주 제

BcN 보안대책

한국정보보호진흥원 이강신, 김호성, 신동훈

차 례

I. 서 론

세계 최고의 정보통신 인프라를 구축하고 있는 우리나라는 앞으로 다가올 유비쿼터스 사회에서도 세계 최고의 정보통신 선도국가로서의 위상을 확보하고 선진한국 건설을 위해 u-Korea를 선포하고 u-IT839 전략을 수립하여 추진하고 있다. BcN (Broadband Convergence Network)은 이러한 u-IT839 전략의 3대 인프라의 하나로서 음성 · 데이터 · 유무선 · 통신 · 방송이 융합되어 언제 어디서나 고품질의 서비스를 제공하기 위한 핵심 인프라인 기반 네트워크 이다.

이러한 BcN 구축을 위해 정부에서는 BcN 1차 시범사업을 통해 국내 주요 통신사와 장비업체들이 참여하는 4개 컨소시움을 구성하여 BcN 기반의 다수의 통합 서비스를 일반가입자에게 시범서비스로 제공하였고 현재에는 2차 시범사업 1차년도 사업이 추진되고 있으며 이를 통해 차세대 멀티미디어 인프라로써의 BcN의 가능성을 제시하고 있다.

음성 · 데이터 · 영상 · 멀티미디어 등 모든 형태의 다양한 정보가 통합 서비스되는 BcN 환경에서 무엇보다도 중요한 것은 서비스 사용자 및 제공자로부터의 안전 신뢰성 확보라 할 수 있을 것이다. 이러한 인식 기반에서 정부에서는 광대역통합망 구축 계획을 수립하고 단계적인 통합망 진화방향과 더불어 정보보호 체계 고도화를 위한 기본계획을 수립하여 추진할 계획에 있다.

BcN의 정보보호는 크게 BcN 인프라 측면과 이러한 인프라 위에서 제공되는 서비스 측면의 두 가지 방향에서 추진되고 있으며, 본 기고문에서는 BcN 인프라 측면에서 다양한 가입자망이 연동되는 경우와 다양한 사업자간 서비스를 연동하는 경우에 발생할 수 있는 정보보호 이슈와 대책들에 대해서 살펴보고자 한다.

II장에서는 BcN 구축 추진현황을 소개하고, III장에서는 BcN의 다양한 음성 · 데이터, 유 · 무선, 통신 · 방송 분야의 대표적인 연동 시나리오 중에서 PSTN과 WCDMA 망을 통하여 서비스를 제공하는 경우에 있어서 시나리오를 제시하고, IV장에서는 연동구간의 주요 보호대상에 대한 위협 및 보호대책을 제시하고, V장에서는 이러한 대책의 보완사항, 향후 추진방향등에 대해서 요약하고, 결론을 맺는다.

II. BcN 구축 추진현황

1. BcN 개요

(1) BcN 정의 및 특성

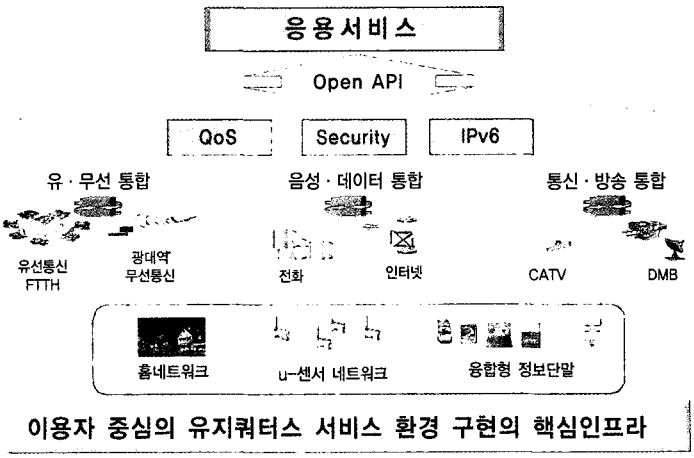
현재, 인터넷 환경은 디지털 정보기술의 급속한 발전으로 음성 · 데이터 · 영상 · 멀티미디어 등 모든 형태의 정보가 다양한 통합 단말 및 서비스를 통해 융합되는 현상 심화되고 있다. 뿐만 아니라, 네트워크 기술의 획기적인 발전으로 그 적용범위가 가전, 자동차, 영상, 콘텐츠, 센서 등 거의 모든 분야로 확대되어 가고 있다. 이에 따라 미래 지식정보사회는 모든 정보단말, 가전기기, 사물 등이 하나의 네트워크에 연결되는 광대역통합망 기반의 네트워크 사회로 빠르게 진화할 전망되고 있다.

