Failure Analysis and Threats Statistic to Assess Risk and Security Strategy in a Communication System

Aurelio La Corte, Marialisa Scata'
Department of Electrical, Electronics and Computer Science Engineering
Faculty of Engineering, University of Catania
viale A.Doria 6, 95125, Catania, Italy
Email:lacorte@dieei.unict.it, lisa.scata@dieei.unict.it

***Abstract*—The paper presents and evalutes one of the most important aspects in an information and communication technology system that is to preserve the information from any attacks trying to ensure the protection of data while maintaining quality of service, confidentiality, availability and integrity. In recent years, the process towards convergence has been devoloped to take into account several evolving trends and new challenges. Most of this is about security. New security issues make it necessary to analyse and manage the safety of the information and communication systems. Thus, an economic investment can not ignore the technical evaluation of the system, vulnerabilities analysis, threats taxonomy, and the estimate of expected risk, in order to ensure proper countermeasures to limit the technological and economic damage over time. Risk analysis involves the technical, human and economic aspects, to guide strategy of investment. Following a bio-inspired approach, this analysis requires knowledge of the failure time distribution and survivor analysis to estimate risk. With this paper, we propose a step-by-step analysis based on bio-inspired models, showing and validating that the risk in the absence of explanatory variables that influence the impact of threats, and neglecting the possible relationships between them, does not change shape.**

Keywords-ICT; Security; Survivor Analysis; Bio-Inspired; VoIP.

I. Introduction

Information and Communication Technology (ICT) is the set of technologies to develop, communicate and share information through digital mean ICT represents the design, development, implementation, support and management of information systems through the use of telecommunications systems. The ICT links two components, the information technology (IT) with the Communication Technology (CT), and at the same time it is an essential resource in modern organizations, within which it becomes increasingly important to be manage to operate quickly and efficiently the use of data and the increasing volume of information. Information is defined in [1][7][8], as an important business asset, that can exist in many forms. Information can be managed, manipulate to be available to the users at any time. Then, we must take note of the means available to analyze the risk and issues to information security. In many processes the security risk has recently gained in significance. Risk analysis is important such as the planning phase of the information system architecture. The objective is to protect the infrastructure, and information from attacks that can compromise the safety requirements, such as confidentiality, integrity and availability. In recent years, technological evolution is faced with the problem of security methodologies that propose remedial actions, and not with estimates and analysis to assess the expected risk. From the Internet network to the future next generation network (NGN), switching to new concepts such as opportunistic communication networks and green, these networks arise from the interaction and the strong conceptual link that exists between the world of technological networks and biological networks. Many devices are now mobile and autonomous and must adapt to its surroundings in a distributed way, even in the absence of coordination central unit. In literature, there are many approaches and models inspired by biological processes as a strategy to design and manage modern networks. Many of these, however, focused only in certain areas. With this paper, we want to address the risk issue of a generic communication system such as voice over IP (VoIP), inspired by bio-inspired models, and making use of survivor analysis. We want to demonstrate, through case study and evaluation of the main threats facing it, that risk is not the shape function depends on the distribution of failure events due to an attack was successful.

After a brief introduction and related work, presented in Section I and Section II, in Section III and Section IV, we discuss about the security issues on communication systems and about the bio-inspired approach. In Section V, we introduce the survivor analysis for ICT security and the model to evaluate the failure time distrubutions. In Section VI, we present the model to estimate risk and failure in a VoIP system, and the test that we have done about three common threats. Finally, we present a conclusion and future works.

II. Related Work

A general consolidated study on the degree of security of an ICT system is still lacking [1]. There is a general tendency to treat the issue of security in communications through taxonomies of vulnerabilities and threats [2][3][4].

ISBN: 978-1-61208-166-3

About risk analysis and management for information system security [9][10][11][13] and statistical methods [5][6][14], there are some papers that deal with the relationship that exists between the two disciplines. About VoIP security we surveyed many research papers, such us [2][3][4]. Most current treatments concerning taxonomies, or security mechanism concerning particular aspects of communication. Recognizing the work presented in many papers also about bio-inspired approach [15][16][19][20], about risk perception and statistical models biologically inspired [12][13][14], and about comparison among computer virus and biological virus [17][18], we believe we can advance 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 limiti the damage, to change the shape of risk, minimising the losses about information and about economic investments [21].

