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

A B S T R A C T

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 Crown Copyright © 2010 Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2010.10.010

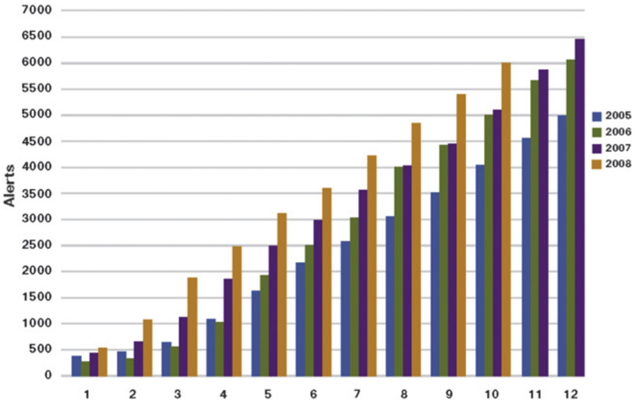

Fig. 1 – Cumulative Annual Alert Totals by month.

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.

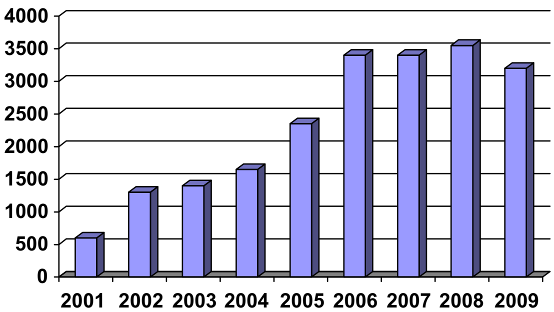

Fig. 2 – Vulnerability Disclosures in the 1st half of each Year 2000-2009.

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

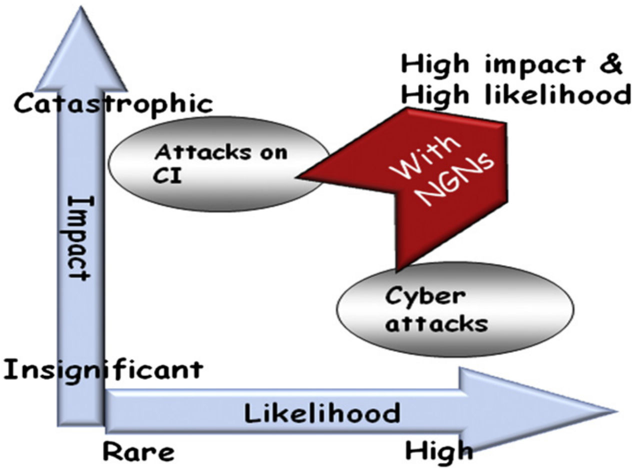

Fig. 3 – An illustration of the high consequence risks with NGNs.

features, which will enable it to dynamically detect vulnerabilities, threats, and to react accordingly.

This paper looks at the security framework for NGNs from a methodological viewpoint. It should be considered that interdisciplinary researches for new technologies are currently being developed looking for new alternative security solutions for NGNs and future networks. Key questions are what has to be protected, and how it has to be protected. The first question concerns both the users and operators of NGN; while the second is influenced by the available technologies and security techniques. These cannot have a final answer, and therefore we defend that any workable and effective solution will have to continuously adapt itself to the implementation and use of NGN systems.

The paper is organized in the following sections; Sections 2 and 3 include information about the NGN general functional architecture (ITU-T Recommendation Y, 2001) and the security architecture model (ITU-T X-805, 2002) proposed by the International Telecommunication Union – ITU-T. Section 4 describes the deficiencies of current security solutions and Vulnerability, Threat, Risk Analysis Methods. Section 5 defines the basic requirements and capabilities for new security solution approaches for NGNs. Section 6 presents the conclusions and future work.

2. NGN architecture model

The aim of NGN is to collect existing 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-2011, 2004). NGN is defined technically by the ITU-T as a “packet-based network able to provide services including telecommunication services and able to make use of multiple broadband, quality of service – QoS enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies”(ITU-T Recommendation Y, 2001).

