International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:10, 2007

Study of Measures to Secure Video Phone Service Safety through a Preliminary Evaluation of the Information Security of the New IT Service

DongHoon Shin, Yunmook Nah, HoSeong Kim, Gang Shin Lee, and Jae-Il Lee

***Abstract*—**The rapid advance of communication technology is evolving the network environment into the broadband convergence network. Likewise, the IT services operated in the individual network are also being quickly converged in the broadband convergence network environment. VoIP and IPTV are two examples of such new services. Efforts are being made to develop the video phone service, which is an advanced form of the voice-oriented VoIP service. However, the new IT services will be subject to stability and reliability vulnerabilities if the relevant security issues are not answered during the convergence of the existing IT services currently being operated in individual networks within the wider broadband network environment. To resolve such problems, this paper attempts to analyze the possible threats and identify the necessary security measures before the deployment of the new IT services. Furthermore, it measures the quality of the encryption algorithm application example to describe the appropriate algorithm in order to present security technology that will have no negative impact on the quality of the video phone service.

***Keywords*—** BcN, Security Measures, Video Phone.

I. Introduction

THE recent rapid advance of communication technology is evolving the network environment into the broadband convergence network [1][2]. Likewise, the IT services that have been operated in the individual network until now are also being quickly being converged and combined in the broadband convergence network environment.

However, the new IT services will be subject to stability and reliability vulnerabilities if the relevant security issues are not answered during the convergence of the existing IT services being operated in individual networks within the wider broadband network environment [3]. Enterprises developing new services using the rapidly evolving information technologies often overlook the issue of service safety in their hurry to launch a new service before their competitors. In such cases, the security threat will only be increased as a result of safety and reliability degradation, and the ensuing intrusion accidents occurring during service operation can incur high costs during service recovery. Studies have indicated that the cost of resolving security flaws is higher during the implementation and testing phase than during the design phase, and that the cost of resolving any flaws discovered during the service operation phase is likely to be 60 to 100 times that of the design phase [4].

Furthermore, if such threats have a negative impact on service quality, the enterprise in question can quickly fall behind amidst the overheated market competition. Bearing such a background in mind, this paper analyzes the possible threats to the video phone service and presents the necessary security measures using an information security preliminary evaluation methodology which is capable of identifying and applying the necessary information security factors from the development phase of new IT services. It also describes the measures required to analyze the impact of applying the security technology, primarily the encryption technology that could affect service quality, to the QoS.

Manuscript received September 29, 2007.

DongHoon Shin, Hoseong Kim, Gang Shin Lee and Jae-Il Lee are with the Korea Information Security Agency, Seoul, Korea (corresponding author to provide phone: +82-405-5272; fax: +82-405-5219 e-mail: dhshin@kisa.or.kr).

Y. Nahis is with Dankook University, 147 Hannam-ro, Yongsan-gu, Seoul, Korea.

II. Related Work

A. TCSEC (Trusted Computer System Evaluation Criteria)

In 1983, the NCSC (National Computer Security Center) of the USA produced the TCSEC draft, otherwise known as the "Orange Book", as the standard by which to assess the safety of computer systems. Two years after that, it was adopted as the Department of Defense standard (DoD STD 5200.28). TCSEC classifies a computer system into 6 levels (C1, C2, B1, B2, B3 and A1) in order to effectively evaluate system security and distribute only those computer systems whose safety and reliability have been proven. TCSEC particularly emphasizes the confidentiality of the security factors. The basic security requirements include: ① security policy; ② marking of the security level; ③ identification; ④ accountability of security; and ⑤ assurance that the security policy, marking, identification and accountability have been applied.

B. ITSEC (Information Technology Security Criteria)

In May 1991 the European countries of France, Germany, the UK and the Netherlands combined each country's security standard and announced the draft version of the ITSEC as the common security evaluation standard for the IT systems. These countries developed the ITSEC in order to bring down the trade barrier between the countries and to use it as the basic standard and guidance for testing. The security functional requirements of the ITSEC are basically divided into security functional standards and assurance requirements. The security functions of the ITSEC are grouped into 3 abstract levels, namely security goal, security function and security system, as well as the 8 basic functions of identification and authentication (the most important aspect of security guidance), access control, recording, audit, object reusability, accuracy, service reliability, and data exchange. The assurance standard includes the guidance concerning the accurate implementation of the security function specified by the system and the guidance concerning the effectiveness of the security function and the security system developed during the system evaluation phase.

