Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp283-287)

Study of Information Security Pre-Evaluation Model for New IT Service

DONGHOON SHIN, SUNGHOON KIM, GANG-SHIN LEE, and JAE-IL LEE
Korea Information Security Agency (KISA)
78, Garak-Dong, Songpa-Gu, Seoul
KOREA

Abstract: With the rapid growth of wired/wireless communication technology, network environments are evolving from a single service network to a broadband convergence network. Accordingly, IT services that used to be operated in a single network are also being converged and created into new services on a broadband convergence network. However, without proper security measures, such convergence of services may result in degrading the stability and reliability of the services. To address this issue, this paper will propose an information security pre-evaluation model that can be used to analyze probable security vulnerabilities and threats even at the planning and designing stage before actually operating a new IT service. The proposed pre-evaluation model will also be applied to a home network service validate the feasibility of the model.

Key-Words: Information Security Pre-Evaluation, New IT service

1 Introduction

With the rapid growth of wired/wireless communication technology, network environments are evolving from a single service network to a broadband convergence network[1][2]. Accordingly, IT services that used to be operated in a single network are quickly being converged and created into new services on a broadband convergence network. However, without proper security measures, such convergence of services may result in degrading the stability and reliability of the services[3]. To address this issue, this paper will propose an information security pre-evaluation model that can be used to analyze probable security vulnerabilities and threats even at the planning and designing stage before actually operating a new IT service. The proposed pre-evaluation model will also be applied to a home network service validate the feasibility of the model.

2 Information Security Pre-Evaluation Model for IT Service

This chapter introduces the information security pre-evaluation model for newly converged IT services that are emerging in a broadband convergence network environment and describes the target of evaluation and execution procedure.

2.1 Overview of Information Security Pre-Evaluation Model

Service providers who are developing new IT services try to gain comparative advantages by launching the services earlier than their competitors. In many cases, this battle against time urges service providers to focus on the performance of the service rather than information security features that can guarantee the security and reliability of the service. In worst cases, sacrificing the security and reliability of a service can result in an intrusion accident during operation, causing extreme damages including shutdown of the service and extensive and incurring extensive recovery costs. According to analysis results, the cost for identifying and solving security defects of an IT service increases dramatically in the implementation and testing stage compared to the design stage, and the cost for addressing such problems in the service Maintenance stage is 60 to 100 times greater than that of the designing stage[4].

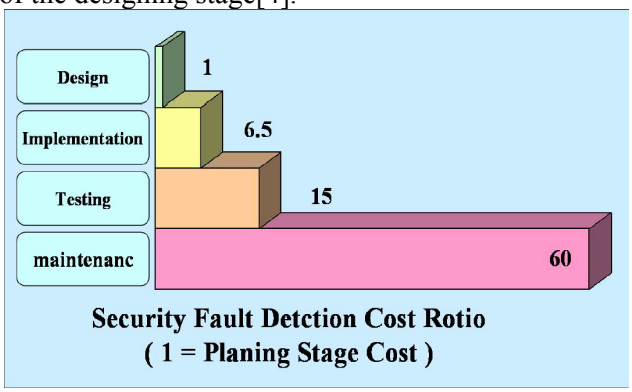

Fig. 1 Security Fault Detection Cost

From this perspective, it is vital to identify and apply key security factors required for information security at the initial stages of developing a new IT service. Through the information security pre-evaluation model, this paper will propose a methodology for analyzing technical, physical and administrative threats and vulnerabilities of a new IT service in its basis building stage and for applying essential security measures. In other words, the information security pre-evaluation model will allow service providers to guarantee security and reliability of a new service at the planning and designing stage.

2.2 Target and Procedure of Information Security Pre-Evaluation

(1) Target of Information Security Pre-Evaluation

The target of a information security pre-evaluation model are newly converged IT services being created in a broadband convergence network. More specifically, the components and the wired/wireless technologies applied to a new IT service are the target of evaluation. Specific target of evaluation may differ between services depending on the characteristics of the services.

Thus we must take into consideration that specific target of evaluation may differ from service to service, and that the system applied in the service planning stage may differ from that applied in the actual implementation stage. Targets of evaluation are categorized and described in [Table 1].

Table 1. Targets of evaluation Category

Category	Evaluation Category	Remarks
Service Management Center	○ Major servers and systems ○ Management of critical information ○ Operation of security solution ○ Network monitoring	○ Information center run by the service provider such as home network service center and telematics service center
Data Transmission Technology	○ Wired/Wireless protocol ○ Security Protocol	○ Data transmission protocols for wired/wirelss networks
User Terminal	○ Terminals and applications	○ Home pad and W-CDMA phones
Contents Provider	○ Major servers and systems ○ Management of critical information ○ Operation of security solution	○ VoD server operator
NGcN	○ Major network equipment ○ Equipment operation status ○ Use of security solution	○ Stability of delivery network, access network and service network

Targets of pre-evaluation are roughly classified into the service management center the provides overall management for new IT services, the data transmission technologies, or wired/wireless communication protocol technologies, user terminals, contents providers providing applications and NGcN.