ITU-T has proposed a standardization studies roadmap for NGN security. The details of security standardization topics for the current Study Period (2009–2012) were proposed at the September 2008 meeting of ITU-T (http://www.itu.int/ITU-T/studygroups/com17/ict/part04.html). Due to the high speed of technological changes, lots of critical security analysis are under development or have just been planned. Obviously no solution can be thoroughly accepted before a complete understanding of the problem space.

The current key concepts for NGN architecture are:(ITU-T Y-2012, 2006)

- Separation between service and transport,
- Personal and terminal mobility,
- Resource and admission control,
- Quality of Service selection & control,
- Security,
- Accommodation of legacy terminals and systems.

The service convergence in NGN will provide the ability to deliver voice, video, audio and visual data via session and interactive based services in unicast, multicast and broadcast modes. This convergence uses both wireline and wireless technologies, which can be applied interchangeably for the delivery of services. The vision is that NGN could be used any time and anywhere across various environments using compatible terminal equipments. For accomplishing this aim, the architecture of NGN is separated into two strata: transportation and services. Each stratum includes management and control functions, and resources. Fig. 4 presents the General Functional Model for NGNs.

3. NGN security architecture model (ITU-T X-805, 2002)

The NGN Security architecture was designed by ITU-T in order to propose solutions for the following questions:(NanoTechnology & Homeland Security, 2003)

1. What kinds of protection are needed and against what threats?
2. What are the distinct types of network equipment and facility groupings that need to be protected?
3. What are the distinct types of network activities that need to be protected?

ITU-T Recommendations X.805 presents the ‘Security Architecture for Systems Providing End-to-End Communications’. They were proposed as the framework for the NGN architecture for achieving end-to-end security in distributed applications. They provide a comprehensive, multi-layered, end-to-end network security framework across eight security dimensions in order to combat network security threats. It also forms the foundation for the proposed ISO/IEC 18028 standard ‘Information technology – Security techniques – Network Security –Part2: Network security architecture’.

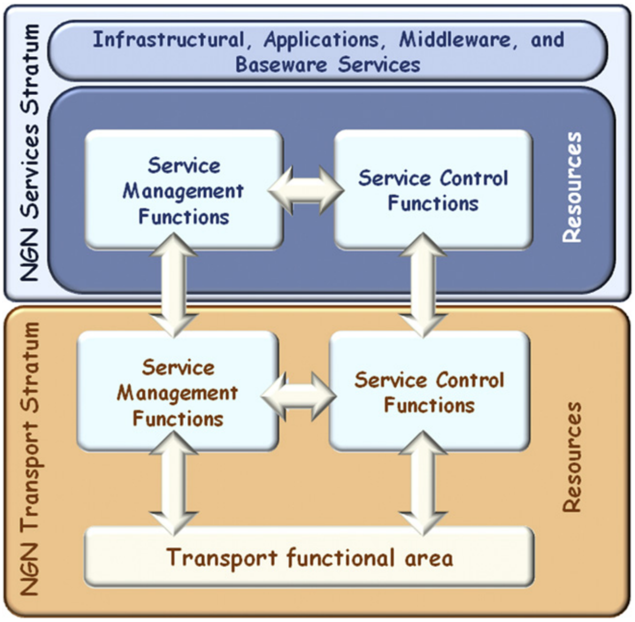
NGN Services Stratum
Infrastructural, Applications, Middleware, and Baseware Services
Service Management Functions
Service Control Functions
Resources
NGN Transport Stratum
Service Management Functions
Service Control Functions
Resources
Transport functional area

Fig. 4 – General Functional Model for NGN (ITU-T Y.2011).

The proposed *Security Dimensions* for NGN are access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy.

The NGN *Security Layers* are a hierarchy of equipment and facilities organized as three layers: infrastructure security layer, service security layer, and application security layer, as shown in Fig. 5. Each layer relates to unique vulnerabilities, threats and mitigation measures.

The NGN *Security Planes* comprises the types of security-related activities that are typically deployed on a network. They are; management security plane, control security plane, end-user security plane. 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.