이러한 네트워크 환경의 변화를 가능하게 해주는 것은 광대역통합망(BcN : Broadband convergence Network)의 발전으로 볼 수 있다. "광대역통합망 기본기획"에서는 BcN의 개념을 다음과 같이 정의하고 있다.

BcN 정의 및 특성

정의	통신 · 방송 · 인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스를 언제 어디서나 끊김없이 안전하게 광대역으로 이용할 수 있는 차세대 통합 네트워크
특징	① 음성 · 데이터, 유 · 무선, 통신 · 방송 융합형 멀티미디어서비스를 언제 어디서나 편리하게 이용할 수 있는 서비스 통합망 ② 다양한 서비스를 용이하게 개발 · 제공할 수 있는 개방형 플랫폼(Open API) 기반의 통신망 ③ 보안(Security), 품질보장(QoS), IPv6가 지원되는 통신망 ④ 네트워크, 단말 등에 구애받지 않고 다양한 서비스를 끊김없이(Seamless) 이용할 수 있는 유비쿼터스 서비스 환경을 지원하는 통신망

다양한 서비스를 제공하는 광대역통합망의 개념은 아래 그림과 같이 표현할 수 있다.



(그림 1) 광대역통합망 개념도

(2) BcN 구축 목표

광대역 통합망의 구축 목표는 다양한 가입자 망을 통해 접속하는 이용자 및 서비스별 요구사항에 따라 종단 간(end-to-end)에 차별화된 품질을 보장하여 서비스를 제공할 수 있는 네트워크 환경의 구축으로 하고 있다. 아래 그림은 TTA에서 제시하고 있는 BcN 목표망의 구조도 이다.

(그림 2)의 BcN 구축 목표망을 기반으로 전달망 계층은 주요도시를 연결하는 Core Network 및 도시 내부 또는 중소 도시 간을 연결하기 위한 Metro Network으로 구현되고, 가입자 망 계층은 유선망, 무선망, 케이블망과 이들 간의 전달망 접속을 위한 엑세스 노드로 구성된 Access Network 형태로 구현이 예상된다.

또한 망 자원의 효율적 제어, 호 처리 및 보안을 위한 망 자원 제어, 유 · 무선 통합 IMS 및 통합 보안 플랫폼 등의 적용이 되어야 할 것이고, 다양한 서비스의 제공 및 응용을 위한 개방형 서비스 플랫폼과 다양한 응용 서비스를 위한 서버들이 구현되고, 이를 위한 다양한 형태의 홈 · 단말기의 개발이 예상된다.

