Challenges for the security analysis of Next Generation Networks

SerapAtay[*], Ph.D. Marcelo Masera
Joint Research Centre, Institute for the Protection and Security of the Citizen
Ispra (VA), Italy

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. The security 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 proposes to use autonomic and self-adaptive systems/applications for assuring the security of NGNs.**

Keywords- network security; next generation networks; internet; security; autonomic computing; self-adaptive systems

I. Introduction

All hardware and software technological improvements or implementations can be the source of new vulnerabilities for the systems and services that rely upon them. For instance according to the "Cisco 2008 Annual Security Report" about the intensity and variety of security vulnerabilities and attacks show that security, reliability and availability problems have not been solved yet. As presented in this report; the number of reported attacks in 2008 increased, compared to 2007, by 11.5 percent[1].

Nowadays, the telecommunication infrastructure is in a conversion phase towards Next Generation Networks – NGNs. Naturally, these developments will inevitably come with many still unknown vulnerabilities, threats, and security risks. The interconnectivity among networks is expanding, and the probabilities and impactof attacks within a NGN scenario, will reach higher values.

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.

Therefore, the aim of this paper is to discuss the possible integration of the proposed ITU-T security model with new additional features for being able to dynamically detect vulnerabilities, threats, and to react accordingly.

The paper is organized in the following sections; the section 2 includes information about the NGN general functional architecture and security architecture model proposed by the International Telecommunication Union - ITU-T. Section 3 describes the deficiencies of current security solutions. Section 4 defines the basic requirements and capabilities for proposed new security solution approach for NGNs. Section 5 presents the conclusions and future work.

II. NGN and Its SecurityArchitecture Model [3]

The aim of NGN is to collect existing networks into unitary packet-based network architecture. The service-related functions in NGNs are independent of the transport technologies. The ITU-T Y.2011 defines the General Functional Model for NGNs.

The NGN Security architecture was designed by ITU-T Recommendations X.805 uses 'Security Architecture for Systems Providing End-to-End Communications'. It was developed as the framework for the NGN architecture for achieving end-to-end security in distributed applications and provides a comprehensive, multi-layered, end-to-end network security framework across eight security dimensions in order tocombat network security threats. It also forms the foundation for the proposed ISO/IEC 18028 standard 'Information technology – Security techniques – NetworkSecurity –Part2: Network security architecture'. It includes three parts as Security dimensions, layers and planes. The **Security Dimensions** are access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy.The **Security Layers** are a hierarchy of equipment and facilities groupings organized asinfrastructure, service and application security layers. The **Security Planes**comprises the types of security-related activities that are typically deployed on a network. Each security plane has to be interconnected with each security layer, so resulting in nine security perspectives. Each security perspective corresponds to unique vulnerabilities and threats.

III. The Deficiencies of Current Security Solutions

The information technology security requirements and objectives for NGNs are defined by ISO/IEC 15408 Part 2 [7]. The main objective is controlling the security risks to an acceptable level for all stakeholders of NGNs.

[*] This work was supported in part by the TUBITAK (Turkish Science and Technological Research Program) under Grant of Bideb2219 Post-Doctorate Research Fellowship.

[1] Cisco 2008 Annual Security Report *www*.cisco.com/web/go/securityreport

Digital Object Identifier: 10.4108/ICST.BROADNETS2009.7470
http://dx.doi.org/10.4108/ICST.BROADNETS2009.7470

As presented in previous sections, security risks are growing and cannot be ignored. Attacks are becoming more sophisticated, unpredictable, frequent and from a wider range of sources. Thestandardizationhasa very importantrole in the achievement of security objectives. However, technologies are developing very fast and the research and standardization organizations do not have enough time to analyze all possible vulnerabilities and threats before the technologies are deployed. See an illustration of this situation in Figure 1. For instance; the web site of ITU-T for 'ICT Security Standards Roadmap, future needs and proposed newsecurity standards' in web site of ITU-T Part 4[2] defines the current process for NGN, while NGNs have already been deployed in many developed countries such as Japan, South Korea, USA, China, UK etc.

