Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp288-292)

ITU-T X.805 based Vulnerability Analysis Method for Security Framework of End-to-End Network Services

YOUNGDUK CHO YOOJAE WON BYONGJIN CHO
Information Security Technology Division
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul, Korea 138-803
KOREA

Abstract: - This paper proposes a ITU-T X.805 based Vulnerability Analysis Method for developing Security Framework of NGN infrastructure and services. It is derived from ITU-T X.805 and security consulting methods. It provides a holistic approach and a systematic vulnerability analysis view of security model for new network infrastructure and services. As a further works, we will apply this methodology to new emerging network infrastructures and services.

Key-Words:- ITU X.805, Vulnerability Analysis, Security Framework

1. Introduction

NGN(Next Generation Network) is a packet-based network which is able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different services providers. With growth of NGN, new multiple network services is toward converging. But broadband convergence network like NGN is expected that a threat effect is considerably enormous extended over a network to overall connected networks. So, security should implement before constructing of new infrastructures and services in networks.

But it is important that the existing network security concept is not robust to adapt to the convergence networks, which is a complex set of multi-infrastructures and services. Also, quality of service related to trade off services performance is increasingly more valuable than ever. For example, if a person using a Internet telephony software in a wireless broadband internet terminal connects a another person using a telephone in PSTN, the person goes through wireless network, Internet, and PSTN. Generally the person has to be controlled doubly the security mechanisms of network itself. Multi-level security facilities and activities often have become a critical services degrade in this situation.

However, the Reference architecture of ITU-T X.805 is useful tool to comprehend a complex set of network infrastructures and services. The reference architecture addresses security concerns for the management, control, and use of network infrastructure, services, and applications. The reference architecture provides a comprehensive, top-down, end-to-end perspective of network security and can be applied to

network elements, services, and applications in order to predict, detect, and correct security vulnerabilities.

2. Related Work

In this section, we provide the vulnerability analysis method that derived from ITU-T X.805 and security consulting methods such as BS7799, IT protection manual and so on.

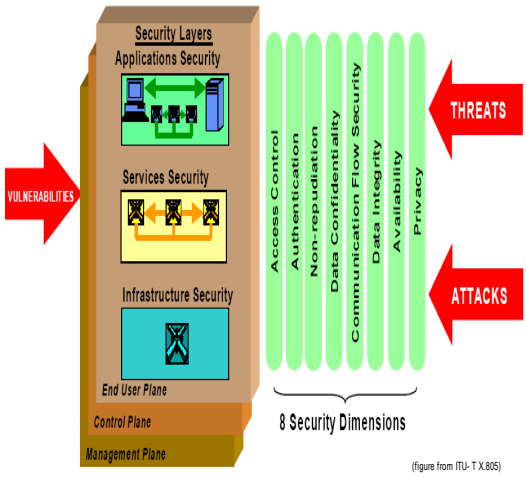

Fig. 1 Reference Architecture for End-to-End Network Security(source from ITU-T X.805)

The X.805 is a standard specification of developing in security model of ITU-T FG-NGN. The X.805 has 3 architectural components – Security Dimensions, Security Layers and Security Planes.

Security Layers are a hierarchy of equipment and facilities groupings, which are 3 layers: (1) Infrastructure security layer, (2) Services security layer, (3) Application security layer. Each security layer has unique vulnerabilities, threats, and mitigations.

Security Planes represent the types of activities that occur on a network, which are (1) Management security plane, (2) Control security plane, (3) End-User security plane. Each security plane is applied to every security layer to yield nine security perspectives. Each security perspective has unique vulnerabilities and threats.

Security Dimension is a set of security measures designed to address a particular aspect of the network security. Security Dimensions are 8 sets – (1) Access control, (2) Authentication, (3) Non-repudiation, (4) Data confidentiality, (5) Communication flow security, (6) Data integrity, (7) Availability, (8) Privacy. 8 Security Dimensions applied to each security perspective.

Fig.1 shows Reference Architecture for end-to-end network security of ITU-T X.805.

