The Role of Service Level Agreements in NGN Security Management Systems

VALENTINA TIMCENKO[1], SLAVICA BOSTJANCIC RAKAS[1], MIRJANA STOJANOVIC[2]
[1]Mihailo Pupin Institute, University of Belgrade, Volgina 15, Belgrade, SERBIA
[2]Faculty of Transport and Traffic Engineering and Faculty of Electrical Engineering, University of Belgrade, Vojvode Stepe 305, Belgrade, SERBIA
[1]valentina.timcenko@institutepupin.com, slavica.bostjancic@pupin.rs, http://www.pupin.rs
[2] m.stojanovic@sf.bg.ac.rs, http:// www.sf.bg.ac.rs/

Abstract: - In this paper we provide a critical evaluation of security issues in a heterogeneous NGN environment. Properly defined SLA represents a starting point for provisioning of secure services with the required quality. We propose a general format of service level specification with particular emphasis to security issues. We also propose a policy-based security management architecture, as an integral part of the provider's quality of service (QoS) management system. The model assumes a central QoS management entity in each administrative domain. This entity encompasses the following functional sub-entities: SLA manager, Policy selector, Network resource manager, Configuration manager and Security manager.

Key-Words: - Next generation network, quality of service, security management, service level agreement.

1 Introduction

Security is an important part of every software development process. Main aspects affecting the degree of software dependability include the expertise for secure product development, quality of development tools, the level of testing procedures completed before releasing the product and the matured practices followed throughout the development cycle [1].

Communication requirements related to the enterprise market are different for different enterprises (small office/home office, small and medium enterprise (SME), large enterprise, and international corporation). Nonetheless, advances in networking technologies set up new opportunities for these enterprises to be more efficient by interconnecting sites, increasing remote access of telecommuters and mobile users, and integrating heterogeneous telecommunication services over the same network [2].

The future telecommunications infrastructure should be built upon the concept of next generation network (NGN). NGN represents architecture of telecommunication core network based on the Internet Protocol (IP) and a diversity of access networks. The access networks can be heterogeneous wireless and wired technologies that provide consistent and ubiquitous services to end users. There must be a support of personal, terminal and session mobility [3], [4]. NGN separates service stratum from the transport stratum with the purpose of provisioning flexibility within common control architecture. IP services deployment can be based on virtual networks that separate the transport network into multiple self-managed subsystems [5].

Provisioning of secure services in a heterogeneous NGN network is a very complex task. An exhaustive research effort is needed for development of new and efficient methods for security risk analysis. Requirements for end-to-end quality of service (QoS) provisioning, network dependability and reliability determine new approaches for development of network management systems. Deployment of automated systems with sets of abstractly defined policies (Policy Based Management, PBM) represents a perspective solution for implementation of scalable management platform.

Standardization of service level specification formats is an important prerequisite for management automation, and for achieving interoperability among service providers. In a heterogeneous NGN environment, each domain should establish and enforce policies for service level agreements (SLAs) to assure the security of its domain and the security of the network interconnections [6]. SLA should specify security services and mechanisms to be implemented to protect the interconnected domains and the communications.

Due to limitations of security technologies and the growth of cyber attacks the efficiency of security management is affected and the activities to be performed by network administrators are increased. Therefore, one of the most important challenges for

provisioning of a reliable and trustworthy NGN services is deployment of highly automated security management system.

2 Security issues in NGN environment

The use of IP technology in business communications has introduced concerns about security, trust, and value added services and raised the need for better resilience and fault tolerance through fine-grained control and management.

There is a strong need for performing a thorough information security risk analysis that is very complex and expensive task. It is very difficult to identify all of the relevant threats as well as to estimate the probability of their occurrence. The problem is particularly visible in SMEs that usually do not employ IT experts and cannot afford an appropriate outsourcing expertise [7].

There can be qualitative or quantitative security risk analysis [8]. While qualitative analysis relies on subjective evaluations (e.g., low, medium or high risk), quantitative analysis is based on a suitable mathematical approach like numeric analysis or statistical methods that specify risk as a numerical value (e.g., in monetary units and threats frequency).

Several proposals that address the problem of security, including security policies, trust relationships, cryptography, anti-spam, anti-attacks, and privacy in NGN environment are described in [9]. One of the proposals presents a network architecture that makes use of secure cryptographic identities to establish relationships among different entities in the NGN environment. Another proposal developed centralized security architecture to protect against malicious network attacks, thus preventing inconsistencies in network security policies by separating them from the underlying network topology. Next proposal deals with methods for protecting user privacy in a network with ubiquitous computing devices, while the last proposal deals with security for the future Internet, defining four main issues: trustworthy network and service infrastructure; technologies and tools for trustworthy networks; networking, coordination, and support.

