%	10.1%	1.2%	3.4%	8.0%	2.9%	8.4%	1.7%	2.0%	17.7%
Password Stealers & Monitoring Tools	6.3%	2.9%	18.9%	2.4%	3.9%	4.8%	6.8%	5.1%	4.2%	2.8%	7.8%
Backdoors	5.8%	4.8%	7.7%	3.3%	3.9%	8.4%	5.8%	6.3%	7.1%	4.6%	5.4%
Spyware	0.3%	0.4%	0.1%	0.1%	0.2%	1.8%	0.2%	0.3%	0.1%	0.3%	0.1%

Figure 2.5: Threats Category prevalence worldwide and in 10 individual locations (2Q11)

the globe. In Figure 2.5 shows the relative prevalence of different categories of malware and potentially unwanted software in several locations around the world in 2Q11, Microsoft Report [Microsoft, 2010]. About Symantec Security Report for the threats and security issues of 2010 the Figure 2.6 shows some interesting results [Symantec, 2011].

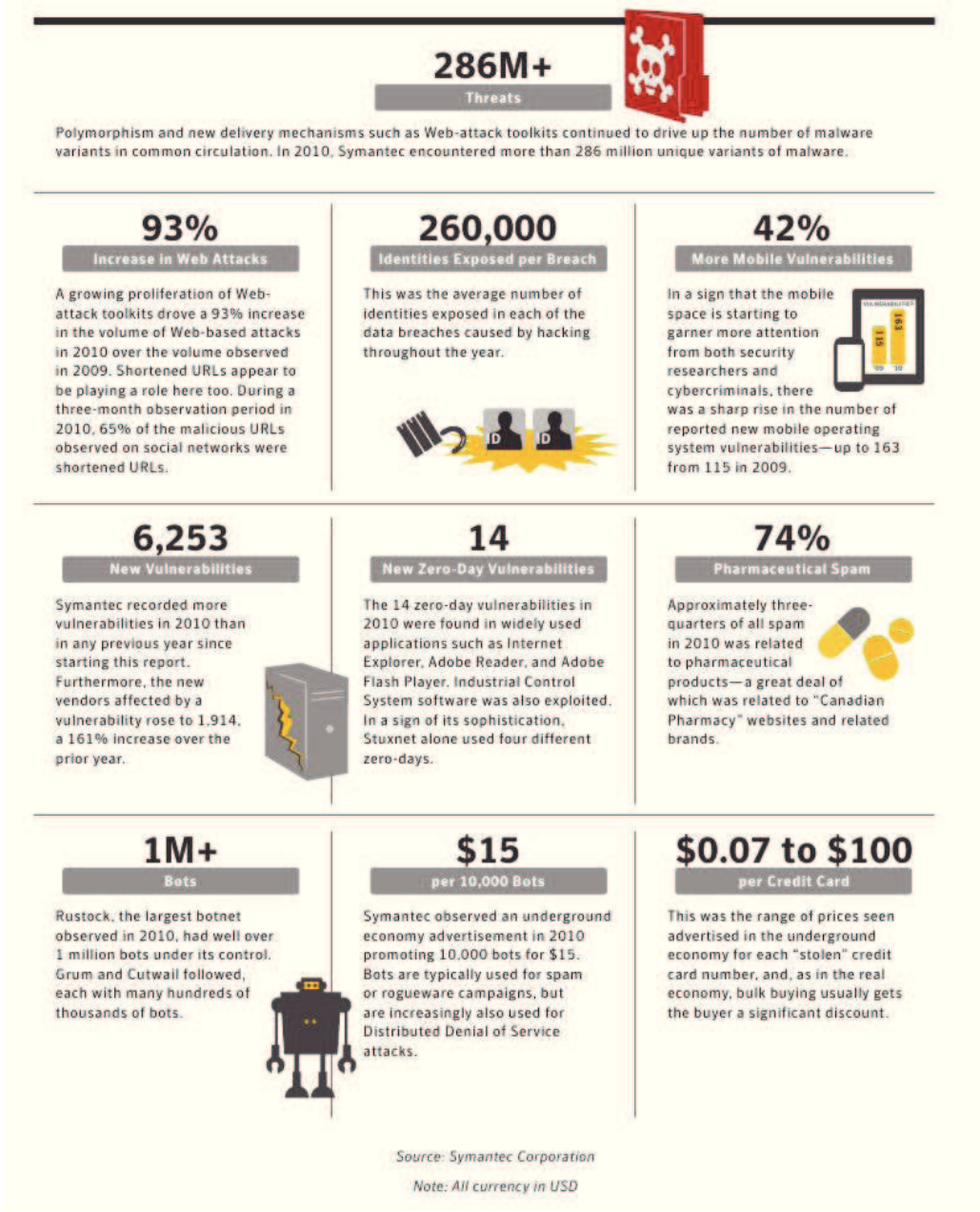


Figure 2.6: Threats in numbers: Symantec Security Report for 2010

2.3 Voice Over IP and Next Generation Network

The evolution of ICT has been characterized over the year by several trends to support information society. More papers like [Lenz and Reichert, 2005][L. Willcocks and Jackson, 1997][M. Buckley and Braswell, 2004] [Heeks, 2008] investigate about ICT applications in various fields. About VoIP (Voice over IP) security, we surveyed many research papers. There is a general tendency to treat the issue of security in communications through taxonomies of vulnerabilities and threats [Ryan and Ryan, 2008a][VOIPSA, 2011][Keromytis, 2009][Keromytis, 2010a]. 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 [VOIPSA, 2011][Keromytis, 2009][Keromytis, 2010a]. 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. 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. Taxonomies and survey show data and results about present statistic information about threats and vulnerabilities. The Figure 2.7 shows results of some survey [VOIPSA, 2011][Keromytis, 2010b]. Different issues, which ranged from relatively straightforward problems that can lead to server or equipment crashes (denial of service or DoS) to more serious problems that let adversaries eavesdrop on communications, remotely take over servers or handsets, impersonate users, avoid billing or charge another user (toll fraud), and so on. In another paper of the same author [Keromytis, 2010b], A.D.Keromytis, Associate Professor of Computer Science and Director of the Network Security

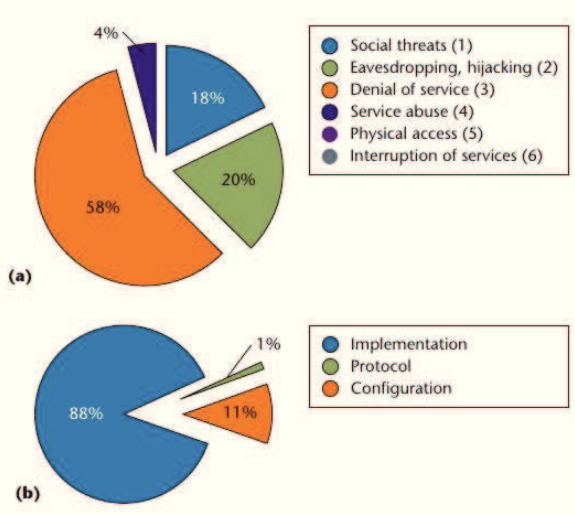


Figure 2.7: Vulnerability and Threats in Voice over IP

Lab at Columbia University in New York, he shows a comprehensive survey of Voice Over IP security academic reasearch, using a set of 245 publications forming a closed cross-citation set. He classified these papers introducing an extension of the VoIPSA Threats Taxonomy, focusing on overview and surveys, fields studies and system/protocol analysis, performance analysis, authentication protocols, architectures, middleboxes, intrusion detection, miscellaneous. In category of Social Threats [Keromytis, 2010b][Keromytis, 2010a], the majority of work in this area focuses on Spam over Internet Telephony(SPIT) detection and prevention, although there are other items included on this category as well. About Spit Detection there are some valuable research results and de- tection methods [Juergen Quittek and Schlegel][MacIntosh and Vinokurov, 2005][Kolan and Dantu, 2007][Dantu and Kolan, 2005], which in general can be divided into three types, signaling-based, content-based and voice-activity based[HUANG Hai and Xiao-Lei, 2009]. The process of migration toward converged networks architecture will cover over time allexisting fixed and mobile networks, but it may not affect Internet. NGN and Internet are both IP-based but they are very different in many aspects, such as services, quality of service, safety and reliability[Keromytis, 2010a]. Ngn should not be regarded as an addition of the Internet network, but a standalone network with its own services. The first step

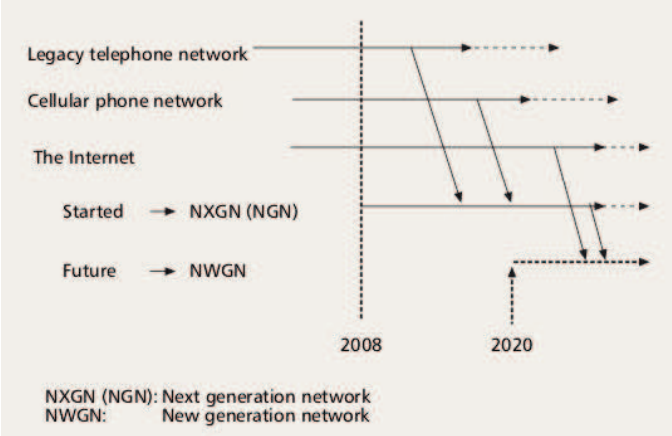


Figure 2.8: NGN and NWGN

towards this new network model is based entirely on IP and IMS (IP Multimedia Subsystem), a multiservice IP-based platform to converge in accessing technology, and whose specifications have been defined by the consortium 3GPP (Third Generation Partnership Project). The general architecture of the NGN reference were instead subject of work of worldwide organization for standardization ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) and European Working Group ETSI TC TISPAN (European Telecommunications Standards Institute, Technical Committee - Telecommunications and Internet converged Services and Protocols for Advanced Networking). With the advent of NGN we see that the standardization goes towards the unification of underlying network technologies, enabling the total convergence of network, processes, and services, and the diversification of services as well as equipment at the network edges.

NGN applies TCP/IP, but is not based on the end-to-end argument, which is one of the fundamental principles for the network architecture of the Internet. Although in these few decades two types of IP-based networks coexist, merging legacy non- IP-based networks, it is time to start research on a future network architecture and protocol beyond the Internet and NGN. Here this is called the new generation network (NWGN) to distinguish it from NGN. NWGN is to have a clean-slate designed architecture, and is not intended to improve TCP/IP-based

networks[Ayoama, 2009]. About Internet is assumed that the two networks will continue to coexist while maintaining their independence. Both could be replaced by networks of totally new and different concept, the New Generation Network (NWGN)[Ayoama, 2009]. The studies on this is at early stage and its development could only begin in a few decades. However we could outline some different features about it. While NGN arise mainly as a development and integration of existing networks, NWGN will not constitute a development of NGN and Internet, but it will be based on total innovative network architecture. Thus, NWGN does not represent a simple attempt to improve the existing protocol stack TCP/IP, but will introduce new protocols and technologies, supporting mobility, ubiquitous, providing broadband multimedia services and reducing energy consumption. This new network could allow to solve all security and quality issues arising from the weaknesses of unsafe and unreliable of the current architectures. The NWGN could be introduced from 2020 and after some decade could replace all IP-based networks, as showed in Figure 2.8.

2.4 Bio-Inspired Models for Communication Networks and Risk Analysis

The similarity between biological processes and computer security problems has long been recognised and studied, over the years. To prove this, in 1987, Adelman introduced the term computer virus, inspired by biological terms, such as Spafford with the term form of artificial life, referring to the virus, and so on. The analogy between the protection mechanisms of living organism and the security could be indeed appealing. Many comparisons have been studied according to several point of view [Ryan and Ryan, 2008b][Dressler and Akan, 2010][Li and Knickerbocker, 2007]. Whereas there have been a moltitude of studies based on a biology-computer analogy for defense methodologies,there have been several studies about similarities between computer worms and biological virus, pathogens. There are many biological terms such us worms, virus, which have been borrowed to name camputer attacks. The term virus is widely used for malicious code af-

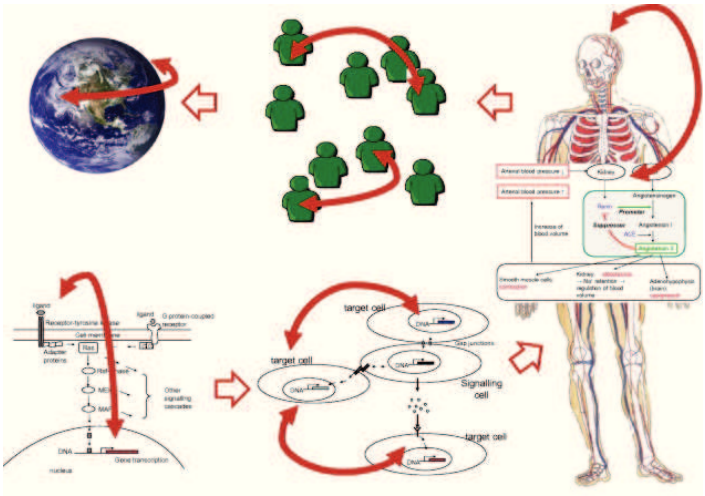


Figure 2.9: Bio-Inspired Approch

fecting computer systems and we could use this term for different threats affecting the communication systems in general. Such usage suggests the comparison with biological diseases. We can describe the computer virus as a program that can affect other programs or entire networks, by modifying them, exploiting vulnerabilities and compromising the security requirements. Recognising that there is a real parallelism between biological systems and computer networking[Dressler and Akan, 2010], we consider the future convergence of the networks and the evolution of the communication systems as a process highly complex, such as a biological entity, as shown in Figure 2.9 .

Our networks are increasingly facing new challages and they grow larger in size, and we want to continue to be able to achieve the same robustness, availability and safety. Biological systems have been evolving over billions of years, adapting to a continuous changing of environment. If we consider information systems and biological systems, they share several properties such as complexity and interactions between individuals of a population (asset of the information systems). There are many analogies between computer systems and biology, and many research studies support this idea [Michael Meisel and Zhang, 2010][Wang and Suda, 2001][C. Lee and Suzuki, 2007]. The reasearch in this area has mostly focused on leveraging epidemiological studies of disease propagation to predict

computer virus propagation[Ryan and Ryan, 2008b][Lachin, 2000][Murray, 1988]. The use of epidemiological model to predict virus is based on a wide range of mathematical models, which has been developed over the years. When considering the spread of an infection through a population many factors are likely to be important, such as the trasmissibility of the agent pathogen, the immune response the general behaviour of the population and the risk perception [Kitchovitch and Lió, 2010]. The risk, like a disease, is the result of three factors: threat, vulnerability and explanatory variables. In the case of a communication system, we talk of the impact of a malicious code or a threat of the network, and therefore, also of damage caused as a result. These results can be distorted because of other variables that somehow might confuse the results, and so called confounding variables (counfonders). These variables may be confounding or interacting variables, also called in econometrics control variables or explanatory variables, which are used into the Cox regression model [Cox, 1972]. The explanatory variable plays a key role in understanding the relationship between cause and effect of a general threat. The explanatory variable is a variable which is used to explain or to predict changes in a value of another variable. This is important to evaluate the relationship between the point events that we define in the next section. To assess the confounding, it is necessary an analysis which provides a collection of epidemiological data sets and informations. This is complex in the case of communications systems and networks. In this case, the analysis is multivariate, because it involved so many factors that influence and change network vulnerabilities. The Cox Model [Cox and Oakes, 1984] also considers the variable time and helps to assess the risk of exposure to a threat in the time. This analysis is embedded in a broader analysis, survival analysis and failure time analysis. As in medical biological models [Ryan and Ryan, 2008b], in this context is necessary to find data that refer to damage to the system or impairment of some or all of the safety requirements imposed in the analysis. Then, from a study done for information security investments [Ryan and Ryan, 2008a][Ryan and Ryan, 2006], the security is hard to quantify and it is seen as the inverse of risk. In that paper the authors develop a mathematical approach to risk management and the detection

of failures requires that what types of failures should be defined. This analysis is important to estimate the expected benefit of a security investment. Everything related to business investment begins with the strategic decisions. To benefit from the investments is essential to understand where, how and when to apply them [Ryan and Ryan, 2008a][Ryan and Ryan, 2008b][Ryan and Ryan, 2006].

Chapter 3

ICT and Information Security

Overview:

|In this Chapter, we want to demonstrate that the importance of security in the strategic planning of an ICT systems security management is directly proportional to the value of the information involved. If this value increases, it follows that the probability of a threat that exploits a vulnerability to successfully attack the system also increases. Therefore, the main problem is to assess and measure the risk of the system. This Chapter sohws the proposal of a step-by-step preventive approach to the problem that allows analysis of the assets, processes, infrastructural vulnerabilities and the threats to the network, and, finally, to manage risk. The proposed architecture provides an all-encompassing framework that aims to address technical, human and economical aspects of the security of a generic ICT system. *Proposal presented in research contributions.*[1]

3.1 Introduction

In any network that allows the dynamic exchange of information,the problem of security is as strong as its weakest link. The main concern has always been the protection of data against potential threats and corruption. In the catchment area, the number of threats and participants involved in the exchange of information is growing every day. Social Networks, Converged Networks [Ayoama, 2009],

[1] [La Corte and Scatá, 2010]

and All-IPs are the future of communications. These networks are designed primarily as a means of sharing and collaboration, and the network makes the sites more flexible and immediate, but also more uncertain. Threats can affect both companies and individuals, and the ICT world has faced new challenges. ICT development has been characterised over the years by several evolving trends [W.J.Vankan et al., 2002][Basole, 2008][Heeks, 2008]. Many aspects can benefit from ICT, ranging from business environments, industrial processes, epidemiologic studies, software development, telecommunications and new generation networks, public services and more. ICT is important for understanding how to develop, manage and organise services; how to improve processes and practices and how to streamline procedures to assist with day-to-day work. In recent years, information and communication technology (ICT) has been characterised by several evolving trends and new challenges. The design, development and management of each information system must address issues related to planning an ICT infrastructure.

Today, all converged networks rely on the means of communication and sharing knowledge and data. Along with many positive benefits, there are several security concerns. New security issues make it necessary to rewrite the safety requirements of the past and to know what the risks are and what can be lost. Information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction and to ensure confidentiality, availability and integrity. A growing number of security research projects are being established[Leveque, 2006][Shneier, 2009], most in the form of taxonomies[VOIPSA, 2011][Keromytis, 2009], but there is currently no agreement on what the security of the future will look like. The Chapter starts with the observation that a new strategic plan is necessary to change how security management is employed. Next it focuses on the requirements that will ICT development in the future. Then, we approach the question of what is the value of the information that an ICT system puts at risk, and the demonstration that the importance of security is directly proportional to the value of the information. The proposal is the Information Security Management Architecture, and the next

sections describe its three step-levels.

3.2 ICT Security Issues

ICT is the study, design, development, implementation, support and management of information systems. The target is to manipulate the data through conversion, storage, protection, secure transmission and safe recovery of information. It is an ongoing process characterised in recent years by the phenomenon of the extension, integration knowledge and dematerialisation of products. In a society based on knowledge and communication, information is the lifeblood, and the nervous system is the Internet, which allows worldwide dissemination. In such a context, the transfer of data, storage, representation and processing via the Internet involves the need for greater security and guarantees against possible damage caused by unexpected events. In [Shneier, 2009], the Internet is described as a means of offering universal access support, providing interface and net neutrality, bypassing censorship, limited surveillance, fighting repression, giving people control over their digital presence, and fostering individual liberty and especially privacy. To secure an information system is more difficult because the natural tendencies of the Internet make privacy more of a challenge. Privacy and security for a system do not occur naturally; rather they must be deliberately planned and built [Shneier, 2009][Leveque, 2006]. Today, the majority of public and private organisations commit processes, whether business or private, to the network. A malicious event, natural or deliberate, can affect information systems, resulting in a sudden interruption of production processes and, thus, compromising continuity. Creating a secure system means dealing with any event, from natural disasters to computer attacks, to ensure the integrity and continuity of processes. ICT can also be seen as an essential resource of organisations, for which it becomes increasingly important to deal quickly, effectively and efficiently with the increasing volume of information.