III. BcN 연동 시나리오 도출

1. BcN 연동 시나리오 도출

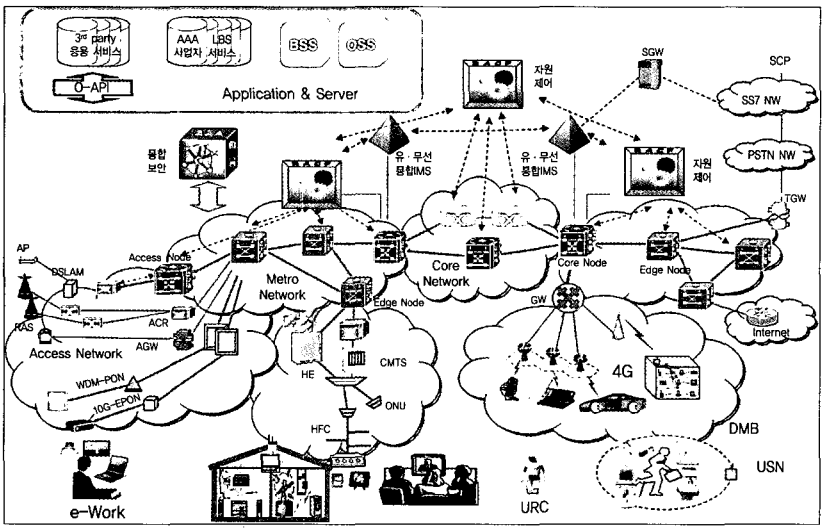
(1) 연동개념

BcN에서의 연동 개념은 아래와 같이 서로 다른 특성을 갖는 가입자망 간의 연동과 서로 다른 환경을 갖는 망 사업자간의 연동으로 나누어 생각해 볼 수 있다.

「BcN망에서의 연동 개념」

1. 서로 다른 가입자망을 통한 연결
   ① PSTN, ② 인터넷, ③ WiBro, ④ W-CDMA 등 연동

2. 서로 다른 망사업자 사이의 연결을 고려
   동일 또는 이종의 가입자망 환경에서
   ㉮ 동일사업자, ㉯ 타사업자간 연동



(그림 2) BcN 목표망

BcN 망에서 융 · 복합형 신규 서비스를 제공하기 위해서는, 각각 서비스의 시그널링 메시지를 통한 과금, 인증, 보안 및 제어 정보를 전달하는 서비스제어 계층사이의 연동과 사용자 데이터를 전송하는 전달망에서의 연동으로 구분하여 접근 할 수 있다.

(2) BcN 망에서의 연동 Case 도출

앞에서 언급한 바와 같이 우선, 다양한 가입자망을 고려한 연동 Case를 생각하여 보자. 각 가입자 망사이의 연동 가능한 Case는 아래 표와 같이 정리할 수 있을 것이다.

구 분	①PSTN	②인터넷	③WiBro	④W-CDMA	⑤방송망
①PSTN	Case ①	Case ②	Case ③	Case ④	Case ⑤
②인터넷		Case ⑥	Case ⑦	Case ⑧	Case ⑨
③WiBro			Case ⑩	Case ⑪	Case ⑫
④W-CDMA				Case ⑬	Case ⑭
⑤방송망					Case ⑮

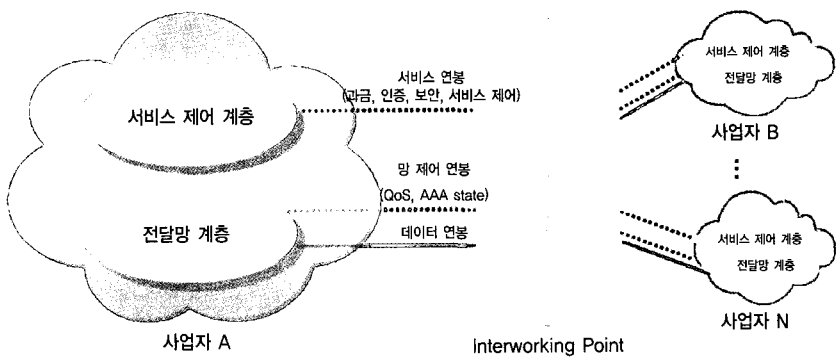
상기에 표시된 연동 Case 중에서 대표적이고 특징적인 Case를 선별하여 시나리오를 도출하고, 이에 대한 위협 및 보호대책 도출이 필요하나 이는 추후 진행이 필요한 부분이며, 본 기고문에서는 PSTN과 WCDMA간의 연동 Case를 중심으로 서술하고자 한다.

IV. BcN 위협 및 보안대책 : PSTN과 W-CDMA 연동 시나리오 중심

이번 장에서는 음성 · 데이터 및 유 · 무선 융합서비스를 제공할 수 있는 PSTN망과 W-CDMA망 사이의 연동 시나라오를 중심으로 발생가능한 보안 위협과 이에 대한 대응책을 알아보기로 한다.