4. The deficiencies of current security Solutions and vulnerability, threat, risk analysis methods

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

As shown in Figs. 1,2 and 3 in the previous sections, security risks are growing and cannot be ignored. Attacks are becoming more sophisticated, unpredictable, frequent and from a wider range of sources. On the other hand, the existing standards, solutions or methodologies do not appear to sufficiently support the required security assessments.

Standardization has a very important role 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 technologies are deployed. See an illustration of this situation in Fig. 6. For instance; the web site of ITU-T for 'ICT Security Standards Roadmap, future needs and proposed new security standards' in web site of ITU-T Part 4 (http://www.itu.int/ITU-T/studygroups/com17/ict/part04.html) 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.

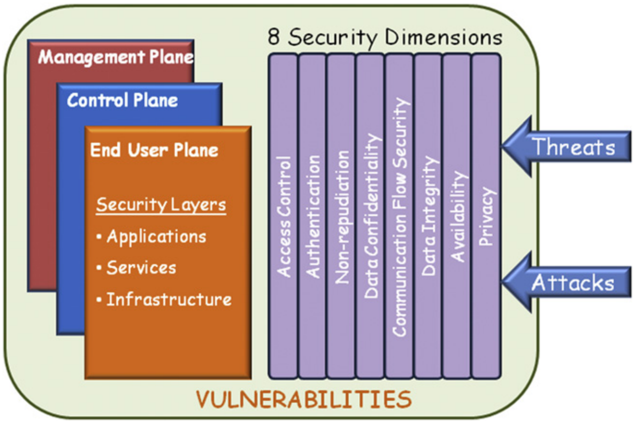

Fig. 5 – ITU-T X.805 security architecture; 'three security layers' X 'three security planes' X '8 security dimensions'.

DELAYING STANDARDS ..
Vulnerabilities, Threats
2010
Standards
2011
Technology
2015

Fig. 6 – 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 reference studies to reach security objectives and standardization of NGNs. We can list these reasons as follows:

- Each new NGN service can include different compositions of many new technological equipment and software solutions, and these compositions entail 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, e.g. the protocols. This makes them inherently vulnerable, for example SIP, 802.11b (Thermos, 2006). SIP (Session Initiation Protocol) as an IP based signaling protocol, which is used by global Voice over Internet providers and plays major role NGN-based telecommunication networks (Weber & Trick,). 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 (Rossebø et al.'Cadzow, 2004) 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 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 always incomplete process.
- Pfleeger in 2000 (Pfleeger, 2000) defined risk as any unwanted event that might have negative consequences. Different methodologies for risk and threat assessment such as Carroll 1996, Nosworthy 2000, Summers 1977, Pfleeger 2000, R.C. Reid 2001 and Bayne 2002, define risk with regard to the threats and threat agents known to the users. Today, total threat 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, NGN risk models cannot ignore this situation.
- Another required feature is security measurement (Jaquith, 2007). No security measurement definition and tool has proven its logical and mathematically validity. Therefore the security of NGN systems cannot be determined in absolute terms, although there is the need to measure in some way the fulfillment of the security requirements. From this the need for appropriate security measurements and metrics. 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 – which depends on time and the chosen reference values. 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 systems 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.

5. The proposed security solution approach

Current standards do not appear to establish all desired security solutions and risk control capabilities for NGN as partially admitted in ITU-T's 'ICT Security Standards Roadmap, future needs and proposed new security standards' (http://www.itu.int/ITU-T/studygroups/com17/ict/part04.html). In addition, available vulnerability, threat and risk analysis methods do not appear to be able to efficiently evaluate the security of NGN networks and services due to the reasons presented in section 4.

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 the new security approach are as follows:

- Current security problems have stochastic characteristics. The vulnerabilities and attack types can have many unpredictable combinations. The established security level cannot be measured and guaranteed by 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 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 structure of 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.

5.1. *Autonomic computing for NGNs*

NGNs are conceived to be 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 an ideal key requirement: i.e. systems that can recognize potential threats and react in an self-governing way towards an acceptable secure state. This approach can be a security solution for NGN that implements an autonomous entity (Internal Functional Architecture of Autonomic Element, 2001), as depicted Fig. 7 (derived from work by IBM). An autonomic application/system is a collection of autonomic elements, which implement intelligent control loops to monitor, analyze, plan and execute actions, using knowledge of the environment by hardware and software entities.