Architecture for Information Security Management is proposed in [10]. Architecture improves security management processes such as monitoring, controlling, and decision making by providing mechanisms for enhancement of the active construction of knowledge about threats, policies, procedures, and risks.

The use of Trusted Third Party (TTP) ensures the confidentiality, integrity and authenticity of data and communications, by enabling trust and using cryptography [11]. The main function of TTP is provisioning of scalable end-to-end security services, which are based on standards and useful across different domains and geographical areas. Such approach is completely compatible with the Third-Party model that should provide end-to-end quality of service (QoS) guarantees in a multi-provider environment [12].

The Open Web Application Security Project (OWASP) deals with enterprise business application security vulnerabilities, implementation assessment guide, vulnerability testing guide and development of free tools for enterprise business applications assessment [13].

Embedded web application firewall model based on "black" and "white" lists of vulnerabilities, allows flexible and efficient development of Web applications firewalls, and adjusted to specific needs of different programs [14].

3 Service Level Agreements

As a result of service negotiation between the customer and the provider, SLA represents a contract that defines all technical, financial and legal aspects of a specific telecommunication service. Regardless of the underlying QoS model, SLAs should consist of the two main parts: the business part and the technical part. The business part deals with financial and legal aspects such as information about pricing, charging, billing and payment, and penalties for both the user and the provider in the case of contract violation. The technical part defines set of descriptors and associated attributes describing the particular service class and the traffic profile.

According to the ITU-T guidelines, SLA consists of five basic entities, regardless of the applied QoS model: service identification, service specification, business part, technology part and QoS report [15].

QoS specification framework that provides a specification language and software tool for definition of QoS requirements, offers and contracts in mobile and wireless environments is proposed in [16]. The provider-to-provider SLA template in wireless networks is proposed in [17]. This template contains all of the necessary parameters to support the services offered by both providers, and every offered service class.

SLAs represent a basis for provisioning of QoS and security services in the NGN environment. Service management is typically performed by the

means of per-domain entities that are responsible for monitoring and management of the service specified by SLA, admission control and network resource management [12], [18].

Users can formalize their service level requirements through SLAs, while service providers can use electronic SLAs to offer their services [12], [19]. Customers can be offered an electronic SLA form (e.g. through an appropriate Web interface) by service providers. By completing this form customers can express their requirements for a particular service and they are informed about the offered service, after processing their requirement.

Different users and environments usually establish different security requirements. Therefore, security services should be negotiated and specified through the SLA. For example, an administrative domain typically offers more than a few QoS classes, while security services are usually not included in those classes. Hence, service description for each class could be enriched by an optional security descriptor with specification of security services and their associated mechanisms [20].

4 PBM security management architecture

Management policies help network administration to achieve certain goals. These policies define goals and associated action for achieving those goals. Management policy represents set of rules used for managing the network behavior, network resources, services and groups of users. For example, one policy can be used for admission control of new traffic flows while the other can be used for information security managing, etc.

The basis for securing NGN services offered to end users represents a properly defined SLA represents. Different users and environments establish different requirements for security, therefore the user and the NGN provider should precisely agree on security services and compensation for those services. To fulfill the negotiated SLA, NGN provider selects the most appropriate security policy.

Providers in NGN environment usually have to keep track of a very large number of SLAs. To implement a various security policies, a configuration of a multitude of parameters in each network element is needed. This particularly goes for IP security (IPsec) protocols that represent a set of open IETF standards providing cryptographic-based protection mechanisms for IP packets [21]. Manual network configuration could be inefficient, since IPsec protocols require several tenths of configurable parameters in each network element [22].

One of the key challenges for NGN network and service providers is automation of security management process. Therefore, deployment of PBM automated systems that encompass sets of abstractly defined policies seems to be a promising approach to fulfill such requirement [23].