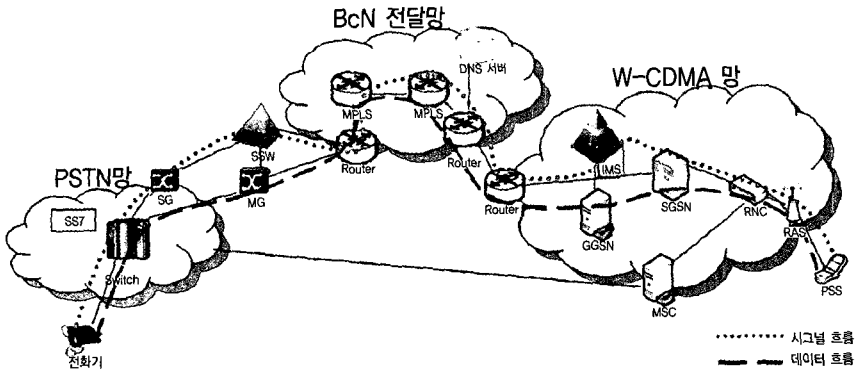
1. 연동 시나리오 분석

PSTN과 W-CDMA간 BcN 망을 추상화한 연동 구조도는 (그림 4)와 같다. PSTN망(예: KT 전화망) 사용자가 W-CDMA 망(예: SK 이동전화망)의 사용자가 통화할 경우, 통화 경로의 흐름은 다음과 같다.



☞ 서비스 제어계층의 연동 : 각 가입자망의 시그널 메시지로 변환 필요
☞ 전달망 계층의 연동 : 각 가입자망의 패킷구조로 변경 필요

(그림 3) BcN 연동 개념 ※출처 : BcN 표준모델 II(안)



(그림 4)

○ Signal

구 간	PSTN망	연동구간	BcN전달망	연동구간	W-CDMA망
Node	전화기↔SG	↔SoftSwitch ↔	라우터↔ MPLS↔라우터	↔라우터↔	GGSN↔ IMS↔ SGSN↔ RNC↔ RAS↔ PSS
주요 Protoco	IDP, DTMF, SS7	SIGTRAN, MGCP, Megaco, TCP/ IP(H.323, SIP)	TCP/IP	TCP/IP	TCP/IP, PPP 등

○ Media

구 간	PSTN망	연동구간	BcN전달망	연동구간	W-CDMA망
Node	전화기 ↔ Switch	↔MG ↔	라우터↔ MPLS↔라우터	↔라우터↔	GGSN↔ IMS↔ SGSN↔ RNC↔ RAS↔ PSS
주요 Protoco	-	ITCP/IP(RTP)	ITCP/IP (RTP)	ITCP/IP (RTP)	TCP/IP(RTP), PPP 등

BcN 전달망, PSTN망, W-CDMA 망 내부는 각 사업자에 의해 관리되는 영역으로서 단일 목적의 서비스만을 제공하므로 연동구간에서 제외한다. 따라서, 연동구간은 End-to-End 서비스 제공을 위해 가입자 망과 BcN 전달망의 정합부분으로, 망간 호처리를 위해 상호 작용하는 시그널링 처리장비(예: IMS), DNS 서버 등을 포함한다.

2. 보호대상 식별

보호대상은 연동 시나리오에서 도출된 연동구간의 연동장비로서, 연동장비 자체에 대한 보호 및 연동장비에서 처리되는 프로토콜 및 미디어에 대한 보호 관점에서 보호대상을 규정할 수 있다. 위의 연동시나리오에 의한 연동구간에서 보호대상 연동장비의 세부기능은 다음과 같다.