C. CC (Common Criteria)

CC is an international standard developed by the security product and system evaluation agencies and R&D staff of different countries. A project to produce a single international standard (CC: common criteria) was begun by the authors of CTCPEC, FC, TCSEC and ITSEC in June 1993, and the official version was announced in January 1996. In Korea, the Korea Information Security Agency revised the Introduction to Information Security announced in 2000 and announced Version 3.0 in 2007. CC seeks to eliminate the waste of resources incurred by duplicated evaluation by unifying the evaluation standards used independently by each country into a single standard. It supports all the viewpoints of the developers, evaluators and users, and provides a rich source of information about systems and products.

D. BS7799

BS7799 was developed by major British companies such as BT, HSBC, Marks and Spencer, Shell International and Unilever under the guidance of the Ministry of Trade and Industry. It is intended for use as a universal reference document - going under the title of The A Code of Practice for Information Security Management - for personnel who have the responsibility to implement and maintain the information security of an organization. It was prepared to be used as the basis for the security standard of those enterprises. BS7799 focuses on publicly verifying that the enterprise assures the confidentiality, integrity and availability of the customer information and can be used both as guidance and as a recommendation for security

E. Trend in QoSS Studies

DARPA Quorum of the US has recognized that the network can be efficiently managed using the variant security in a part of the project to deploy an efficient resource management system (RMS) in order to effectively control armed forces scattered around the world as units of the army, navy and air force, and to dynamically and quickly cope with military conflicts. It used the term QoSS (Quality of Security Service) [5] to represent the different levels of security service quality. The organization is continuing with its study of components, user interface, prototype development of the actual system, and expected benefits.

III. Methodology of Preliminary Diagnosis of Information Security for New IT Services (KISA)[6]

A. Overview

- definition of Methodology

A series of procedures designed to: 1) analyze the potential technical, physical and managerial threats and vulnerabilities by identifying the service characteristics during the service planning and design phase before the actual operation of a new IT service; 2) deduce the essential security requirements; and 3) present security measures in order to prepare the advance safety management system of a new service.

- Evaluation Subject

The subjects of an information security preliminary evaluation model are the components of a new IT service and the wired/wireless communication technologies applied to that service.

B. Information Security Preliminary Evaluation Procedure

The procedure for the evaluation of the information security preliminary evaluation model in order to apply the security measures before the service development and operation phase is shown in (Fig. 1) below.

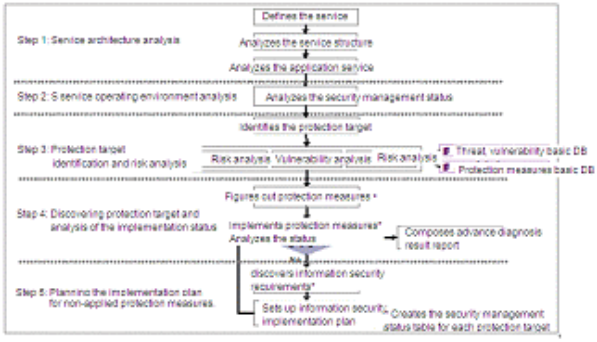

Fig. 1 Preliminary Diagnosis Process

The above diagram shows the internal evaluation step as performed by the service provider and the consulting step performed by an outside consulting company. During steps 1 to 3, the service characteristics as well as the information security vulnerability and other threats are analyzed and the necessary information security measures are identified. Once these steps have been completed, the results of the review of the service characteristics analysis, the results of the information security vulnerability and threat analysis, and the information security measures are performed by outside consultants to supplement

the results of each step. During steps 4 and 5, the detailed implementation plan and testing plan are prepared for each information security measure, and the information measures are implemented in accordance with the implementation plan; thereafter, the implementation is verified by carrying out testing in accordance with the testing plan. Once these steps have been completed, the implementation and testing results are reviewed by the external consultants in order to verify the implementation once again. The results of the review by the external consultants are used as feedback for the previous steps to complement any inadequate areas of information security. External consulting can be performed again if needed after the revision.