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

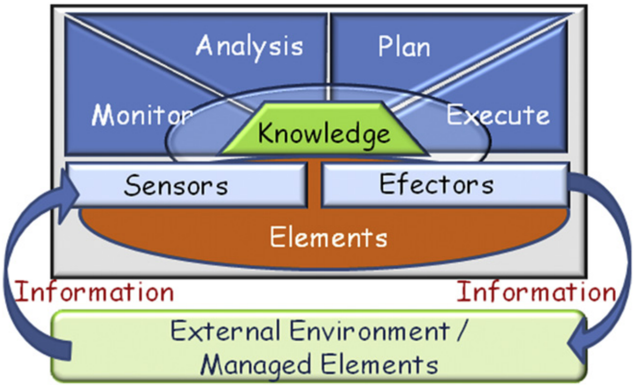

Fig. 7 – The Autonomous Element.

hardware/software 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 (Hariri and Parashar, 2005).

NGN networks can use autonomic applications/systems to handle complexity and uncertainties with minimum human intervention. Autonomic applications and systems have eight characteristics (Horn, Oct 2001):

1. *Self Awareness*: It "knows itself" and is aware of its state and its behaviors.
2. *Self Configuring*: It should be able configure and reconfigure itself under varying and unpredictable conditions.
3. *Self Optimizing*: It should be able to detect suboptimal behaviors and optimize itself to improve its execution.
4. *Self-Healing*: It should be able to detect and recover from potential problems and continue to function smoothly.
5. *Self Protecting*: It should be capable of detecting and protecting its resources from both internal and external attacks and maintaining overall system security and integrity.
6. *Context Awareness*: It should be aware of its execution environment and be able to react to changes in it.
7. *Open*: It must function in a heterogeneous world and should be portable across multiple hardware and software architectures. Consequently it must be built on standard and open protocols and interfaces.
8. *Anticipatory*: It should be able to anticipate to the most possible extent, its needs and behaviors and those of its context, and be able to manage itself proactively.

The usability of autonomic applications/systems by NGN would be an important leap forward, and currently several research efforts are focused on enabling autonomic properties to address four main areas: self-healing, self-protection, self-configuration, and self-optimization. At the hardware level, systems may be dynamically upgradable, while at the operating system level, active code may be replaced dynamically. Efforts have also focused on autonomic middleware, programming systems and runtime. At the application level, self-optimizing databases and web servers dynamically reconfigure to adapt service performance. These efforts have demonstrated both the feasibility and promise of autonomic application/system (Parashar and Hariri, 2005).

The main issue 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.

5.2. *Self-adaptive systems for NGN services and applications*

Self-adaptive features for security purposes can be added to software NGN components, in the different security layers and planes foreseen for the NGN architecture, and considering the different security dimensions as depicted in Fig. 8. How this solution can implement the ITU-T X.805 security architecture and improve the e-TVRA (threat, vulnerability and risk analysis) method for NGNs, will be discussed in section D.

In general terms, the architecture of autonomic systems consists of autonomic elements, each performing a fixed function and interacting with other elements, possibly in very dynamic environments. An autonomic element is commonly viewed as being comprised of one or more managed elements (also referred to as functional units), each performing its operational function, with one autonomic manager (management unit) that controls the managed elements' configuration, inputs, and outputs. The hardware or software autonomous entities are able to recognize the security problems (self-healing, -protection), sharing information with other autonomic NGN components (context awareness), for then selecting the more appropriate reaction behavior and implementing the necessary changes (self-optimizing and configuring) for the whole system.

This architecture with self-describing, self-organizing, self-managing, self-configuring, and self-optimizing features can provide a seamless communications infrastructure composed of multiple technologies and able to leverage local information and decisions without sacrificing global performance, robustness, and trustworthiness.

