Security Measures for the Convergence of Voice and Data in the Broadband Convergence Network

DongHoon Shin, HoSeong Kim, Gang-Shin Lee*
* Korea Information Security Agency
78, Garak-dong, Songpa-gu, Seoul KOREA

Abstract

The Korean government has established 'The Basic BcN (Broadband convergence Network) Plan II', and organized a consortium for its full-scale implementation as part of its attempt to create the ubiquitous society through a mixed and converged service based on the integrated network. The BcN, which interconnects various subscriber networks having such characteristics as PSTN and WCDMA, could potentially affect other subscriber networks if infringement incidents occur in the specific subscriber network. Therefore, the need to secure safety from the BcN network setup stage has emerged as an important issue. Accordingly, this paper analyzes the characteristics of the pilot project that are being executed to establish the BcN in Korea, and the infrastructure and interworking scenario with a focus on PSTN and WCDMA, which is the representative interworking scenario, so that security measures against potential infringement incidents can be proposed.

Key words: Convergence of Voice and Data, BcN, Security Measures

1. Introduction

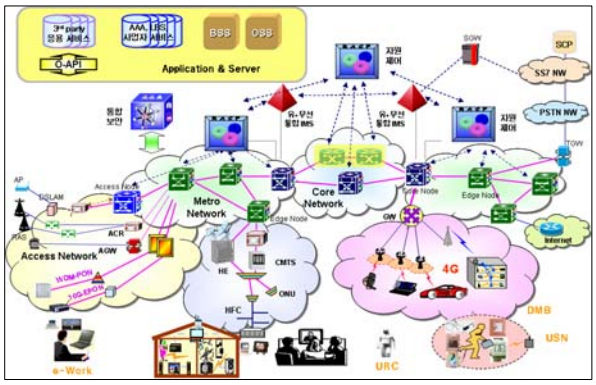
Voice/data, wire/wireless, and communication/ broadcasting services are converging rapidly, as the information and communication technology develops rapidly, leading to an intelligent, converged network infrastructure and fast broadband services. To address this trend, the Korean government set up the "Basic BcN Establishment Plan II" and organized 4 consortiums. Currently, the full-scale implementation of stage 2 BcN establishment projects is being carried out. The BcN focuses on the transmission network, and subscriber networks having various features are interworking within it. Actually, as the BcN consists of an environment that integrates several service providers' networks with an heterogeneous security policy, if any security incident occurs in any component network, it is highly likely to affect the other networks.

Accordingly, this paper analyzes the characteristics of the pilot project that are being executed to establish the BcN in Korea, as well as the infrastructure and the interworking scenario with the focus on PSTN and WCDMA, which is the representative interworking scenario, so that security measures against potential infringement incidents can be proposed.

2. BcN Overview and Status of Pilot Project Implementation

2.1. BcN Overview

According to "The Basic BcN Establishment Plan II," the BcN can be defined as a next-generation integrated network that provides a high quality service at any time and place, as communication, broadcasting, and Internet are converged. Figure 1 shows its structure.



(Fig.1) BcN Overview

The transmission network layer of the BcN is implemented via the core network that connects major cities, and the metro network that connects within the city or between small and medium-sized cities, whereas the subscriber network layer is composed of

the fixed network, the wireless network, and the cable network, as well as an access network composed of the access node to provide the connection of the transmission network among these networks. In addition, efficient control of the network resources, network resource control for call processing and security, wire/wireless integrated IMS and the integrated security platform will be applied, and an open service platform for the provision and application of various services as well as servers for application services will be implemented, and various types of home terminals will be developed for these services.