ICT is a strategic resource capable of providing information and data of higher quality. Thanks to the diffusion of technology and interconnectivity, ICT can enable organisations to redefine their relationships with clients, suppliers and other

organisations. Today, there is a global and highly competitive environment, and ICT can provide a means of streamlining organisations, public or private, with their processes and management control strategies, which can offer a real advantage for competitive decisions. The purpose of this study is to introduce ICT tools with a maximum impact, especially at the enterprise level, and that are grouped to reduce technological, organisational and managerial risks. ICT professionals are tasked with offering multiple surge capacity (from installation to design telematics architectures), management of databases (in the design of integrated services for the convergence of computing) and telephony (in telematics for new methods of transmitting information). The evolution of ICT has been characterised over the years by several trends that support todays information society with multidisciplinary coordination and cooperation. The first characteristic is that the knowledge gained over the last twenty years is greater than all the wealth of knowledge accumulated in recent years. Most of the products and services that we use today did not exist two decades ago. The second characteristic is the increased integration of knowledge used in making products and services. The third characteristic is the dematerialisation of products and the convergence of technologies. The evolution of ICT and its use can provide solutions in terms of tools, techniques and methodologies in different branches of modern digital society[W.J.Vankan et al., 2002][M. Buckley and Braswell, 2004][Heeks, 2008].

A telecommunication network capable of providing essential elements such as multimedia, pervasiveness, mobility and personalisation will be required in the near future. Despite arguments that research within this domain has been exhausted, ICT continues to be a topic of great interest. Many studies have highlighted why and how ICT tools are adopted and implemented. The research concerning this topic is characterised by dierent application environments, including enterprise information systems, electronic commerce, database management systems, network and telecommunications infrastructure, computer hardware, enterprise architecture components, and business productivity applications along with a variety of academic disciplines, such as information systems, computer science, marketing, and strategic management[Basole, 2008]. In this paper, we

want to focus this issue on the evolution of communication systems. Telecommunications must face technological challenges not only to try to introduce more specialised networks, but also more efficient networks. But, in an era that looks to convergence and multiservices, the rebuilding of a new type of communication can determine the natural collapse of the system even before the initial impetus. This problem results from the lack of the analysis and management of security and risk. In just the last year, ICT technologies have pervaded all critical infrastructures. Thus, in many processes, the security risk has recently gained in significance due to the cumulative adoption of ICT-systems. All of these are examples that show that understanding how to apply ICT in various fields has become essential to understanding how to protect what led to its introduction. ICT is capable of addressing todays business issues and the business issues that will continue to emerge. The adoption of ICT by enterprises is a phenomenon that grows continuously and that allows the implementation of innovative solutions, exploiting emerging technologies and supporting decisions and management processes that are otherwise enormously complex in the absence of certain instruments. Innovation in the ICT enables the design of security solutions in many areas of study and work.

However, ICT still lacks a standard application and an assessment methodology for analysing the most appropriate technologies and resources for using services in danger of attack and addressing the weaknesses of the infrastructure system. ICT is applied in different kinds of environments, from urban security to digital forensics. The study presented in [Basole, 2008] resulted from the identification of 390 studies from 61 journals published between 1974 and 2006. The purpose of this research was to provide a sufficient assessment of the current state of adoption of ICT in enterprises. Despite the growing interest in the research and standardisation of communities regarding the security of computer science and communication systems, a general consolidated study on the degree of security of an ICT system is still lacking. Ongoing standardisation activities attempt to solve the security problems of ICT systems by promoting use of many different models of study and analysis. Additional studies [Lenz and Reichert,

2005][L. Willcocks and Jackson, 1997][M. Buckley and Braswell, 2004][Heeks, 2008] have investigated ICT applications in various fields. Relatively little research has been conducted concerning mobile/wireless ICTs, software-as-service, RFID, storage infrastructure, social computing networks and VoIP. Reviewing the literature on VoIP security there is a general tendency to treat the issue of security in communications through taxonomies of vulnerabilities and threats [VOIPSA, 2011][Keromytis, 2010a]. Risk is rarely mentioned in quantitative terms. Recognising what is already described by other studies [Ryan and Ryan, 2008a][Ryan and Ryan, 2008b][Ryan and Ryan, 2006] on risk management for information system security, this Chapter remainder proposes and contextualises the analysis of the communication system to extend the risk analysis models, showing the proposal ISMA architecture.

3.3 A Strategic Model to protect Information

As explained in [ISO/IEC, 2008],information can be defined as an important business asset that can exist in many forms. The concept of information security is more complex to explain and to develop. Information security is defined as a range of controls that is needed for most situations in which information systems are used. This standard is recognised as essential for information security. It represents a process and a methodology that aim to preserve three main requirements: confidentiality, availability and integrity[ISO/IEC, 2008]. Information security means improving the system and protecting assets from various kinds of threats. These threats come through the system to damage and disrupt the processes and the continuity that characterise the system itself, acting on and exploiting vulnerabilities. Information security also involves the planning, analysis and management of a system to minimise risk, reduce vulnerability and provide protection using opportune countermeasures and security investments. It is an important action that requires a specific design and strategic development of new study models to establish, implement, monitor, review and improve single assets or whole systems. We may find a compromise regarding the availability and integrity of information; it is more difficult to ensure the confidentiality of

information because of the high risk to the safety of the whole system. To secure an information system from possible risks, it is necessary to establish a process outlining an information security management system. Thus, a business risk approach is taken to establish, implement, operate, monitor, review, maintain and improve information security, as explained in [Leveque, 2006].

Safety management must not be understood as something purely technical and practical, but as a logical process to identify, assess, and analyse the overall information system. We first need to identify the assets and activities of the system because any activity uses the resources and information to enable the transformation of inputs into outputs. The need for security is generally linked to the value of the information transmitted, which is an important value to consider with respect to whether to invest in a security and information protection strategy. Recent years have highlighted the increasing need for the protection of personal data of individuals and legal entities to ensure their privacy. Thus, the need to rewrite the policy measures governing the security of new systems, such as communications that favour interconnectivity and facilitate the exchange of multimedia data between users,arises. At the same time, new communications systems are generally more vulnerable to networks becoming a continuous source of new threats. Therefore, it is essential that, in addition to the new strategy, changes be made in the way that the value of exchanged information is determined. In[Leveque, 2006],the subject strategy is defined as the science and art of planning, which requires accurate methods. A good strategy model based on three steps, which are situation, target and path:

1. Situation: the current environment of a communication system with several security requirements and security weaknesses.

2. Target: the strategy goal and, thus, the desired managed information system.

3. Path: the method of moving from the situation to obtain the target.

The three steps follow the process model PDCA,which is proposed in [ISO/IEC, 2008] and can be applied to information systems. The target is to arrive at a

specific, final situation to minimise the risk and manage the policies and controls of a communication system. This goal is achieved through strategic planning, starting from an initial situation that analyses the environment and main characteristics of the context case study (situation) and building a model of security management architecture (path).

3.4 Security Degree and Optimal Investments

The importance of security is directly proportional to the value of information in any ICT system. A company or an individual who decides to invest in safety should be able to tell if the planned expense of the infrastructure improvement, such as protection of the assets of the system, is needed. They should also be able to assess, in advance, the expected benefits from this investment for proper strategic planning. The information system can be found in many forms, whether public or private, and it can be a critical business process, or it can be redundant. For the general user, then, information can be more or less sensitive, and each database can be more or less confidential. In general, there may theoretically be a multitude of degrees of confidentiality and secrecy. The safety requirements vary from system to system, and they acquire different levels of importance depending on the surrounding environment. Under these considerations, the value of information today, in any form, increases significantly if it is exchanged and shared with any form of communication that exists today. Meanwhile, the communication network, which is approaching total convergence, is increasingly subject to a number of threats to the entire system. 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. The higher the stakes, the more the attacker is determined to damage the system, or at least part of it. Thus, to design a security infrastructure, it is necessary to properly assess the importance of security and to ask what the value of the information is that is at risk if it is shared and communicated in the absence of an analysis that adequately estimates the risk. The Informative Value, as defined in eq.3.1, of a

generic ICT system is a function of three parameters:

$$V_{ICT=}f(C,S,E) \tag{3.1}$$

C= Informartion Constant of the System

S= Sharing Variable of a Communication Process

E= Environment Variable of the System

We consider two systems hypothetically. For the first and second system, at t_0, we have the following equations:

$$V_1^0 = C_1^0 + \ E_1 \tag{3.2}$$

$$V_2^0 = C_2^0 + \ E_2 \tag{3.3}$$

Then, the first system becomes the source of sharing. It exchanges a quantity of information with the second system, involving certain assets and communication processes, to share different types of data. So at t_1:

$$V_1 = \ V_1^0 + S_{12}t \tag{3.4}$$

$$V_2 = \ V_2^0 + S_{12}t \tag{3.5}$$

S_{12} is the sharing variable of this communication beetwen these two system:

$$S_{12} = \ \gamma_{12}C_1 + \mu_{12}E_1 + \beta_{12}E_2 \tag{3.6}$$

It depends on three factors. The information constant of the source of sharing is weighted by a value,γ_{12}, which we call the sharing fraction. The environmental variables of the two systems are weighted by two constants,μ_{12} and β_{12}. These constants depend on the assets and processes involved. In the time interval of the communication, the value of the information shared grows according to this trend, depending on S_{12}.

$$V_{S12} = \ S_{12}t \tag{3.7}$$

Therefore, this proposal defines define I_S as the Importance Security Factor. I_S is an essential parameter for all ICT systems. It allows for evaluation of the

importance of the strategic planning of security for the entire system. For a generic system ,i, that wants to share and communicate with a generic system, j, the Importance Security Factor is a function of the sharing variable S_{ij}. Thus, for the first system of our example:

$$I_{S1} = f\left(S_{1j}\right) \quad with \quad j = 2, \ldots\ldots, n \tag{3.8}$$

$$S_{1j} = \gamma_{1j} C_1 + \mu_{1j} E_1 + \beta_{1j} E_j \tag{3.9}$$

$$I_{S1} = a_{12} S_{12} + a_{13} S_{13+} a_{14} S_{14} + \ldots + a_{1j} S_{1j} + \ldots + a_{1n} S_{1n} \tag{3.10}$$

The Importance Security Factor is the linear combination of the S_{ij}, and the a_{1j} depends on the weakness of the system and the threats.

$$a_{1j} = th + w \tag{3.11}$$

If S_D is the Security Degree of the system, according to equations 3.9,3.10, we arrive at this conclusion:

$$I_{Si} \propto \frac{1}{S_D} \tag{3.12}$$

$$S_D \propto \frac{1}{Risk} \tag{3.13}$$

The security decisions are generally taken outside of the strategic planning context and are made after the damage occurs when a network threat successfully exploits a vulnerability of the system. A Security Investment does not stem only from a statistical evaluation of threats and vulnerabilities, or from the subsequent action that is taken as the result of an attack that has already happened, but from the study of the system in its entirety. To benefit from the investments, it is essential to understand where, how and when to apply them**?**. Thus, the Security Investment in the Strategic Planning of security of an ICT System is proportional to the Risk and Importance Security Factor, which is the inverse of the Security Degree of the System:

$$SEC_{INV} \propto \frac{Risk \cdot I_S}{S_D} \tag{3.14}$$

In this way, we demonstrate that to decide the optimal investment, we must address three key stages:

1. For the assessment of I_S, we need to know the system information, assets and processes involved in communication, and we must assess the threats and vulnerabilities of the system and network.

2. The analysis of risk requires knowledge of the probability of failure and the its distribution.

3. Finally, we can assess the degree of system security and analyse the existing countermeasures to try to decrease the risk, minimise the losses, and manage the security.

In the next secrton these three phases and the three step-levels of the proposed architecture are presented and proposed. The proposal is about a novel architecture to assess the information security of an ICT system. Through a process approach, the Information Security Management Architecture is constructed by systematically considering the various kinds of knowledge that affect this type of system. The interactions and relationships between technological, procedural and security aspects of the system are illustrated in the following paragraphs. These interactions enable the construction of the management architecture and the development of the protection of information assets. The value of the information plays a key role when the assets are exchanged. The assets must then be protected in proportion to their value. It is necessary to identify, assess and classify the assets of the system, the processes concerning it and the common threats.

3.5 ISMA:Information Security Management Architecture

The architecture planning is divided into three steps: understanding the security issues; evaluating the risk and the probability of damage that can crash the system or part of it; and, finally, the countermeasures and strategic decisions to manage the risk by seeking to ensure the highest degree of security. The targets of the model of ISMA are the following:

1. Demonstrate the validity of the study through the assessment of the value of the information. The interest in the protection of the information exchanged should be directly proportional to its value. This factor leads to greater investment in security, which are former terms of economic and human resources and technology involved.

2. Identify, assess and analyse the environment and the processes concerning it. To understand where we can act in terms of establishing security, we must picture the state of the system and the conditions under which it exists. Forgetting something would mean the loss of security investments and would increase the vulnerability and potential attacks.

3. Contextualise the system under consideration on the basis of security issues. Contextualising means rewriting parts of the system in light of the vulnerability and threats that can appear subsequent to an attack. In this way, the assets have to be identified, to be analysed in terms of system weaknesses.

4. Classify the logical information assets.

5. Manage the system by seeking to ensure the highest degree of security. The proposed architecture is a way of understanding a system and a way of analyse and contextualising security issues. At the same time, the proposed architecture provides a step-by-step process of evaluation, analysis and management.

Thus, the proposal is a high-level of security architecture to:

1. estimate the information value;

2. protect information

3. evaluate the risk measures

4. identify the countermeasures

5. decide the security investments

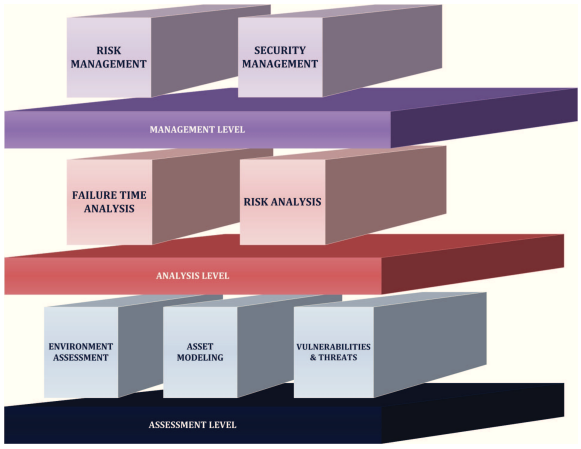


Figure 3.1: ISMA process-approach oriented

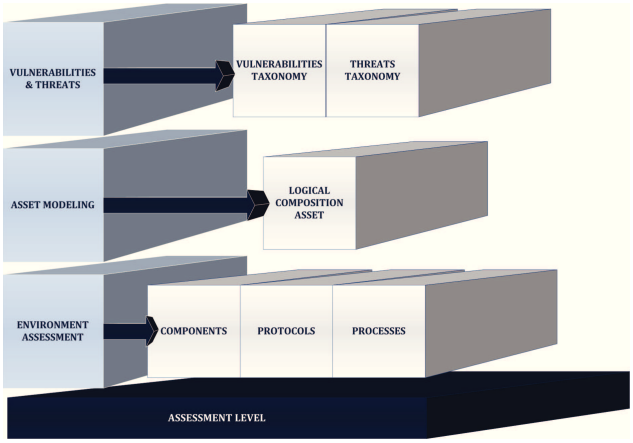


Figure 3.2: SL1-Assessment

To analyse, identify, solve and, finally, manage VoIP security issues, it will be necessary to act with greater awareness in the future to strategically plan a network that will converge communication technologies, but such networks will inherit the weaknesses of each system. The architecture applied to VoIP allows us to display a first application of the proposed architecture. This, as mentioned above, is a process-oriented architecture that on the one hand allows one to settle a high-level security architecture of a system, and on the other hand allows one to analyse a communication system step-by-step. The ultimate goal is to be able to manage the security of this system.

In this architecture, as in Figure 3.1, the phase of management is not just a separate process, but an architectural level of abstraction that allows us to read differently each asset and to give a general measure of the degree of security. This level, thanks to the results obtained in the layers below, not only provides a measure of the degree of security, but it can also provide support for decision making in terms of economic investments to make the system more secure. We can use the policies and patterns of monitoring countermeasures that are more efficient in terms of performance, to manage the system. The process specified in the strategic planning becomes ISMA-oriented. This architecture consists of three levels, and it should be read from the bottom to the top:

1. Assessment
2. Analysis
3. Management

Each level is a fundamental part of the study of a complex communication system in terms of security. SL is the Step-Level to highlight its dual nature. This architecture could be aimed at various sectorsof interdisciplinary RD:

1. Failure Time Distribution based on Biological Models
2. Risk Analaysis for Communication System
3. ICT Management tools
4. Security Economic Investments
5. Decision Support IT Enterprise System

3.5.1 Assessment Level

The level of Assessment, as shown in Figure 3.2, is the first step-level of the architecture. The Assessment level includes all of the procedures and stages for the evaluation and analysis regarding the initial study of the system. Recalling that the architecture is characterised by a process approach, this step includes

all of the procedures and processes for evaluating the general environment in its physical components and logical components. There are three phases that characterise this level:

1. Environment Assessment
2. Asset Modelling
3. Vulnerabilities and Threat Assessment

The first step, Environment Assessment, is to identify and assess the main characteristics from the environment and to picture the initial state of the system. This level identifies the components of the physical system, the protocols in use, and the exchanged information assets to certain processes that in some way can expose the system to the likely risks caused by security incidents. The second step, Asset Modelling, is to identify and classify, on the basis of the results of the assessment level, the asset structure of the system. This step allows the identification of abstraction levels that stem from an action mapping between processes and components, and it thus identifies the assets of a logical system of interactions involving dierent types of information exchanged. Finally, the third step, Vulnerabilities and Threat Assessment, identifies the causes of likely security incidents and writes the taxonomy of common threats. In so doing, the analysis is of the system by identifying its vulnerabilities and malicious actions as may exploit them.

3.5.2 Analysis Level

The level of Analysis, as shown in Figure 3.3, is the central part of the architecture and the second stage. The analysis level comprises the phases of Failure Time and Risk Analysis. To manage a system well, it is necessary to analyse each aspect of security. Before looking at the two phases, we offer the following definitions:

1. Failure may not necessarily mean the catastrophic destruction of information assets or systems. Rather, it is a real or potential compromise of

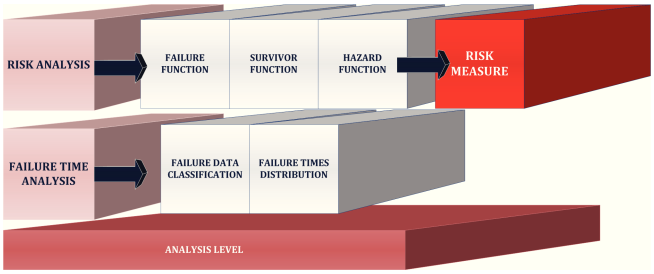


Figure 3.3: SL2-Analysis

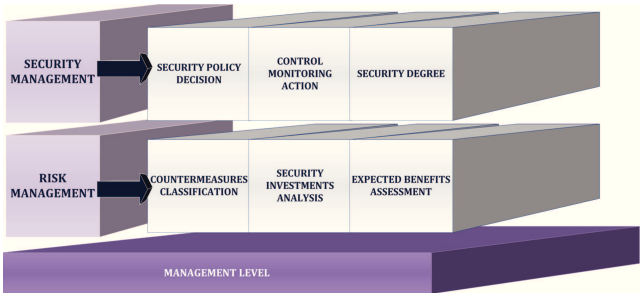


Figure 3.4: SL3-Management

confidentiality, availability and integrity. Thus, the detection of a failure requires that we carefully define what types of assets are to be considered.

2. Failure Time Analysis was primarily developed in the medical and biological sciences, but is also widely used in the social and economic sciences.

Thus, there are two phases that characterise this step:

1. Failure Time Analysis.

2. Risk Analysis.

3.5.3 Management Level

The final level is the these Management Level, as shown in Figure 3.4. The Management level represents the level of abstraction through which it is possible to have an overview of the system in terms of risk and security. This level evaluates the countermeasures and the possible security investments required to optimise

the system. On the basis of the first and second levels, this is the abstraction level, where it is possible to have a global and general vision of the degree of the systems security. There are two phases:

1. Risk Management.

2. Security Management.

Risk Management involves the identification and evaluation of existing countermeasures. Then, considering the behaviour of the risk function, it assesses the likely security investments by checking that there is a positive expected benefit from these actions. Finally, in the Security Management phase, we can give a complete measure of the security degree of the system, and we can decide the policies of control and monitoring.

3.6 Some Considerations and Summary

This chapter shows and presents a new model of study and analysis by process-oriented architecture. The architecture allows a stratification of the management of security of information exchanged in a system. At the same time, a step-by-step process through the sequential levels is presented. The ultimate goal is to provide a procedure that applies to any system, allowing the calculation of risk and the application of the appropriate investment in safety to manage security systems. The route to this final state is through the assessment of every aspect of a system, including the environment, communications and relations, and technological and human resources. The information exchanged adds value to the simple data, and it adds resources.