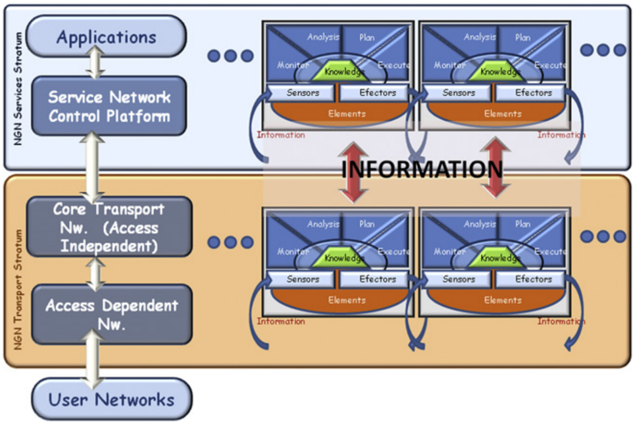

Fig. 8 – Proposed Security Solution for NGNs with Autonomous systems/applications.

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 the sensor system of NGN networks. The self-adaptive applications should monitor and organize the global reaction, such as 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.

Requirements for self-adaptive systems were discussed by Horward Shrobe in 2001 (Shrobe, 2001). Then a project was started in MIT for developing the concept. The aim of their project was that of restructuring software applications as self-adaptive survivable systems to protect infrastructures. Those software systems must be informed by a trust model that indicates which resources are to be trusted. When such a system starts a task, it chooses the method that the trust model indicates as most likely to avoid compromised resources. In addition, such a system must be capable of detecting its own malfunctioning, diagnose the respective failure, and consequently repair itself. For example, a system might notice through self-monitoring that it is running much slower than expected (Shrobe, November 4, 2002). The central idea in self-adaptive systems is that in many cases computer systems may have more than one way to perform a task. Self-adaptive systems involve making dynamic choices between such alternatives. The results of the technical report from MIT showed that (Shrobe et al., April 10, 2007) self-awareness and self-adaptivity can be successfully applied to monitoring the behavior of systems, diagnose failures, and adapt and recover from both insider and external attackers.

Therefore our proposal is to develop a complete NGN security solution including self-adaptive systems and applications, supported and integrated with autonomic NGN components. In other words, smart autonomic network entities as presented in Fig. 7 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.

5.3. *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 4) security can only be ensured when the solutions 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 guaranteeing the attainment of an acceptable global solution. An important advantage with current hardware and software technologies, embedded and intelligent equipment is that it is possible to implement those autonomic characteristics and self-adaptability without affecting the performance of the networks.

In the following we discuss the characteristics of the proposed approach and how it can be integrated into the ITU-T X.805 based Vulnerability Analysis Method (e-TVRA) for NGNs.

5.4. *Integration 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 for monitoring, self-management, self-healing, and self-protection, among others;
2. Designing and implementing NGN self-adaptive software solutions, which will provide the capabilities for 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 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.

ITU-T X.805 is a useful framework for understanding NGN infrastructures and services security issues (Cho et al., 2005), as it provides a comprehensive, top-down, end-to-end perspective of NGN security. The two proposed solutions, autonomic and self-adaptive capabilities by hardware and software respectively, should be applied to each of the NGN security modules described by ITU-T X.805, as shown in Fig. 5. There are 9 security modules, which should be analyzed according to the 8 security dimensions proposed by the ITU-T X.805 modular structure of NGN security architecture.

While analyzing each of those 9 modules, it is important to identify their software and hardware entities and the respective roles with regard to the infrastructure, services and application layers as depicted in Fig. 9. 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 defining 'security information sharing domains'.

5. Connecting the ITU-T X.805 Security Architecture and the e-TVRA security method, with the proposed solution based on autonomic and self-adaptive capabilities. This interaction will enrich both, the security analysis and the implementation of the resulting security.

Fig. 10 shows that *the restrictions of mutuality* between the e-TVRA (ETSI threat, vulnerability and risk analysis method) (Rossebø et al.,) and the ITU X.805 NGN security architecture for NGNs. Also in the figure it is shown the weak point regarding the handling of information on vulnerabilities, threats and unwanted incidents. The continuous and prompt update of this information is fundamental for achieving the security of the operating NGN systems.