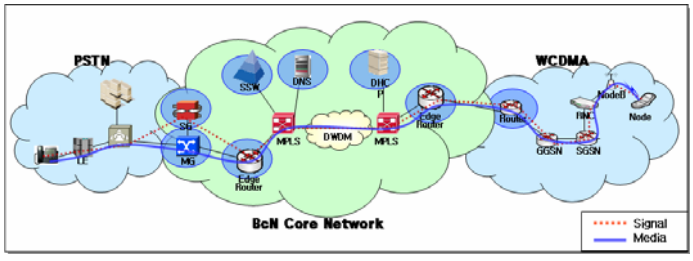
3. Figuring out the BcN interworking Scenario

3.1. Concept of BcN interworking

The BcN provides the service based on interworking between several subscriber networks and service providers. That is, the "interworking" concept in BcN implies that the convergence service is provided by exchanging control information and data among diverse subscriber networks, as well as other items of information such as billing, authentication, and control, in order to provide the service in a network environment composed of the connections between various subscriber networks.

3.2. Scenario of interworking among the voice and data networks

A variety of interworking scenarios could exist. However, this study mainly analyzes the interworking scenario with a focus on the PSTN network and the WCDMA network, which involves interworking between voice and data – the representative interworking scenario. The following figure shows the structure of interworking between PSTN and WCDMA, the signal data for interworking, and the media data flow.



(Fig.2) Interworking among the voice and data networks

The following table shows the call path when a call is made between a PSTN (voice call) service subscriber and a WCDMA (mobile communication) service subscriber. (Original draft: Major equipment for service provision.)

o Signal Data

Segment	PSNT	interworking	Trans-mission	interworking	WCDMA
Node	Telephone	SG ↔SoftSwitch	Router↔ DWDM↔ Router	Router	GGSN↔SGSN↔ RNC ↔NodeB ↔ Node
Protocol	DP, DTMF, SS7	SIGTRAN, MGCP, Megaco, H.323, SIP	SIP	SIP	SIP

o Media Data

Segment	PSNT	interworking	Trans-mission	interworking	WCDMA
Node	Telephone	MG	Router↔ MPLS↔ Router	Router	GGSN↔ SGSN↔ RNC ↔NodeB ↔ Node
Protocol	-	UDP (RTP)	UDP (RTP)	UDP (RTP)	UDP (RTP)

The interworking segment that this paper describes is the subscriber network that provides the end-to-end service and the interface part of the BcN transmission network. It is defined as the area which includes the equipment that converts signals among networks (e.g. soft switch) and the DNS server.

3.3. Identification of the information security target in the BcN interworking segment

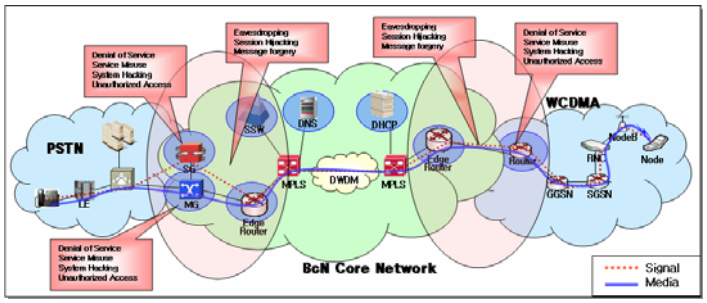
The following table shows the target to protect, while concentrating on the major components for interworking between PSTN and WCDMA.

Protection target		Major function
Soft switch	CSC (Call Session Controller)	oCall connection and session control among subscriber networks -interworking with various application servers and standard interfaces -Provides functions including subscriber authentication and registration, session control and service routing, management of registered subscriber profiles, number analysis and conversion, and SIP/SDP message compression and decompression.
	MGC (MG Controller)	oControls to convert PSTN traffic to packet traffic like IP-based SIP or H.323.
SIP erver	Register (Registra) Server	oSaves the user registration information using the Register message. oProvides information on the access address of the specific user.
	Proxy Server	oWhen the connection request message is received, the connection establishment path is determined, some of the header fields are modified, and then the connection request is processed directly.
	Redirect Server	oProcesses session connection by responding to the client's call establishment request, using a re-direction response that includes the address of the network hop server's address.
Gate way	SG (Signal Gateway)	oControls MG that handles interworking of the media transmission between PSTN and the IP network. oConverts and transmits the line-based traffic between PSTN and the IP network to IP-based SIP

		and H.323 packet traffic.
	MG (Media Gateway)	oConverts and transmits the line-based traffic between PSTN and the IP network to IP-based traffic.
MPLS Router		oTransmits the IP data at the BcN transmission network and the boundary of each subscriber network.

