available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

# Challenges for the security analysis of Next Generation Networks☆

*Serap Atay* [a], *Marcelo Masera* [b,*]

[a] *Izmir Institute of Technology, Department of Computer Engineering, Izmir, Turkey*
[b] *Joint Research Centre, Institute for the Protection and Security of the Citizen, Ispra (VA), Italy*

*Keywords:*
Network security
Next generation networks
Internet
Security
Vulnerability
Threat
Risk analysis
Autonomic computing
Self-adaptive systems

ABSTRACT

The increasing complexity of information and telecommunications systems and networks is reaching a level beyond human ability, mainly from the security assessment viewpoint. Methodologies currently proposed for managing and assuring security requirements fall short of industrial and societal expectations. The statistics about vulnerabilities and attacks show that the security, reliability and availability objectives are not reached and that the general threat situation is getting worse. With the deployment of Next Generation Networks – NGNs, the complexity of networks, considering their architecture, speed and amount of connections, will increase exponentially. There are several proposals for the network and security architectures of NGNs, but current vulnerability, threat and risk analysis methods do not appear adequate to evaluate them. Appropriate analysis methods should have some additional new characteristics, mainly regarding their adaptation to the continuous evolution of the NGNs. In addition, the application of security countermeasures will require technological improvements, which will demand further security analyses. This paper evaluates the current vulnerability, threat and risk analysis methods from the point of view of the new security requirements of NGNs. Then, the paper proposes to use autonomic and self-adaptive systems/applications for assuring the security of NGNs.



## 1. Introduction

Communications technologies are evolving fast, following the demand for more and newer services anywhere and at any time. The drivers for this trend come from the economy, military defense, health and education fields, and match the request for more efficiency, and more comfortable and safe daily life. As a rule, new technologies are put into use as soon as they are available.

The many technological developments accomplished in the last decades have a direct impact on communication networks. Nevertheless, all hardware and software technological improvements or implementations can be the source of new vulnerabilities for the systems and services that rely upon them. The statistical reports about the changing intensity and type variety of security vulnerabilities and attacks show that integrity, reliability and availability problems are far from being solved – see Figs. 1 and 2 (IBM Internet Security Systems X-Force®, 2009).

As shown in Fig. 1, the number of reported vulnerabilities in "Cisco 2008 Annual Report" increased, compared to 2007, by 11.5 percent (Cisco, 2009).

According to "IBM Internet Security Systems X-Force 2009 Mid-Year Trend", as shown in Fig. 2, the disclosure rate of

☆ An earlier version of this paper was presented at the Broadnets 2009 Conference in Madrid, Spain, 14–17 Sept. 2009, and published by LNICST, doi:10.4108/ICST.BROADNETS2009. Revised date is Sept. 2010.

* *Corresponding author.*
E-mail address: Marcelo.Masera@ec.europa.eu (M. Masera).

1363-4127/$ – see front matter 
doi:10.1016/j.istr.2010.10.010

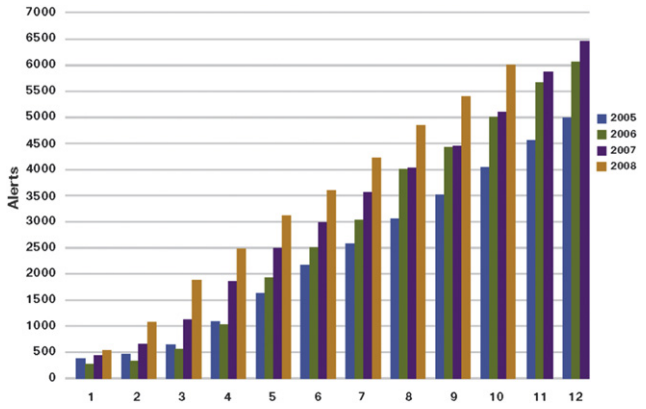


**Fig. 1 – Cumulative Annual Alert Totals by month.**

vulnerabilities has decreased in 2009 due to the solution of vulnerabilities such as SQL injections and ActiveX controls.

According to the Cisco "2009 Annual Report", the exploit and attack threat levels increased by 57 percent when comparing the 2008 and 2009 values. In 2009 the new attacks generally affect social media users, exploiting their willingness to respond to messages that supposedly originate from people they know and trust. This kind of attacks is relatively easy to launch, and can be deployed to steal personal information.