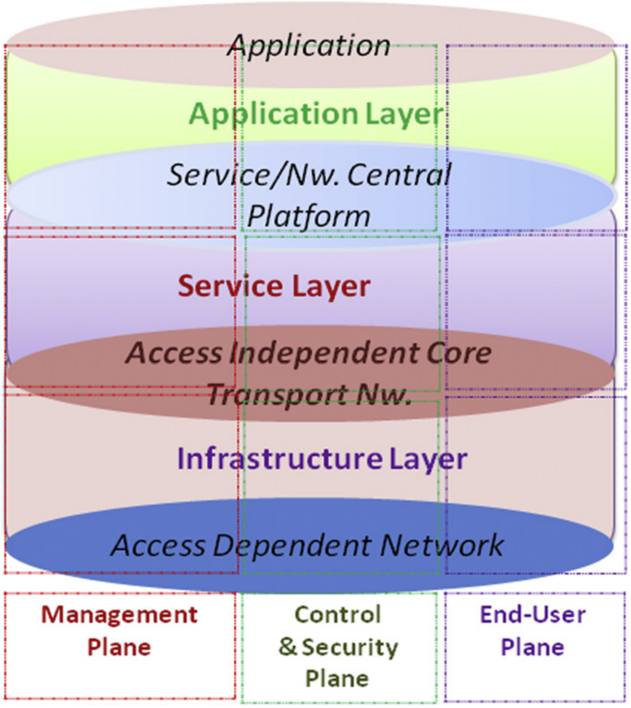

Fig. 9 – The proposed solution for the NGN network architecture as harmonized with the ITU-T X.805 NGN security architecture model.

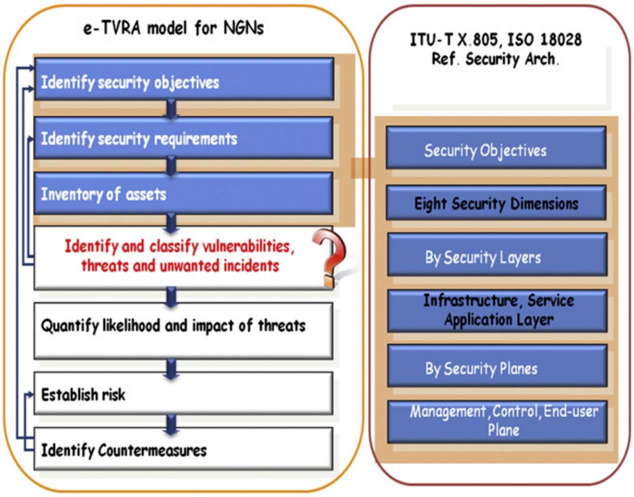
e-TVRA model for NGNs
Identify security objectives
Identify security requirements
Inventory of assets
Identify and classify vulnerabilities, threats and unwanted incidents
?
Quantify likelihood and impact of threats
Establish risk
Identify Countermeasures
ITU-T X.805, ISO 18028 Ref. Security Arch.
Security Objectives
Eight Security Dimensions
By Security Layers
Infrastructure, Service Application Layer
By Security Planes
Management, Control, End-user Plane

Fig. 10 – The interlink between e-TVRA and ITU-T X.805.

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 as introduced in Section 5.3. This information sharing should be established dynamically and continuously between the NGN architecture and the e-TVRA method in real time. Thereby both the e-TVRA model can be efficiently applied for assessing the risk and identifying the more appropriate countermeasures, and the NGN security architecture can be updated accordingly. In addition this information feedback regarding vulnerabilities, threats and risk analysis can enable the proposed autonomic and self-adaptive capabilities. Furthermore, this approach can improve the speed and completeness of the application of the e-TVRA tool.

6. 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:

- Localization of the security problems, for assuring their effective detection and mitigation;
- Information sharing among NGN components,done according to need-to-know, segregation and fragmentation rules.
- Vulnerability, threat and risk analysis tools carrying out more effectively their assessments by exploiting real time information sharing.
- Creation and use of 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. Future work should take advantage of the many research projects regarding autonomic and self-adaptive applications/systems active today –e.g. 'Autonomic Internet', supported by the EC's FP7 (http://ist-autoi.eu/autoi/; http://www.future-internet.eu/home.html).