4. BcN Security Threats and Information Security Requirements

Security threats in the interworking segment that were found in the interworking scenario may occur in the interworking equipment itself, the protocol and the media processed by the interworking equipment (system security), and the network connected to the interworking equipment. The following figure shows the potential threats in the interworking segment.



(Fig.3) Security threats in the Convergence of Voice and Data

4.1 BcN security threats

4.1.1 Tapping

o Tapping the control message like signaling: The signaling information can be tapped via sniffing, proving, malicious code insertion, or session hijacking in various sectors including: 1) soft switch ↔ edge router of the BcN transmission network; 2) edge router of the BcN transmission network ↔ edge router of the WCDMA network; and 3) soft switch ↔ MG segment. These tapping activities can lead to a secondary attack such as billing information modification or authentication information modification.

o Tapping the media data: Media information can be tapped via various attack techniques such as sniffing, proving, malicious code insertion, or session hijacking in various sectors including: 1) MG ↔ edge router of the transmission network; 2) edge router of the transmission network ↔ edge router of the WCDMA network; and 3) edge router of the WCDMA network ↔ internal WCDMA network. Media tapping can involve serious infringements against personal information, as voice and video contents are directly exposed.

4.1.2 Denial of service

o The attacker can stop or deactivate the inter -working service by exhausting the equipment or line resources, using various methods such as excessive session connection requests, TCP/UDP flooding, transmission of a large volume of abnormal packets, DNS request, or transmitting large amount of illegal spam data in several segments, including: 1) soft switch ↔ edge router of the transmission network; 2) edge router of the transmission network ↔ edge router of the WCDMA network; and 3) soft switch ↔ MG segment.

4.1.3 Message forgery and alteration

o The attacker can forge or alter the signal information transmitted between the 1) soft switch ↔ edge router of the transmission network, 2) edge router of the transmission network ↔ edge router of the WCDMA network, and 3) soft switch ↔ MG segment, via hacking activities against the interworking equipment such as soft switch, MG, and edge router. These attacks can also modify billing information and user authentication information, and cause malicious information display on the user's terminal.

4.1.4 Illegal access

o The attacker can access the interworking equipment illegally without normal authentication, using various attack techniques such as spoofing and session hijacking against the interworking equipment including soft switch, MG of the WCDMA network that converts and/or transmits signals and media in the interworking segment, and by taking advantage of a configuration error in the interworking equipment, such as an absence of user authentication, terminal authentication, and the mutual authentication mechanism of the interworking equipment. Such attacks can lead to illegal service use, illegal manipulation of interworking equipment, information disclosure or damage against the subscriber and billing data saved in the interworking equipment, and exploitation as the base for a third party attack.

4.1.5 System hacking

o The attacker can exploit system OS and application program vulnerabilities, which are caused by the insufficient use of security patches, insufficient access control and authentication function, errors in system parameter setting, and the use of a vulnerable protocol in major interworking equipment including soft switch, MG, BcN transmission network, and edge router of the WCDMA network, in order to infiltrate the Interwork system, invalidate the interworking equipment function, disclose and damage information, insert or distribute malicious programs, and exploit it as a base for third party attacks.

5. Preventive Measures against BcN Infringement Incidents

The following table shows information security measures against threats that can occur in the major equipment located in the BcN interworking segment.

Threat	Attack technique	Security measures
Tapping	o Sniffing o Session hijacking o Proving o Malicious code insertion	o Signaling data encryption o Media data encryption o Audit and countermeasures against malicious codes and unauthorized processes
Denial of service	o Excessive session connection request o TCP SYN Flooding o UDP Flooding o Large amount abnormal packet transmission o Excessive DNS query	o Unauthorized data access control o Signaling and media data authentication o Resource use amount control o Network and system resource monitoring error response
Message forgery and alteration	o Session hijacking o Spoofing o Proving o System hacking o Malicious code insertion	o Provides integrity of the stored data o Provides integrity or encrypts the transmission data o Audit and countermeasures against malicious codes and unauthorized processes
Illegal access	o IP address spoofing o Session hijacking o Authentication detour o Replay attack o IP spoofing o Access control detour	o User's mutual authentication for access to the interworking equipment o Mutual authentication of the terminal interworking equipment o Unauthorized data access control
System hacking	o Worm/Virus o Malicious code insertion like backdoor o Access control detour o Authentication detour o Exploiting protocol vulnerabilities o Exploiting S/W deficiency o Exploiting OS	o System access control o Proper system parameter configuration o Security patches for systems and application programs o Audit and countermeasures against malicious codes and unauthorized processes o System monitoring and coping with the fault

