QoS Guaranteed Secure Network Service Realization using Global User Management Framework (GUMF)

- Service Security Model for Privacy

Byeong-Cheol Choi*, Kwang-Sik Kim*, Dong-Il Seo*

* Information Security Research Division, ETRI, Korea
(Tel : +82-42-860-3858; E-mail: corea@etri.re.kr)

Abstract: GUMF (Global User Management Framework) that is proposed in this research can be applied to next generation network such as BcN (Broadband convergence Network), it is QoS guaranteed security framework for user that can solve present Internet's security vulnerability. GUMF offers anonymity for user of service and use the user's real-name or ID for management of service and it is technology that can realize secure QoS. GUMF needs management framework, UMS (User Management System), VNC (Virtual Network Controller) etc. UMS consists of root UMS in country dimension and Local UMS in each site dimension. VNC is network security equipment including VPN, QoS and security functions etc., and it achieves the QoSS (Quality of Security Service) and CLS (Communication Level Switching) functions. GUMF can offer safety in bandwidth consumption attacks such as worm propagation and DoS/DDoS, IP spoofing attack, and current most attack such as abusing of private information because it can offer the different QoS guaranteed network according to user's grades. User's grades are divided by 4 levels from Level 0 to Level 3, and user's security service level is decided according to level of the private information. Level 3 users that offer bio-information can receive secure network service that privacy is guaranteed. Therefore, GUMF that is proposed in this research can offer profit model to ISP and NSP, and can be utilized by strategy for secure u-Korea realization.

Keywords: GUMF, Network Service, QoS, QoSS, U3P

1. INTRODUCTION

Next generation network may become BcN (Broadband convergence Network) that wire/wireless communication and network, Internet is amalgamated. BcN is a network that can use various QoS guaranteed broadband multimedia services by single mobile device. Present security framework can not keep away being killed by spread of cyber threats and growth of new attacks in this network environment, and it can not guarantee warranty of quality of service, network survivability and availability. Therefore, this next generation network needs a new security framework that can offer safety of service, and this is involved with service user's privacy.

Lately, security threats are happening before announcing the patches, and it is the reason that hackers can create quick attack code through reverse engineering. These zero-day attacks usually happen before 30 days after being announced the vulnerabilities. Fig. 1 displays the changes of network security technology by security threats. The intrusion detection technology is changing by intrusion prevention technology recently. [1-4]

- 1st generation (Protection): IDS, Firewall, ESM
- 2nd generation (Mitigation): IPS, L3~7 Switch, VAM (Vulnerability Analysis & Management)
- 3rd generation (Tolerance): Next Generation Firewall and Switches, ISM(Intelligent Security Management), etc

But, this security threats is due to anonymity of Internet, and network security is not escaping this limit yet. That is, present security technology is not reducing intrusion detection's false alarm because of the anonymity of Internet.

Present Internet was a best-effort service that it has user's anonymity and QoS is not guaranteed. However, requirements of end-to-end QoS became many gradually, and various QoS technologies that use RSVP according to special quality of network, IntServ, DiffServ etc. were developed. Lately, flow based switching over MPLS is studied. But, it is limited to realize safe network by this QoS technology. That is, cyber attacks by user's anonymity are indwelled still. Even if we say that current cyber attacks happen because of user anonymity guarantee justly, saying too much is not.

This research proposes next generation network security framework of GUMF (Global User Management Framework) that can analyze problem about user's anonymity of present Internet and solve this. We studies the limitation of packet mode communication way that guarantee existent anonymity considering the security advantages of user's real name or identification of circuit communication way.

Elements of threat in BCN that accomplish base of the ubiquitous environment are as following. Firstly, threat that is happened in frail existent Internet net in cyber attack spreads by each individuation network through broadband integration network and the damage may be connected to telecommunication network, broadcasting network, and USN (Ubiquitous Sensor Network). Secondly, BcN may exist various threats according to the change of IP network such as IPv4 network vulnerabilities, IPv4/IPv6 multi-network vulnerabilities, and IPv6 vulnerabilities. Thirdly, threat of expected discontinuance and so on of normalcy service by network resource exhaustion in USN is expected to be linked to broadband integration network. [5]

Security considerations of threats in ubiquitous network environment are as following.