III. Bio-Inpired Models for ICT Security

In examining some of the most common structures or algorithms used today in telecommunications networks, we can find striking similarities with biological systems [13][14][15][16]. Evidence suggests that the nature and the designers of the networks have had to not only solve similar problems, but they are also arrived at similar solutions. Seems entirely reasonable, then, to think that the new problems in systems communication may have much in common with biological issues already known and have been resolved long ago. With the increase in size, interconnectivity and number of access points, computer networks have become increasingly vulnerable to various forms of attack. Similarly, biological organisms can be considered as interconnected complex systems with a high number of access points, subject to attacks by microorganisms [17][18]. However, during evolution, biological organisms have successfully developed the immune system that allows them to detect, identify and destroy pathogens outside. The technological challenges is leading us towards a world where myriad devices, fixed or mobile, interact with each other in many ways. Many of these devices are mobile and autonomous,and they must then adapt to its surroundings in a distributed way and without a coordination of a central entity. Recently, a number of approaches have been proposed, inspired by biological processes and mechanisms as a strategy to manage the complexity of distributed systems like Internet, sensor networks, wireless and ad hoc networks. The aim of bio-inspired approaches is to discover and adapt traditional principles of biological systems to technical solutions, which have characteristics of stability, adaptability and scalability. Many studies aim to highlight the achievements under the new Bio-Inspired Networks [19][20]. In particular, the topic that focuses identification of mechanisms and models applicable to biological technical solutions for ICT systems. This is the attempt to compare directly the technical solutions, the theoretical principles and mathematical models used by biological systems and the challenges of communication systems and information systems. We can summarize the main aspects of networking and communications systems that are addressed using an approach Bio-Inspired as follows:

- Self-organizing communication systems.
- Evolutionary and adaptive systems and protocols.
- Scalable and adaptive protocols and network architectures.
- Self-learning algorithms.
- Self-healing systems and protocols.
- Security mechanisms.
- Network algorithms and protocols.
- Congestion control mechanisms.
- Performance evaluation of bio-inspired networks.

The similarity between the defense mechanisms of living organisms and security problems of telecommunications networks has attracted great interest among researchers, who already have long studied the similarities. The thinking behind these efforts is to capture the dynamics that rule biological systems and understanding the foundations, to develop new methodologies and tools for the design and management of the information and communication systems. Communication systems such as biological systems are characterized by high complexity, high connectivity and dynamics. Both allow for extensive interaction between the components, and heterogeneity in terms of capacity. They have both vulnerability to external intrusion, intentional or not, which can cause system failures resulting in degradation of safety requirements. Thus the similarities are not limited to those between pathogenic agents that can infect a organism, and malicious code that can infect communication system. There is also similarity between the process of safety management, and global view of relationships between vulnerability, threat and asset, just like the relation between biological viruses, vulnerabilities, and people in a population. The final result is a risk of failure and impairment of confidentiality, integrity and availability in an ICT system, such as the risk of the occurrence of a disease in a biological organism. The analysis of risk requires knowledge of the probability and its distribution and the probability that an attack occurs [5][6][9][11]. We can asses the degree of the system security and analyse the existing countermeasures to try to decrease the risk and minimimise the losses, maintainng the security requirements for an ICT systems:

- Confidentiality
- Availability
- Integrity

IV. Overview of Survivor and Failure Analysis

In many biomedical applications, the variable is the time it takes a certain event to occur, that is, how much time elapses from the beginning of the study of the ”system” so that a given event occurs. For example, the event may be the death of an organism, from the time it takes for a patient to show signs of reaction to a therapy or the time to recurrence of a disease. In practical cases we may be interested in determining a statistical distribution of the times of occurrence of events for a population of individuals, or to compare the times of occurrence between distinct populations (for example the case of two populations, a subject to a therapy clinic another and not receiving any treatment), or to determine a relationship between the times of occurrence and other variables that may affect the entities in question. Both in biomedical applications as the observation of a telecommunications system, measurements of the times of occurrence of the events are carried out within a period of limited extent. A consequence of this limitation is that not all individuals will be affected by the occurrence of an event. All this characterizes what is called Survival Analysis [5][6]. We indicate with T a positive random variable representing the time of occurrence of our events. Thus, we can define the survival time as the interval between the birth of an individual after his death. For obvious reasons, the survival is linked to the notion of failure. A failure event in general, could be due to an attack by malevolent individuals or groups that want to damage the security system. A failure doesn’t meaning the total distruction of the system, but even the impairment of the informations that it holds. Ryan and Ryan in [9][10][11] 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={α_k:k $\in$ I }. Threats can destroy or only degrade information, compromising the security requirements. For each individual asset and for the entire system it is possible to define the following functions:

- Survivor Function S(t), which is the probability of being operational at time t :
$$S[t] = P_r[T \geq t] = 1 - F(t) \tag{1}$$
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:
$$f(t) = \frac{dF(t)}{dt} = -\frac{dS(t)}{dt} \tag{2}$$
- Hazard Function h(t), which is the probability that an individual fails at time t, given that the individual has survived to that time:
$$h(t) = \lim_{\delta \to 0^+} P_r(t \leq T < t + \delta \mid T \geq t)/\delta \tag{3}$$
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):
$$H(t) = -\log S(t) \tag{4}$$

V. RISK AND FAILURE IN A VOIP SYSTEM

The VoIP system, in this case we will discuss in this paper, is the ”population” under observation and individuals of that population are so-called information assets. Each asset is involved in the processes that regulate VoIP, and each is vulnerable to a range of possible threats. An attack occurs when a threat occurs, using the right vulnerability and causing a failure. The risk is simply the probability that this event occurs. The damage is the impact on the system. In this case we do not consider the influence of an asset attacked to another asset not attacked, and how the spreading of risk within the system itself. In this paper we consider the global system failure and the events affecting it.

A. VoIP and Threats Taxonomy

The new trends of the communication is the move towards the transmission of voice over traditional packet switched IP network, voice over IP. VoIP is the rst step for the future convergence.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 is 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. The main advantages of VoIP are flexibility and low cost. The first comes from an open architecture and a software implementation, while the second is due to the emergence of a new business model, the unification of devices and network links for the transport voice and data. Thanks to these benefits, VoIP has seen a rapid spread in both enterprise that among private users. A growing number of companies has already converted or are being converted to VoIP, to allow the implementation of new features, both to reduce management costs. Among the private account, the main point of attraction of VoIP is the low cost service. To offset the high flexibility of VoIP we have an equally high complexity, due to architectural and protocol factors. 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[2][3][4]. The VoIP infrastructure is characterised by several assets:

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

Threats	C	I	A
Eavesdropping	x		
DoS			x
Vishing	x	x	
Fraud		x	
Masquerading		x	x
Physical Intrusion	x	x	x
Service Abuse		x	x
Social Threats		x	x

Table I
THREATS IMPACT ON CIA REQUIREMENTS

- Business Areas.

Although it is a technology that is being rapidly deployed, there are many security challenges and the benefits of VoIP are as strong as security issues. We briefly listed the main threats associated with this technology [2]:

- Eavesdropping.
- DoS.
- Vishing.
- Fraud.
- Masquerading.
- Physical Intrusion.
- Service Abuse.
- Social Threats.

In Table I, we listed the principal threats and the assessment of the impact on confidentiality, integrity and availability, that are the most important security requirements also called CIA requirements.

B. Analysis Model

A VoIP system, such as any other information systems or network communication can be compared to a biological system. Each of its constituent elements can be seen such as a individual of a population. From the perspective of the study of threats and resistance to their attacks, a VoIP system can be studied following the models and mathematical principles of Survival Analysis, which is widespread in the study of the effectiveness of therapies clinical population suffering from certain diseases. For this reason it is possible to characterize a VoIP system through its survival function, or through its hazard function. We have simulated a VoIP system under stressful conditions. The test is stopped after a fixed amount of time, Toss. As results, some items fail during the test, while other survive. We considered three types of threats during a fixed period of 100 days. The threats considered are those that statistically, are the most frequent: Denial of Service (58%), Eavesdropping (20%) and Social Threats (18%). These threats have a relapse rate of respectively cases of failure of a VoIP system. By hypothesis each of these threats gave rise to the failure of system that were distributed along the 100-day period and each of these threats acting on the system, and causes of failure, exploiting the vulnerability. We assume an observation time 100 days, and three possible cases of distribution:

- Case 1: The failure events caused by the three threats are distributed according to a Weibull distribution, with equal parameters, scale factor A=50, shape factor B=10, as in Figure 1.
- Case 2: The failure events caused by the three threats are distributed according to Weibull distribution, but are considered different values for each,DoS (A=50, B=3) Eavesdropping (A=50, B=5), Social Threats (A=50,B=10), as in Figure 2.
- Case 3: The failure events caused by the three threats are distributed according to 3 different distributions, Weibull, Exponential and Rayleigh, as in Figure 3.