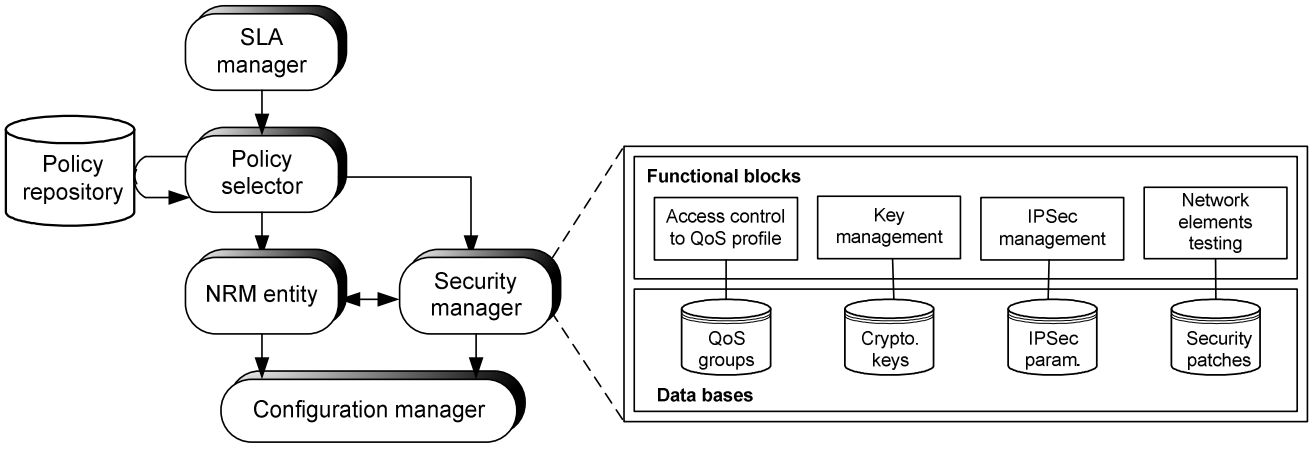

Fig. 1. Functional model of security management architecture

Figure 1 presents a proposal of security management architecture, which is considered in the wider context of quality of service PBM oriented system. In each administrative domain we suppose central QoS management entity, which encompasses five functional blocks [12]:

(1) **SLA manager** provides the following functions: dynamic service negotiating for novel traffic flows; comparison of QoS requirements with profiles of service classes offered by the network and selection of the appropriate class and pricing model.

ISBN: 978-1-61804-134-0

(2) **Policy Selector** chooses the appropriate security policy from the policy repository, based on the relevant SLA parameters obtained from the SLA manager. Selected policy is then forwarded to NRM (Network Resource Manager) entity and Security manager.
(3) **NRM entity** implements admission control procedures and decides whether SLA request should be accepted, denied or renegotiated.
(4) Relevant parameters, obtained from NRM entity and Security manager, are configured by **Configuration manager,** which forwards them to network elements.
(5) Four functional blocks, associated with the appropriate databases assemble **Security manager entity** (Figure 1):

- Access control of the new traffic flow to a particular QoS profile. Access control policy should be implemented using different options of operating systems and communication devices by assigning user names and passwords to all users.
- IPsec management. Application of the set of IPsec protocols assumes implementation of the appropriate security policy in network elements, which support IPsec.
- Key management. It refers to dynamic establishment of cryptographic keys that are used in the IPsec, as well as in different security mechanisms for control protocols (routing, signaling).
- Testing of network elements and distribution of security patches. It includes different control functions for detection and correction of errors in operating systems, as well as for updating of anti-virus programs and their associated data bases. Testing of network equipment is required on a daily basis and depending on these test results, distribution of security patches should be initiated.

5 Conclusion

Evaluation of security of a particular product is very complex issue. First of all, the enterprise's security requirements should be defined, and then the requirements, analysis and comparison of available products should be identified. It is extremely desirable to perform an information security risk analysis, but, a proper expertise is often very expensive and complex task.

In this paper we claim that properly defined service level agreement represents the basis for securing a wide spectrum of NGN services which should be offered to end users in a consistent and ubiquitous manner. Since different users and environments pose different security requirements, the NGN provider and the user should precisely agree upon security services to be provided and also compensation for those services. We also propose a policy-based security management model that encompasses the following functions: access control to a particular QoS profile, IPsec management, cryptographic key management, testing of network elements and distribution of security patches.

Acknowledgement. This work was supported in part by Serbian Ministry of Education and Science (R&D projects TR 32025 and TR 36002).