- Enlargement of survivability and availability guarantee of the network and services
- Necessity of global security policy management framework
- Necessity of security function extension of global network like BcN
- Request of multistage intelligence security functions

Depending on these security requirements, current black security of attack detection, prevention, blocking may be changed by white security technology that it takes a important view that offer safety and reliability about normal user's service from attacker for future ubiquitous information security, and GUMF that is proposed in this research is it.

2. PROPOSED METHOD

GUMF (Global User Management Framework) is composed, and need definition about personal information grade for user level of service judgment by security management Framework, UMS, VNC etc. Fig. 2 explains the concept of GUMF. Usually, present Internet and network offered the simple QoS can assume that is formed in VN-Level 0. Therefore, most cyber attacks that happen current Internet and future ubiquitous network can expect to happen in VN-Level 0, and this may use always normal service if use user's information more than Level 2 to except that user requests service by anonymous user's group. However, some damages happen to users of level 1 when e-ID is stolen by hacker, but this level has robustness against attacks of bandwidth consumption. VN-Level 1 can offer the indirection paths about several attacks that happen in VN-Level 0 through virtual network sharing between Level 0 and Level 1 according to necessity. In this time, flows that have high position priority of VN-Level 0 in QoS viewpoints necessarily can use only extra bandwidth of VN-Level 1. Secure network service channel is offered for normal user except hacker in VN-Level 2 and VN-Level 3.

UMS - User Management System

UMS has the conceptual structure similar to DNS of present Internet, and Root UMS has 1 or more than. We define the domain as network area that Root UMS is installed in. Local UMS is installed by site unit that individual security policy can be applied. UMS operates security information management according to user's grade of registration, preservation, delete etc. Also, it is established so that communication for user information interchange of site or domain unit may be available through working together other UMS.

The following is user grade and required user information that is using in UMS.

- Level 0 : Anonymous user
- Level 1 : Global ID/Password or E-ID user
- Level 2 : Third party authentication user (ex. PKI user authenticated by licensed agency)
- Level 3 : Bio-information user

VNC - Virtual Network Controller

VNC analyzes network flow that end-to-end QoS is offered with user information that is supplied by UMS, is established so that can divide virtual network level and form secure channel and this is structure that existent QoS/VPN and security function are mixed.

We analyzed about structure of GUMF and details of systems so far, and following contents is the operating scenario of the GUMF. This is described with concept of GUMF in Fig. 3. [6]

(1) Self Authentication (User A)
User A does to present own identification and specify user security grade and service target before receive service through network.

(2) User A <-> Local UMS (Site 1)
Local UMS achieves role that sort grade according to user information level by step (1). Here, site means area that can apply single security policy and user's information management is available. Usually, this is LAN or WAN of enterprise network level.

(3) Local UMS (Site 1) <-> Root UMS (Domain 1)
Grade of user information that is supplied in step (2) delivers to root UMS. Here, we define the domain as network area that Root UMS is installed in and root UMS has 1 or more than by country unit.

(4) Local UMS (Site 1) <-> VNC Node (Site 1)
VNC Node selects the level of QoS guaranteed virtual network that appropriates to the user grade in step (2).

(5) Root UMS (Domain 1) <-> Root UMS (Domain 2)
When site 1 and site 2 are situated to different domains, user's information grade is passed through information interchange between root UMS.

(6) Root UMS (Domain 2) <-> Local UMS (Site 2)
User information is supplied to local UMS (Site 2) via user information level in step (3).

(7) VNC Node (Site 2) <-> Local UMS (Site 2)
Level of QoS guaranteed virtual network of VNC Node (Site 2) is decided with information that is supplied in (5).

(8) VNC Node (Site 1) <-> VNC Node (Site 2)
Trusted secure channel between two VNC Nodes that confirm level of QoS guaranteed virtual network that is established step (4) and step (6) is formed.

