Security Challenges for Next Generation Networks

Anusha G E

Asst Professor, *Dept of CSE, Jyothy Institute of Technology, Bangalore.*

anushaeshwar@gmail.com

***Abstract*- Increasing the complexity of information and telecommunications systems, networks is reaching a level beyond human ability, mainly from the security assessment viewpoint. Currently proposed methodologies for managing and assuring security requirements fall down for industrial and society 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 worst. With the deployment of Next Generation Networks (NGN), 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 NGN, but current vulnerability, threat and risk analysis methods do not appear 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 counter measures will require technological improvements, which will demand further security analyses. Then evaluates the current vulnerability, threat and risk analysis methods from the point of view of the new security requirements of NGNs.**

This uses autonomic and self-adaptive systems/applications for assuring the security of NGNs.

***Index Terms*- Network security, Next generation networks, Vulnerability, Threat, Autonomic computing, Self-adaptive systems .**

I. INTRODUCTION

Communications technologies are evolving fast, 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.

Communication networks have become a key economic and social infrastructure in world economies. The network infrastructure supports all economic sectors, and is therefore crucial to the national and international exchange of goods and services.

In Centre for the Protection of National Infrastructure (CPNI), the report on the identification of the high consequence risks faced by the UK, highlights that the expanding interconnectivity among networks influences the probabilities and impact of attacks within an NGN scenario, Figure 1 shows illustration of this trend towards scenarios characterized by high-impact, high-likelihood risk of particular relevance are 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 and their disturbance or disruption can severely impair society at large.

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 applicable to NGN, composed of three security layers, three security planes, and eight security dimensions. Although providing a comprehensive view of network security, puts strict 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.

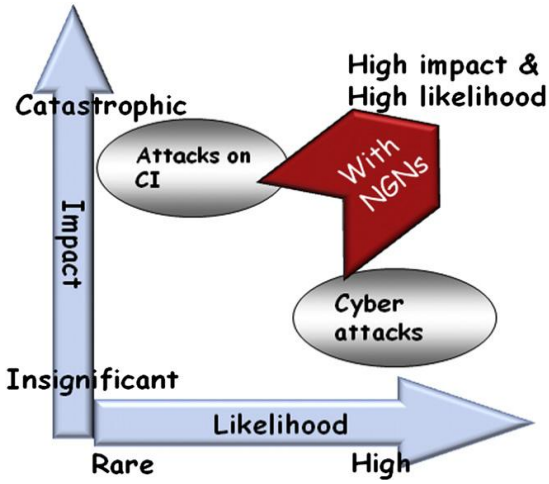

Figure 1: An illustration of the high consequence risks with NGNs.

The aim of this paper is to discuss the possible integration of the proposed ITU-T security model with new additional 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 chapters; chapters 3 and 4 include information about the NGN general functional architecture and the security architecture model proposed by the International Telecommunication Union- ITU-T. Chapter 5 describes the deficiencies of current security solutions and Vulnerability, Threat, Risk Analysis Methods. Chapter 6 defines the basic requirements and capabilities for new security solution approaches for NGNs. Finally it presents the conclusions and future work.

II. NGN ARCHITECTURE MODEL

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. 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 has proposed a standardization studies roadmap for NGN security. The details of security standardization topics for the current Study Period (2009 to 2012) were proposed at the September 2008 meeting of ITU-T. 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:

- 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 wired and wireless technologies, which can be applied interchangeably for the delivery of services. The vision is that NGN could be used anytime and anywhere across various environments using compatible terminal equipments. For accomplishing this aim, the architecture of NGN is separated into two strategies: transportation and services. Each strategy includes management and control functions, and resources. Figure 2 presents the General Functional Model for NGNs.

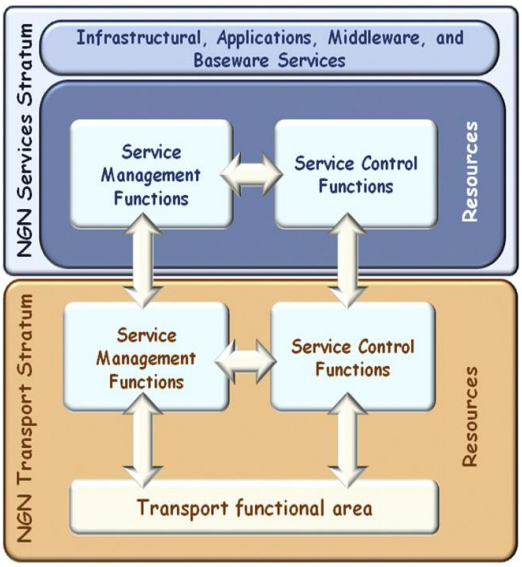

Figure 2: General Functional Models for NGN (ITU-T 2011)

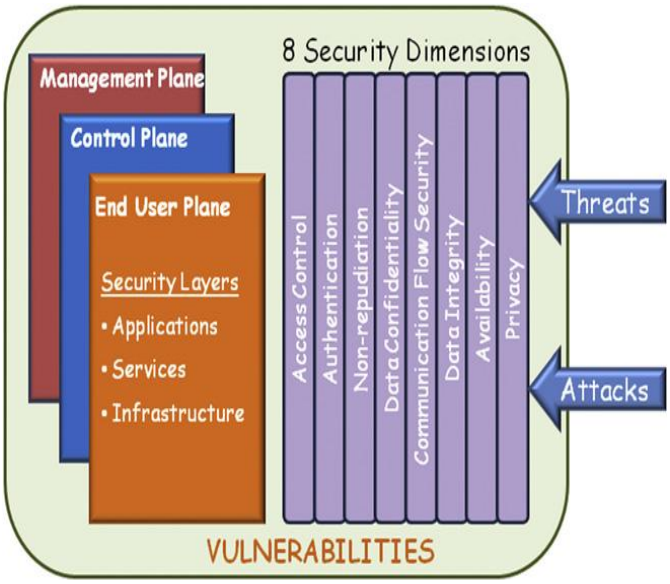

Figure 3: ITU-T X.805 Security Architecture 'Three security layers' X 'three security planes' X '8 security dimensions'

III. NGN SECURITY ARCHITECTURE MODEL

The NGN Security architecture was designed by ITU-T in order to propose solutions for the following questions:

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

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 Figure 3. Each layer relates to unique vulnerabilities, threats and mitigation measures.