Nowadays, the telecommunication infrastructure is in a conversion phase towards Next Generation Networks – NGNs. According to ITU's Telecommunication Standardization Sector – ITU-T report "Trends in Telecommunication Reform: the Road to NGN" published in September 2007, it is predicted that full implementation of NGN in fixed line networks in developed countries will be deployed by 2012 and in mobile networks by 2020 (Next-Generation Networks and Energy Efficiency, 2008). With this new network infrastructure, information can be reachable whenever and wherever, by who needs it. Hence, in the corporate world, the border between traditional company and office environments will diminish. Naturally these developments will inevitably come with many still unknown vulnerabilities, threats, and security risk.

In line with the aforementioned reports, the Centre for the Protection of National Infrastructure – CPNI, in the report on the identification of the high consequence risks faced by the UK (National Risk Register of UK Government, 2008), highlights that the expanding interconnectivity among networks influences the probabilities and impact of attacks within an NGN scenario. See Fig. 3 as an illustration of this trend towards scenarios characterized by high-impact, high-likelihood risk.

Of particular relevance are the so-called Critical Infrastructure. Companies and operators in the banking and finance sectors, energy and natural resources, telecommunications and internet service providers, transportation and mass transport, chemical production and storage, food distribution and government services are considered critical infrastructure –as their disturbance or disruption can severely impair society at large.

The report "In the Crossfire; Critical Infrastructure in the Age of Cyber War" published by the anti-virus company McAfee and coordinated by the Centre for Strategic and International Studies in Washington, DC in January, 2010, discusses this latter problem The report is based on data from a survey of 600 IT and security executives in enterprises that own and/or operate critical infrastructure in 14 countries across the world. The survey data gathered for the report paints for the first time a detailed picture of the way those in charge of the protection of critical IT networks are responding to cyber-attacks, attempting to secure their systems and working with governments. According to this report; 80 percent of executives working for entities that use SCADA (supervisory control and data acquisition) or industrial Control Systems say their systems are connected to the internet or some other IP network, putting them at possible risk of intrusion (http://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf).

This situation forces research institutes and standardization bodies to adapt their research areas, rules and policies to meet the security needs of the new technological improvements. A key issue is the lack of an adequate approach to guarantee that all security requirements will be satisfied. ITU-T presented a security model (ITU-T X-805, 2002) applicable to NGN, composed of three security layers, three security planes, and eight security dimensions. Although providing a comprehensive view of network security, puts stringent demands that could be difficult to satisfy in realistic settings, mainly due to the continuous changes in technologies and system architectures. Although security has been recognized as a key enabler and differentiator for NGN, its eventual assurance is still an open question.

The aim of this paper is to discuss the possible integration of the proposed ITU-T security model with new additional

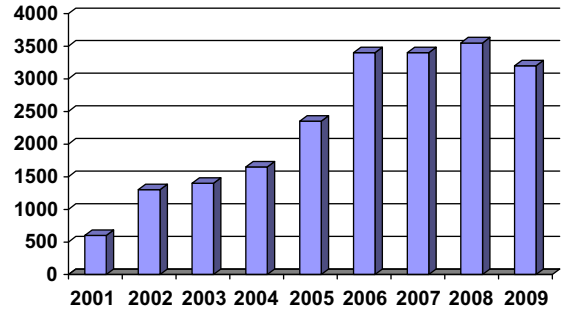


**Fig. 2 – Vulnerability Disclosures in the 1st half of each Year 2000-2009.**

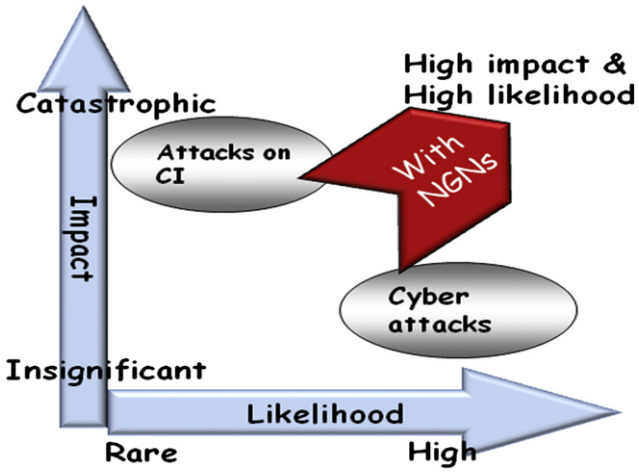


**Fig. 3 – An illustration of the high consequence risks with NGNs.**