IV. Preliminary Diagnosis of U-Service with Video Phone Service

A. [Step 1] Service Architecture and Environment Analysis

The video phone service under the BcN network can be described as follows.

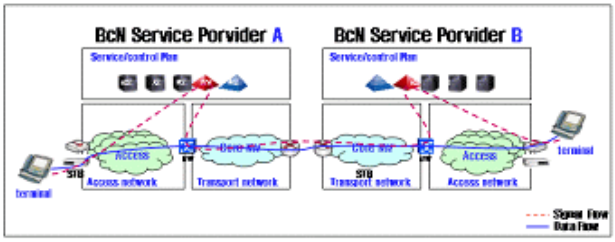

Fig. 2 Video phone service architecture on BcN

As shown in the diagram below, the video phone service is a BcN-based convergence service and must be delivered regardless which of the various access networks the user terminal is connected to. As the call must be connected to the terminal of another carrier, a network link between the carriers is required.

B. [Step 2] Security Subject Identification and Threat Analysis

The main systems for connection control data processing and data transfer to provide the video phone service can be identified as shown in the following table.

TABLE I
Video Phone Service Component

	component	protocol
Singal	SoftSwitch, IMS, SIP Sever	SIP
Data	STB, MPLS Router, GW, DNS, DHCP	TCP/IP, UDP, RTP/RTCP

Signal control systems such as the soft switch, IMS and SIP server perform the function of receiving the video phone signals (call request message, etc) from the user and processing them.

Data transfer systems such as STB deliver the terminal processed video phone call packets to the IP network. The MPLS router and gateway transfer the video phone IP packets by linking the different subscriber networks and carriers. DNS and DHCP manage the IP address resources of the video phone terminal.

The components of the video phone service entail the following threats or vulnerabilities [11].

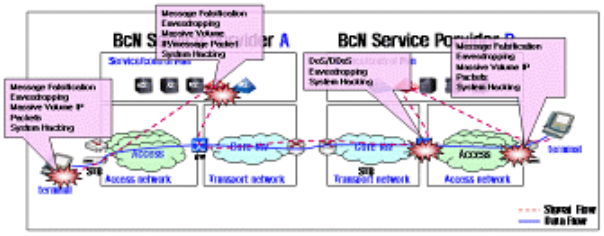

Fig. 3 Threats or vulnerabilities of video phone service

C. [Step 3] Deduction of Security Measures to Reduce the Threats

The following table shows the countermeasures required for each threat in order to prevent intrusion incidents against the components identified in Step 2.

TABLE II
Security Measures

Threat	Security Measures
Subscriber Registration Message Falsification	o Control of system access by ACL configuration, IP filtering, firewall, etc.
	o User authentication using ID/password authentication, PKI based authentication and MAC address authentication technology
	o Encryption of subscriber registration message - Encryption of session layer using SSL and TLS, encryption of transfer layer using IPSec, etc.
Eavesdropping by session hijacking on the Subscriber Network Link Zone	o Encryption of section control message - Encryption of session layer using SSL and TLS, encryption of transfer layer using IPSec, etc.
Infusion of QoS Altered Packet into the Network Transfer Equipment	o Control of system access by ACL configuration, IP filtering, firewall, etc. o Control of unauthorized users using high quality through user profile-based QoS control and others
	o Control of excessive abnormal QoS traffic through QoS resource and traffic monitoring - QoS class usage monitoring
Transfer of Massive	o Control of system access by ACL