The NGN security plane 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.

IV. SECURITY SOLUTIONS AND ANALYSIS METHODS

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

As shown in Figures 1, 2 and 3 in the previous chapters, 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 Figure 4.

Figure 4: The continuous security gap between technology and standards

NGNs have already been deployed in many developed countries such as Japan, South Korea, USA, China, UK etc.

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. 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. 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 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 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. No security measurement definition and tool has proven it's 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.

V. SECURITY SOLUTION APPROACH

Current standards don't 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'. 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 chapter 5.

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.

A. 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 a self-governing way towards an acceptable secure state. This approach can be a security solution for NGN that implements an autonomous entity, as depicted Figure 5. 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.

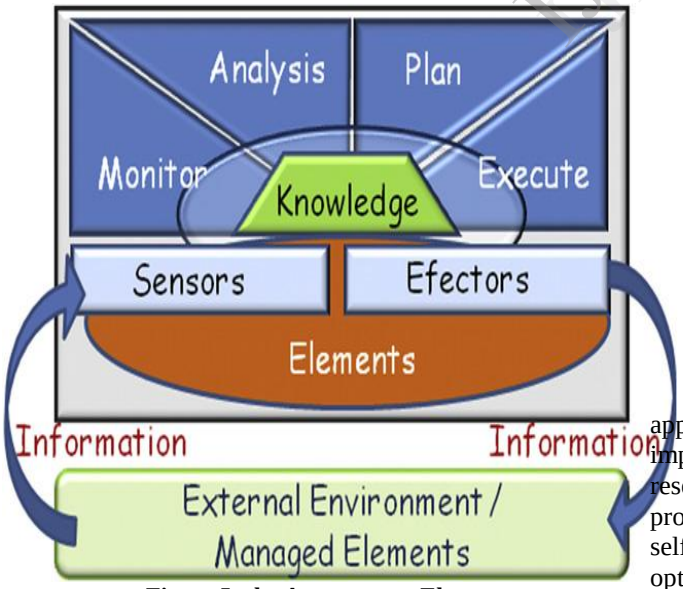

Figure 5: the Autonomous Element

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 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.

NGN networks can use autonomic applications/systems to handle complexity and uncertainties with minimum human intervention. Autonomic applications and systems have eight characteristics:

- Self Awareness: It "knows itself" and is aware of its state and its behaviors.
- Self Configuring: It should be able configure and reconfigure itself under varying and unpredictable conditions.
- Self Optimizing: It should be able to detect suboptimal behaviors and optimize itself to improve its execution.
- Self-Healing: It should be able to detect and recover from potential problems and continue to function smoothly.
- 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.
- Context Awareness: It should be aware of its execution environment and be able to react to changes in it.
- 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.
- 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.

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.

B. 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 Figure 6. How this solution can implements, the ITU-T X.805 security architecture and improve the TVRA (threat, vulnerability and risk analysis) method for NGNs.

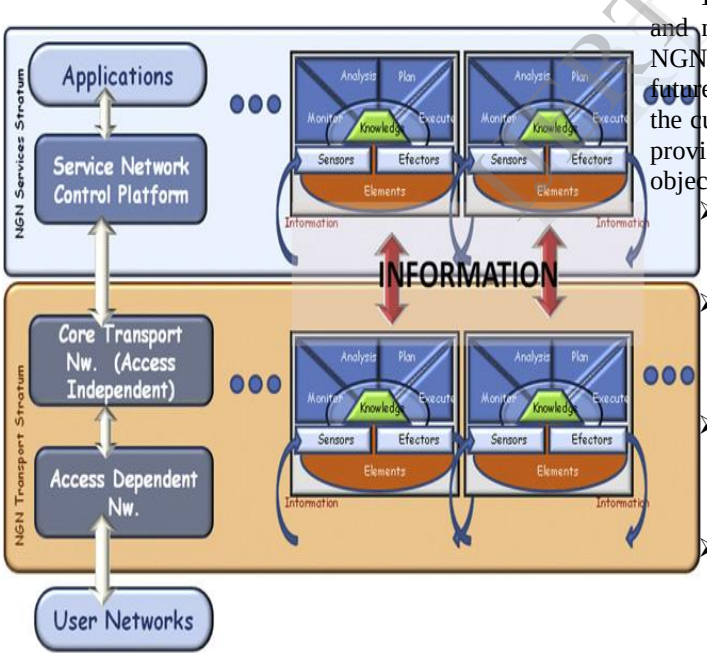

Figure 6: Proposed Security Solution for NGNs with Autonomous systems/applications

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.

VI. CONCLUSION

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

[2] 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 16e18, 2005.p. 288e292.

[3] Cisco. Annual security report, www.cisco.com/web/go/ security report; 2009.

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

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