Chapter 4

Voice Over IP Security

Overview:

| A Security Analysis Model of communication system is still lacking because these systems, starting from PSTN (Public Switched Telephonr Network), have never suffered from serious security problems. Now, VoIP (Voice Over IP) has become a valid alternative to the traditional telephone network. It is a technology that has a key role in the development of convergence in the near future, but with VoIP to ensure privacy is extremely difficult. This Chapter presents an overview of VoIP technology, the study of safety issues related to it and to general communication systems. This Chapter shows the ISMA architecture presented in the previous chapter, applied to VoIP case and propose a user-profile framework against Spit (Spam over Internet Telephony) to evaluate and identify the best security path of countermeasures. *Proposal presented in research contributions.*[1]

4.1 Introduction

The communication is the driving force of the society through a network and the information is the most important asset [Heeks, 2008][Leveque, 2006]. 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

[1] [La Corte and Scatá, 2010][Scatá and La Corte, 2011]

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. 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 a generic VoIP 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 [VOIPSA, 2011] [Keromytis, 2009] [Keromytis, 2010a]. 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.This Chapter proposes and introduces 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. The next sec-

tion defines general profiles based on certain parameters, and with a user-profile matching we can identifies the best security path which must be applied.

4.2 Communication Security Issues

One of the most important process is the communication of voice. Today we can reach any other through the telephone communication by simply lifting the handset and dialing the corresponding number. 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. 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.

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. This 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 [Ayoama, 2009]. Convergence is the process of evolution of telecommunications networks(6-IJISR). 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 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 [VOIPSA, 2011]. In accordance with the definition of ITU, a Next Generation Network (NGN) 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
- functionalities 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.

4.3 VoIP Overview

VoIP is a the transmission of voice over traditional packet switched IP networks and it is one of the hottest trends in telecomunications. VoIP wantrs to provide the efficiency of a packet switched network while rivaling the voice quality of a circuit-switched network. VoIP can be implemented in several ways. A Public Switched Telephone Network (PSTN)-based telephone can communicate with a VoIP application. It is useful to begin in this section with a brief explanation of VoIP which is not one service but rather a multitude of possible services.

It is an application conveying real-time information emulating and improving traditional telephone service. VoIP refers to a class of products that enable advanced communication services over data networks. VoIP has seen rapid uptake in both the enterprise and consumer markets. An increasing number of enterprises are replacing their internal phone switches with VoIP-based implementations, both to introduce new features VoIP is one of the application that provides global interconnectivity at a low cost or in cases where calls are established between peers in an IP network the cost is negligible or non-existent. This technology refers to a class of products that enable advanced communication services over data networks. This technologies offer higher flexibility and more features than traditional telephony (PSTN) infrastructures.

PSTN comprises thousand of interconnected network elements over dedicated circuit-switched facilities that use SS7 for signaling. PSTN is based on a model of trusted neighbors, that maintain a closed network where access is limited only to carriers and service providers. This technology requires a great financial investment and very high cost of access. PSTN is composed of interconnected circuit-switched networks that are built, owned and operate by private or governmental organizations. VoIP as it is used today has some fundamental differences compared to speech transmission in the PSTN:

- The end-terminals in PSTN are easy-to use dumb terminals that are connected to a smart and complex network, the AIN (Advance Intelligent Network).
- In PSTN we have the physical separation of signaling messages and circuit data/voice. The signaling is done in a separate and closed network. In VoIP signaling is done in an open, highly insecure network. The signaling media traffic is transmitted using the same physical medium.
- VoIP offers mobility, not PSTN, and because of there is no mobility in PSTN, authentication is not necessary, instead it is necessary in VoIP.
- In circuit-switched the access to the network is limited, whereas access to a VoIP network is not restricted.

VoIP data processing consists of four steps:

- Signaling.
- Encoding.
- Transport.
- Gateway Control.

About Protocols:

- for signaling SS7/Q.931/SIGTRAN - H.323 - SIP - SCCP - RTSP - SDP - MGCP/H.248.
- for encoding/transport RTP - RTCP.
- other protocols IPV4/IPV6 - SCTP - TLS - DHCP/DNS/ENUM -SIGCOMP - RSVP

Signaling is to create and manage connection between endpoints. H.323 [Goode, 2002] and SIP [J. Rosenberg, June 2004][Rosenberg, 2008] are two widely used signaling standard for call setup and management. They also handle establishment setup negotiation, modificationand teardown of session. H.323 is a 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, e.g. 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 adresses many security issues and can use SSL for transport-layer security. H.323 protocol stack is designed to operate above the transport layer of the underlying network, it requires three logical entities: gateways, gatekeepers and MCUs. SIP was designed sepcifically for the Internet. It is a IETF standard and it is responsible to establish, modifyt or terminate a call between two o more users. A client send 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. SIP exploits the manageability

of IP and makes developing a telephony application relatively simple. It is an application-layer control protocl for creating, modifying and terminating sessions with one or more partecipants. About Enconding, when the conversation commences, the analog signal produced by the human voice need to be encoded in digital format suitable for transmission across an IP network. Here a compression algorithm can be used to reduce the volume of data to be transmitted. A number of factors must be taken into account:

- bandwidth usage.
- silence compression.
- intellectual property.
- resilience to loss layered coding.
- trade-off between voice quality and bandwidth used.
- algorithmic delay introduced by coding/encoding sequence.

The voice samples, in the transport phase, are inserted into data packets to be carried on the internet using typically the real-time transport protocol(RTP) and real-time control protocol(RTCP). The media transport protocols control digitizing, encoding, decoding and ordening of voice samples for real-time communications: RTP[H. Schulzrinne, 1996] is the real time transport protocol according to RFC 1889. 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 and video over the internet. It include services such as payload-type-identification, sequence numbering and time stamping. RTCP [M. Baugher, 2006] is a real-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. Gateway Control phase is important because the IP network itself must then ensure that the real time conversation is transported across telephony system to be converted by a gateway to another format into interoperation with different IP-based multimedia scheme.

The network architecture for VoIP is neither simple nor homogenous. The real key advantages list of VoIP are the following items:

- Open Architectures.
- Software-based Implementation.
- Enabled to advanced communication services.
- New equipment and network-link consolidation.
- Ubiquitous consumer-grade broadband connectivity.
- Benefits in both enterprises and consumer markets
- New features for VoIP in NGN.
- Elimination of redundant equipment.

The VoIP network architectures have many similarities to both legacy telephone networks and traditional IP networks. After all, the features, network design, functional components and deployment principles are drawn from traditional networks such as PSTN telephony, peer to peer communications and enterprise IP networks. Consumers have enabled a slew of technologies with different features and costs including:

- P2P calling - VoIP in Peer to Peer IP Telephony
- Internet to PSTN network bridging.
- VoIP in Enterprise Network.
- VoIP in Carrier Networks.
- VoIP in Service Provider Architecture.
- Softswitch Architecture.
- IP Multimedia Subsystem.

- Wireless VoIP.

These technologies and business models are the engine and the bases for the creation of startup companies that are challenging the traditional status quo in telephony and personal communications. A number of PSTN providers have already completed or are in the process of transitioning from circuit-switched networks to VoIP-friendly packet-switched backbones. Thus, the convergence of voice and data worlds introduced exciting opportunities and benefits, the total challenge is complex to manage, in terms of infrastructure, real reliability and trying to maintain bridging, real and virtual, with traditional models, in terms of legacy, security, quality and general performances. The VoIP Infrastructure can be visualized in three layers:

- End-Users Layer.
- Network Layer.
- Gateway Layer.

A VoIP phone, or terminal, is used to initiate and receive calls. THe end-users equipment provides an interface for users to communicate with other users. Is possible to identify "soft phones" and "hard phones". A soft phone is a software based VoIP implementation that runs on desktop PCs, mobile phones, and other platforms, that emulates a telephone. A hard phone has an interface very similar to a traditional telephone where the VoIP software can run on the appliance. The end-users equipment is the first interface with user and can be deployed in different kind of environments. In a broader vision, depending on the architecture, the VoIP terminals can also be a called user agent (UA) or terminating user agent. Another case could be a VoIP terminal that consist of software that automatically receives (voice mail) or make (auot-dialer) calls. The security of such end-users components depends on how they are installed and who have the access and the permissions to use it, rarely the equipment have complex security features built in or they could have simple countermeasures to avoid access. The network layer is characterised by different comonents. Some of these belong to service infrastructure and some to the supporting infrastructures.

If we consider each network components, we can identify security concerns resulting from the past linking to the traditional IP-network and the new vulnerabilities due to the voice traffic introduction. About Gateway Layer, gateway is responsible in integrating the IP network with the PSTN. Care should be taken to ensure security countermeasures, monitoring and specific policies against attack and to reduce vulnerabilities. Gateway has a key role in functionalities include compression and decompression, signaling control, call routing and packetization. A gateway can operate between similar network, or it can act as a proxy between different architecture and protocols. VoIP gateway interface with external controllers such as proxies, gatekeeper, media gateway, network management systems and billing systems. They presents potential weaknesses and attackers can exploit them to make malicious actions. Usingthe step-by-step ISMA Architecture model is possible to summarize, classify assets, processes, vulnerabilities and threats, proposed in previous Chapter.

4.4 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 voice spam or 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.

4.4.1 Vulnerabilities and Threats

The security of communication networks can be analyzed from several different perspectives. In this context, to understand the security in VoIP first should be analyze vulnerabilities, which represents probable and potential breaches, caused by weaknesses in different part of infrastructure assets and processes. Although IP telephony differs from traditional legacy telephony, it maintain common features and business requirements. The IP protocols family has inherit vulnerabilities related to the core IP services and issues linked to message sequences used in some mechanisms. The weaknesses affect services and mechanisms on top of IP networks and can be used to perform various attack. In any VoIP implementation

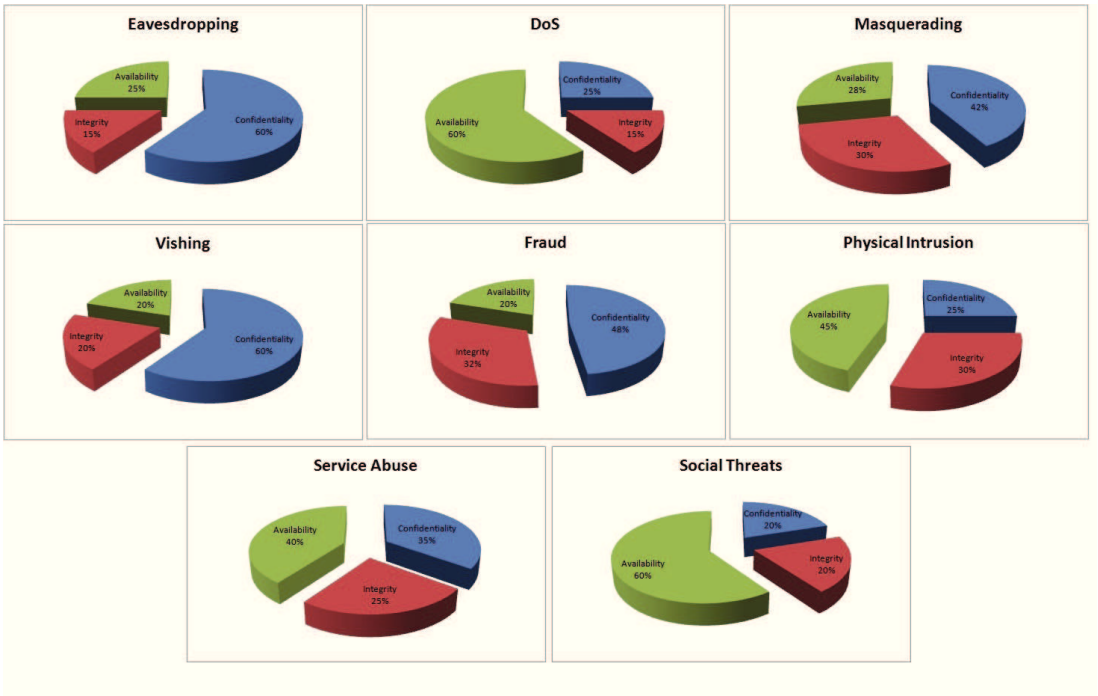


Figure 4.1: Impact on CIA requirements

the areas that should be protected from possible attacks are:

- Signaling and Media Protocols (that support the services).
- Service Infrastructure (phones-equipment, proxy, gateway).
- Supporting Infrastructure (router, dns server, switch, NTP server, etc.)
- APIs
- Network Peering.
- Administration Interface.

The threats can exploits them and cause attacks and a serious impact on CIA requirements (Confidentiality, Integrity and Availability) as in Figure 4.1 . 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 suchas 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. There is a general tendency to treat security issues through taxonomy. The taxonomy is the practice of science of classification or the result of it. Taxonomy uses taxonomy units and is a particular classification characterised by a hierarchical structure or classification scheme. Now, follows a list of main threats [VOIPSA, 2011][Keromytis, 2009][Keromytis, 2010a] 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 vic-

tim 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. This category includes

- 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 the Spam over Internet Telephony (Spit), which is discussed in the next section.

4.5 Spam over Internet Telephony

VoIP, due to it openness to open IP world is more vulnerable to security threats. Spam is one of these. 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. Spam over Internet Telephony (SPIT), or voice over IP (VoIP) spam. 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 communica-

tions disturb the users with unwanted calls and advertisements unsolicited. Spit can be defined also as "unwanted", "bulk" or "unsolicited" calls over IP telephony network. This threat is very similar to Spam in the email systems but it is deliverwed by means of voice calls.

Users of VoIP are troubled with unsolicited telephone calls from telemarketers, advertisers etc. Spit calls can be telemarketing calls used for influencing callees to sell products, for example. They can affect performance, quality and security of the network but also annoyed users. 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. 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 difcult 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. IP-based SPIT is three orders of magnitude cheaper to send than traditional telemarketing calls [Juergen Quittek and Roman Schlegel, 2008]. 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 real 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. The main problem of the detection of Spit are the following items:

- decision time

- real-time analysis and detection
- request of feedback
- unavailable of content
- similarity of signaling messages for both Spit and not-Spit calls
- speed of the detection
- intrusive methods
- efficiency

So taking into account the difficulty of existing detection models. In this dissertation the proposal is a different way to assess the problem of the Spit with a different point of view. The proposal is 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.

In the proposed model we classify users according to certain parameters in order to associate to each the most appropriate countermeasure. Thi strategy could be needed to increase effectiveness and to adapt the detection methods to special environments. 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 [Juergen Quittek and Roman Schlegel, 2008]:

- minimize the probability of blocking legitimate 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, the framework proposed in the next section is to suggest solutions to these issues, combining the capabilities offered by different countermeasures methods and the user-behavioural assessment model to efficiently block SPIT calls while requiring the least possible interaction with caller and callee, in some cases, a faster resolution in other cases, or a high effectiveness. The model evaluate the nature of caller in terms of probability by analyzing the users social habits during the observation period. Then with the information extracted, the model allow to decide if a call could be a Spit call or not, and the best path of security countermeasures against Spit, referring to the right profile of users. A Spit may be advertisment call to the end of users or may be another attack hidden, such as vishing if the attack wants to convince the users to dialed some expensive phone numbers or make users to diclose his personal information, or a Denial of Service (DoS), if the attackers make flooding calls compromising telephony services.

4.5.1 Countermeasures

We describe briefly the existing countermeasures [Lee and et al.] [G.F. and et al., 2007][Juergen Quittek and Roman Schlegel, 2008] 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.

Now,follow the countermeasures described above in a conceptual map where the nodes are the antispit methods. The proposal assesses each of them, as in Figure 4.2. Each method is characterised by a different value, High (H), Low (L),

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 4.1: Spit Countermeasures Assessment

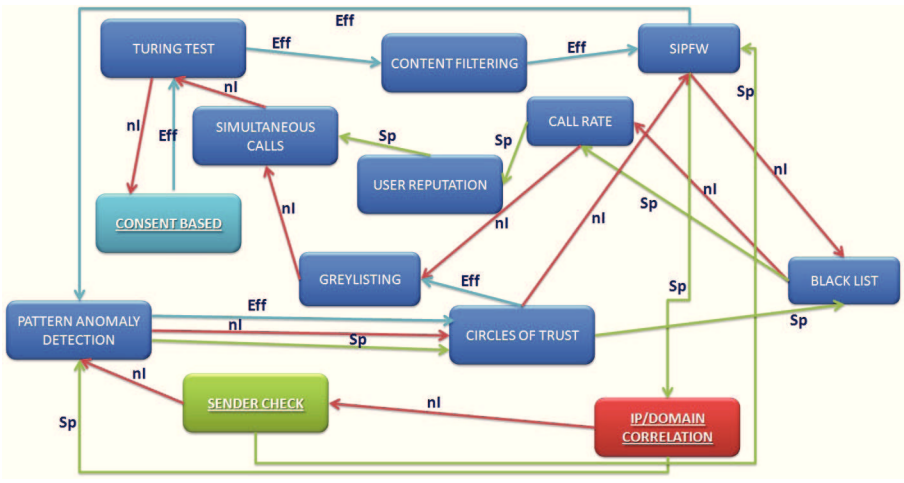


Figure 4.2: AntiSpit Methods Assessment

Medium (M), Medium Low (ML) , Medium High (MH), of three parameters as in Table4.1, 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 call, to determine more velecomente and 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 spam or not. This is at the expense of speed and therefore of the degree of intrusion detection. The map in Figure 4.2, shows 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.

4.5.2 User-Profile Framework against a Spit Attack

The framework that will be presented below, allows 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, it allows to 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 4.3.

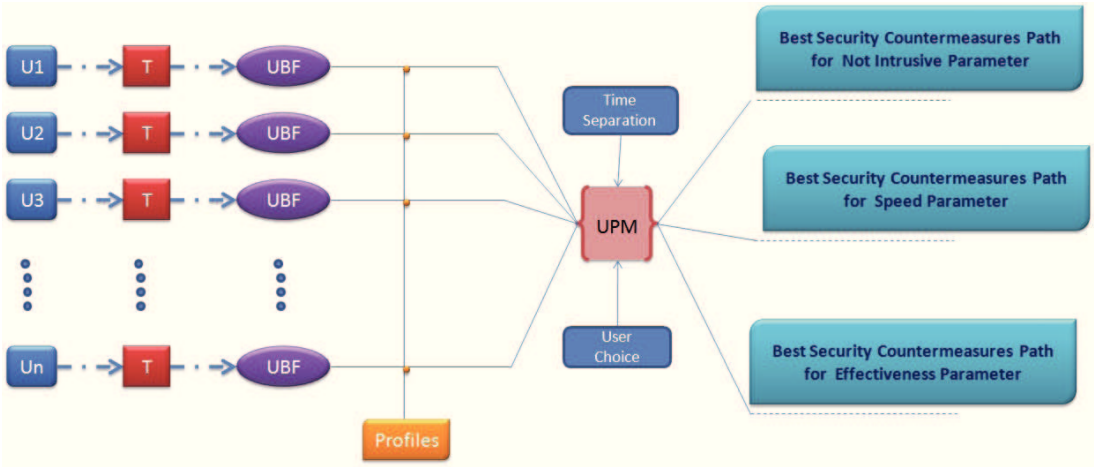
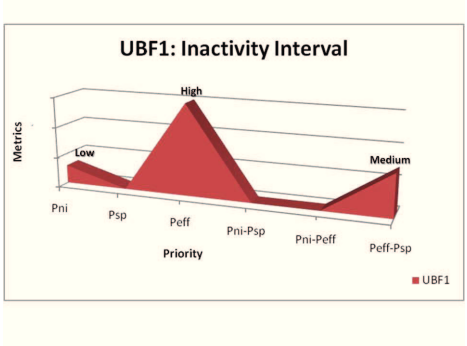


Figure 4.3: User-Profile Framework

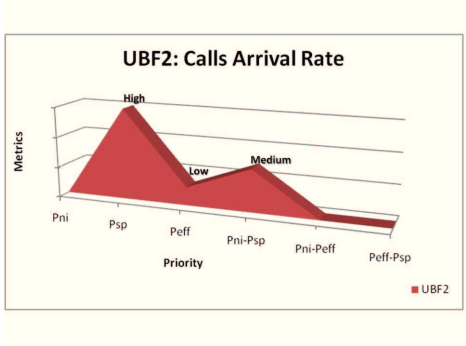
We can identify the following parties:

- 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;

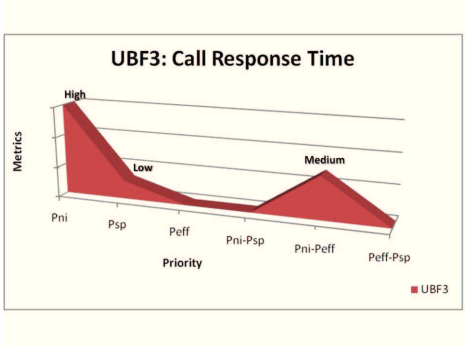
In order to describe the features of the framework, the following definitions have to be given:



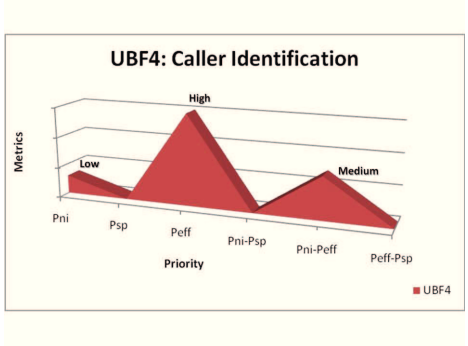
(a) Inactivity Interval Assessment



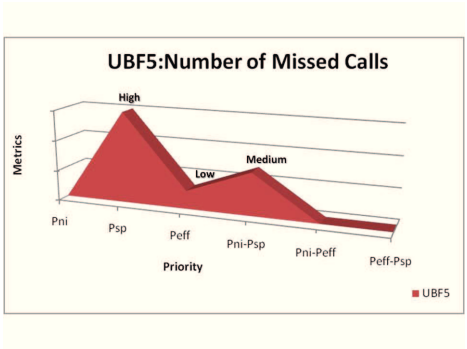
(b) Calls Arrival Rate Assessment



(c) Call Response Time



(d) Caller Identification



(e) Number of Missed Calls

Figure 4.4: User-Behavioral Features Assessment

- 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 definitionare 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

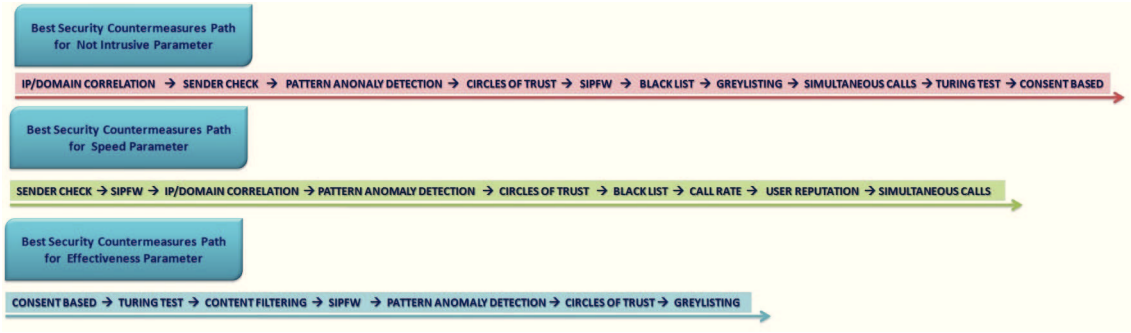


Figure 4.5: Security Countermeasures Path

the User Choice and Separation Time, we associate a qualitative measur (High Medium and Low) to each UBF observed during the observation period T.Each measure of UBFs, matches a priority of parameters among not Intrusive,Speed and Effectiveness: as in Figure 4.4.