5.1 Preventive measures against tapping threats

5.1.1 Signaling and media data encryption

o Signaling data such as H.323 and SIP should be encrypted between the interworking segment soft switch and WCDMA network; this can be achieved by using a security protocol such as TLS and IPSec in the interworking equipment, or the VPN solution which provides a separated encryption function.

o The MG (Media Gateway) control message should be encrypted between the interworking segment soft switch or IMS and MG, which can be achieved by security enhanced Megaco/H.248.

o The media data needed for voice or video call should be encrypted between the interworking segment MG and the edge router of the WCDMA network, or the networks inside the WCDMA network; this can be achieved by using a security protocol such as SRTP (Secure Real-Time Transport Protocol) for the MG or the equipment inside the WCDMA network, or by using an encryption solution that provides a separate encryption function.

5.1.2 Audit and countermeasures against malicious codes and unauthorized processes

o A comprehensive management activity plan should be established and operated to counter malicious codes and unauthorized processes.

o A regular malicious code check and activated process check should be executed for soft switch, IMS and MG in the interworking segment, so that the activity of the unauthorized program can be monitored.

o Once a malicious code has been found, it should be removed immediately. Or, if the unauthorized program is found, it should be stopped immediately and the starting time of the program concerned should be investigated; then, additional data disclosure should be checked according to the pre-defined procedure.

5.2 Preventive measures against the denial of service

5.2.1 Unauthorized data access control

o Soft switch, MG, and IMS in the WCDMA network should be able to block unauthorized address, protocol, and abnormal packet via filtering and other methods.

o Soft switch, MG, and IMS in the WCDMA network should be able to block data that is not related to the ongoing call connection status and the caller information via filtering and other methods. This can be implemented by other solutions such as firewall or SBC (Session Board Controller).

o Soft switch, MG, and IMS in the WCDMA network should prevent external attackers from accessing major interworking equipment using network covert techniques like the private network.

5.2.2 Signaling and media data authentication

o Soft switch, MG, and IMS in the WCDMA network should be able to perform authentication in order to secure effectiveness while keeping the status information on the ongoing call or newly established call, and block the data without the authentication information via filtering and other methods.

5.2.3 Resource use amount control

o Soft switch, MG, and IMS in the WCDMA network should define and operate the threshold value for the maximum number of sessions, call generation amount

per unit of time, disk use amount, number of processes, and memory space in consideration of system performance and bandwidth, in order to maintain normal service.

- o Soft switch, MG, and IMS in the WCDMA network should consider operation of the method to keep services running smoothly (e.g. processing by priority of each service, and rate limit setting for each service, etc).
- o Soft switch, MG, and IMS in the WCDMA network should be able to trace, limit, and investigate the future responsibility regarding single numbers that generates excessive calls.
- o The edge router in the BcN transmission network and the WCDMA network should process excessive traffic properly to secure the viability of the system.
- o The edge router in the BcN transmission network and the WCDMA network should maintain a minimum service even when traffic is concentrated.

5.2.4 Network and system resource monitoring error response

- o The system should be monitored using the network management system or the security system (number of maximum sessions, CPU, disk, and memory usage amount, bandwidth usage amount, etc.), so that the proper service can be maintained.
- o When the service cannot be provided due to resource exhaustion of the interworking equipment, errors should be analyzed and the response procedure should be carried out according to the service recovery procedure.
- o Infiltration via the traffic coming through the interworking equipment should be detectable, and proper measures should be taken to prevent system error once infiltrated.
- o A close linkage and joint response system should be established and operated among the service providers that are related with the interworking equipment, so that service can be provided smoothly and prompt action can be taken against the error.