(9) Communication Process (User A <-> Server B)
User A and server B are communicated with trust channel that is formed by step (7), and secure QoS guaranteed service of level that user wants is offered.

Analysis levels of the virtual network

- VN-Level 0
  Anonymity user of user's security level 0 is usable virtual network, and offers anonymity like current internet. All attacks that VN-Level 0 can happen to the current Internet. QoS is offered but the availability, reliability and survivability are not offered.
- VN-Level 1
  e-ID user of user's security level 1 is usable virtual network, and all services can approach and is serviced through e-ID that is individual's global ID. Some damages happen to users of level 1 when e-ID is stolen by hacker, but this level has robustness against attacks of bandwidth consumption.
- VN-Level 2
  Certificated of authentication user of user's security level 2 is usable virtual network, and it is the grade that are guaranteed by reliability and survivability that can respond to almost attack.
- VN-Level 3
  Bio-information user of user's security level 3 is usable virtual network, and it is the grade that are guaranteed by reliability and survivability highly. Because bio-networking is possible that use bio-information in here, it is grade that can provide service that is guaranteed the best survivability such as importance information exchange service between the country to user.

3. APPLYING TO SECURE U-KOREA

GUMF that is proposed in this research does based on governmental e-Korea and IT839 strategy, is expected to propel by main government authorization agenda at centralization of power latter term and use to framework that can solved information dysfunction that can happen in

u-Korea fulfillment that do. [7-9]

Here, local UMS achieves personal information grade management and cyber transaction through U3P (User Profile Protection Provider) agency, and root UMS and legislation may be possible actually if full equipment operates nationalistically through NUMA (National User Management Agency).

If GUMF comes true as national management dimension through this U3P and NUMA, it will be used by u-Korea's point strategy that serve of realization. Also, the effect is expected as following.

- Because it can minimize information dysfunction through secure management of personal information, secure u-Korea realization is possible.
- Also, because good environment realization to promote an undertaking worldwide through secure cyber environment construction is possible, country accreditation and market competitive power elevation are available.
- It can be new profit model of ISP and NSP, and may create profit of 2.4 trillion won in 2010 that BcN comes true.

4. CONCLUSIONS

We proposed the next generation network security framework of GUMF (Global User Management Framework) that can analyze problem about user's anonymity of present Internet and solve this. It is the user's own real-name service framework that is for QoS guaranteed secure network service realization. GUMF consists of core management framework, UMS (User Management System), and VNC (Virtual Network Controller). UMS is very similar to DNS schema and VNC is the combinations of QoS and VPN functions. Levels of virtual network are four. In level 4, we use bio-information for authentication.

We will apply GUMF to secure u-Korea realization using U3P (User Profile Protection Provider) and NUMA (National User Management Agency) - all new organization. This secure u-Korea realization model can give the profits to all of the country, people, and corporation nationalistically.

REFERENCES

[1] Yankee Group's Special Report: "Next-Generation Network Security Requires an Adaptive Approach", 21 September, 2004

[2] Latis Networks White paper: "Beyond the Firewall: The Next Level of Network Security", January 2003

[3] Gartner Group Research Note, "Predicts 2005: Security Focuses on Attack Prevention", 29 October 2004

[4] A White Paper Prepared by Enterprise Management Associates, "Behavioral Analysis Enables a New Level of Network Security Awareness: Network Behavioral Analytics", June 2004

[5] BcN, QoS, IPv6, VoIP, etc., IT DB, http://library.etri.re.kr

[6] UML, Rational Rose Enterprise Edition, http://www.uml.org

[7] Articles of related u-Korea, Electronics Newspaper (p1 and 5), 17 January 2005

[8] J. S. Jang and S. H. Park, "Five Information Security Technologies for Secure u-Korea", IITA Weekly Journal, March 2005, http://www.itfind.or.kr