- 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 the proposal defines the three profiles based 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 4.5 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. In the next future the aim is to improve and to extend and to test this framework. This is 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. This model uses 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.

4.6 If VoIP goes in Wireless

Voice over Internet Protocol technology facilitates packet based IP network to carry voice. VoIP offers telephony (voice and fax) services and together with traditional data services over the same IP infrastructure allows to increase the

process of the convergence and facilitates the business and management models. When we construct a VoIP telephony service over a wireless network, understanding requirements for VoIP is important. In this case, the requirements are classified as follows:

- infrastructure requirements
- quality requirements
- capacity requirements
- security requirements

This section describes the main implications of using VoIP over wireless, paying attention not only to quality problems, but also to safety. When the voice packet traveling over the wireless must contend with advantages and limitations that may affect the overall voice quality and security. About voice quality and capacity, the principal factors are:

- CODEC: Voice equipment uses Compression/Decompression (CODEC) technology for converting audio signals into digital bit stream and vice versa. The most popular CODECs, such as G.71, G.723, G.729, were developed allowing a reduction in the required bandwidth while preserving voice quality.
- Packet Loss: it occurs when packets sent are not properly received by the other end, causing them to be discarded by the receiver. Packet loss can be caused by many different reasons: overloaded links, overload in the receiving device, excessive collisions in the wireless link, physical media errors due to interference or low link quality, and others.
- Latency:it is the mouth-to-ear overall delay. A two-way phone conversation is quite sensitive to latency. Most callers notice round-trip delays when they exceed 250 ms, so the one-way latency budget should typically be lower. VoIP services over 802.11 based networks cause collisions in the wireless link, reduce capacity and increase latency and jitter.

- Jitter: a voice source generate voice packets at a constant rate. The packet-by-packet delay inflicted by the network, for network congestion, timing drift, or route changes, may be different for each packet. Since the receiving decompression algorithm requires fixed spacing between the packets, the typical solution is to implement a jitter buffer.

- Packet Duration: it is a critical limit fo VoIP on wireless, because of the limitation that the wireless medium imposes on the link in terms of packet per second.

- Parameters: voice payload size, packet size, packet per second, packet duration

Wireless local (WLAN) and wireless personal (WPAN) area networks are being used progressively to implement VoIP services to allow user mobility, setup flexibility, increasing transmission rate. Supporting realible real-time service is one of the major concerns for widely deployment of VoIP in these wireless IP-based networks. The recent growth in wireless deployment has generated significant interest in combining this technology with VoIP. The most important applications include wireless phones in the enterprise, dual mode cellphones, and Vow-enabled personal digital assistants (PDA). It takes proper planning to address the balance between voice quality and efficient use of spectrum. It is important that the wireless network provide better service to real-time traffic for VoIP. WLANs experience significantly higher delay, with more network jitter and packet loss than wired LANs, and these conditions have significant impacts on the perceived quality of a telephone conversation. A careful design is necessary to deal with some issue about, quality and security. VoIP in the wireless network has higher security vulnerabilities. VoIP network security issues include both voice-packet security and IP security. Although each of these technologies offer some security mechanisms, they have some flaws which need to be addressed by an additional level of security. With VoIP on wireless, these factors are in addition to the threats linked to wireless weaknesses:

- Data Interception: data sent over wirelss can be easily captured by eaves-

droppers even farther with directional antennas. Fortunately, all wireless network certified products now support AES-CCMP data encryption and integrity, but there are still legacy products that only speak TKIP, and many WLANs are configured to accept both AES and TKIP.

- Denial of Service: WLANs are inherently vulnerable to DoS. Everyone shares the same unlicensed frequencies, making competition in populated areas.

- Rogue APs: it refers to network penetration by unknown, unauthorized APs has long been a worry. Many WLANs now use legitimate APs to scan channels for possible rogues in their spare time but verify true rogues by tracing their wired network connectivity is a skill that ordinary WLAN gear has yet to perfect.

- Wireless Intruders: malicious clients operating in or near airspace. However, truly effective defense requires up-to-date.

- Misconfigured APs: when standalone APs were individually-managed, configuration errors posed a significant security threat.

- Misbehaving Clients: Clients that form unauthorized wireless connections of any type, accidentally or intentionally, put themselves information and sensitive data at risk.

- Endpoint Attacks:it refers to attack on over-the-air encryption and network-edge.

- Wireless Phishing: methods to phish the users. and extract personal and important information to make a fraud.

All of this affects the reliability and the quality of the voice communication services. The problem of offering security to wireless is that security does not come for free and, security and efficience are conflicting requirements. The introduction of a security mechanism engine to overcome these issues impacts directly in

the speech quality of established calls and in the channel capacity. Moreover, largely deployed radio technology standards as IEEE 802.11 and Bluetooth used to achieve wireless connectivity have several constraints when delivering real-time traffic, as transmission errors at the channel, introducing delay and loss which with security mechanisms impact can lead to low quality VoIP calls. Although these technologies offer some security mecha- nisms, they have some flaws which need to be addressed by an additional level of security. In WLANs, privacy is achieved by data contents protection with encryption.

4.7 VoIP in Next Generation Network

The reasons that lead to the creation of next generation networks is not unique to the integration and convergence of network technologies and protocols, but also of services, to create a single IP-based network technology that converges the entire service offering high and very high speed fixed and mobile, traditional and innovative, and accessible from different networks. Each type of service must be available indoor, outdoor, mobile, and must be independent of underlying network technology. The drive towards this direction has been given by the growth of Internet traffic due to the use of customized content UGC (User Generated Content) especially video, the growth of peer-to-peer and social networking applications and instant-messaging, the growth of IP-based services and applications such as VoIP (Voice over IP). The applications are supported in Release 1 and consists of multimedia communication services and real-time and not real-time communication services. The most important are:

- voice over ip;
- messaging services, including Instant Messaging, Short Messaging Service (SMS) Multimedia Messaging Service (MMS);
- interactive multimedia services, point-to-point, including video telephony;
- collaborative interactive communication services, such as games, e-learning multimedia conferencing and file-sharing applications;

- content distribution services such as streaming video and radio service,music or video on-demand television content and distribution of information and images;
- multicast and broadcast services;
- road conditions;
- presence and notification services;

Support of telephony services in an NGN network is done in ways different simulation and emulation of PSTN/ISDN, mobile cellular networks with the integration and delivery of VoIP service. VoIP is a telephony service over packet switched networks based on IP network protocol, allowing communication between fixed and mobile terminals, and is different from traditional circuit switched telephony. The reasons of the importance of VoIP service in NGN concern both users and service providers. The user has the option of using an innovative alternative to traditional telephony, the most beneficial and economical. Emerging telecom operators can further their development, and traditional ones can remain competitive and increase their profits. The reasons for the spread of VoIP also affect the growth of new multimedia content user.

In NGN convergence andintegration technologies address not only the network but also the services, the unification of networks will lead to the unification of the services. As the NGN network based on packet-switched IP network protocol, any kind of service will be delivered as a stream of IP packets. The benefits of VoIP are as strong as the security and quality problems. VoIP provides an extended range of telephony services, added to traditional PSTN services. So, for this, it is important to maintain the same security requirements, the same reliability, and the same quality to compete with the traditional telephone network. This technology is economically viable and highly effective. 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.

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, and many quality issues. A Next Generation Network (NGN) or Next Generation Internet is becoming a multi-service network enabled with QOS based routing/traffic engineering to provide end users with a good quality of experience (QOE)[Hany, 2010][Janez Sterle and Kos, 2011] for the various services deployed, such as alsoVoice over IP (VoIP). The quality of voice communication across a network is well defined in a number of international standards and so it is important to analyze the requirements of each service introduced and converged in the next generation network.

4.8 Some Considerations and Summary

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 newchallenges, 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. Thus, after this Chapter about VoIP security, Spit attack and the proposal of VoIP assessment and user profile framework, the next Chapter will continue with NGN context.

Chapter 5

Security and Quality of Next Generation Network

Overview:

| Communication technologies are evolving very fast, following the current trend of the time when everything is becoming digitized and the demand for new ubiquitous services is growing. This process has enabled the advent of the Next Generation Network (NGN). With the development of the Next Generation Network, considering the proposed infrastructure, speed, services and amount of connections will increase exponentially. At the same time vulnerability, threats, risk and quality of service (QoS), should be adequately assessed for the continuous evolution of the converged network, which will define roles and relationship in the future information and communication environment. In this section an overview of the Next Generation network addressing the new challenges of the converged infrastructure is explained and then the proposal framework to assess quality of service and security features, giving an appropriate analysis method regarding certain parameters and requirements. *Proposal presented in research contributions.*[1]

[1] [La Corte and Scatá, 2011a]

5.1 Introduction

Communication is the driving force of society through a network. Over the years, information has always changed in form but not in the ultimate goal. The meaning of communication is always the same, but what has become increasingly important is the need to communicate quickly and in real-time, to be able to access any type of resource from anywhere, and to be able to access and share information as safely as possible. Today, all converged networks rely on the means of communication and sharing knowledge and data. Social Networks, Converged Networks [Ahmad A.Almughaless, 2010], and All-IPs are the future of communications. These networks are designed primarily as a means of sharing and collaboration, and the network makes the sites more exible and immediate, and in this context the convergence of communication systems through next generation networks has also had a significant impact. Nowadays the telecommunication infrastructure is in a conversion phase towards NGN. According to ITU'T Report [Y.2001, 2004][Y.2011, 2004][Marco Carugi, 2005], a full implementation of NGN in fixed line will be deployed by 2012 and in mobile network by 2020. Thus, the user's lifestyle will also change because information can be reachable and shared whenever and wherever with an intelligent, dynamic and mobile converged network. The border between several different communication domains will diminish through the natural fusion in a single infrastructure of the three different technologies computers, Internet, and mobile networks.All telecommunicatio noperators are now on a journey towards a NGN built on new horizontal planning, moving away the traditional vertical structure of the networks. Along with many positive benefits, there are several security and quality concerns. This results in a waste of resources due to the lack of strategic vision and plan to evaluate the appropriate parameters and requirements to estimate the risk and the quality of a network. The next section illustrates the issues regarding the challanges of the information and communication technology towards the convergence, gives a brief overview of next generation network, its architecture and infrastructure features, and finally an Analysis Model to assess Security and Quality of Service Parameters and requirements for Next Generation Network is presented.

5.2 Changing towards Convergence

The term of Next Generation Networks (NGN) refers to the evolution of telecommunications networks planned for the next decade, which will be characterized by the integration of technologies and services into a single converged network broadband solution based on the network protocol IP (Internet Protocol), capable of supporting the continued growth in the number of users and information submitted and also to offer innovative services. With next-generation network, the services, protocols, and existing technologies, fixed and mobile, will converge in a single domain, All IP, which will be a single platform transport based on packet switching and IP network protocol allow you to transfer large volumes of traffic of any kind, voice, video and data, as flows of IP packets. All types of end user and technology will converge to a single access network infrastructure, and each type of service will be supported and provided regardless of the technologies and network access. There are many reasons that lead to the unification of networks and services, in particular the need to reduce architectural complexity and operational and to overcome the issues of existing technologies, to offer a wide variety of services more secure and reliable, to increase the bandwidth available for users. Underlying the need to develop the NGN there is also the great increase in Internet traffic due increasing use of custom user content, especially video, to growth of peer-to-peer and social networking applications and instant-messaging and IP-based services and applications such as VoIP (Voice over IP), ToIP (Telephony over IP) and IPTV (IP Television). During the migration from existing networks to NGN, telecommunications operators and service providers will have to introduce innovations in networking technologies and transport access, minimizing development costs and risks. We must take into account the factors, which in the coming decades could become predominant: support user mobility and ubiquitous, robustness and security of the network, reduction of energy consumption, convergence and simplification of the architecture network and services. To do this, we must develop new architectural standards, protocols, mechanisms for the management of QoS and Security.

The implementation of next generation networks is still in the world in the

planning stages by the telecommunications operators. The migration from existing networks towards NGN may follow two different orientations. The first approach is the revolution of the network, namely the construction of entirely new features and architectures. The second is the evolution of the network, or the updating and replacement of some functional components, while maintaining compatibility with existing features and services. However, with many positive benefits, there are several security and quality concerns. The earliest systems involved in the process of migration to NGN will Worldwide fixed telephone networks PSTN (Public Switched Telephone Network). At this stage, each telecom operator could follow a different strategy, based on various factors. In particular, we have three different scenarios of migration [Ahmad A.Almughaless, 2010]. The first scenario is the overlay: it consists in maintain the existing fixed telephone network, such as with TDM (Time Division Multiplexing) transport of voice, and building in parallel new network architecture. Replacement is the second scenario, which consists the replacement of the PSTN: TDM switches are replaced with IP-based devices with new features. The last scenario is Upgrade: is updating the existing TDM network with the addition of capabilities of its IP NGN. Choosing the best strategy depends on objectives of the manager, network status and economic factors. NGN, whose development started in recent years, will spread over the next decade, incorporating fixed telephone network and later cellular telephone network.

About Internet is assumed that the two networks will continue to coexist while maintaining their independence. Both could be replaced by networks of totally new and different concept, the New Generation Network (NWGN)[Ayoama, 2009]. The studies on this is at early stage and its development could only begin in a few decades. However we could outline some different features about it. While NGN arise mainly as a development and integration of existing networks, NWGN will not constitute a development of NGN and Internet, but it will be based on total innovative network architecture. Thus, NWGN does not represent a simple attempt to improve the existing protocol stack TCP/IP, but will introduce new protocols and technologies, supporting mobility, ubiquitous, pro-

viding broadband multimedia services and reducing energy consumption. This new network could allow to solve all security and quality issues arising from the weaknesses of unsafe and unreliable of the current architectures. The NWGN could be introduced from 2020 and afer some decade could replace all IP-based networks.

5.3 Standardization Process

The general architecture of the NGN reference were instead subject of work of worldwide organization for standardization ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) and European Working Group ETSI TC TISPAN (European Telecommunications Standards Institute, Technical Committee - Telecommunications and Internet converged Services and Protocols for Advanced Networking). With the advent of NGN we see that the standardization goes towards the unification of underlying network technologies, enabling the total convergence of network, processes, and services, and the diversification of services as well as equipment at the network edges. The aim of NGN is to collect networks into unitary packet-based network architecture (ITU-T Y-2001,2004). The service-related functions in NGNs are independent of the transport technologies (ITU-T Y-2001,2004). ITU-T work on NGN Since 2003,[Y.2001, 2004][Y.2011, 2004][Marco Carugi, 2005][Recommendation, 2005], and in particular the group FGNGN (Focus Group on NGN) produced the recommendations of the Y series,the two key documents that describe services,property and architecture for NGN, Recommendations Y.2001 and Y.2011 are. They produced two release,each with a clearly defined scope. NGN is defined technically by the ITU-T as a packet. The Release 1 defines a model of NGN applying the general principles set out in Recommendation Y.2001. Release 2, the Y.2011,whose standardization work is still ongoing, focuses its attention on supporting streaming services such as IPTV service, and support for full mobility users, so the connection is maintained without interruption even if the user moves through different access networks. The Y.2001 recommendation, that is "General Overview of NGN" [Y.2001, 2004] defines the general principles underlying

a NGN, in relation to property, services, and network architecture.

The definitionidentifies a number of features necessary in a NGN: packet switching, heterogeneity of the network to support QoS, the separation between the transport layer and level of service, mobility support general users. This is defined in the same recommendation as the ability to use the services offered even in case of the users location changing, or variations in technical conditions, it also includes the ability to use a service with continuity or not, depending on the degree of availability of the service depends on several factors. The Recommendation also defines a set of objectives that must reach NGN: to promote fair competition, encourage private investment, meet the requirements of various regulations, provide open access to networks, ensuring universal access to services, promote fair opportunities for all citizens, promote also cultural and linguistic diversity of content, recognize the need for worldwide cooperation with particular attention to the less developed countries. Finally, the Recommendation identifies a number of crucial areas of study, including architectural principles, QoS, service platform, network management, security, generalized mobility, network control architecture and protocols. The Recommendation Y.2011,General Principles and General Reference Model for Next Generation Networks defines a general model for the functional architecture of NGN and the services provided, realizing the basic principles specified in Recommendation Y.2001.

There are some differences between the model of a layered architecture and NGN reference model OSI seven-layer BRM (Open Systems Interconnection Basic Reference Model) defined in ITU-T Recommendation X.200, these differences are generally in the number and characteristics of the levels, and adopted protocols. Recommendation Y.2011 defines then a high-level functional model for the NGN, which is based on the division of network functions in a layered architecture. The general architecture of reference must support all the features described in Recommendation Y.2001 specified, must be neutral and specific protocols or technologies. ETSI TISPAN has worked since 2003 to develop legislation in Europe about the architecture of an NGN and the services offered, and this activity was conducted in parallel and in accordance with global standardization activities

conducted by ITU-T, and it is the basis for future practical implementation[ETSI, 2008][ETSI, 2002]. In 2005 it was realized the Release 1: it takes the 3GPP IMS to support multimedia applications based on IP and SIP-based applications, but is also based on the functional entities for support of other applications. Release 2 was released in 2008, it brings of the changes from the previous release, in particular with regard to the Support for IPTV applications. Since 2008, ETSI TISPAN is also involved in Release 3 of the specification, focusing on consolidating VoIP technology, the evolution of IPTV on the development of access to ultra bandwidth, the interconnection between IP networks and NGN interoperability with other networks or not.

5.3.1 Requirements and Features

The features of NGN are given in Recommendation ITU-T Y.2001, and can be defined through a series of requirements and capabilities that the network must satisfy. An NGN should be a packet switched network with an open architecture and flexible to provide support for a variety of services, applications, and new and traditional mechanisms. Users must have unfettered access to services offered by different service providers and through different access and transport technologies. Users should to access our services even in mobility. Each service must have an appropriate level of guaranteed QoS. The network must provide mechanisms for protection and safety of users and data.The architecture should be divided into two independent levels, service layer and transport layer, so we can have separation between the functions related to network, transport, and those relating to applications. The architecture must allow inter-working with existing traditional networks through open interfaces.