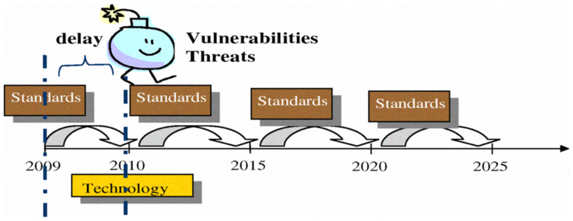

Figure 1. The continuous security gap between technology and standards

There are several reasons for the insufficiency of the current methods for analyzing vulnerabilities, threat and risks as a reference studies to reach security objectives and standardization of NGNs. The reasons are listed in this section:

Each new NGN service can include different compositions of many new technological equipment and software solutions, and these compositions have different complex threats and risks. The composition of services does not necessarily imply that the upper services inherit the security attributes of its components. Each new composition adds and amplifies vulnerabilities and threats, and therefore each new service would require a specific security analysis. For instance, the traditional communication network 'PSTN', its protocols and the Internet infrastructure are used together for VoIP.

Vulnerabilities derive from errors or oversights in the design of the protocols. This makes them inherently vulnerable. As a matter of fact, protocols are deployed without a complete and unquestionable proof of their security properties. During their lifetime, protocols change, incorporating patching and evolving with the addition of new features. Each new version is vulnerable in some ways not totally known when being deployed, and differing from its previous versions.

The current vulnerability, threat and risk analysis methodologies such as e-TVRA for NGNs [8] typically focus on known threats and vulnerabilities – because this is the available information. All threats, vulnerability and risk analysis methods continuously need to update their knowledge of new weaknesses of the assets being studied, to identify how these weaknesses can be exploited, for then evaluating the security risk, and defining and implementing the needed countermeasures. As the information basis for those analyses is incomplete, new evaluations will be needed in time. The set of security data is never complete, and assessments should be redone with each array series of new data. In addition, it is known that information on attacks is not promptly disclosed due to their sensitivity. When disclosed, it should be taken into consideration for remaking the security assessment of the systems for which it is relevant. Therefore the improvement of NGN security systems via vulnerability, threat and risk analysis tool is a time consuming and incomplete process.

Today, total threat and risk assessments are rarely possible due to the complexity of systems and networks: threat scenarios can affect many components, generate intricate and multifaceted failure mechanisms, and propagate within the systems in complicated ways (e.g. in long times, with small progressions, etc.). So, current risk models should take this into consideration for NGNs.

Another required feature is security measurement [4]. No security measurement definition and tool has proven its logical and mathematically validity. Therefore the security of NGN systems cannot be determined in quantitative ways. This is fundamental for evaluating whether new security scenarios or solutions have positive or negative effects upon the NGN network and its services.

An important attribute of any security evaluation is uncertainty. It depends on time and the reference point. As security is a function of time, evaluations should provide a proper answer about its evolution, and its dependency upon the changes in different factors. In addition, as NGN system put together many actors, security might have different quantitative values for each one of them. The measurement of security should be a continuous activity, dynamically evolving according to the changes in the NGN architecture and service, and to the points of view various stakeholders.

IV. THE PROPOSED SECURITY SOLUTION APPROACH

The main goal of the approach we are presenting for NGN security is to help in reducing the window of opportunity for the security problems that will inevitably continue to appear.The requirements of new security approach can be defined as follows:

- The vulnerabilities and attack types can have many unpredictable combinations. The established security level also cannot be measured and guaranteed by the current available solutions. Therefore new security approaches should match the nature of the security problems, capable of adapting the strategy to new threats/attacks and of generating solutions dynamically.
- A successful security approach should be deployable and feasible for all network components, either hardware or software.
- The security approach should be effective against new kinds of attack.
- The responses of the security approach should be monitored and controlled. The collected information about vulnerabilities and new attacks should be processed to improve the security level of the system. This critical information collection and exchange

[2] http://www.itu.int/ITU-T/studygroups/com17/ict/part04.html

Digital Object Identifier: 10.4108/ICST.BROADNETS2009.7470
http://dx.doi.org/10.4108/ICST.BROADNETS2009.7470

should be organized and managed using secure information sharing models.

This approach will require the application of concepts such as self-adaptation and autonomic systems/applications.Autonomic computing should provide NGN architectures with the capability of self-managing their security status, overcoming unpredictable security incidents, while hiding the complexity of the overall NGN architecture to each element facing the security problem.A step forward should be the introduction of self-adaptation mechanisms, which could support the change of the behavior or of the structureof NGN software components for adapting them temporarily or permanently to some new security condition. In addition, this approach will require the permanent collection of data about vulnerabilities, threats and attacks, which then can foster the analysis of the security conditions of the NGN systems, and prepare their reaction to the related security scenarios.