5.3 Preventive measures against message forgery and alteration

5.3.1 Provides integrity of the stored data

- o Soft switch, MG, and IMS in the WCDMA network should be able to check the integrity of the saved data – which is needed for call processing – using the keyed hash method or other methods, if necessary.

5.3.2 Provides integrity or encrypts the transmission data

- o Signaling data such as H.323 and SIP should be encrypted between the interworking segment soft switch and the WCDMA network; this can be achieved by using a security protocol such as TLS and IPSec in the interworking equipment, or by a VPN solution that provides a separated encryption function.
- o The MG (Media Gateway) control message should be encrypted between the interworking segment soft switch or IMS and MG; this can be achieved through a security enhanced Megaco/H.248.
- o The media data needed for voice or video call should be encrypted between the interworking segment MG and edge router of the WCDMA network or the networks inside the WCDMA network; this can be achieved by using a security protocol such as SRTP (Secure Real-Time Transport Protocol) for the MG or the equipment inside the WCDMA network, or using an encryption solution that provides a separate encryption function.

5.3.3 Audit and countermeasures against malicious codes and unauthorized processes

- o A comprehensive management activity plan should be established and operated to counter malicious codes and unauthorized processes.
- o A regular malicious code check and activated process check should be executed for soft switch, IMS and MG in the interworking segment, so that the activity of unauthorized programs can be monitored.
- o Once a malicious code has been found, it should be removed immediately; or, if an unauthorized program is found, it should be stopped immediately and the starting time of the program concerned should be investigated. Then, additional data disclosure should be checked according to the pre-defined procedure.

5.4 Preventive measures against illegal access

5.4.1 Physical protection of the interworking equipment

- o Physical access control should be applied to spaces installed with the interworking equipment, and the access control details should be logged.

5.4.2 User's mutual authentication for access to the interworking equipment

- o Soft switch, IMS, and MG in the interworking segment must mutually authenticate the user who attempts to access the system directly or via the network, using the challenge-response protocol before providing the service. In this case, the interworking equipment can directly

handle authentication, or authentication can be implemented using an authentication protocol such as Diameter or Radius.

- o When minimum security is applied to call processing interworking equipment such as soft switch or IMS, the default user authentication information must be changed. The password should be longer than 8 characters using a combination of numbers, special characters, and alphabets, and should be changed regularly.
- o The interworking equipment should not be managed remotely as much as possible. When remote management is carried out, user access control and identification checks should be strictly applied.

5.4.3 Mutual authentication of the terminal interworking equipment

- o Soft switch, IMS, and MG in the interworking segment must mutually authenticate a terminal that accesses for provision of the service using the challenge-response protocol before providing the service.
- o Call processing interworking equipment such as soft switch or IMS should operate the appropriate mutual authentication mechanism, so that malicious users cannot use the equipment abnormally through abnormal methods like copy or theft.

5.4.4 Unauthorized data access control

- o Soft switch, MG, and IMS in the WCDMA network should be able to block unauthorized address, protocol, and abnormal packet via filtering and other methods.
- o Soft switch, MG, and IMS in the WCDMA network should be able to block the data that is not related to the ongoing call connection status and the caller information via filtering and other methods. This can be implemented by other solutions such as firewall or SBC (Session Board Controller).
- o Soft switch, MG, and IMS in the WCDMA network should prevent external attackers from accessing major interworking equipment using network covert techniques like the private network.

5.5 Preventive measures against system hacking

5.5.1 System access control

- o Soft switch, MG, and IMS in the WCDMA network should be able to block unauthorized address, protocol, and abnormal packet via filtering and other methods.
- o Soft switch, MG, IMS, and the edge router should be able to prevent the data from being sent to the unauthorized destination via itself, using the filtering method or other methods.
- o Soft switch, MG, and IMS in the WCDMA network should prevent external attackers from accessing the major interworking equipment using network covert techniques like the private network.