References:

[1] S. R. Vadalasetty, Security Concerns in Using Open Source Software for Enterprise Requirements, *SANS Institute, white paper,* 2003. Retrieved October 10, 2010, from http://www.sans.org/reading_room/whitepapers/awareness/security-concerns-open-source-software-enterprise-requirements_1305

[2] M. Stojanovic, V. Acimovic-Raspopovic, Communication Issues for Small and Medium Enterprises: Provider and Customer Perspectives, *In Enterprise Information Systems for Bussiness Integration in SMEs: Technological, Organizational, and Social Dimensions*, Hershey - New York: Information Science Reference, pp.230-251, 2009.

[3] International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), General overview of NGN. ITU-T recommendation Y.2001. Geneva, ITU-T, 2004.

[4] J. I. Agbinya, *IP Communications and Services for NGN*, Auerbach Publications, Taylor & Francis Group, 2010.

[5] R. Good et al., The use of NGN / IMS for Cloud and Grid Services Control and Management, *Proceedings of the Southern African Telecommunication Networks and Applications Conference – SATNAC 2009*, Mbabane, Swaziland, August 2009.

[6] International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), Security mechanisms and procedures for NGN. ITU-T recommendation Y.2704. Geneva, ITU-T, 2010.

[7] J. Beachboard et al., Improving Information Security Risk Analysis Practices for Small- and

Medium-Sized Enterprises: A Research Agenda, *Issues in Informing Science and Information Technology*, Vol. 5, 2008, pp. 73-85.

[8] T. Tsiakis, Information Security Expenditures: A Techno-Economic Analysis, *International Journal of Computer Science and Network Security*, Vol. 10, No. 4, 2010, pp. 7-11.

[9] S. Paul et al., Architectures for the Future Networks and the Next Generation Internet: A Survey, *Computer Communicatins*, Vol. 34, No. 1, 2011, pp. 2-42.

[10] M. Hantea, Intelligent System for Information Security Management: Architecture and Design Issues, Issues in Informing Science and Information Technology, Vol. 4, 2007, pp. 29-43.

[11] D. Zissis, D. Lekkas, Addressing Cloud Computing Security Issues, *Future Generation Computer Systems*, Vol. 28, No. 3, 2012, pp. 583-592.

[12] M. Stojanovic et al., End-to-End Quality of Service Specification and Mapping: the Third Party Approach, *Computer Communications*, Vol. 33, No. 11, 2010, pp.1354-1368.

[13] Open Web Application Security Project (OWASP), OWASP Enterprise Application Security Project, 2009. Retrieved, February 08, 2011, from http://www.owasp.org/index.php/OWASP_Enterprise_Application_Security_Project

[14] E. Kazanavicius et al., Securing Web Application by Embedded Firewall, Elektronika Ir Elektrotechnika, (Electronics and Electrical Engineering), Vol. 119, No. 3, 2012, pp. 65-68.

[15] International Telecommunication Union – Telecommunication Standardization Sector (ITU-T). Guidelines for the definition of SLA representation templates. ITU-T Recommendation M.3342. Geneva ITU-T, 2006.

[16] C. Wang et al., Quality of Service Contract Specification, Establishment, and Monitoring for Service Level Management, *Journal of Object Technology*, Vol. 6, No. 11, 2007, pp. 25-44.

[17] C. Gizelis, D. Vergados, SLA Factors of Interconnecting Wireless Networks QoS, Cost Estimation Point of View – the IC-DBMS Approach, *Proceedings of the International Conference on Telecommunications & Multimedia – TEMU 2006*, Crete, Greece, July 2006.

[18] J. Zeng, N. Ansari, Toward IP Virtual Private Network Quality of Service: a Service Provider Perspective, *IEEE Communications Magazine*, Vol. 41, No. 4, 2003, pp.113-119.

[19] P. Hasselmeyer et al., Implementing an SLA Negotiation Framework, *Proceedings of the eChallenges e-2007 Conference*, Hague, Netherlands, 2007.

[20] M. Stojanovic et al., Security Management Issues for Open Source ERP in the NGN Environment, *In Free and Open Source Enterprise Resource Planning – Systems and Strategies*, IGI Global, 2011, pp. 165-181.

[21] S. Kent, K. Seo, Security Architecture for the Internet Protocol. IETF RFC 4301, 2005. Retrieved April 16, 2012 from http://www.rfc-editor.org/rfcsearch.html.

[22] M. Li, Policy-Based IPsec Management, *IEEE Network*, Vol. 17, No. 6, 2003, pp.36-43.

[23] D. C. Verma, Simplifying Network Administration Using Policy-Based Management, *IEEE Network*, Vol. 16, No. 2, 2002, pp. 20-26.