5.3.2 Architectural Model

With regard to the architecture of NGN, ITU-T and ETSI have implemented two functional models, respectively, at world and Europe, with the openness and flexibility than the development of future new standards and features. These models are characterized by the decoupling between ”transport” and ”service” between

"network" and "applications". The two models are based on a general model reference based on the division of network functionality into four levels. In general, the network architecture of an NGN is structured into four main functional levels, that interact via appropriate interfaces and protocols [Keith Knightson, 2005][Kyung-Hyu Lee, 2003][Lee, 2009].

- The highest level is the Application and Service Layer, which features development, management and delivery of various services.
- The Control Layer has control capabilities of network elements, management of network resources, control and integration of services in packet streams IP.
- The Transport Layer is characterised by different types of IP transport and traffic services between the entities of the architecture, for any access mode and type terminal user. Transport Layer resides in the Media Gateway (MGW) devices.
- The Access Layer consists of the access networks that connect the user to transport network.

5.4 Security and QoS in NGNs

In the design of converged network architectures to develop new mechanisms to ensure Quality of Service (QoS), especially in the case of real-time multimedia applications, is needed. At the same time Next Generation Networks are vulnerable and sensitive to external attacks, as established by the interconnection of different networks and because they are accessible to any user through any type of terminal. Thus, security and quality of the network are therefore key issues to assure good performances of the convergence. To guarantee the QoS we must adopt strategies of differentiation and traffic engineering and services: the different traffic flows are classified in Class of Service (CoS), characterized by a different treatment in the network and a different level of service quality from Best Effort level to QoS Guaranteed. One of the main requirements of an

NGN is to provide QoS end-to-end users in a heterogeneous network scenario. An NGN should therefore be based on a model to support QoS, which must take into account the different applications and their requirements for quality and performance. The Working Group 3 of ITU-T FGNGN dealt with the issues of QoS and Network Performance (NP) of NGN [Jongtae Song and Joung, 2007]. It has been involved in defining requirements and architecture for supporting QoS end-to-end, studying some problems such as resource management and admission control. The model developed by ITU QoS and NP-T is based on the architecture of the NGN functional layers, consisting of a transport level that supports service level.

Taking into account the functional architecture for NGN developed by ETSI TISPAN, in accordance with the general reference model described by ITU-T, the capabilities of QoS control and management are performed by subsystem RACS (Resource and Admission Control Subsystem) [ETSI, 2005]. According to the approach ITU-T/ETSI, there are different scenarios for control QoS achieved by RACF or RACS according to the user terminal, also called Customer Premises Equipment (CPE) [Recommendation, 2005]. The Best Effort model it is suitable for Internet applications such as File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP), but not is suitable for real-time multimedia services that have stringent requirements in terms of bandwidth, packet loss and delay, such as VoIP (Voice Over IP), IPTV (IP Television), audio and video streaming, video conferencing. The IETF has developed some QoS management models for packet networks such as IP-based Internet: network architectures, Integrated Services (IntServ) and Differentiated Services (DiffServ) the RSVP (Resource Reservation Protocol) used in IntServ, the model MPLS (Multi Protocol Label Switching) is used in DiffServ. Unlike the Internet, NGN proposes to offer users a variety of services, both traditional and innovative ensuring adequate levels of quality and performance, these networks however, the management QoS is more complex. Some approaches are based on the use of a core network of IP transport using MPLS and DiffServ. Ultimately, the control mechanisms QoS developed for third generation mobile networks and the IMS are not suitable in a

scenario that integrates different technologies, and a user of a domain can freely use the services offered by other domains, and should therefore be appropriately extended[Mehdi Mani, 2007]. Security is not a separate issue, but is linked to the control and management of QoS network and services. NGN must provide both a transport layer that level of service mechanisms to protect information transmitted from fraudulent use, and the architecture of the network from external attacks. We must therefore develop an architecture and strategies that may predict, detect and correct possible attacks and threats. Safety becomes an add-on to something that already exists and is almost never designed in a way that is timely and proactive.There are three requirements that must be maintained:

- Confidentiality
- Integrity
- Availability

Threats can cause damage by intervening directly in the information exchanged or by interrupting the continuity of certain procedures, aecting the system, destroying a part of it, or violating the rules of privacy. The damage may be multiple, and its nature is not limited to a few unfortunate events. The aim is to limit the number and impact of risks, knowing that systems will never be fully shielded or closed off to attacks. The correct operation is to maintain technological advantages in maximum security with a minimal degree of risk in terms of probabilities, not absolutes. The Working Group 5 of ITU-T FGNGN dealt with security aspects in NGN [X.805, 2003] It is particularly focused on defining requirements and guidelines as part of Release 1. The requirements relate to the services, users, and interfaces layers of transport and service architecture for NGN.The security architecture in the NGN must protect interconnection and interoperability strategies between NGN and existing networks, the communication must be secure even with little trust networks like the Internet. NGN inherits the security problems of traditional networks, the mechanisms used to protect these networks, especially in mobile networks and the Internet, can be used in the NGN to provide security independently from technology access and the terminal user,

suitably extended and optimized. NGN then inherits the security problems in networks based on IP protocol as the Internet, and must also deal with new attacks, threats and intrusions caused by the interconnection between different networks and domains. The definition of an architecture for security in NGN networks is under development, the basic idea is the division of the network in different security domains that adopt the standard mechanism such as IPSec. Strategies for Security and Defence have developed for the NGN based on knowledge of the behavior of possible threats and vulnerability of the system[Long Zhang, 2008].

5.5 Analysis Model

The proposal of this section is a framework to assess the QoS and Security in NGN networks and a comparison with networks that are converging, that must take into account two factors:

- parameters that describe the main aspects of quality and safety of the network;
- factors of influence that degrade the quality and security of the network;

Quality parameters allow to characterize and measure the performance of a telecommunications network and the quality of services offered. The security parameters allow to characterize and measure the networks ability to identify and protect against threats and attacks. The network is divided into four main levels: access, transport, control and service. This reference model is general and is also applied to NGN: the level of audit control features transfer data at the transport layer, and together constitute the core network package. For each level we must consider the standards of quality and safety, and factors of influence. We propose a model characterised by two distinct phases in the assessment of QoS and security in networks NGN:

- The first step is to assign to each of the four levels NGN architecture a weight to each parameter and factor of influences. The weight is a score that indicates how the parameter of quality or safety is important at that

Value	Impact
0	Negligible
1	Low
2	Medium
3	High

Table 5.1: Wheights of Parameters and Factors of Influence

Symbols	Meaning
$\gg$	Much greater than not converged solutions
$>$	Higher than not converged solutions
$\approx$	Equal to not converged solutions
-	Negligible in both solutions

Table 5.2: Symbols for Comparison between not converged solutions and converged solutions

level, and how much influence factor affects the quality or safety of that level.

- The second stage consists in a comparison between the network and NGN networks not-convergent relative to the weight of the factors of influence. We show for each level if the degradation of quality and safety due the impact of a particular factor is approximately equal to the NGN network, the more or much greater than traditional networks. In some cases one factor may have no influence to a certain level of network architecture.

The Table 5.1 and Table 5.2 define the meaning of the weights, and of the symbols used for the comparison between converged network and not-converged network.

5.5.1 Results for QoS

The parameters that allow to characterize the quality of services offered, from a telecommunications network will differ in the type of network, circuit or packet switching, and depending on the service. They may well be related to network performance and the degree of user satisfaction. These parameters are random variables, ie casual and unpredictable, as are the random network characteristics

and traffic data. It is not possible to predict in a deterministic features such as the number of users or devices connected, the status of the buffers of network nodes, the amount of resources available, the occurrence of failures. The main parameters that characterize the quality that we consider for our model are:

- Bit Error Rate(BER).
- Out-of-Order Delivery.
- Delay.
- Jitter.
- Packet Loss.
- Throughput.

The factors of influence are:

- Network Fault-Tolerance.
- Buffer sizes of network nodes.
- Availability of resources.
- Service Availability.
- Failure.
- Time Network Access.
- Time system operation.
- Dimension of the Network.
- Heterogeneity of network.

	Parameters						Factors of Influence								
	BER	Delay	Jitter	Loss	Out of Order	Throughput	Fault Tolerance	Buffer Size	Availability of Resources	Service Availability	Heterogeneity og Net.	Fallure	Time Access	Time System	Dim of the Network
Access Layer	0	3	0	0	0	0	0	0	3	0	2	0	3	0	2
Transport Layer	3	3	3	3	3	3	3	3	3	0	2	3	0	3	2
Control Layer	3	2	2	3	3	2	3	3	3	0	2	3	0	1	2
Service and Application Layer	3	3	3	3	3	3	3	3	3	3	2	3	2	3	2

(a) Qualitative Parameters and Factors of Influence Assessment for QoS

	Factors of Influence								
	Fault Tolerance	Buffer Size	Availability of Resources	Service Availability	Heterogeneity og Net.	Fallure	Time Access	Time System	Dim of the Network
Access Layer	-	-	>	-	>>	-	>	-	>>
Transport Layer	≈	≈	>	-	>>	≈	-	>	>>
Control Layer	≈	≈	>	-	>>	≈	-	>	>>
Service and Application Layer	≈	≈	>	≈	>>	≈	>	>	>>

(b) Impact Comparison between not converged and converged solutions for QoS

Figure 5.1: QoS Analysis Model

The Figure 5.1 shows the results for the QoS Assessment. The figure makes a comparison between the NGN and not-converged networks respect to the weight of influence of factors affecting the quality of the network at different levels. In particular, if the means for each level of quality and performance degradation due to the incidence of a specific factor in the NGN network is about equal, greater or much greater than traditional networks. In an NGN network, the weight of the influencing factors at different levels network architecture is comparable to some factors than the networks do not converging, for others more. In particular, the heterogeneity of the network, characteristic of next generation networks, and the volume of the network, are more relevant to quality and system performance, and tend to increase the influence of other factors. Factors affecting the quality of the data transfer transport layer, faul-tolerance or reliability of the network buffer size of the network elements, the probability of failure, are believed to have influence over comparable not-convergent networks, provided adequate control and management of transport network-level control. The availability of the service is considered comparable with respect to the networks do not converging as it does not depend on technology access or transport network, but by the service provider. At any level of the network architecture of the weight factors of influence is considered less than traditional networks that are converging, as the NGN network is born as an integration of existing networks and inherits the characteristics and problems. In a converged network scenario you can see two trends: on the one hand you have a higher rate than not-convergent solutions by factors of influence, in particular because of the characteristics of higher volume and greater heterogeneity of the network itself, on the other hand, the network has potentially good performance and is able to satisfy the coverage at each level of the quality parameters required. The good coverage of the qualitative parameters despite the increased incidence of parameters of influence can be explained considering the nature of the network, characterized by the integration of different network technologies into a single transport platform and the integration of different control mechanisms and management a single control platform and the different services into a single platform.

	Parameters								Factors of Influence				
	Access Control	Authentication	Non-repudiation	Confidentiality	Communication Security	Data Integrity	Availability	Privacy	Destruction	Corruption	Removal	Disclosure	Interruption
Access Layer	0	3	3	0	0	0	3	3	0	0	0	3	0
Transport Layer	3	0	3	3	3	3	3	1	3	3	3	3	0
Control Layer	3	0	3	3	3	3	3	1	3	3	3	3	0
Service and Application Layer	3	3	3	3	3	3	3	3	3	3	3	3	3

(a) Qualitative Parameters and Factors of Influence Assessment for Security

	Factors of Influence				
	Destruction	Corruption	Removal	Disclosure	Interruption
Access Layer	-	-	-	>	-
Transport Layer	>	>	>	>	-
Control Layer	>	>	>	>	-
Service and Application Layer	>	>	>	>	>

(b) Impact Comparison between not converged and converged solutions for Security

Figure 5.2: Security and QoS Analysis Model

5.5.2 Results for Security

Recommendation X.805 defines eight dimensions of security. These parameters can be considered as safety parameters for describing and measuring different aspects of safety at every level of the network architecture:

- Access Control.
- Authentication.
- Non-repudiation.
- Data Confidentiality.
- Communication Security.
- Data Integrity.
- Availability.
- Privacy.

Recommendation X.805 defines five security threats. These values can be considered as influence factors:

- Destruction.
- Corruption.
- Removal.
- Disclosure.
- Interruption.

In Figure 5.2, the results for Security Assessment. In an NGN network, the weight of the factors of influence, which affect degrading security is considered higher than the not-converged networks at all levels network architecture. This is due to the convergent behavior of the network itself, not only inherits all the

security issues of traditional networks, but is more vulnerable and subject to attacks because of the large size, the large number of users, and the numerous interconnections between different networks and domains. Each connection point is in fact a potential weak point where the system can be attacked. At any level of the network architecture of the weight factors of influence is considered less than the networks do not converge, as the NGN network is born as an integration of existing networks and inherits the characteristics and problems.

5.5.3 Converged Network and Factors of Influence

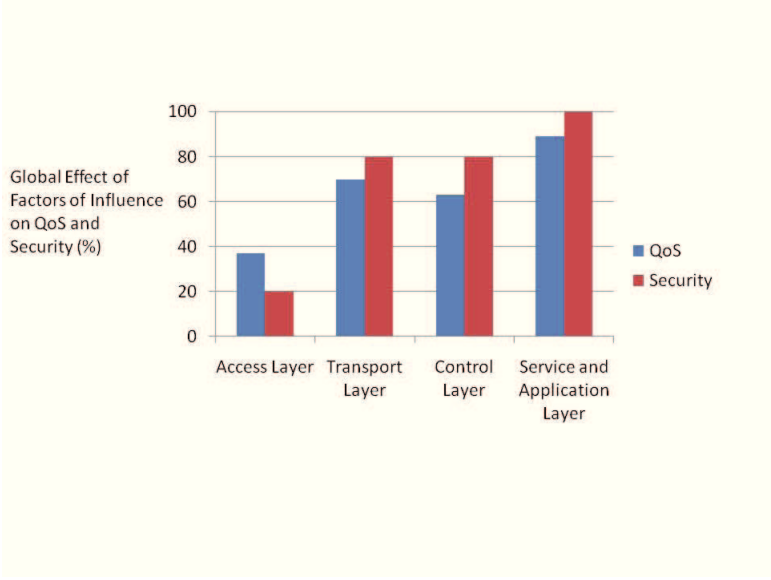
In a converged network scenario you can see two trends: on the one hand you have a higher rate than not-convergent solutions by factors of influence, particularly because of the characteristics of greater heterogeneity and greater volume of the network itself, on the other hand, the network has the potential for good performance and manages to satisfy on every level coverage of the quality parameters required. Good coverage of qualitative parameters, despite a higher incidence parameters of influence can be explained considering the nature of the network:

- integration of different network technologies in a single transport platform.
- integration of different control mechanisms and management in a single control platform.
- integration of different services into a single service platform.

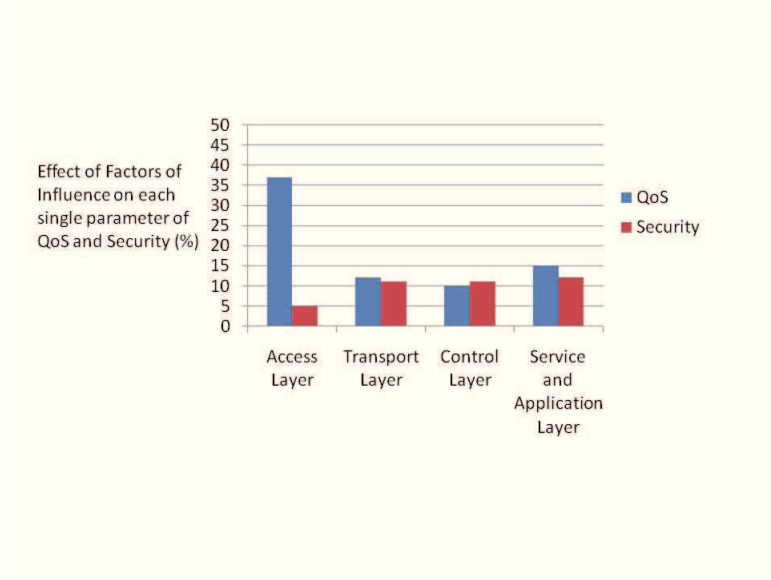
The Figure 5.3 shows the trend of the global effect of Factors of Influence on QoS and Security and the effect on each single parameter that characterize the security and the quality of the next generation networks.

5.6 Some considerations and Summary

NGN is an evolution of existing networks, and inherit characteristics and properties as well as defects and problems in particularly relating to the quality and safety. On the one hand the new networks want to optimize and enhance the performance and network security existing, on the other side we must come to



(a) Global Effect on QoS and Security



(b) Effect on each single paramenter of QoS and Security

Figure 5.3: Security Analysis Model

terms with the same problems and should seek to adapt the existing control and management mechanisms to the new architecture network. The management of service quality and safety in new networks generation has also more complexity than the existing networks, as the problems inherited that adding new issues due to heterogeneity of the network. The variety of interconnected domains and technologies access may in fact represent a weakness of the system. Applying the models of NGN QoS and Security Assessment, the proposal of this Chapter allows to know the issues and the real weaknesses of this new infrastructure also in comparison with traditional networks, based on some important parameters and factors of influence that could affect the performance and and could favors the network threats. The next-generation networks present difficulties and limitations, which are still based on existing networks, particularly NGN networks and the Internet, although different, share similar challenges quality and safety, as both large-scale heterogeneous networks where interconnection between different domains is possible thanks to the protocol IP network. The limits of existing networks can be overcome by developing new concept and new assesment and analysis model to estimate the risk of failure and the performance, in qualitative and then quantitative terms, to decide after the suitable investments on security and QoS, that are based on an attempt to improve the protocols, processes, existing networks, and new generetion of converged networks.

Chapter 6

Bio-Inspired Approach to Analyse and Manage the Security

Overview: |This Chapter demonstrates the importance of taking advantage of biological models, processes and systems to inspire information and communication security. Examining some of common structures that will characterize the future of the ICT we can find some striking similarities to biological systems. This chapter provides motivations about using the bio-inspired approach to design a security infrastructure, to properly assess the risk to protect data and systems to assure security requirements. This Chapter shows the proposal about the model to analyze the risk, manage the security based on biological approach, and the strategic decisions about security investments, to understand where, how and when to apply them. *Proposal presented in research contributions.*[1]

6.1 Introduction

In recent years, the need for the protection of personal data of individuals and legal entities, in order to ensure their privacy, increased. From this, the need to rewrite the policy metrics of security for new systems arises, like those of communications, which favour the interconnectivity and facilitates exchange of multimedia data between users. At the same time the other aspect is that the new communication system is generally more vulnerable to network, becoming

[1] [La Corte and Scatá, 2010][La Corte et al., 2011][La Corte and Scatá, 2011b]

continuous source of new threats. It is essential, in addition to the new strategy, to change the way how analyze and evaluate the contexts in which the information value exchanged has a certain weight. The complexity of the systems handling the information and communications, is changing. The networks are evolving towards convergence, and the aim is to form a single complex, dynamic and communicative body, capable of providing services, applications, dynamic models around each of users. With the increase of size, interconnectivity and the convergence, the networks have become vulnerable to various forms of threats. The evolution of the communication implies the need of the new security requirements, new security mechanisms and efficient countermeasures. Biological organisms are also complex interconnected systems with many points of access. Using the concepts of biological systems and models can inspire information and communication security. About these topics, risk analysis and management for information system security [Ryan and Ryan, 2008b][Ryan and Ryan, 2006][Lachin, 2000] and statistical methods [ISO/IEC, 2008][Ryan and Ryan, 2008a][Kalbfleish and Prentice, 2002], there are some papers that deal with the relationship that exists between the two disciplines. Recognizing the work presented in many papers also about bio-inspired approach [Murray, 1988][Wang and Suda, 2001][C. Lee and Suzuki, 2007], about risk perception and statistical models biologically inspired [Kitchovitch and Lió, 2010][Lachin, 2000][Kalbfleish and Prentice, 2002], and about comparison among computer virus and biological virus[Li and Knickerbocker, 2007][Michael Meisel and Zhang, 2010], this chapter endorses the hypothesis to investigate the security issue in a broader vision, to estimate the economic risk as a result of an investment in security, obviously linked to the technological risk of a communication system. This is important to assess in the future the best countermeasures to limit the damage, to change the shape of risk, minimising the losses about information and about economic investments. The analysis of risk requires knowledge of the probability of failure and its distribution and the probability that an attack occurs, that is when a threat exploits a vulnerability, because of the lack of proper security measures. Thus, the proposal present the model to asses the degree of system security and analyse the existing countermeasures triyng to decrease the

risk, minimise the losses, and successfully manage the security.