5.5.2 Proper system parameter configuration

- o The default parameter setting value that is related with the security attribute of the interworking equipment OS should be examined and set appropriately for usage.

5.5.3 Security patches for systems and application programs

- o Soft switch, MG, IMS, and edge router should regularly check the security patch status of systems and application programs, and keep them up-to-date.

5.5.4 Audit and countermeasures against malicious codes and unauthorized processes

- o A comprehensive management activity plan should be established and operated for malicious codes and unauthorized processes.
- o A regular malicious code check and activated process check should be executed for soft switch, IMS and MG in the interworking segment, so that the activity of unauthorized programs can be monitored.
- o Once the malicious code has been found, it should be removed immediately; or, if an unauthorized program is found, it should be stopped immediately and the starting time of the program concerned should be investigated. Then, additional data disclosure should be checked according to the pre-defined procedure.

5.5.5 System monitoring and coping with the fault

- o The system should be monitored using the network management system or the security system (number of maximum sessions, CPU, disk, and memory usage amount, bandwidth usage amount, etc.), so that the proper service can be maintained.
- o When the service cannot be provided due to resource exhaustion of the interworking equipment, errors should be analyzed and the response procedure should be carried out according to the service recovery procedure.
- o Infiltration via the traffic coming through the interworking equipment should be detectable, and proper measures should be taken to prevent system errors when infiltrated.
- o A close linkage and joint response system should be established and operated among service providers that

are related with the interworking equipment, so that the service can be provided smoothly and prompt action can be taken against any error.

- The occurrence of an infringement incident should be detected immediately and responded to via regular vulnerability and worm/virus checks against systems and networks.

6. Conclusion

Voice/data, wire/wireless, and communication/ broadcasting services are converging rapidly, along with the speedy development of information and communication technology, leading to an intelligent, converged network infrastructure and fast broadband services. The network infrastructure, which is becoming the basis of this process of evolution, is also evolving quickly towards the BcN. To address this trend, many overseas countries are implementing projects to establish the next-generation network environment; likewise, the Korean government has set up the Basic BcN Establishment Plan II.

With BcN, which interconnects various subscriber networks with various characteristics such as PSTN and WCDMA, there is a high possibility that other subscriber networks will be affected when an infringement incident occurs in a specific subscriber network. Therefore, the need to secure safety right from the BcN network setup stage has emerged as an important issue.

Accordingly, this paper analyzed various scenarios of interworking between PSTN (voice network) and WCDNA (wireless data network) among the BcN subscriber networks, in order to identify any major security threats that may occur in the core interworking systems in the interworking segment, and then proposed information security measures against such threats as well as protective measures designed to prevent infringement incidents. It is significant that the paper could lay the foundations for establishing a safe BcN environment as a prerequisite for the promotion of various BcN-based services.

However, it is expected that more threats could materialize as BcN network establishment advances and new IT services appear. Therefore, the interworking equipment protection measures proposed in this paper alone would be insufficient to cope with all the security threats arising in the BcN to be established. To protect BcN information security properly, information security measures for the new BcN service should be added, and countermeasures should be developed from the policy aspect in consideration of the various service provider environments in order to provide the service smoothly, when the service in lined among service providers. In addition, protection measures and an information security check list should be continuously developed for the infrastructure equipment, which will be newly introduced in line with the progress of BcN network establishment.

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]BcN Infrastructure Information Security, Korea Institute of Information Security & Cryptology, 2005. 6.

[5]Basic u-KOREA Plan (2006~2010)(draft), Ministry of Information and Communication, 2006. 3.

[6]Status of BcN Information Security Technology Development, ETRI, 2005. 9.

[7]VoIP Security and Privacy Threat Taxonomy, VoIPSA, 2005. 10.

[8]Next Generation Networks and Security: An Introduction, voipsecurity.org, 2005. 4.

[9]TISPAN NGN Security (NGN_SEC) Requirements, NGN Release1(draft ETSI TS 187 001),2005.10.

[10]ITU-T FGNGN, http://www.itu.int/ITU-T/ngn/fgngn/