Connection Request Messages	configuration, firewall, ALG, etc, in the system
	o User authentication using ID/password authentication, PKI based authentication and MAC address authentication technology
	o Resource and traffic monitoring and control of number of connection requests in a certain period
Transfer of Massive Volume IP Packets	o Control of system access by ACL configuration, firewall, ALG, etc, in the system
	o Resource and traffic monitoring
Transfer of Connection Termination or Complement Messages	o Control of system access by ACL configuration, firewall, ALG, etc, in the system
	o User authentication using ID/password authentication, PKI based authentication and MAC address authentication technology
DiffServ Resource Stealing	o Control of system access by ACL configuration, firewall, ALG, etc, in the system o User profile-based QoS control
	o User authentication using ID/password authentication, PKI based authentication and MAC address authentication technology
	o QoS resource and traffic monitoring, QoS class usage monitoring, etc.
System Configuration Error	o Control of system access by ACL configuration, firewall, ALG, etc, in the system
	o User authentication when connecting to the major system o Use of more secure protocol and authentication when remotely connecting - Administrator connection using SNMPv3 or HTTPS and ID/password and OTP authentication, etc.
	o Change of default values such as the administrator mode password when installing the major system o Execution of the latest updates and security patch after system installation o Preparation of the enterprise security policy and periodic audits
Remote Connection Protocol Vulnerability	o Control of system access by ACL configuration, firewall, ALG, etc, in the system
	o Use of more secure protocol and authentication when remotely connecting - Use of HTTPS and ACS/TACACS+ authentication, etc.
	o Encryption of the transfer data when remotely connecting - Transfer of the data through SSL
	o Maintenance of the latest updates and security patches for the operating system and application programs o Preparation of the enterprise security policy and periodic audits
Operating System and Application Vulnerability	o Control of system access by ACL configuration, firewall, ALG, etc, in the system
	o Maintenance of the latest updates and security patches for the operating system and application programs, and removal of unnecessary services o Auditing of unauthorized processes and logs in the major system o Preparation of the enterprise security policy and periodic audits

In order to increase the effectiveness of the information security preliminary evaluation, the identified security measures will be reviewed by information security experts.

D. [Step 4] Detailed Security Measure Implementation Plan and Testing Plan

The detailed implementation plan of the security measures established in the previous 3 steps has been prepared. In addition, a testing plan to verify whether the security measures are being properly implemented has also been prepared. Examples of the implementation plan of the security measures established in the previous 3 steps are described as follows.

TABLE III
IMPLEMENTATION PLAN

Threat	Security Measures	implementation plan
Registration Hijacking	o HTTP Digest authentication o IPSec o TLS o S/MIME	o User authentication using HTTP Digest authentication o Message encryption using TLS, S/MIME and IPSec in order to protect message confidentiality
Seesion message Falsification		
SIP INVITE flooding		
Cancel/bye attack		
RTP SSRC Collision	o SRTP(Secure	o Application of SRP encryption and

RTP flooding	RTP)	authentication for RTP and RTCP (STRP Standard: RFC 3711)
RTCP Insertion		
Eavesdropping		

E. [Step 5] Security Measure Implementation and Testing Result Analysis

The impact of applying the encryption protocol (originating from the authentication and encryption technology presented in the previous 4 steps) to the RTP in order to protect the media data to the service quality is analyzed.

(1) Measurement of Jitter

Jitter in the case of not encrypting the RTP video phone data packet and in the case of applying the DES, 3DES, SEED or AES encryption was tested as shown in the figure below.

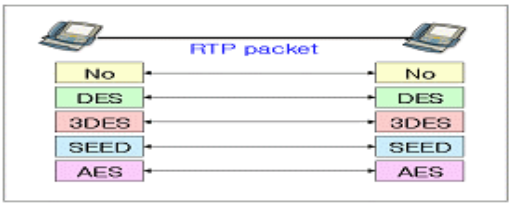

Fig. 4 Encryption was tested on jitter

The result shows the percentage of packets arriving within a 50msec delay time. As shown in the table, applying no encryption yielded the best result, while applying the 3DES encryption yielded the worst.