(2) Information Security Pre-Evaluation Procedure

Fig.2 illustrates the execution procedure of the proposed pre-evaluation model.

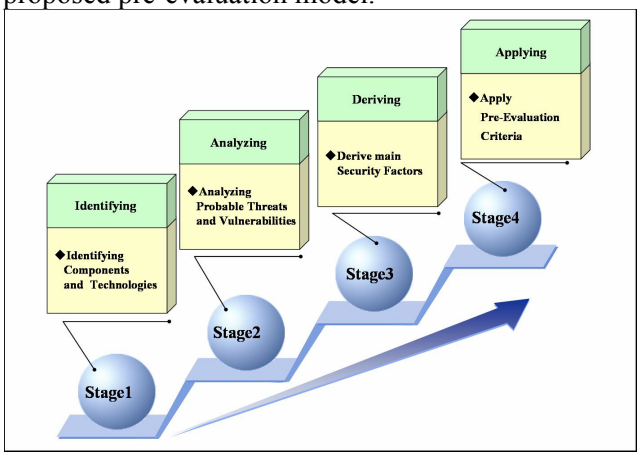

Fig. 2 Information Security Pre-Evaluation Procedure

Stage 1 of the execution procedure is for identifying the target of evaluation, stage 2 for analyzing probable threats and vulnerabilities, stage 3 for deriving effective technical and administrative security measures against the threats and vulnerabilities and for developing the pre-evaluation criteria, and stage 4 for applying the pre-evaluation criteria to the service. Detailed procedures for each stage are described in the example of applying the information security pre-evaluation model to a home network service.

3 Example of Applying the Information Security Pre-Evaluation Model to Home Network Service

This chapter describes detailed execution procedures of the pre-evaluation model by using an example of applying the model to a home network service.

3.1 Stage 1 : Identifying Target of Evaluation

(1) Concept of Home Network Service

Home network services contain services described in [Table2], which provide various domestic conveniences[5].

Table 2. Identifying of Home Network Service

Category	Service Type
Convenient Home	○ 1on1 customized education, medical service, health management ○ Control of information devices and home appliances
Entertaining Home	○ Interactive DTV, VOD, and online games ○ Customized info such as community news and daily info
Secure Home	○ Crime prevention, fire monitoring, gas leak prevention, information management ○ home viewer, theft, intrusion monitoring
Enriched Home	○ Interactive home shopping and home banking services ○ Energy management

(2) Identifying Components of Home Network Service

Components of a home network service are illustrated in (Fig.3).

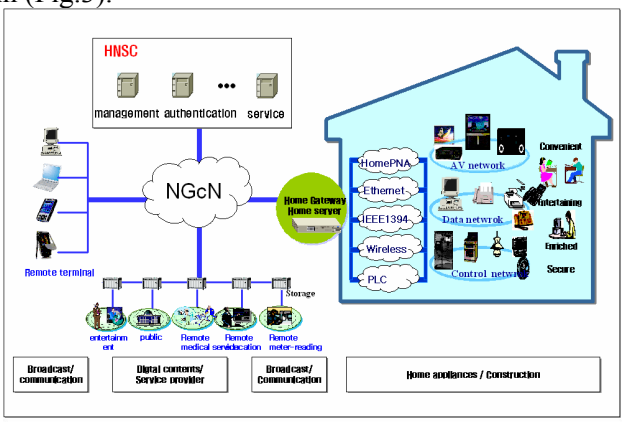

Fig. 3 Components of a home network service

(3) Identifying Transmission Technology of Home Network Service

Communication technologies used in a home network service are divided into cable network communication technologies and wireless network communication technologies as shown in [Table 3].

Table 3. Transmission Technology of Home Network Service

Category		Description
Cable Network	Ethernet	Connects home servers
	Phone Line	Uses existing phone cables
	Power Line	Uses home power cables
Wireless Network	Home RF	2.4Ghz radio frequency
	WLAN	IEEE 802.11b
	Blue Tooth	2.4Ghz radio frequency

3.2 Stage 2 : Analyzing the Threat and Vulnerability of the Target of Evaluation

(1) Types of Security Threats and Vulnerabilities of Home Network Service

(Figure 4) shows the type of security threats and vulnerabilities that may occur in components and transmission technologies of a home network service[6][7][8].