6.2 Challenges in Networking

The term virus is widely used for one type of malicious code affecting computer systems and networks. This suggests the natural similarity of malicious code or a general network virus as a disease infecting computers and implies that information security can use a biological paradigm for protecting against diseases and model security strategies[Ryan and Ryan, 2008b]. This Chapter addresses how these similarities, already useful to design new network infrastructure, may be useful to inspire methodologies and strategies of risk analysis and management, and security of ICT systems. The first computer viruses appeared in the early 1980s, although self-replicating programs had been described in science fiction even earlier. A computer virus was described as a program that can infect other programs by modifying them to include a possibly evolved version of itself[Ryan and Ryan, 2008b][Dressler and Akan, 2010].

Viruses and worms were not the only biological models used in investigating information security threats. If we consider the next generation information systems,they are envisioned to be charcaterized by an invisible and ubiquitous cloud of information and communication services, which should be easily accessible by users ensuring privacy and quality. The new trend is a result that will be a pervasive and living network extending the current Internet capabilities. This ubiquitous networking space will include, in addition to the traditional devices, others and different networked entities/nodes which are in much closer interaction and they include:

- wereable networks.
- in-body molecular communication network.
- unattended ground, air, underwater sensor networks.
- self-organizing sensor and actor networks.

- locally intelligent and self cognitive devices.

Clearly, the new networks have to face with scalability, heterogeneity and complexity which are new by-products of the challenges in ICT environments in the last few decades. They have been successfully dealt with by the nature for quite some time. The dimanics of many biological processes and laws governing them are based on a surprisingly small number of simple generic rules that allows:

- effective collaborative.
- task allocation.
- effective resource managament.
- synchronization.
- protection against pathogens.
- relative stable equilibrium state.
- adaptive to the dinamicity of environment features and circumstances.
- robust and resilient to the failures caused by internal and external agent.
- high complexity, high connectivity and extensive interaction between components/nodes/systems.
- numerous entry points.
- complex behaviours with limited set of basic rules.
- able to learn, evolve and self-organize.
- energy efficiency.

The two fields have a much stronger connection that on might expect. All these features that characterize the biological systems are due to millions of years of evolution in biology, thus we can guide ICT based on these principles. The key of drawing useful corralations between biological world and ICT world is

a proper selection of topics and a right comparison. The need is to integrate highly intelligent processes to improve their robustness, scalability, efficiency and reliability. For this, biologically inspired mechanisms have been applied in recent years to diverse type of network (e.g. sensors, wireless, fixed networks, services). The most important requirements for the future are:

- adaptive, pervasive, opportunistic and ubiquitous infrastructure of networks.
- large-scale networking.
- Heterogeneity, coexistence, cooperation and social-friendly environment among different types of networks.
- internet of things.
- self-properties: self-organization, self-management,self-learning.
- security, quality of service and energy efficiency (e.g. Sustainability of ICT).

6.3 Bio-Inspired Security

6.3.1 Approach

Historically, the risk analysis has been applied to areas other than telecommunications, and task-force or security have always been in the IT sector or economic sector. The scientific documentation has several publications on the theme of safe in different diverse areas. Epidemiology is concerned with analyzing the causes, course and outcome of diseases, through mathematical and statistical models that analyze the spread of disease in certain populations. Hence the need to investigate the statistical methods that fall in the analysis of the failure of systems, Failure Time Analysis. These statistical models as well as outlining the distribution of the moments of failures and survivals of systems used to assess the hazard of a system subject to such threats. The next sections prove that the study of diseases in a biological sense and anticipation of its release could be very similar

to what we have defined as communication risk. The first scope is to introduce a general approach to bio-inspired security with the aim to derive optimized technical solutions in the future not only for security in ICT. Looking at many papers and proposals that have been derived in recent years, analyzing many methods and techniques four steps can be identified to design a bio-inspired approach for security in ICT environments:

- Identification, Assessement, Analysis of Similarities and Analogies among the biological systems and information systems.
- Classification of Methodologies, Positive Aspects and Drawbacks.
- Selection of Macroareas of Interest.
- Understanding of biological models.
- Design and Engineering of Bio-Inspired Approach.

In this way, the proposal of this Chapter remainder identifies structures and methods that seems to be similar to processes, infrastructures and environments. The proposal identifies and understands statistical models, biological computing, biological real behaviour, and all the rules that controls and mange the processes in the nature. Finally, after choosing the macroareas (e.g. security and risk/failure and disease/attack similarities) it design and develop a biologically inspired model for dynamic, adaptive converged information adn communica- tion systems to estime a quantitative measure of risk. This involves the knowledge of proportional hazard models, Cox regression models, angent based models, cross-correlation, life table of assets,adaptive networks. The measure of risk will be useful to evaluate the most appropriate security countermeasures, to the expected benefits of an investment and therefore, to manage the safety, balancing costs, benefits and efficiency of a network.

6.3.2 Analyzing Risk with Biological Model

This section presents and proves a close similarities between the biological diseases, and what I defined as communication risk. Starting from several stud-

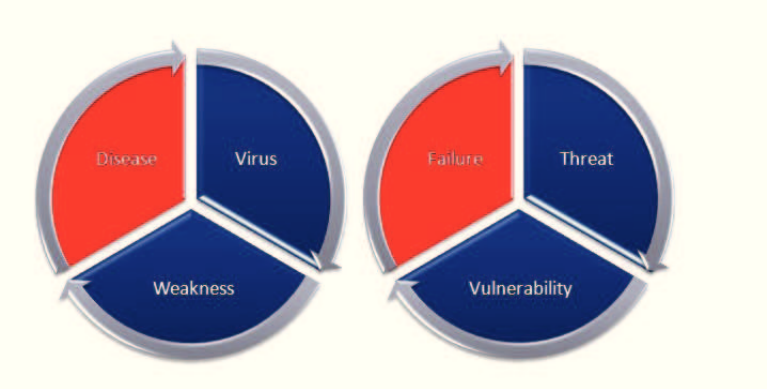


Figure 6.1: Bio-Inspired Similarities

ies of medical and biological models [Cox and Oakes, 1984][Cox, 1972][Lachin, 2000][Kalbfleish and Prentice, 2002], the target was to find a comparison between security and medical-biological disciplines.

This section propose and shows the possible links between biomedical disciplines and the safety review. Among the biomedical disciplines, epidemiology there seemed to be more suitable for comparison.

6.3.2.1 Epidemiology

In recent years there had been a growing interest in using biological, epidemiological models to gain insights into information and communication systems. These approachs developed through the years are based on several models[Murray, 1988]. Some of this looked at the effect of the network topology on the speed of virus propagation, some looked at virus spread on different network, and some the risk perception in epidemics. Different studies have also used several biological models for immunisation strategies. As a result, biologically inspired research in information and communication security is a quickly growing field to elucidate how biological or epidemilogical concepts in particular have been most successfully applied and how we can apply these to the safety strategies for risk analysis and management[Lachin, 2000]. Through this study, we notified a close similarities between the biological diseases and, what we define as communication risk. Starting from several studies of medical and biological models, we targeted to

find a comparison between security and medical-biological isciplines. We realized the possible links between biomedical disciplines and the safety review. Among the biomedical disciplines, epidemiology there seemed to be more suitable for comparison. Epidemiology is a methodology, a technical approach to problems, a "philosophy". Epidemiology is a "different" way to study health and disease, and it is cross-science. Epidemiology is working with the clinic and preventive medicine. It is involved in analyzing the causes, the course and obviously, the consequences of diseases, by mathematical-statistical models that analyze the spread of disease in populations. Purposes of Epidemiology are:iccsa

- Determine the origin of a disease whose cause is not known.
- Investigate and control a disease whose cause is known.
- Acquire informations about the natural history of disease.
- Plans programs and activities of control and monitoring of disease.
- Assess the economic effects of disease and analyze the cost-benefit.

About epidemiological model, the factors are virus, exposure, and explanatory variables. In this way, individuals of a population exposed to a particular virus, are like the information assets of the communications system, exposed because of their vulnerability to network threats. The threat can damage one or all of the assets of the information system, and it represents a potential cause of an accident or deliberate accidental, as a malicious code. The vulnerability is a weakness of the system for the security of informations. The attack occurs when the vulnerability is exploited by threat agents. Many epidemiological studies are designed to verify the existence of associations between certain events, in this case, we talk of the incidence or of the onset of a disease in a population of individuals. Epidemiology is a methodology of study. The same can be said for safety. Using these concepts and models, it can inform, guide, inspire information security, and understand, prevent, detect, interdict and counter threats to information assets and system. The risk, like a disease, is the result of three factors: threat, vulnerability and explanatory variables. In the case of a communication system, we

talk of the impact of a malicious code or a threat of the network, and therefore, also of damage caused as a result. These results can be distorted because of other variables that somehow might confuse the results, and so called confounding variables (counfonders). These variables may be confounding or interacting variables, also called in econometrics control variables or explanatory variables, which are used into the Cox regression model [Cox and Oakes, 1984][Cox, 1972]. The explanatory variable plays a key role in understanding the relationship between cause and effect of a general threat. The explanatory variable is a variable which is used to explain or to predict changes in a value of another variable. This is important to evaluate the relationship between the point events that we define in the next section. To assess the confounding, it is necessary an analysis which provides a collection of epidemiological data sets and informations. This is complex in the case of communications systems and networks. In this case, the analysis is multivariate, because it involved so many factors that influence and change network vulnerabilities. The Cox Model also considers the variable time and helps to assess the risk of exposure to a threat in the time. This analysis is embedded in a broader analysis, survival analysis and failure time analysis.

6.3.2.2 Failure Time Distributions and Survival Analysis

A failure doesn't meaning the total distruction of the system, but even the impairment of the informations that it holds. An information asset, which represents and holds a collections of information necessary for the network and its maintenance(i.e. databases or software), must have the three security requirements CIA (Confidentiality,Availability, Integrity). These three features can be compromised very easily from natural threats, viruses and malicious individuals, such as hackers. It was shown that the arrival of an attack is not predictable, so it is random, and we can also say that these occur in bursts. The initial conditions, that reflect the majority of cases, are those in which the system operating in normal, peacetime conditions and threats, that may attack the system, can be of various kind (malicious code, hackers, thieves and spies). This section wants to give a brief overview of the study done about survivor analysis and failure time

distributions models, which allows us to estimate the risk. Ryan and Ryan [Ryan and Ryan, 2008a][Ryan and Ryan, 2008b][Ryan and Ryan, 2006] models a general information infrastructure in number of finite information systems $\{S_i : i \in I\}$, where, $S_i \neq S_j$ if $i \neq j$, and the set I= {0,1,2,3,.....}. Each system, which purpose is to preserve the information, can be thought as a finite collection of information assets S_i=$\{\alpha_k$:k $\in$ I $\}$. Threats can destroy or only degrade information, we can practice information security at the system and network level, where it is easier for designers to act in different ways to reduce risk. Each system is also characterized by a vector X_i. called the decision vector, where each element is determined by the decisions and the strategies chosen to manage risk. Obviously threats that can affect the system are many, and then many variables should be introduced, but in this case they are reduced to a small number in order to analyze the model more accurately. The potential threats can attack the system in a single finite set $\{T_j$:j $\in$ I$\}$, and it can damage each information asset $\{\alpha_k\}$. The consequences of a successful attack of a threat T_j at time $t_i$is called *impact*, but if the attack failed *impact* is zero. The danger of each threat on each information asset, is the impact may have on each characteristic, and adding all these quantities to obtain the total probability. For each information system during the time interval of observation, it is necessary to do a distinction between *complete data* and *censored data*. Complete Data come from those systems whose failure causes are well-known and which occur during the observation period. Censored Data come from those systems that have no failure during the observation period, or if a failure occurs and the cause is unknown. For each individual system it is possible to define the following functions, and summarise the main functions involved as follow:

- Survivor Function S(t), which is the probability of being operational at time t :

$$S[t] = P_r[T \geq t] = 1 - F(t) \tag{6.1}$$

  Where F(t) is the Failure function, which tell us the probability of having a failure at time t.

- Failure Density Function f(t), which is the probability density function:

$$f(t) = \frac{dF(t)}{dt} = -\frac{dS(t)}{dt} \tag{6.2}$$

- Hazard Function h(t), which is the probability that an individual fails at time t, given that the individual has survived to that time:

$$h(t) = \lim_{\delta \to 0^+} P_r(t \leq T < t + \delta \mid T \geq)/\delta \tag{6.3}$$

  where $h(t)\delta t$ is the approximate probability that an individual will die in the interval $(t, t + \delta t)$, having survived up until t

- Cumulative hazard function H(t):

$$H(t) = -\log S(t) \tag{6.4}$$

In this regard, it is possible to introduce estimators of these functions S(t), F(t), f(t), h(t), referring to *complete data*, then neglecting *censored data*. Consider N systems and suppose that n(t) is the number of failure that occur before time t, the number of systems that most likely will have a failure in the interval $[t, t + \delta]$ is denoted by $n(t + \delta) - n(t)$ and N-n(t) is the number of systems still operating at time t. An empirical estimator for the function S(t) is :

$$S(t) = \frac{N - n(t)}{N} \tag{6.5}$$

An empirical estimator for the function F(t) is:

$$F(t) = \frac{n(t)}{N} \tag{6.6}$$

Instead for the function f(t) is :

$$f(t) = \frac{n(t + \delta) - n(t)}{\delta N} \tag{6.7}$$

For small value of , it is possible to calculate an empirical estimator for the function h(t), which is:

$$h(t)\delta = \frac{f(t)\delta}{S(t)} \tag{6.8}$$

Unfortunately, these definitions are not valid for data which are Censored, but it is possible to give alternative definitions to match the previous one to the case of interest. Using the first method, called Kaplan-Meier, we denote by:

$$t_{(1)} < t_{(2)} < t_{(3)} \ldots < t_{(m)}$$

the distinct ordered times of death(not considering the censored data). We define $d_{(i)}$ the number of failure at time $t_{(i)}$, and $n_{(i)}$ the number of surviving system just before the instant $t_{(i)}$. The estimator for the function S(t) can then be defined as follows:

$$S^{KM}(t) = \prod_i (\frac{n_i - d_i}{n_i}) \tag{6.9}$$

for $t_j \leq t < t_{j+1}, j = 1, 2, 3, \ldots, k-1$. The explanation of why this expression is valid even if there are Censored Data is very simple. To be alive at time t, a system must surely survive even in the moments before time $t_{(1)}$,$t_{(2)}$ .. because for sure in this interval $[t_{(i)}, t_{(i+1)}]$ there is no failure. So the probability of a failure at time $t_{(i)}$ is equal to $d_{(i)}/n_{(i)}$, taken for granted that the system survived in the previous interval. Obviously if there are not Censored Data, the estimator expression coincides with the previous case. The expression for other functions are:

$$F^{KM}(t) = 1 - S^{KM}(t) \tag{6.10}$$

$$H^{KM}(t) = -\log S^{KM}(t) \tag{6.11}$$

$$h^{KM}(t) = \frac{d_j}{n_j(t_{j+1} - t_j)} \tag{6.12}$$

The second method, called Nelson-Aalen, may be considered better than the Kaplan-Meier, as the latter can be considered an approximation when d_j is smaller than n_j. In this case the expressions become:

$$S^{NA}(t) = \prod_j \exp(-\frac{d_j}{n_j}) \tag{6.13}$$

$$F^{NA}(t) = 1 - S^{NA}(t) \tag{6.14}$$

$$H^{NA}(t) = -\log S^{NA}(t) = \sum_{j=1}^{r} \frac{d_j}{n_j} \tag{6.15}$$

$$h^{NA}(t) = \frac{d_j}{n_j(t_{j+1} - t_j)} \tag{6.16}$$

6.4 Risk Analysis Model

The risk analysis model, presented in this section, is based on a bio-inspired approach. Each ICT system consists of a series of assets. Each asset is linked to each other and both exchange information and are actively involved in the processes within the system, and are interconnected and communicate with the external environment. A biological system, a human body for example, has many similarities with ICT systems:

- High Complexity.
- High Connectivity.
- Numerous Access Points.
- Communication, Cooperation and Coordination on micro and macro level
- Vulnerabilities to several threats
- Relation with other systems of the same nature
- Relation and Communication with external environment

Thus, the proposal defines in both contexts:

- Biological Risk: the probability that a virus exploits a vulnerability. This can provide a disease of a single individual human body or it can spread causing an epidemic.
- ICT Risk: the probability that a threat exploits a vulnerability of an asset or of the system to cause an attack, compromising the security requirements of confidentiality, integrity and availability.
- Biological Failure: it is the event linked to an outbreak of a disease.

- ICT Failure: it is an event linked to the damage in the system, which is manifested, for example, with a denial of service.

Based on previous observations and definitions, the proposal defines the risk of a system as the sum of two components:

$$R = R^* + R_r \tag{6.17}$$

the first term is a function of the failure time distribution $F(t)$, while the second represents the Residual Risk R_r. It is the minimum achievable risk threshold of each system. Below this threshold it is impossible to get off, because there are not systems with a risk threshold equal to zero. The risk analysis aims to estimate these values and contextualizing them in the test system, we can then determine the safety measures to be taken to minimize component dependent failure distribution. Thus, Risk R^* can assume three different values :

- R_{nt}= Not Tolerable Risk. It is the maximum risk threshold above which the system has serious security problems.
- R_u= Unprotected Risk. It is the risk threshold of a system where there are not investments of any kind.
- R_t=Tolerable Risk. It is a risk threshold that we want to achieve, decreasing the threshold R_u, applying a certain investment I. Now we identify four ideal cases, based on the strategic choice of investment in the system.

6.4.1 Initial investment, made in the initial planning stage

The initial risk is R_t, because there is an initial investment I. The risk of the system is maintained within the range $R_t - R_u$, because the system is not totally exposed to threats. There can be intermediate investments but they are inappropriate or negligible and therefore they are not considered (for example an antivirus update unscheduled).

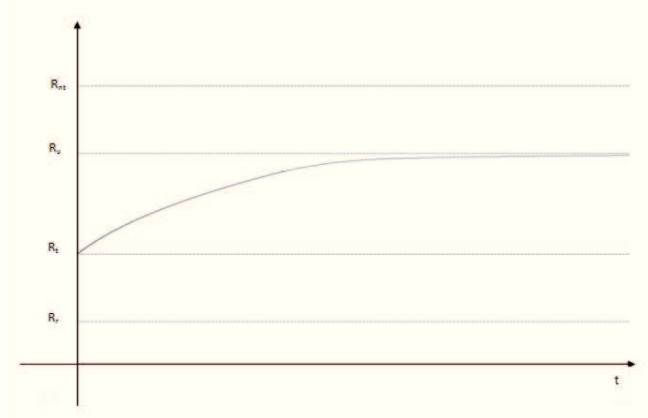


Figure 6.2: Initial investment

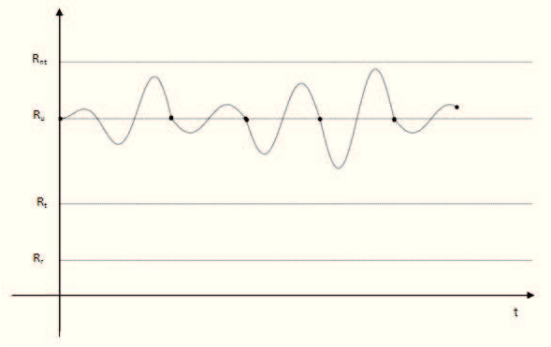


Figure 6.3: Intermediate investments

6.4.2 Intermediate investments (maintenance, protection/shelter after an attack of a threat)

In this second case, the initial investments are negligible. Investments, in this case, are done for a scheduled maintenance of the system, or after a successful attack of a threat. The points indicated by the arrows are times where the investments are applied. The function oscillates aroud R_u

6.4.3 Initial and Intermediate Investments

The risk, in this case, has small peaks over the threshold R_t, and oscillates around R_t, and sometimes tends to the minimum threshold of R_r, without touching it.