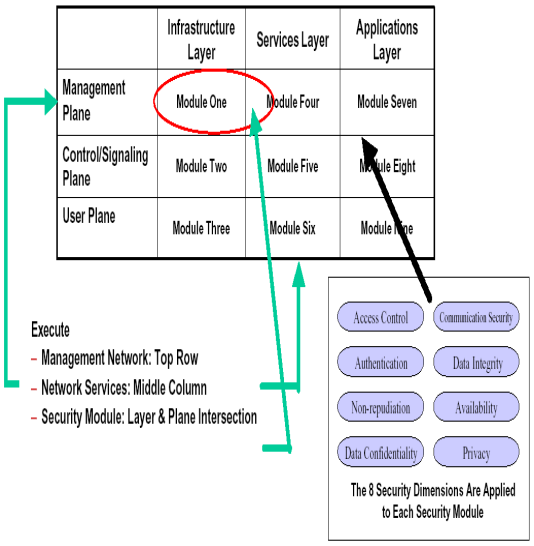

Fig. 2 Modular Form of X.805

(source from ITU-T X.805)

Fig.2 shows provides a systematic, organized way of performing network security assessments and planning. This is the best merits of X.805.

The usage of Security Consulting method is to analysis the risk assessment of specific organization. Risk assessment methods are BS7799, OCTAVE(Operationally Critical Threat, Asset and Vulnerability Evaluation), ISO 13335 GMITS(Guidelines for the management of IP security), and so on. Fig.3 is a general procedure of these methods.

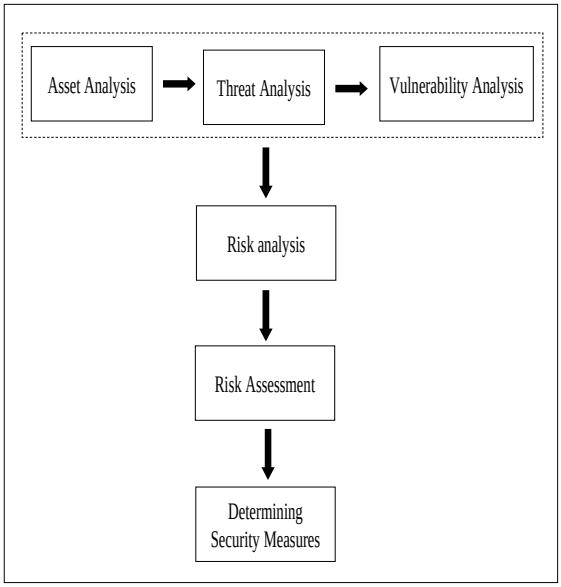

Fig. 3 General procedure of Risk Assessment Method

3. ITU-T X.805 based Vulnerability Analysis Method

In this section, we propose the vulnerability analysis method to develop NGN Security Framework that is motive from ITU-T X.805 and security consulting methods such as BS7799, IT protection manual and so on. This analysis model is useful of applying to any network technology and any scope of network function.

Fig. 4 tells that the proposed method is similar to security consulting method. But, this is focused in discriminating protection target, especially multi-facet network infrastructures and services.

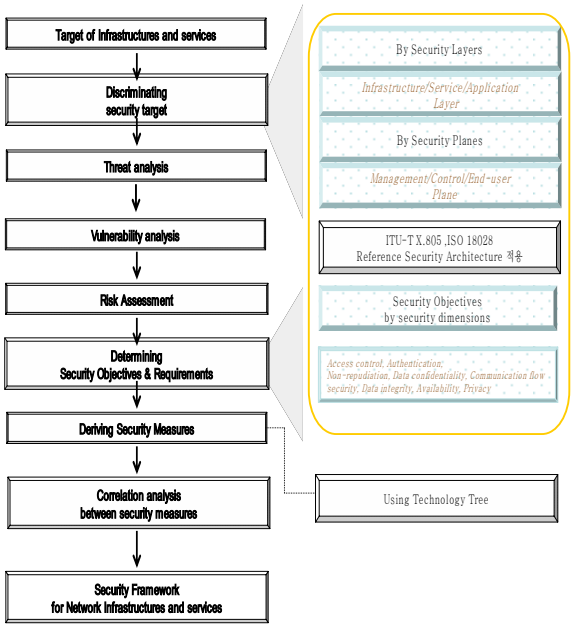

Fig. 4 ITU-T X.805 based Vulnerability Analysis Method

As it offers a systematic view of the protected target, we can consider wholly threats and vulnerabilities without exception. Security measures of unrealized network infrastructures and services can be reflected in the step of the implementation.