Each of these distributions are "weighted" according to a coefficient given by the statistical impact of the threat.

$$F_{tot}[t] = th_{1\%}F_1[t] + th_{2\%}F_2[t] + ...th_{n\%}F_n[t] \tag{5}$$

$$H_{tot}[t] = -log(1 - F_{tot}[t]) \tag{6}$$

The trend of the function of the total hazard is independent of the particular case. From the viewpoint of security countermeasures to be taken in a VoIP system, it is not important to know in advance the distribution of failure associated with threats. This assertion is supported by the evidence that changing characteristic parameters of the distributions involved, the total hazard function did not show significant changes in its trend. This result shows that, with random distribution of possible threats, the distribution of failures and the shape of the risk remains unchanged at less than a constant. This suggests that the shape of the risk function is not depends on the timing distributions of failures. The risk increases dramatically if you do not act in any way with security investment. In this case, we can see the change of the survival distribution with different distributions. The curve move to the right if we change the distributions. This tells us that the only influence is in the delay of the distributions of failure events so this allows an extension of time for decisions and managing security in an information system. In this case we considered the total absence of security investment [21]. We showed that the risk in the absence of explanatory variables that influence the impact of each threat, and neglecting the possible relationships between the different threats, does not change shape. A good economic investment then applied in order to improve security, must take into account these claims. This is important for future consideration of countermeasures and the choice of strategy to use when referring to safety action to be taken.

VI. CONCLUSION AND FUTURE WORK

In this paper, we introduced and proposed a different bio-inspired approach for the security of information systems. The bio-inspired in the ICT should help inspire the design of a system for managing network security measure to

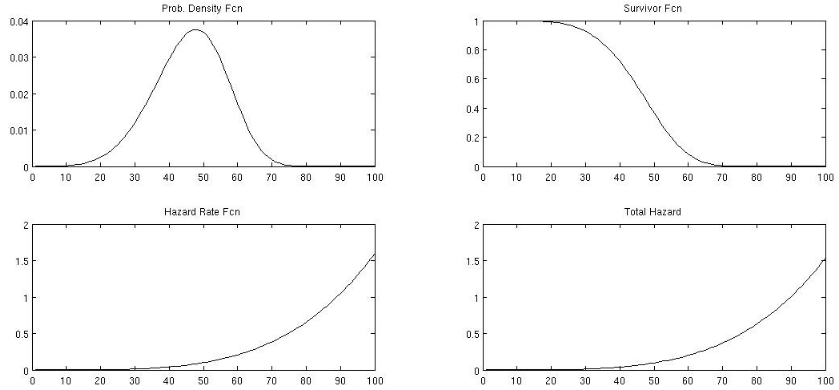

Figure 1. Weibull distribution

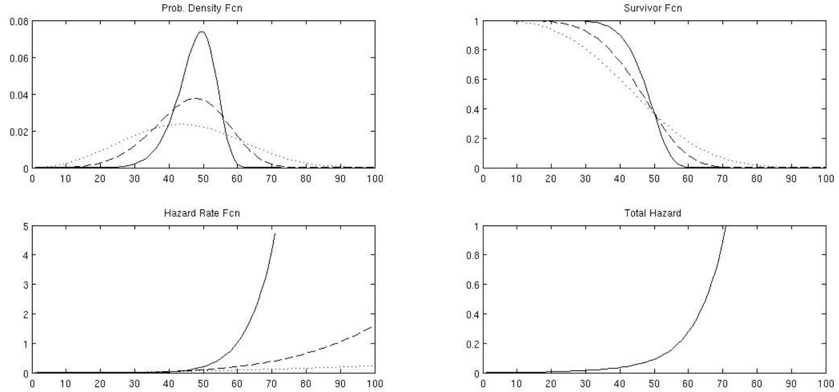

Figure 2. Weibull distribution with different parameters

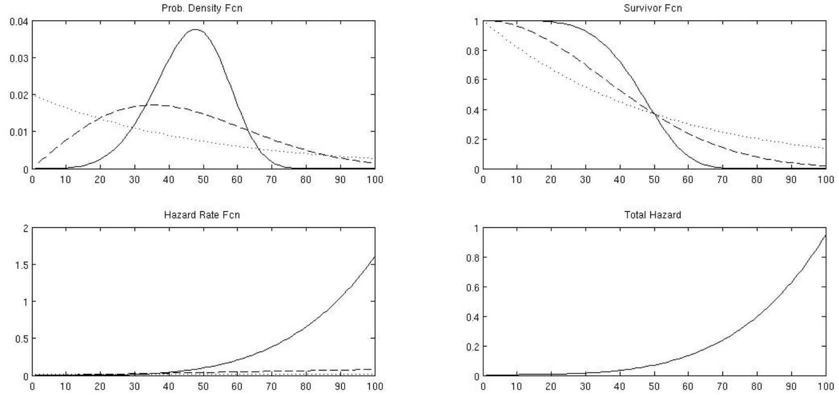

Figure 3. Weibull distribution, Exponential distribution, Rayleigh distribution

prevent the attack, and to estimate the risk, to assess the expected risk, to decide strategically technological and economic investments,maintaining good relationship between the quality of service, security and network reliability. Following the study of the behavior of a VoIP system in against a combination of these threats, each with a well defined distribution function of failure times within a 100-day period, the results allow us to say that in terms of countermeasures to be implemented for the protection of a VoIP system against threats how Denial-of-Service, Social Eavesdropping Threats, is not essential to know in advance distribution time of failure associated with them. In future the intention is to study the impact of a threat in terms of technological and economic risks, and the influence that an attacked asset, within a VoIP system, can have on asset logically associated with it. The study is a starting point for a deeper analysis of the risk in a VoIP system upon application of Bio-Inspired approach.