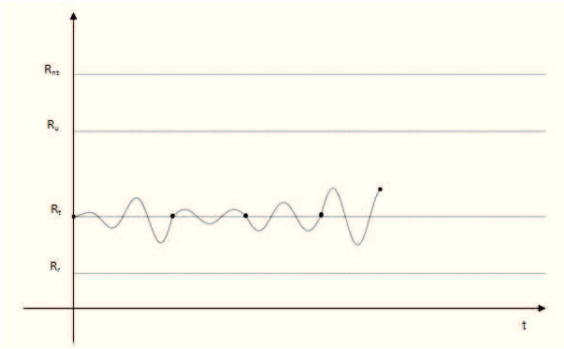


Figure 6.4: Initial and Intermediate Investments

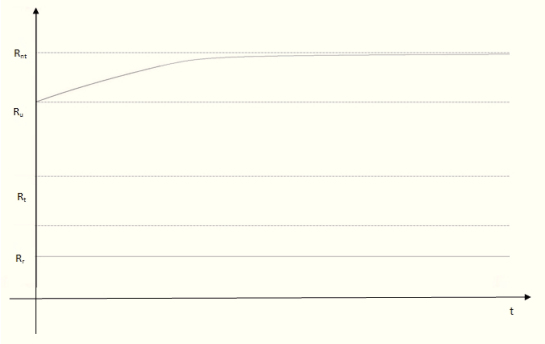


Figure 6.5: No investments

6.4.4 No investments

In this case the initial and intermediate investments are not necessary equal to zero, but they can be inappropriate or applied in non- strategic instants of time. There is the absence of a strategic security planning.The risk increases dramatically.

6.5 Some Considerations and Summary

The study of this dissertation revealed, in particular in the evaluation of the assets of a information system, an analogy between the security of information systems and epidemiological disciplines. The proposal of this Chapter identifies structures and methods that seems to be similar to processes, infrastructures and environments. It identifies statistical models, biological computing, biological real

behaviour, and all the rules that controls and mange the processes in the nature. Hence the interest in deepening this relationship is that at a glance was called Bio-Inspired Telecommunication Security, proposing a bio-inspired approach to risk analysis and defining a matching between Biologial Risk and ICT Risk, Biological Failure and ICT Failure.

Chapter 7

The Economy of Risk

Overview: |There are two real reasons that cause a failure in ICT systems. This can be caused at least as often by bad incentives as by bad design. There are some difficult to estimate the risk in different termes. The risk of Failure has three different components, technological, social and economical aspects. The impact on the information systems terminates the processes and compromises the infrastructure, causing economic losses, due to some security investments and not only them, and finally could be violate privacy social rights. This Chapter continue the assumption and the model proposed in the previous sectios focusing on the economical point of view and showing the proposal about the risk analysis model linked to the security investment issue and the possible economical loss. *Proposal presented in research contributions.*[1]

7.1 Introduction

Network insecurity is something that can occurs for technical issues that cause weaknesses but also for the users, that in many cases do not bear the full consequences or their actions. Malicious code, malware, spam and moreover dominates the market for the simple reason that many users don't distinguish the insecure software from secure software. This mechanism cause the increment of markets for vulnerabilities to test software security, but many times the trend shows that

[1] [La Corte et al., 2011]

developers on security are not always compensated for costly efforts to strenghten their code and software. This is caused by a separation between development, risk analysis and economic investments, in this way is not possible to be able to assess the impact of an successfully attack under all conditions. Vieweing security as the inverse of risk enables us to use computations of expected loss to propose a model to measuring gains in security by estimating decreases in risk after security investment.

7.2 Approach to known and unknown Risk

The challenges in networking growing quickly in terms of large-scale, heterogeneity, dinamicity and opportunistic. Biological models, the bio-inspired approach and medical models presented in the previous sections, have recently proven useful for information security in risk management and in the evaluation of proposed investments in information security, both of which depend on having knowledge of the probability distributions associated with successfully attack s on information assets and systems. Little real data is available upon which we can realy to estimate the required probability distributions. Emerging risks also sometimes called global risks are large-scale events or circumstnces that arise from global trends, are beyond any particular party's capacity to control. Emerging risks are those large-impact hard to predict and rare events beyond the normal expectations.

This is what the philosopher-epistemologist Nassim Nicholas Taleb calls "balck swans", in references to the fact that Europeans once knew that all swans were white until explorers in Australia discovered black ones. The Black Swan logic makes "what you don't know" far more relevant that what you do know. The events that have the power to change the statistic are unexpected. The example is the terrorist attack of September 11, 2011:

> "...had the risk been reasonably conceivable on September 10, it would not have happened. If such a possibility were deemed worthy of attention, fighter planes would have circled the sky above the twin towers, airplanes would have had locked bulletproof doors, and the attack

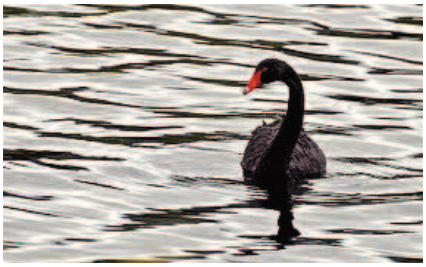


Figure 7.1: Back Swan

would not have taken place, period. Something else might have taken place. What? I don't know."

"The Black Swan" by Nassim Nicholas Taleb.

All these risks present high impact but low probability and fall beyond the organization's direct control to mitigate, they are often found to be under-resourced. When competing for budgets, those risks with greater probability of occurrence tend to win. When competing for management attention, those risks deemed more likely to impact performance targets and rewards win again. However, failure to understand and track these risks can lead to a situation in which todays afterthought becomes tomorrows global headline issue. With adequate information analysis, assessment and estimating risk and expected losses, the unexpected can often be predicted by extrapolating from variations in statistics based on past observations. This is possible if there is a complete analysis and assessment of the general information system hypotetically vulnerable and then apply the risk analysis considering global risk that involve every asset and processes. These risks are often referred to as the unexpected or the unknown, and one can argue that "almost all consequential events in history come from the unexpected".

7.3 The Economy of ICT Security

Threats include natural threats such as fire, flood, earth quake, tornado, ice, and so forth; threats by undirected entities such as malicious code; and directed threats by individuals and groups, including hackers, spiesm thieves,psychotics,

terrorists, and enemy military forces. Our information assets are those buts and aggregations of information, processes and environement that are important to us in performing and conducting networking and in some cases business. Information assets, for examples, may include databases, product designs, software, images, text files, audio files, or video files. Information assets are created, stored, processed, communicated but also stolen, improperly disclosed and misused, illicit modified or destroyed. To prevent failures or to minimize their consequenes when they cannot be prevented a mix of policies, practices, procedures, insurance, technologies and legal action are needed. Decisions concerning investments in information security, about new or additional procedures or technologies that are expected to enhance the ICT systems, will be informed by quantitative analysis. Everything related to business investment begins with the strategic decisions. To benefit from the investments is essential to understand where, how and when to apply them. Historically, security decisions are taken outside of the context and after the damage occurred. The security is hard to quantify and it is seen as the inverse of risk. Failure does not necessarily mean the catastrophic destructions of information assets, of a process or system. It is real or potential compromise of confidentiality, availability and integrity. So, detection of Failures requires that we carefully define what types of asset are to be considered in the failure data definitions and in the security requirements. For an ICT system, the failure time distribution must weigh the value of information exchanged, assets, processes and therefore the whole system, thus, following the proposal of this Chapter:

$$F_s(t) = F_a(t) * F_p(t) \tag{7.1}$$

With $F_a(t)$ "assetr failure function",$F_p(t)$ "process failure function", $F_s(t)$ "system failure function". The "asset failure function" is the probability that a failure event affects an asset of the system. The "process failure function" is the probability that a failure event compromises a process of the system. In every asset and every process of a communication system are involved more information sets that must be protected in accordance with the requirements and the security goals. Information set has a value, which gives a degree of importance of information exchanged very vulnerable to the likely impairment due to an external agent.

Taking into account the value associated to information set can give a weight to the asset failure,α and the process failure β. There will be two different cases:

$$\gamma = \alpha + \beta \tag{7.2}$$

$$\gamma = max(\alpha, \beta) \tag{7.3}$$

In the first case, the event associated with asset failure is independent from the event associated with process failure. In the second case, instead, events are not independent. In a communication system we identify these failure events:

- Asset or Process Failure for an unknown cause.
- System security requirement compromise for an unknown cause.
- Asset or Process Failure for a specific cause.
- System security requirement compromise for a specific cause.
- Asset or Process Failure with a countermeasure.
- System security requirement compromise with a countermeasure.

The security degree isa a function of $F(t)$ and it is the inverse of $H(t)$, the Hazard Function. With S_{dICT} Security Degree and R_{ICT} Risk Measure:

$$S_{dICT} = R_{ICT}^{-1} \tag{7.4}$$

and R measure is function of $F(t)$, Explanatory Variables and Threats. Following the Cox Model [Cox and Oakes, 1984][Cox, 1972], $H(z, \delta_1)$ and $H(th, \delta_2)$, identify respectively ther vectors of explanatory variables and threats weighted on the coefficient δ_1 and δ_1, as in:

$$R_{ICT} = \gamma * H(z, \delta_1)H(th, \delta_2) \tag{7.5}$$

Thus, vieweing security as the inverse of risk enables us to use computations of expected losses to develop a quyantitative approach to measuring gains in security by measuring decreases in risk. Making decisions concerning investments

in information security requires calculations of net benefits expected to result from an investment I[Ryan and Ryan, 2006]. Expected loss provides a useful metrics for evaluating whether an investment in information security is warranted. Since expected loss is the product of the loss ν that would be realized following successful attack on the systems comprising our information infrastructure and the probability that such a loss will occur. If p_0 is the losses occuring with the investment I and p_i of the losses occuring without the investment i, the expected net benefit of the investment i is, then:

$$E_{NB}[i] = p_0\nu - p_i\nu - i = (p_0 - p_i)\nu - i \tag{7.6}$$

A positive expected net benefit characterizes attractive investment opportunity[Ryan and Ryan, 2008a][Ryan and Ryan, 2006].

7.4 Strategic Decisions and Business Investments

The ideal analysis should allow so great a risk estimate. The Case 3, presented in previous chapter, is the ideal case where investments are allocated at the beginning and at intermediate time. An optimal strategy also considers the economic tradeoff between the timing of investment, its value and cost-effective. To improve the security of a system it should make investments a way to protect the system from possible threats. It is obvious that this investment must be profitable for the system and prevent any attacks, or survive if there was one. The developments in technology have improved performance, in terms of security systems, but it has meant that the threats, that can attack a system, evolved. For this reason, before investing the money, it is necessary to make appropriate assessments. Resuming the previous definitions of hazard function, we can consider two different systems and compare them. In the first system we suppose to make investments to improve security and define $h_1(t)$ its instantaneous failure rate, in the second system we decide not to invest in security and call $h_0(t)$ its hazard rate. It is possible to relate the two quantities through the following relatioship:

$$h_1(t) = kh_0(t) \tag{7.7}$$

Assuming that the hazard function is continuous, although in reality it is not very likely, it is assumed that the processes of censored always occur after a failure. From this report it is possible to evaluate the benefit that an investment can result in increasing the security of a system. The parameter k is called Hazard Ratio, and through its value it is possible to make the following observations :

- If $k < 1$ the probability of succumbing to an attack is less in a system on which we decide to invest.
- If $k = 1$ there is no advantage on investing, because the two systems, when being attacked, would behave the same way.
- If $k > 1$ the system in which we have invested money succumb more easily to an attack and then invest money is not beneficial.

If we decide to invest for the security of the system, the benefits that we expect to obtain is given by the following formula (13,iccsa):

$$E_{NB}[i] = p_0 L - piL - i \tag{7.8}$$

where p_0 and p_i are the loss probabilities for the system on which we invested and the one without, respectively, and L is the loss. A positive value of E_{NB} means that the investment has made benefits. If we apply the investment, the Survivor Function is shifted to the right, this means that systems survive longer than others. Thus, the proposal introduces and proposes the loss variable definition for an ICT system, as:

$$L = L_{inf} + L_E \tag{7.9}$$

Where L_{inf}, is the information loss, reported to confidentiality, integrity and availability:

$$L_{inf} = L_{infC} + L_{infINT} + L_{infAVAIL} \tag{7.10}$$

And L_E is the economic loss due to the information loss. At each risk threshold it is possible to match a loss threshold.

- L_u is the information and economic loss in an unprotected system.

- L_t is a tolerable information and economic loss of system whit a tolerable risk threshold.
- L_r is the minimum information and economic loss (ideal case) of a system ideally with no risk.
- L_{nt} is a non tolerable loss associated to a non tolerable maximum risk.

7.5 Risk Management and Security Investments

The perfect investment I will allow minimizing $R_{ICT}(t)$, optimizing the countermeasures and managing the security degree. Investment does not stem only from a statistical evaluation of threats and vulnerabilities, or from a next simple actions, result of an attack already happened, but from study of the system in its entirety. For this Investment have to follow the approach proposed in the previous sections, and it is function of the decisions making during each phase of the Information Security Management Architecture:

$$I = f(Assessment, Analysis, Managament) \tag{7.11}$$

The investment have to follow the system security requirements and have to comprises the evaluation of the importance of the vulnerability and the probable breach. Many times the investment is not done for a vulnerability with a great risk and with a low probability, but sometimes, especially some companies decide to invest in security for real and probable vulnerability with medium risk but high probability of breach.

7.6 Some Considerations and Summary

The interest is in protecting information infrastructures and communication infrastructures and the information assets within them from all type of compromise. It is well recognize that attacks can result in compromise of each type of security requirements decided in planning phase. Our willingness to accept certain risks and therefore our choices in investments in information security to abate those

risks, must be informed by the consequences of the impacts of each type of threat as well as of the combined threat. The greater difficulty in estimating the risk is surely that the risk itself cannot be managed better until it can be measured better. Making decisions concerning investments in information security, his approach requires calculation of net benefits expected to result from the economic strategy of security management linked to the information system analysis and assessment.

Chapter 8

Conclusions and Future Work

Overview: |This Chapter revisits the research questions posed in the first Chapter outlining possible avenues for future research and summarising the main contributions of this disseration.

8.1 In conclusion...what is Security?

"The security for an ICT system is the strategic plan of a set of phases including assessment, analysis of assets and processes, classification and analysis of vulnerabilities and threats, decision making steps, implementation of countermeasures, monitoring and control policies, risk analysis and risk management, which evaluate and estimate, in a timely, economic, technological and social aspect of a potential damage as a result of an successfull attack texploited a weakness of a system. It is an ongoing process, which should be based on the global vision of an ICT system, its main features, how it will change in the near future, the context and environments with which it is connected to the network, the users who benefit from services and users who can access and modify information, guaranteeing always the safety requirements established in the design phase, which are based on confidentiality, integrity and availability and also with the possibility to extend them."

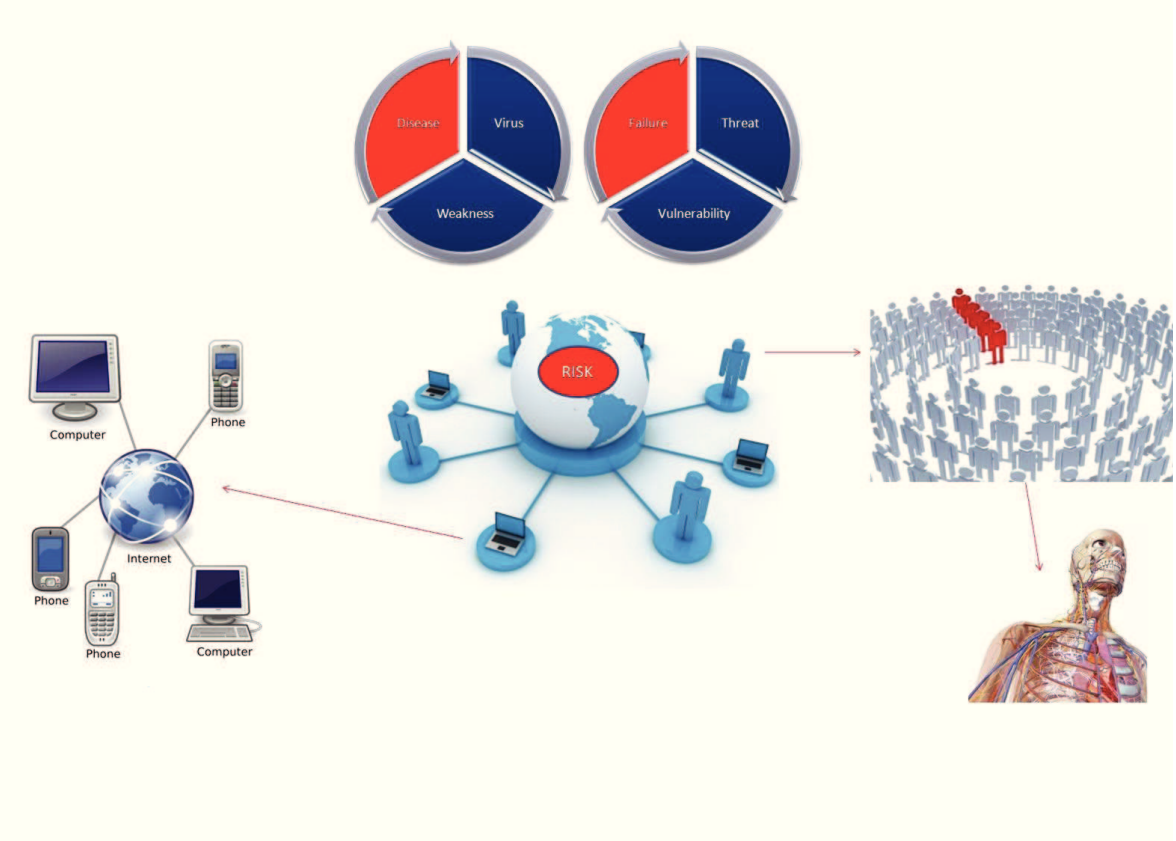


Figure 8.1: Bio-Inspired Models and ICT

8.2 Research Contributions and Questions Revisited

This dissertation has made the following contributions, listed answering questions asked in the first Chapter:

- ***Can ecurity of an ICT system be analyzed and managed strying to provide at least the requirements of confidentiality, integrity and availability of information system?*** Chapter 3 showed and proposed an all-encompassing framework that aims to address technical, human and economical aspect of the security through ISMA Model.

- ***How we can identify Assets, Threats and Vulnerabilities? How we can investigate and use these information to estimate the risk? Can Spam on VoIP be identified and can Spit calls be minimized maximizing the security degree of the system?*** Chapter 4 showed and present an overview of VoIP applying ISMA model to case

of this technology, proposing also a user-profile framework against Spit.

- ***To what extent can quality and security of the next generation network be considered improved in comparison with not-converged solutions?*** Chapter 5 presented a model of analysis to assess and compare the requirements and factors of influence of security and quality of converged and not-converged solutions.

- ***To what extent can analytical models and biological processes inspire the analysis and management of the trend of risk, useful in decision making strategies of countermeasures and safety policy?*** Chapter 6 showed the proposal about model to analyse risk and manage security based on bio-inspired approach linking the issues to the decision making about investments.

- ***What kind of strategy and investment can be applied to an ICT system to produce a positive expected benefits. Can Survivor Analysis be useful to give a realistic measure of risk and to evaluate the impact on security requirements?*** Chapter 7, continuing the proposal of Chapter 6 focused on the economical point of view showing economical losses, expected benefit and discussing about the economy of risk.

- ***How dinamically chooses routing and find an optimal routing mechanism according to dynamic network condition in wireless ad hoc networks, to obtain improvement in terms of energy consumption in a mobile ad hoc network? ... How to generate the bio-diversity in terms of single node and in terms of network domain? How to use the diversity and heterogeneity among nodes and between domains to bring out the best path to identify the points of the network more secure?*** In Conclusions, the Section 8.3 present two issues and research topic, as further work, about energu consumption and green sustainability of the future of ICT and a bio-inspired

approach to introduce bio-diversity and heterogeneity to improve robustness, high performances and reliability.

8.3 Further Work and Future Research Items

The emerging information society is widely explected to experience massive embedding of both fixed and portable devices into our local physical spaces, with more and more devices having the capacity to initiate, store and communicate information and content in all aspect of life. When designing an information system, anything can be underestimated. The system consists of assets, is characterized by processes and provide a range of services to users who use it. When economic investments are addressed and directed to a system, several factors come into play, related to each other. Mistakes and incorrect estimates in terms of future predictions must take into account several aspects. The main ones, are in particular the requirements of privacy and security, maintenance and warranty of performance, and last but not least, the attention to energy consumption. The issues of the next future that will rule the new generation network are classified in three topics, Security, Quality and Energy consumption. To understand how an information and communication system could add value to guarantee good performance of every systems in terms of these three issues or how improve ICT system itself based on the estimate of risk, quality and energy consumption, both questions are open problems. The key of challenge is in the structure of the human societu of the next future. The rules of the new human society are different and the social network changed everything, dinamic of sharing, the need of people, the distances and the multimedia pervasivness. Everything is different, because the social human society, now lives in social networks. Starting from the fundamental principles of social networks analysis, published in "The Strenght of Weak Tie" by Mark Granovetter, and discussing about the challenges of human society structure, this chapter presents a topic related to the previous keywords topic following the Mind Map of Keywords in the first Chapter, and it is now and open research problem. Two key questions summarize these new topic, the first

one is:

> Based on social structure of mobile node community and on new human society ties using local and global information, how dinamically choose rules and mechanisms according to dynamic networks to obtain improvement on energy consumption, ensuring quality and security ate the same time?