Fig.5 describes the detail steps of proposed Vulnerability Analysis Method. In addition to following a general procedure of Security consulting method, it references ITU-T X.805 to analysis the protected target. So, this

method is more comprehensive end-to-end network view of security than ITU-T X.805.

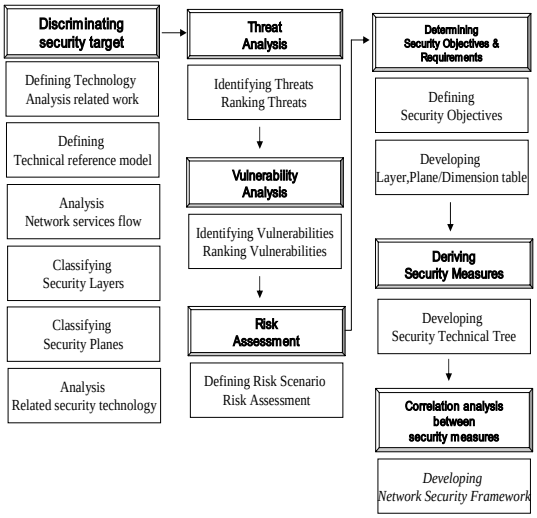

Fig. 5 Steps of Proposed Vulnerability Analysis Method

This method chooses the technical tree development for making security measures. Fig.6 explains to making a technical tree. The merits of this way can deduce a number of new security measurements.

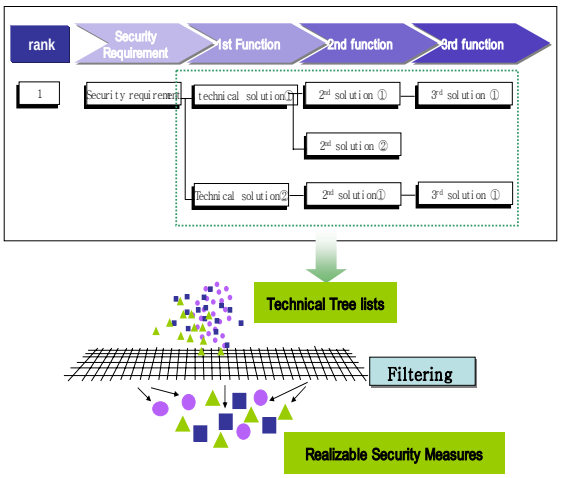

Fig. 6 Technical Tree Development

4. Conclusion and Further Works

We propose a ITU-T X.805 based Vulnerability Analysis Method for developing Security Framework of NGN infrastructure and services. It is derived from ITU-T X.805 and security consulting methods. It provides a holistic approach to network security and guides for NGN security.

In Korea, new network infrastructures and services has been constructed in according to IT839 strategy. IT839 strategy means 3 Infrastructures(Broadband Convergence Network, IPv6, Ubiquitous Sensor Network), 8 Services(Voice over IP, Home Network, Digital Multimedia Broadcast, Digital TV, Wireless Broadband Internet, RFID, Telematics, WCDMA) and 9 New Growth Engines(Next-generation mobile communications, Digital TV, Home Network, IT SoC, Next-generation PC, Embedded SW, Digital contents, Telematics, Intelligent Service Robot).

In further works, we will apply this vulnerability analysis method to 8 Services and BcN. So we will present a NGN Security Framework model, which will be reflected in implement of BcN infrastructure and services.

References:

[1] ITU-T X.805, *Security Architecture for Systems Providing End-to-End Communications*

[2] S.Kim, J.Jee, T.Nam, S.Sohn, C.Park, *Framework of Network Security Service for Next Generation*, Proceeding. WISA 2002, 123-130

[3] ITU-T SG17 Q.5, *ITU-T Rec. X.805 and its application to NGN*, ITU-T FG-NGN Workshop Proceeding, 2005 April

[4] Korea Information Security Agency, *Vulnerability Analysis & Assessment*

Methodology version, 2002

[5] Kong, Luo, Xu, Gu, Gerla, Lu, *Adaptive Security for Multi-layer Ad-hoc Networks*, Wireless Communications and Mobile Computing, Wiley Interscience Press, 2002

[6] Bass T., *Intrusion detection systems and multi-sensor data fusion*, Communications of the ACM, vol.43, issue 4, 2000 April