보호대상		주요기능
IMS (IP Multi media Sub system)	P-CSCF (Proxy-CSCF)	○사용자단말기가 IM 멀티미디어망에 접속하는 첫번째 지점 ○사용자단말기에게 SIP 메시지를 요구 또는 응답 ○Bearer 자원의 권한 검증과 QoS 관리
	I-CSCF(Inter-rogate CSCF)	○사용자단말기의 홈망에 접속하는 첫 포인트 지점 ○타 망으로부터 수신한 SIP 메시지를 S-CSCF로 routing
	S-CSCF (Serving CSCF)	○실제 등록된 사용자단말기의 세션 상태관리를 하면서 제어 서비스를 수행 ○사용자단말기에게 서비스 자원과 관련된 정보를 제공
	HSS (Home Subscriber Server)	○가입자의 마스터 데이터베이스 ○호 제어를 위한 가입자의 모든 정보들을 관리 ●가입자 식별자 - 번호 및 주소정보 ●가입자 보안정보 - 인증및 권한 검증을 위한 망 액세스 ● 가입자 위치정보 - 등록 및 Inter-system 레벨의 이동 정보 ● 가입자 서비스 프로파일 정보
	MGCF (Media Gateway Control Function)	○MGCF는 PSTN/PLMN의 종단으로 MGW의 미디어 채널을 위한 연결 제어에 관련된 호를 제어 ○기존 망에서 입력된 호에 대하여 라우팅 정보로 CSCF를 선택하며 기존망과 All-IP 망 호 제어 프로토콜 간의 프로토콜 변환을 수행
Soft Switch	CSC (Call Seesion Controller)	○ PSTN과 W-CDMA 망간의 호 연결, 세션제어 기능 수행 - 다양한 응용서버와 표준인터페이스로 연동하여 다양한 서비스 제공 - 인입호 관문, 가입자 인증 및 등록, 세션제어 및 서비스 라우팅, 등록 가입자 프로파일 관리, 번호 분석 및 변환, SIP/SDP 메시지 압축 및 해제기능 제공
	MGC(Media Gateway Controller)	○ 미디어 게이트웨이 제어 - 회선기반 PSTN망의 트래픽을 IP기반 SIP, H.323 등의 패킷트래픽으로 변환하도록 제어

보호대상	주요기능
MG(Media Gateway)	○PSTN과 W-CDMA 망사이에서 회선기반의 트래픽을 IP 기반의 SIP, H.323 패킷트래픽으로 또는 그 반대로 변환하여 전송
Edge Router	BcN 전달망, W-CDMA 망 경계에서 IP 데이터 전송
DNS 서버	○IP 기반 SIP 등의 호처리 프로토콜에 사용되는 Domain Name 정보 제공
MPLS 라우터	○BcN 전달망 내부에서 IP 데이터 전송

※ 시그널링 처리 및 MG 제어를 위해, Softswitch의 위치에 H.323 Getekeeper 또는 SIP 서버를 적용할 수 있으나, SoftSwitch의 기능에 포함하므로 별도의 연동장비로 도출하지 않음

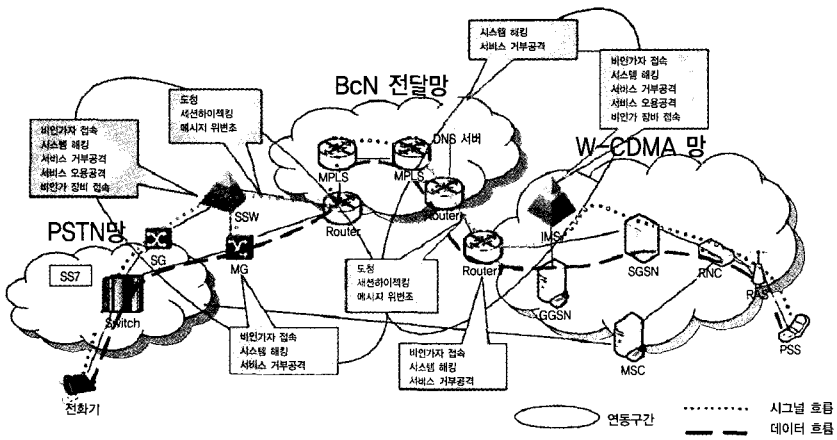
3. 보안위협 및 취약성

연동 시나리오에서 도출된 연동구간의 보안위협은 연동장비 자체 및 연동장비에서 처리되는 프로토콜 및 미디어(시스템 보안), 연동장비와 연결되는 망(네트워크 보안)에서 발생가능하며, 연동구간의 위협에 대한 그림은 (그림 5)와 같다.