REFERENCES

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

[2] VoIP Security Alliance, *VoIP Security and Privacy Threat Taxonomy*, available at www.voipsa.org, [accessed: Oct., 2011].

[3] A. D. Keromytis, 2010, *Voice-over-IP Security: Research and Practice*, IEEE Computer and Reliability Societies, Secure Systems, Vol. 8, Issue 2, pp. 76-78.

[4] A. D. Keromytis, 2009, *Voice over IP: Risk, Threats and Vulnerabilities*, In Proc. of the Cyber Infrastructure Protection (CIP) Conference, New York, NY.

[5] D.Roxbee Cox and D. Oakes, 1984, *Analysis of Survival data*, CHAPMAN & HALL/CRC.

[6] D. Roxbee Cox, 1972, *Regression Models and life-tables*, Journal of the Royal Society, Series B (Methodological), Vol. 34, No. 2, pp. 187-220.

[7] International Standard ISO/IEC 27002:2005, *Information Technology Security techniques. Code of Practice for information security management*.

[8] International Standard ISO/IEC 27005:2008, *Information Technology Security techniques. Information Security Risk Management*.

[9] J. C. H. Ryan and D. J. Ryan, 2008, *Performance Metrics for Information security Risk management*, IEEE Computer Society, Security and Privacy, Vol. 6, Issue 5, pp. 38-44.

[10] J. C. H. Ryan and D. J. Ryan, 2008, *Biological System and models in information Security*, Proceedings of the 12th Colloquium for Information System Security Education, University of Texas, Dallas.

[11] J. C. H. Ryan and D. J. Ryan, 2006, *Expected benefits of information security investments*, Computer and Security, Vol. 25, Issue 8, pp. 579-588. ScienceDirect, www.sciencedirect.com.

[12] Stephan Kitchovitch and Pietro Lió, 2010, *Risk perception and disease spread on social networks*, International Conference on Computational Science, Vol. 1, Issue 1, pp. 2339-2348.

[13] J. M. Lachin, 2000, *Biostatistical Methods: The Assessment of Relative Risks*, John Wiley & Sons.

[14] J. D. Kalbfleish and R. L. Prentice, 2002, *The Statistical Analysis of Failure-Time Data*, 2nd edition, Wiley.

[15] W. H. Murray, 1988, *The application of epidemiology to computer viruses*, Computer & Security, Vol. 7, Issue 2, pp. 139-145.

[16] Falko Dressler and Ozgur B. Akan, 2010, *A Survey on Bio-Inspired Networking*, Elsevier Computer Networks, Vol. 54, Issue 6, pp. 881-900.

[17] Jun Li and Paul Knickerbocker, 2007, *Functional similarities between computer worms and biological pathogens*,Elsevier Computer & Security, Vol. 26, Issue 4, pp. 338-347.

[18] Michael Meisel, Vasileios Pappas, and Lixia Zhang, 2010, *A taxonomy biologically inspired research in computer networking*, Elsevier Computer Networks, Vol. 54, Issue 6, pp. 901-916.

[19] M. Wang and T. Suda, 2001, *The Bio-Networking Architecture: A Biologically Inspired Approach to the Design of Scalable,Adaptive, and Survivable/Available Network Applications*, in 1st IEEE Symposium on Applications and the Internet (SAINT), San Diego, CA, pp. 43-53.

[20] C. Lee, H. Wada, and J. Suzuki, 2007, *Towards a Biologically-inspired Architecture for Self-Regulatory and Evolvable Network Applications*, in: F. Dressler, I.Carreras (Eds.), Advances in Biologically Inspired Information Systems - Models, Methods, and Tools, Studies in Computational Intelligence (SCI), Springer, Berlin, Heidelberg, New York, Vol. 69, pp. 25.

[21] Aurelio La Corte, Marialisa Scatá, and Evelina Giacchi, 2011, *A Bio-Inspired Approach for Risk Analysis of ICT Systems*, Computational Science and Its Applications - ICCSA, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 652-666.