In this section, we define the concepts of autonomic systems/applications and self-adaptive systems. Then, we explain how these approaches can be used for improving the security architecture of NGNs, and their vulnerability, threat and risk assessments.

A. *Autonomic Computing for NGNs*

NGNs are composed of many systems and networks, globally aggregating large numbers of independent computing and communication resources, data stores and sensor networks. For security purposes, the self-immunity of systems is a key requirement. It has to be supported by local sensor mechanisms, for instance for detecting threats or identifying faults in vulnerable components. Detecting security problems in local entities is similar to the behavior of biological systems when they have to deal with similar challenges of scale, complexity, heterogeneity, and uncertainty – a vision that has been referred to as autonomic computing [5].

NGN networks can use autonomic application/system to handle complexity and uncertainties with minimum human intervention. Autonomic applications and systems have eight characteristics as self-awareness, self-configuring, self-optimizing, self-healing, self-protecting, context awareness, open and anticipatory [2]. The usability of autonomic application/system for NGN is important and currently several research efforts has focused on enabling the autonomic properties to address four main areas: self-healing, self-protection, self-configuration, and self-optimization [6].

The main risk for the proposed autonomic network components of NGNs is that each element has to be designed with the overall architecture in mind, and generally can only be add-on afterwards with difficulty. Delayed introduction of autonomic attributes could hamper the overall functionality of the NGN architecture.

B. *Self-Adaptive systems for NGN services and applications*

Self-adaptive features for security purposes can be added to software NGN components, corresponding to the different security layers and planes foreseen for the NGN architecture, and considering the different security dimensions.

Self-adaptation can occur at the NGN service or transport stratum, and can affect management or control functions, resource or function elements. Self-adaptation can change the behavior of a component, or the structure of a system, affecting their input/output, operations (e.g. filtering), resource access, resource monitoring, management of other components, etc.

For this end, the autonomic characteristics described in the previous section are an essential element, acting as a sensor system of NGN networks. The self-adaptive applications should monitor and organize the global reaction like the immune system of a living organism. In a self-adaptive system and/or network, services are able to recognize the security problems, sharing information with other autonomic NGN components, for then selecting the more appropriate reaction behavior and implementing the necessary changes.

Therefore our proposal is to develop a complete NGN solution including self-adaptive systems and applications, supported and integrated with autonomic NGN components. In other words, smart autonomic network entities are the key element to create a self-adaptive secure NGN networks. Thereby, the proposed security solution approach will show the desired characteristic of dynamically evolving and reacting according to the best security solutions they can be implement.

C. *Both local and end-to-end security solutions are required*

All NGN stakeholders look for end-to-end security solutions. However (due to the problems previously discussed in section 3) security can only be ensured when the solution to vulnerability, threat and attacks can be initiated locally for then being coordinated globally. In other words, NGN end-to-end security objectives depend upon both the satisfaction of security requirements for local network components, and the coordination among relevant components in the overall architecture.

Faster detection of security issues also means better reaction times. For being effective, security solutions must be absorbed by all the stakeholders dealing with the NGN networks and service. Thereby, security should be guaranteed by and for all the fundamental network operational processes and network infrastructural elements of NGNs. The end customers should perceive all these solutions as end-to-end automatic protection.

The local threat/vulnerability-detection sensor mechanisms are the triggering element for the local immune reaction systems. All layers of the network architecture should be proactive and detect local security problems dynamically. Abnormal situation at the network fundamental service processes are the most urgent, as they might affect all other services and applications. Problems, threats or attacks can be isolated, reported and alternative solutions can be selected and applied by the local entities – while communicating and interacting with other entities for reaching an acceptable global solution. To success that there is an important advantage with current hardware and software technologies, embedded and intelligent equipment can implement those autonomic characteristics and self-adaptability without affecting the performance of the networks.