[9] B. C. Choi, K. S. Kim, D. I. Seo, and J. S. Jang, "Information Security Strategy for Secure u-Korea – Security Belt", ETRI Monthly Journal, April 2005, http://ettrends.etri.re.kr

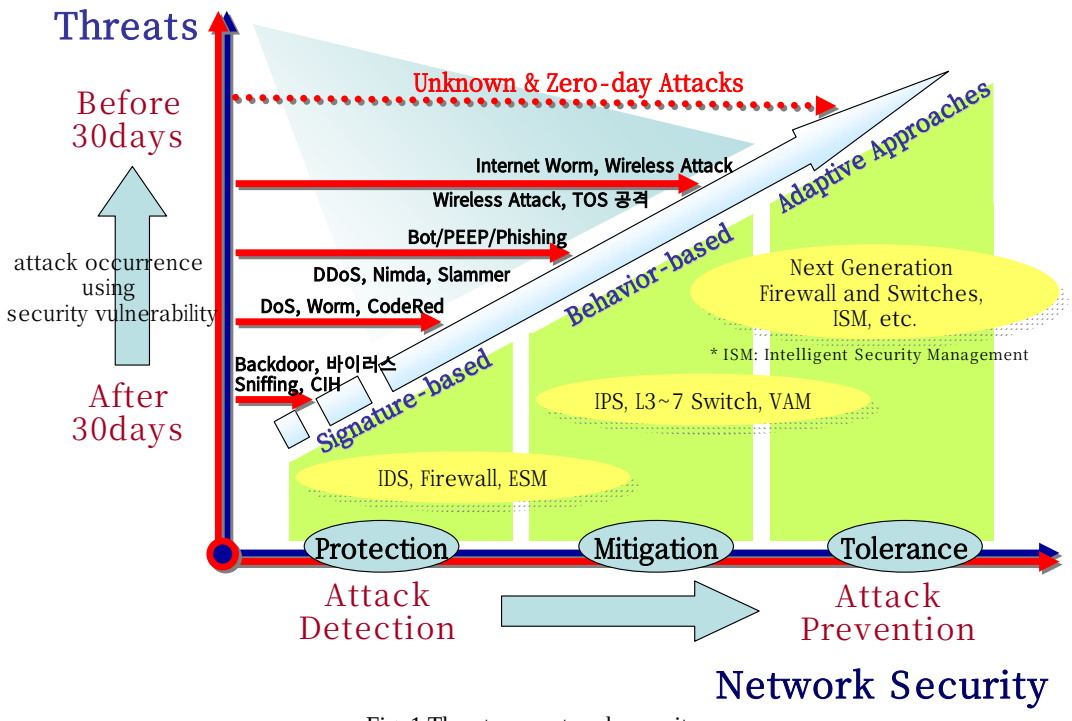