TABLE IV
MEASUREMENT OF JITTER

algorithm	Ave. jitter (50msec or under)
No encryp.	98.50 %
DES	98 %
3DES	94.06 %
SEED	98 %
AES	95.59 %

(2) Measurement of Delay

Delays in the case of not encrypting the RTP video phone data packet and in the case of applying the DES, 3DES, SEED or AES encryption were tested as shown in the figure below. Rather than measuring the delay in each terminal, the RTT (round trip time) of each packet was measured.

TABLE V
MEASUREMENT OF DELAY

algorithm	Ave. Delay
No encryp.	0.18286 sec
DES	0.21200 sec
3DES	0.20189 sec
SEED	0.19768 sec
AES	0.20739 sec

Applying no encryption yielded the lowest delay, while applying the DES encryption algorithm yielded the highest. The delay was measured with an RTP payload of 132 bytes. The times needed for encryption and decryption were minimal. The test showed that the impact of encrypting/decrypting the video phone packets on the service quality was minor. In particular, the DES, SEED and AES encryption algorithms had minimal impact on the service quality. 3DES, however, indicated a significant impact on the packet processing time. Since the video phone service deals with the real-time data transfer and is very sensitive to the service quality, the encryption/decryption of the transferred packet must have no negative impact on the service quality. That being the case, the use of the 3DES algorithm must be decided upon after assessing its feasibility by measuring the video phone system processing speed and calculation capability.

V. CONCLUSION AND FUTURE STUDIES

The advance of information and communication technology is leading the network infrastructure to evolve towards the broadband convergence network. In Korea, the "Basic BcN Deployment Plan" was finalized by the 22nd Informatization Steering Committee review in February 2004, and the BcN Deployment Project Phase 1 (2004~2005) was initiated in accordance with the plan. Thereafter, the Ministry of Information and Communication announced the "Basic BcN Deployment Plan II" and is carrying out the Phase 2 and Phase 3 BcN Pilot Projects (2006~2010) under the management of the National Information Society Agency (NIA). However, as the BcN infrastructure integrates various networks of different types, it will inherit the security threat inherent to each individual network. The proliferation of damage is also expected to be fast and wide, since the infrastructure integrates the communication/broadcasting/Internet networks and provides a broad bandwidth of 50~100Mbps or higher. Furthermore, the quality sensitive real-time services of voice and image will be passed through the various networks, increasing the possibility that a problem in a single network will threaten the quality degradation of the whole network service.

This paper identified the threats to the video phone service and the relevant countermeasures by applying an information security preliminary evaluation methodology in order to secure the reliability and safety of the video phone service, which is the new IT service to be operated over the BcN. Some of the technologies for the security measures were tested for their impact on service quality in order to describe the appropriate way to apply the technology. Once the BcN has been deployed and stably operated in the future, many new IT services will be introduced. To prepare for the situation, the information security preliminary evaluation methodology described in this paper must be enhanced in order to make it more detailed and

applicable to other different IT services. Furthermore, studies on how to assure the quality of the new services must be continued.

REFERENCES

[1] Basic BcN Establishment Plan II (draft), Ministry of Information and Communication, 2006.3.
[2] Standard BcN Model v2.0, TTA, 2006. 12. 21.
[3] Status of BcN Information Security Technology Development, Korean Society for Internet Information, 2005. 9.
[4] IBM Systems Science Institute.
[5] Cynthia Irvine, Timoty Levin, "Quality of Security Service", pp22-25, DARPA/ITO Quorum PI Meeting, New Orleans, LA May.2001.
[6] DongHoon Shin, "Study of Information Security Pre-Evaluation Model for New IT Service", Korea Information Processing Society, 2005.11.
[7] Status of BcN Information Security Technology Development, ETRI, 2005. 9.
[8] VoIP Security and Privacy Threat Taxonomy, VoIPSA, 2005. 10.
[9] Next Generation Networks and Security: An Introduction, voipsecurity.org, 2005. 4.
[10] TISPAN NGN Security (NGN_SEC) Requirements, NGN Release1 (draft ETSI TS 187 001), 2005.10.
[11] ITU-T FGNGN, http://www.itu.int/ITU-T/ngn/fgngn/