Digital Object Identifier: 10.4108/ICST.BROADNETS2009.7470
http://dx.doi.org/10.4108/ICST.BROADNETS2009.7470

D. How the proposed approach can be integrated into the NGN architecture and ITU-T X.805 security architecture

The integration of the proposed approach and the ITU-T X.805 security architecture is important in light of the standardization studies and security evaluation of NGNs. Our approach foresees five main steps for secure NGNs:

1. Designing and implementing NGN autonomic components, which will provide capabilities of monitoring, self-management, self-healing, and self-protection, among others;
2. Designing and implementing NGN self-adaptive software solutions, which will provide the capabilities of evolving the security mechanisms by dynamically changing their behaviors and structure, according to the self-awareness developed by the NGN autonomic systems;
3. Creating a 'security information sharing domain' between autonomic and self-adaptive components. This domain requires the definition of the information sharing rules and protocols. It should be organized according to a strict 'need-to-know' rule, segregating and fragmenting the problem space.
4. Adjusting the typical NGNs network and security architecture for making it suitable to using the autonomic and self-adaptive solutions.
5. Connecting the ITU-T X.805 Security Architecture and the ETSI threat, vulnerability and risk analysis method e-TVRA [8] with the proposed solution based on autonomic and self-adaptive capabilities. This interaction will enrich both, the security analysis and the improvement of the resulting security.The continuous information sharing about vulnerability, threat and attacks can establish horizontal and vertical links among all related hardware and software components in the NGN architecture.This working style can improve the speed and completeness of the standardization studies with e-TVRA tool.

ITU-T X.805 is a useful framework for understanding NGN infrastructures and services security issues [1], as it provides a comprehensive, top-down, end-to-end perspective of NGN security. The two proposed solutions, autonomic and self-adaptive capabilities should be applied to each of the NGN security modules described by ITU-T X.805, as defined in section 2. While analyzing each of those 9 security modules, it is important to identify their software and hardware entities and the respective roles with regard to the infrastructure, services and application layers. Then, those entities have to be re-designed or integrated with new components for satisfying the required self-adaptive and/or autonomic characteristics that will support the security objectives. This solution can facilitate the sharing of vulnerability, threat and attack information across horizontal and vertical layers/planes among all the related entities. This information sharing can be established by defined 'security information sharing domain'.

V. CONCLUSIONS

This paper presents the requirements for a new and more effective security solution approach of NGNs. Due to the characteristics of the current and future security problems of NGNs, we argue that the current standardization efforts may fall short of providing a comprehensive solution. The objectives of proposed solution approach are:

- Localized the security problems, for detection and effectively mitigation,
- Information sharing should be done according to need-to-know, segregation and fragmentation rules with related network security components.
- Vulnerability, threat and risk analysis tools should carry out more effectively their assessments of NGNs by using real time vulnerability, threat and attack information sharing.
- Create and use autonomic and self-adaptive components to assure the security, reliability and availability of the systems and networks.

The main tools of the proposed solution are autonomic and self-adaptive applications/systems. They should enable the choice of the more appropriate security solution for each circumstance, resulting in the improvement of the security, availability and reliability of the application and network services. Many research projects for autonomic and self-adaptive applications/systems are active today [9].

The authors plan to work on reviewing and describing the security requirements for each stratum and security dimension of the NGN architecture, in light of possible applications for autonomic and self-adaptive components.

REFERENCES

[1] Y.Cho, Y. Won, B. Cho, 'ITU-T X.805 based Vulnerability Analysis Method for Security Framework of End-to-End Network Services', Proceeding of the 4th WSEAS Int. Conf. on Information Security, Communication and Computers, (pp288-292) Tenerife, Spain, December 16-18, 2005.

[2] P. Horn, Autonomic Computing: IBM's perspective on the State of Information Technology. http://www.research.ibm.com/autonomic/, Oct 2001. IBM Corp.

[3] ITU-T X-805, Draft-Security architecture for systems providing end-to-end communications, 2002.

[4] A. Jaquith, Security Metrics Replacing Fear, Uncertainty and Doubt, Addison Wesley, 2007.

[5] S. Hariri and M. Parashar. Handbook of Bioinspired Algorithms and Applications, chapter The Foundations of Autonomic Computing. CRC Press LLC, 2005.

[6] M. Parashar, S. Hariri, Autonomic Computing: An Overview, J.-P. Banatre et al. (Eds.): UPP 2004, LNCS 3566, pp. 247–259, 2005. Springer-Verlag Berlin Heidelberg 2005.

[7] ISO/IEC 15408-2: "Information technology-Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[8] J. E. Y. Rossebø, Scott Cadzow, Paul Sijben, eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope, Second International Conference on Availability, Reliability and Security (ARES'07).

[9] http://ist-autoi.eu/autoi/

Digital Object Identifier: 10.4108/ICST.BROADNETS2009.7470
http://dx.doi.org/10.4108/ICST.BROADNETS2009.7470