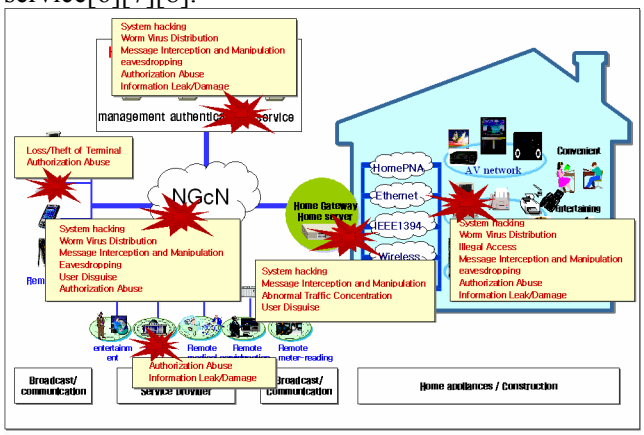

Fig. 4 Types of Security Threats and Vulnerabilities Example

3.3 Stage 3 : Deriving Information Security Pre-Evaluation Criteria

In stage 3, security requirements and specific evaluation criteria for each component are derived using the result of analyzing the probable threats and vulnerabilities (result of stage 2) for the identified components (result of stage 1).

(1) Deriving Security Requirements

[Table 4] shows the security requirements derived according to the type of threats and vulnerabilities analyzed earlier

.

Table 4. Security Requirements

Types of Threats and Vulnerabilities	Security Requirements
Loss/Theft of Terminal	○ Increase terminal management, set user login password
Message Interception and Manipulation	○ Data encryption, VPN
User Disguise	○ Data encryption
Abnormal Traffic Concentration	○ Auto prevention of harmful traffic
Illegal Access	○ Intrusion prevention, detection
Authorization Abuse	○ User/Device authentication, access control
Worm Virus Distribution	○ Vulnerability diagnosis, virus detection
Information Leak/Damage	○ Storage data encryption

(2) Deriving Pre-Evaluation Criteria for Each Component

In this section, the pre-evaluation criteria are derived from the security requirements for the threats and vulnerabilities of each component. [Table 5] shows an example of pre-evaluation criteria that must be applied for each component of the home network service. The criteria are divided into physical, technical and administrative criteria for each component.

Table. 5 Deriving Pre-Evaluation Criteria for Each Component

Component	Security Area	Pre-Evaluation Criteria
Remote Terminal	Physical	○ Prevent loss and theft by storing terminals in locations where unauthorized access is restricted
	Technical	○ Use login passwords ○ Use user authentication ○ Use security solutions such as access restriction and virus vaccines ○ Security patch and OS upgrade
	Administ-rative	○ Maintain terminal management book ○ Enhance management of login password and authentication data
NGcN	Physical	○ Restrict unauthorized access for connection lines and main network equipment
	Technical	○ Use data encryption and VPN ○ Prepare plans for auto preventing harmful subscriber traffic ○ Use anti-hacking solutions such as intrusion prevention and detection ○ Prepare anti-virus plans such as virus prevention system
	Administ-rative	○ Conduct regular vulnerability checks on the network system ○ Network system patch and upgrade

3.3 Stage 4 : Applying the Pre-Evaluation Criteria

In stage 4, the result of stages 1 through 3, the pre-evaluation criteria is applied to the home network service. The criteria should be applied sequentially starting from the planning and designing stage of developing a home network service. As mentioned earlier, security problems that may occur otherwise can be prevented by applying the criteria at the initial stages of developing a service.

4 Conclusion

With the rapid growth of wired/wireless communication technology, network environments are evolving from a single service network to a broadband convergence network[1][2]. Accordingly, IT services that used to be operated in a single network are quickly being converged and created into new services on a broadband convergence network. However, without proper security measures, such convergence of services will be vulnerable to electronic intrusions, which can cause extensive damage.

Such security issues in convergence IT services have surfaced through trial services, and the market is in urgent need of countermeasures.

This paper has proposed an information security pre-evaluation model as a method of guaranteeing the security and reliability of converged IT services that will be operated in a broadband convergence network. In addition, the feasibility of the model is validated by applying it to a home network service.

Numerous new convergence IT service will appear as the construction of broadband convergence network progresses. To this end, the method of identifying the target of evaluation and the execution procedure of the

proposed pre-evaluation model need to be further specified and standardized through future studies in order to apply the model to various types of new IT services.

References

[1]"Broadband convergence Network Plan" MIC Korea, 2004
[2] Young-Ro Lee, "Progress and Prospects of BcN Trial Project", TTA 96, 2004.
[3] "Information Security Requirement Analysis on Eight Major Services", ETRI, 2004
[4] IBM Systems Science Institute
[5] "Accomplishments and Plans of Home Network Trial Project", MIC Korea, 2004
[6] Byeong-Gyu Rho, "Intrusion Threats and Action Prospects of Ubiquitous Home Network ", 1st Home Network Security Workshop, 2004
[7] Heung-Ryeol Yeom, "Home Network Security", KRnet2004
[8] KISA, "Home Network Security Vulnerability Analysis", 2004