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.

Acknowledgement

This work was supported in part by the TUBITAK (Turkish Science and Technological Research Program) under Grant of Bideb2219 Post-Doctorate Research Fellowship. And carried out in JRC in between 2008–2009.

REFERENCES

Cadzow SW. 'Security assu rance and standards – design for evaluation. Cadzow communications Consulting Ltd. UK: IEEE Explore; 2004.

Cho Y, Won Y, Cho B. 'ITU-T X.805 based vulnerability analysis method for security framework of end-to-end network services'. In: Proceeding of the 4th WSEAS Int. Conf. on Information Security, Communication and Computers, Tenerife, Spain; December 16–18, 2005.p. 288–292.

Cisco. Annual security report, www.cisco.com/web/go/securityreport; 2009.

National Risk Register of UK Government, last updated 09 Nov. 2008. http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/national_risk_register/national_risk_register_introduction.pdf.

Hariri S, Parashar M. Handbook of bioinspired algorithms and applications, chapter the foundations of autonomic computing. CRC Press LLC; 2005.

Horn P. Autonomic computing: IBM's perspective on the State of information technology. IBM Corp, http://www.research.ibm.com/autonomic/; Oct 2001.

IBM Internet Security Systems X-Force®. Mid-year trend statistics, www-304.ibm.com/businesscenter/cpe/download/183714/IBM_XFORCE_H1_2000.pdf; 2009.

Internal Functional Architecture of Autonomic Element. "IBM autonomic element architecture", http://www.research.ibm.com/autonomic; 2001.

ISO/IEC 15408–2: "Information technology-security techniques – evaluation criteria for IT security – part 2: security functional requirements".

ITU-T Recommendation Y. Approved in December 2004, Available from: http://www.itu.int/ITU-T/studygroups/com13/past-results.html; 2001.

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

ITU-T Y-2001, General overview of NGNs; 2004.

ITU-T Y-2011, General principles and general reference model for Next Generation Networks; 2004 October.

ITU-T Y-2012, Functional requirements and architecture of the NGN. Release 1, 2006 September.

Jaquith A. Security metrics replacing fear, uncertainty and doubt. Addison Wesley; 2007.

NanoTechnology & Homeland Security. Leveraging new technology to counter new threats. A white paper. NOVA Workforce Board; 2003.

Next-Generation Networks and Energy Efficiency, ITU-T technology Watch Briefing Report Series, No. 7, August 2008.

Parashar M, Hariri S. UPP 2004, LNCS 3566. In: Banatre J-P, et al., editors. Autonomic computing: an overview. Berlin Heidelberg: Springer-Verlag; 2005. p. 247–59.

Pfleeger S. "Risky business: what we have yet to learn about risk management,". Journal of Systems and Software 2000;53:265–73.

Rossebø J.E.Y., Scott Cadzow, Paul Sijben. eTVRA, a threat, vulnerability and risk assessment method and tool for eEurope. In: Second International Conference on Availability, Reliability and Security (ARES'07).

Shrobe H. 'Model-based diagnosis for information survivability. In: Laddaga R, Robertson P, Shrobe H, editors. Self-adaptive software. New York: Springer-Verlag; 2001.

Shrobe H, Laddaga R, Balzer R, Goldman N, Wile D, Tallis M, et al. 'Self-adaptive systems for information survivability: PMOP and AWDRAT'. MIT-CSAIL-TR-2007-023. MIT Cambridge: Computer Science and Artificial intelligent laboratory Technical Report, www.csail.mit.edu; April 10, 2007.

Shrobe H. 'Computational vulnerability analysis for information Survivability'. AI Magazine November 4, 2002;23.

Thermos P. VoIP security behind the Dialtone; vulnerabilities, attacks and countermeasures. Presentation of Polindrome Technologies; 2006.

F. Weber, U. Trick, VoIP – SIP-based via internet or NGN, research group for telecommunication networks, University of Applied Sciences Frankfurt/M., Kleiststr. 3, D-60318 Frankfurt/M., Germany.