To maintain robustness of the system, high performances, reliability and to balance the energy of the system how it was an ecosystem, a bio-inspired approach could be useful and the introduction of bio-diversity could be the proper solution to apply. Thus the second one is:

> How to generate the bio-diversity in terms of single node and in terms of network domain, and how to use the diversity and heterogeneity among nodes and between domain to bring out the best path to identify the points of the network more secure?

This section introduce both of topics and related works. If we consider the networks of today, they are characterized from cooperation and sharing of information. Cooperations binds but also divides human society into communities. Members of the same community interact with each other preferentially [Pan Hui and Yoneki, 2010]. Community is an important attribute of PSNs. A PSN is a Pocket Switched Network uses contact opportunities to allow humans to communicate without network infrastructure. A PSN is formed by people which have social relationships. The community where the people has this relationship is characterized by mobility. Community is an important attribute of PSNs. Within a community some people are more popular and interact with more people than others, thus they have high centrality. It well known that some nodes may be more highly connected to each other than the rest of the network. The set of such nodes are ususally called cluster, communities, cohesive groups or modules. Popularity ranking is one aspect of the population and can characterize the communities. To understand the habits of the people, the way of sharing information, and forward data, or about energy consumption, detect the interation

among people of the same community, and among people of different communities is necessary. Methodologically, community detection in complex network have been proposed in many different way in scientific literature. Community detection can help us understand the local structure in mobility traces and to good design strategies for information sharing and data forwarding. Considering the next future in terms of total wireless and mobility communication and networking, movung from first generation 802.11 LANs and cellular servicesm through second generation of Mobile Ad Hoc Networking and now on third generation with PSN, like as a category of Delay tolerant Network, we need to rewrite the requirements for security, quality and now, to pay attention to the new issue of energy awareness. DTNs architecture offers support to communication scenarios where nodes are sparse and the contacts between them are short-lived, due to high node mobility. In this complex context, that will characterize the future of the network with high level of nodes, dinamicity, mobility, delay-tolerant, pervasivness, opportunistic features, the design of efficient routing protocols is a fundamental problem, to analyse the other problems such as privacy, performance of quality, and energy consumption. Evaluating the energy consumption of network protocols requires a compromise between precise estimation of enery and high-level insight into protocol behaviour. Thus, drawing inspiration from sociology, with the idea of correlated interaction, we can understand the community structure how is changing thanks to the new networking, adapat the routing protocol, to have a rule of forwarding based on social behaviour and social human structure, to have the best community in terms of security, performance and energy consumption. The aim is to drawing inspiration from new algorithm based on social-forwardin, such as BUBBLE-RAP[Pan Hui and Yoneki, 2010], useful to improve the forwarding efficiecy compared with the oblivious forwarding scheme. BUBBLE-RAP combines the knowledge of community structure with the knowledge of node centrality to make forwarding decisions. The knowledge on the local structure, the degree of connectivity and centrality of the nodes, message size, speed and topology, features of community, through an extension of the existing algorithms, can contribute to risk analysis and therefore security, as more nodes

are central and connectedmore they are exposed to a number of risks. At the same time local and global features, and rules of forwarding can be used for the dissemination and sharing of information in order to maximize the awareness of energy consumption and network security, ensuring a quality service at acceptable levels according to the requirements. To have a good balance of energy, quality and securty, a good idea is to drawing inspiration from biology. The bio-inspired approach is the line that this dissertation has like aim to guide and inspire strategy for ICT and new generation network. The diversity of some biological communities, is an important cue for design robustness[Forrest and Ackley, 1997][Khoo and Lio, 2011]. The aim is to find a technique for automatically protecting against any flood invasion, following the security issue, through the introduction of heterogeneity degree, but this heterogeneity has a cost. Nature seems to suggest that even a high cost for heterogeneity is preferable. A stable ecosystem contains many different species which occur in highly-conserved frequency distributions. If this diversity is lost a few species become dominant, the ecosystem becomes susceptible to perturbations. Thus introducing deliberately diversity into communities of nodes in information and communication systems, means to make them more robust against the spreas of attack and at the same time using an optimal strategy for energy consumption. In conclusion, to summarize the work of this Ph.D. thesis, the list of keywords, which represents the topics discussed in this dissertation:

- ICT Security.
- Risk Analysis and Security Management.
- Risk Analysis and Security Management.
- Spit Prevention Model.
- Bio-Inspired Telecommunication Security.
- Bio-diverity for security of the networks.
- Sustainable ICT for Security and Energy Consumption.

Some results of a research referred to the keywords of this dissertation are presented in the figure 8.2, following a structured methodology and approach and identifying the state of research contributions in the period 2006-2011, referred to the topic of this Ph.D. thesis. To evaluate the importance of the topics presented in this dissertation, the collection of papers searched was based on:

- Personal Knowledge of specific papers.These were grouped into broader category topics referring to the keyword and topics choosed.
- Searches on:

  CiteSeer.

  IEEE Xplore.

  ACM Digital Library.

  Google Scholar.

  SciVerse.

The keywords list used for the Survey is:

- ICT Security. (discussed in Section 3)
- Information Security. (discussed in Section 3)
- Information Security Awareness. (discussed in Section 3)
- Network Security.(discussed in Section 3)
- Communication Security. (discussed in Section 3)
- Privacy.(discussed in Section 3)
- VoIP Security.(discussed in Section 4)
- VoIP Vulnerabilities. (discussed in Section 4)
- VoIP Attacks. (discussed in Section 4)
- Spit. (discussed in Section 4)

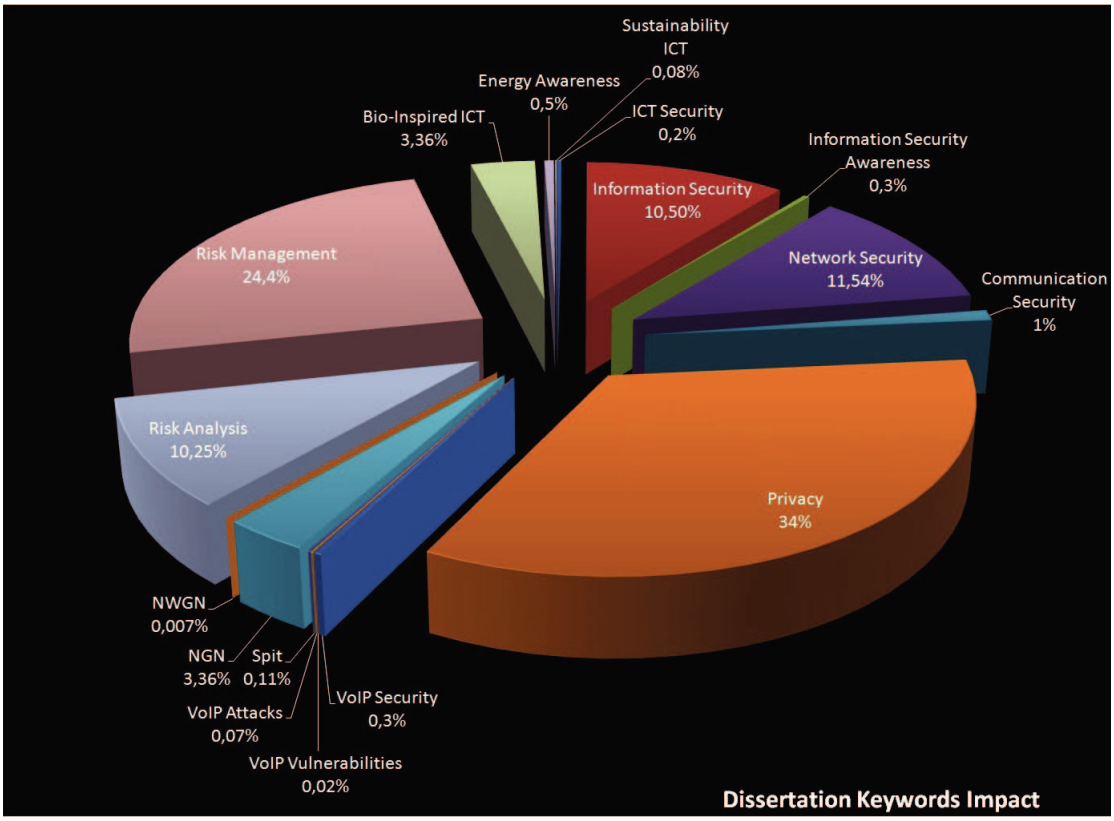


Figure 8.2: Importance Dissertation Keywords

- NGN. (discussed in Section 5)
- NWGN. (discussed in Section 5)
- Risk Analysis.(discussed in Section 6 and 7)
- Risk Management. (discussed in Section 6 and 7)
- Bio-inspired ICT. (discussed in Section 6 and 7)
- Energy Awareness. (discussed in Further Work in Section 8)
- Sustainability ICT. (discussed in Further Work in Section 8)

The key aim is to have a social community of networks, smart and sustainable, that shares informations and knowledge in a secure way,

focusing on energy consumption issues, maintaining the work of the network more efficient, balancing costs of investments and expected benefits. This will result in significant challenges for communication and information provision, based on required scalability, efficiency in forwarding, heterogeneity re-configurability, security and dynamicity. In this context the need is to find an optimal set of rules and method, to implement and develop technologies to guarantee security, quality and energy consumption and awareness of these issues, to allow the future of ICT also in term of green sustainability. For this reason, I am keen to continue for further works and and developing and deepening my own idea about the topics and issues presented in this dissertation.

References

Ali M.Alsaih Ahmad A.Almughaless. Optimum migration scenario from pstn to ngn. 2010. 81, 83

T. Ayoama. A new generation network: Beyond the internet and ngn. *IEEE Communications Magazine*, 2009. 26, 30, 50, 83

R. C. Basole. Enterprise adoption of ict innovations: Multi-disciplinary literature analysis and future research opportunities. 2008. 31, 33, 34

H. Wada C. Lee and J. Suzuki. Towards a biologically-inspired architecture for self-regulatory and evolvable network applications. *Advances in Bio-Inspired Information Systems in Computational Intelligence (SCI), Springer*, 69:25, 2007. 27, 101

Cisco. Cisco annual security report. 2010. 17

Lizzie Coles-Kemp and Yee-Lin Lai. Privacy on the internet:attitudes and behaviours. 2010. 17

D. Roxbee Cox. Regression models and life-tables. *Journal of the Royal Society, Series B (Methodological)*, 34(2):187–220, 1972. 28, 106, 108, 121

D.Roxbee Cox and D. Oakes. *Analysis of Survival data.* CHAPMAN & HALL/CRC, 1984. 28, 106, 108, 121

R. Dantu and P. Kolan. Detecting spam in voip networks. in proceedings of the steps to reducing unwanted traffic on the internet workshop. 2005. 24

M.T. Dlamini, J.H.P. Eloff, and M.M. Eloff. Information security: The moving target. *Computers & Security*, 28(3-4):189–198, 2009. 14, 17

Falko Dressler and Ozgur B. Akan. A survey on bio-inspired networking. *Elsevier Computer Networks*, 54(6):881–900, 2010. 26, 27, 102

ETSI. Telecommunications and internet converged services and protocols for advanced networking (tispan),es 282 001 v3.3.0. 2002. 86

ETSI. Telecommunication and internet converged services and protocols for advanced networking (tispan); next generation network (ngn); quality of service (qos) framework and requirements, ts 185 001 v1.1.1. 2005. 88

ETSI. Telecommunications and internet converged services and protocols for advanced networking (tispan),ts 185 006 v2.1.2. 2008. 86

Somayaji A. Forrest, S. and D.H. Ackley. Building diverse computer systems. *The Sixth Workshop on Hot Topics in Operating Systems*, 5-6:67–72, 1997. 132

Marias G.F. and et al. Sip vulnerabilities and anti-spit mechanisms assessment. *Proceedings of 16th International Conference on Computer Communications and Networks, ICCCN 2007.*, pages 597–604, 2007. 64

B. Goode. Voice over internet protocol (voip). *Proceedings of the IEEE*, 90(9): 1495 – 1517, 2002. 53

R. Frederick V. Jacobson H. Schulzrinne, S. Casner. *RTP: A Transport Protocol for Real-Time Applications*. IETF RFC 1889, 1996. 54

Siddique Saha Pran Kanai Hany, Umma Hossain. Qos optimization and performance analysis of ngn. 2010. 79

R. Heeks. Ict4d 2.0:the next phase of applying ict for international development. *Computer, IEEE Computer Society*, 41:26–33, 2008. 15, 23, 31, 33, 35, 47

YU Hong-Tao HUANG Hai and FENG Xiao-Lei. A spit detection method using voice activity analysis. 2009. 24

International Standard ISO/IEC. Information technology security techniques. information security risk management:27005. 2008. 35, 36, 101

et al. J. Rosenberg. *SIP: Session Initiation Protocol*. IETF RFC 3261, June 2004. 53

Urban Sedlar Janez Bester Janez Sterle, Mojca Volk and Andrej Kos. Application-based ngn qoe controller. *IEEE Communications Magazine*, pages 92–101, 2011. 79

Soon Seok Lee Jongtae Song, Mi Young Chang and Jinoo Joung. Overview of itu-t ngn qos control. *Communications Magazine, IEEE*, 45:116–123, 2007. 88

Sandra Tartarelli Juergen Quittek, Saverio Niccolini and (NEC Europe Ltd.) Roman Schlegel. On spam over internet telephony (spit) prevention. *IEEE Communications Magazine*, 46(8):80–86, 2008. 62, 63, 64

Sandra Tartarelli Juergen Quittek, Saverio Niccolini and Roman Schlegel. Detecting spit calls by checking human communication patterns. *IEEE International Conference on Communications, 2007. ICC '07.* 24

J. D. Kalbfleish and R. L. Prentice. The statistical analysis of failure-time data. 2002. 101, 106

Thomas Towle Keith Knightson, Naotaka Morita. Ngn architecture:generic principles. *Functional Architecture, and Implementation, Communications Magazine, IEEE*, 43, 2005. 87

A. D. Keromytis. Voice over ip: Risk, threats and vulnerabilities. *In Proceeding of the Cyber Infrastructure Protection (CIP) Conference*, 2009. 23, 31, 48, 60

A. D. Keromytis. Voice over ip security: Research and practice. *IEEE Computer and Reliability Societies, Secure Systems*, 8(2):76–78, 2010a. 23, 24, 35, 48, 60

A.D. Keromytis. A comprehensive survey of voice over ip security. *Columbia University Computer Science Technical Reports*, 2010b. 23, 24

Wei Ming Khoo and Pietro Lio. Unity in diversity: Phylogenetic-inspired techniques for reverse engineering and detection of malware families. *First SysSec Workshop (SysSec)*, 6:3–10, 2011. 132

Stephan Kitchovitch and Pietro Lió. Risk perception and disease spread on social networks. *International Conference on Computational Science*, 1(1):2339–2348, 2010. 28, 101

P. Kolan and R. Dantu. Socio-technical defense against voice spamming. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 2, 2007. 24

Kwon-Chul Park Kyung-Hyu Lee, Kyu-Ok Lee. Architecture to be deployed on strategies of next generation networks. 2003. 87

W.Currie L. Willcocks and S. Jackson. Radical re-engineering and information systems: evidence form uk public services. *Fifth European Conference in Information Systems.Cork*, 1997. 15, 23, 35

A. La Corte and M. Scatá. A process approach to manage the security of the communication systems with risk analysis based on epidemiological model. *Fifth International Conference on Systems and Networks Communications (ICSNC)*, pages 166–171, 2010. 30, 47, 100

A. La Corte and M. Scatá. Security and qos analysis for next generation networks. *International Conference on Information Society (i-Society)*, pages 248–253, 2011a. 80

A. La Corte and M. Scatá. Failure analysis and threats statistic to assess risk and security strategy in a communication system. *Sixth International Conference on Systems and Networks Communications (ICSNC)*, 2011b. 100

A. La Corte, M. Scatá, and Giacchi E. A bio-inspired approach for risk analysis of ict systems. *Computational Science and Its Applications - ICCSA 2011, Lecture Notes in Computer Science,Springer Berlin (Heidelberg)*, 6782:652–666, 2011. 100, 117

J. M. Lachin. Biostatistical methods: The assessment of relative risks. 2000. 28, 101, 106

Hyeong Ho Lee. Signaling architecture and protocols for the next generation network. 2009. 87

TaiJin Lee and et al. User reputation based voip spam defense architecture. *International Conference on Information Networking, 2009. ICOIN 2009.* 64

R. Lenz and M. Reichert. It support for healthcare processes. *Business Process Management*, 2005. 15, 23, 34

V. Leveque. *Information Security: A Strategic Approach.* IEEE Computer Society, J. Wiley and Sons., New Jersey, 2006. 15, 31, 32, 36, 47

Jun Li and Paul Knickerbocker. Functional similarities between computer worms and biological pathogens. *Elsevier Computer & Security*, 26(6):338–347, 2007. 26, 101

Kai Zhao Long Zhang. Study on security of next generation network. 2008. 90

E. Carrara M. Baugher. *The use of timed efficient stream loss-tolerant authentication (TESLA) in the secure real-time transport protocol (SRTP).* IETF RFC 4383, 2006. 54

K. Shindler C. Alphonce M. Buckley, H. Kershner and J. Braswell. Benefits of using socially relevant projects in computer science and engineering education. *SIGCSE*, 2004. 15, 23, 33, 35

R. MacIntosh and D. Vinokurov. Detection and mitigation of spam in ip telephony networks using signaling protocol analysis. *IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communications*, pages 49–52, 2005. 24

Atsunobu Narita Marco Carugi, Brent Hirschman. Introduction to the itu- t ngn focus group release 1: Target environment, services and capabilities. *Communications Magazine, IEEE*, 43, 2005. 81, 84

Noel Crespi Mehdi Mani. Inter-domain qos control mechanism in ims based horizontally converged networks. 2007. 89

Vasileios Pappas Michael Meisel and Lixia Zhang. A taxonomy biologically inspired research in computer networking. *Elsevier Computer Networks*, 54(6): 901–916, 2010. 27, 101

Microsoft. Microsoft security intelligence report. 2010. 17, 19, 21

W. H. Murray. The application of epidemiology to computer viruses. *Computer & Security*, 7(2):139–145, 1988. 28, 101, 106

Yury Namestnikov. Information security threats in the first quarter of 2010. 2010. 17

J. Pan Hui, Crowcroft and E. Yoneki. Bubble rap: Social-based forwarding in delay-tolerant networks. *IEEE Transactions on Mobile Computing*, 10:1576–1589, 2010. 130, 131

ITU-T Recommendation. Ngn fg proceedings. 2005. 84, 88

C. J. J. Rosenberg. *The Session Initiation Protocol (SIP) and Spam*. IETF RFC 5039, 2008. 53

J. C. H. Ryan and D. J. Ryan. Expected benefits of information security investments. *Computer and Security, Elsevier, ScienceDirect*, 25(8):579–588, 2006. 28, 29, 35, 101, 109, 122

J. C. H. Ryan and D. J. Ryan. Performance metrics for information security risk management. *IEEE Computer Society, Security and Privacy*, 6(5):38–44, 2008a. 23, 28, 29, 35, 101, 109, 122

J. C. H. Ryan and D. J. Ryan. Biological system and models in information security. *In Proc. of the 12th Colloquium for Information System Security Educatione*, 2008b. 26, 28, 29, 35, 101, 102, 109

M. Scatá and A. La Corte. Security analysis and countermeasures assessment against spit attacks on voip systems. *World Congress on Internet Security (WorldCIS)*, pages 177–183, 2011. 47

B. Shneier. Architecture of privacy. *Security and Privacy, IEEE Computer Society*, 7(1):88, 2009. 15, 31, 32

Symantec. Symantec internet security threat report,trends for 2010. 16, 2011. 21

A. Da Veiga and J.H.P. Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, 2010. 14

VOIPSA. Voip security and privacy threat taxonomy. *available at voipsa.org*, 2011. 23, 31, 35, 48, 50, 60

M. Wang and T. Suda. The bio-networking architecture: A biologically inspired approach to the design of scalable,adaptive, and survivable/available network applications. *IEEE Symposium on Applications and the Internet (SAINT)*, pages 43–53, 2001. 27, 101

W.J.Vankan, R. Maas, and M.T. Dam. Ict environment for multy-disciplinary design and multi objective optimisation: A case study. 2002. 31, 33

ITU-T Recommendation X.805. Security architecture for systems providing end-to-end communications. 2003. 89

ITU-T Recommendation Y.2001. General overview of ngn. 2004. 81, 84

ITU-T Recommendation Y.2011. General principles and general reference model for next generation networks. 2004. 81, 84