Fig. 1 Threats vs. network security

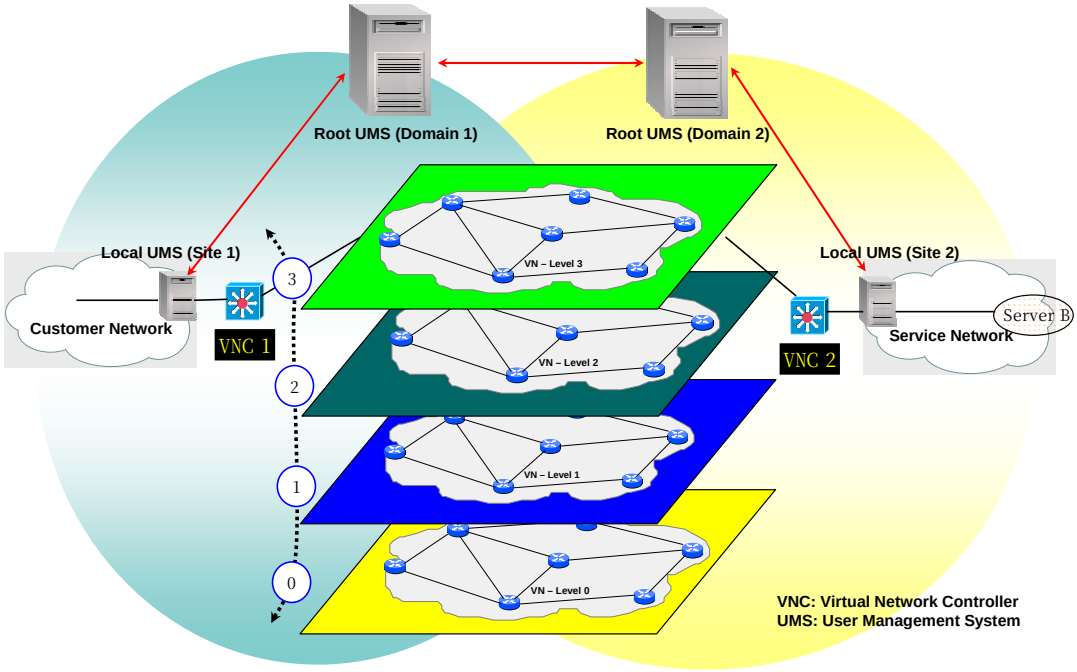

Fig. 2 The concept of GUMF

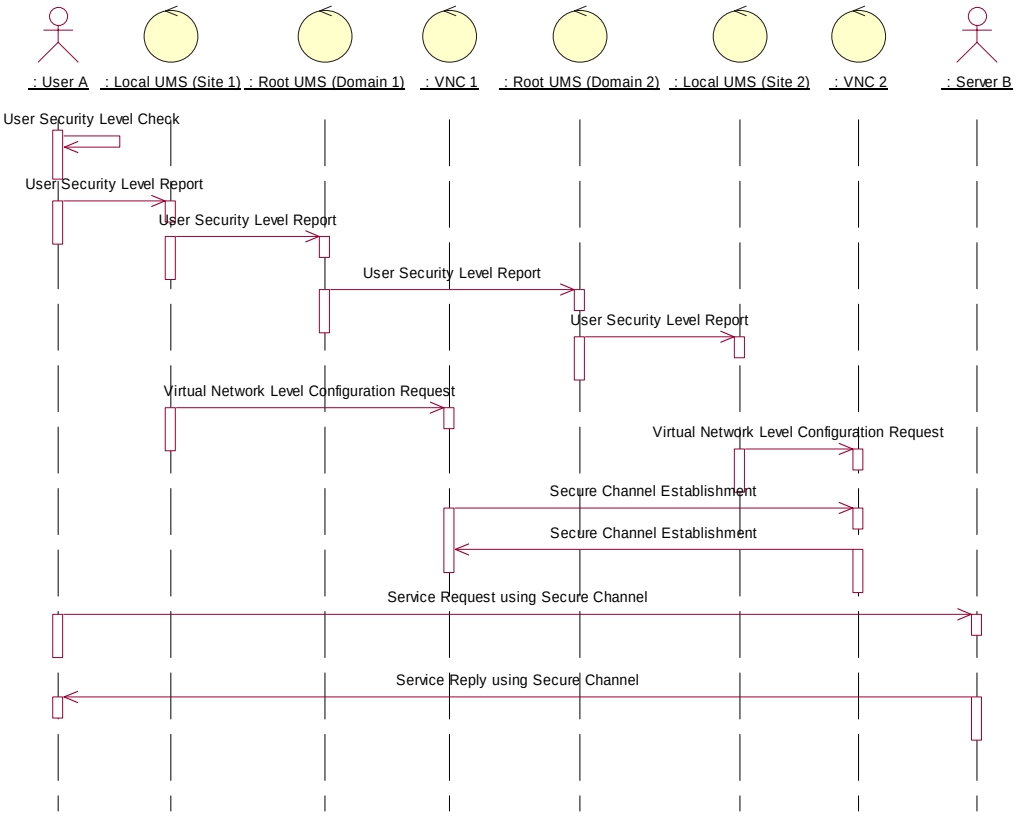

Fig. 3 The operating sequence-diagram of GUMF