각 위협별 시나리오 및 세부내용은 다음과 같다.

○ **도청**

- 시그널링 등 제어 메시지 도청 : 연동구간에서 시그널링 정보가 흘러가는 ① 소프트스위치↔BcN 전달망의 에지 라우터, ② BcN 전달망의 에지라우터 ↔ W-CDMA망의 에지라우터, ③W-CDMA망의 에지라우터 ↔ W-CDMA망의 IMS, ④소프트스위치 ↔ MG 구간에서 공격자가 연동장비 또는 망 자체에 대한 스니핑, Proving, 악성코드 삽입, 세션 하이잭킹 등의 공격기법을 통해 시그널링 정보가 도청될 수 있다. 시그널링 정보의 도청은 2차 공격을 위한 사전조사 성격으로 과금정보의 변경, 인증정보의 변경 등을 초래하여 금전적 피해 등을 야기할 수 있다.
- 미디어 데이터 도청 : 연동구간에서 미디어 데이터가 전송되는 ①MG↔ BcN 전달망의 에지 라우터, ②BcN 전달망의 에지라우터 ↔ W-CDMA망의 에지라우터, ③W-CDMA망의 에지라우터 ↔ W-CDMA망의 내부망 구간에서 공격자에 의해 스니핑, Proving, 악성코드 삽입, 세션 하이잭킹 등의 공격기법을 통해 미디어 정보를 도청할 수 있다. 미디어의 도청은 직접적으로 음성, 영상 등으로 통화하는 양자간의 주고받는 내용이 노출된다는 점에서 심각한 개인정보의 피해를 야기할 수 있다.



(그림 5) 연동시나리오에 따른 보안 위협 및 취약성

○ **서비스 거부**

- 연동구간에서 시그널링 및 미디어 정보가 흘러가는 ①소프트스위치↔ BcN 전달망의 에지 라우터, ②BcN 전달망의 에지라우터 ↔ W-CDMA망의 에지라우터, ③W-CDMA망의 에지라우터↔W-CDMA망의 IMS, ④소프트스위치 ↔ MG 구간에서 공격자가 IMS, 소프트스위치, DNS 서버, MG 등의 연동장비에 대한 과도한 세션연결 요청, TCP SYN Flooding, UDP Flooding, 다량의 비정상 패킷 발송, DNS 쿼리, 대량의 불법 스팸 데이터 전송 등을 통해 장비 및 회선의 자원을 고갈시켜 정상적인 서비스의 일시적 중단 또는 마비를 초래할 수 있으며, 타 가입자망으로 전파되어 피해를 확산 시킬 수 있다.
- 또한 서비스 융합에 따라 WiBro, 인터넷 액세스망 등 타 망에서 발생한 비정상 트래픽 데이터가 BcN 전달망을 통해 에지 라우터로 과다 유입되는 등의 문제로 서비스가 중단될 수도 있어 서비스 거부공격은 IP 기반의 서비스에서 매우 취약하고 대응이 어려운 공격이다.

○ **메시지 위변조**

- 연동구간에서 시그널링 및 미디어 정보가 흘러가는 ①소프트스위치↔ BcN 전달망의 에지 라우터, ②BcN 전달망의 에지라우터 ↔ W-CDMA망의 에지라우터, ③W-CDMA망의 에지라우터↔W-CDMA망의 IMS, ④소프트스위치 ↔ MG 구간에서 공격자가 IMS, 소프트스위치, MG, 에지 라우터 등의 연동장비에 대한 시스템 해킹을 통해 전송되는 시그널 및 미디어를 위조 또는 변조할 수 있다. 위변조 공격을 통해 공격자는 과금정보 및 사용자 인증정보 등의 조작, 사용자 단말에 악의적인 정보 출력 등의 피해를 야기할 수 있다.

○ **비인가 접속**

- 연동구간에서 시그널링 및 미디어 변환/전송을 처리하는 소프트스위치, W-CDMA망의 IMS, MG 등의 연동장비에 공격자가 스푸핑, 세션 하이잭킹 등의 공격기법이나 사용자 인증, 단말기 인증, 연동장비 상호인증 메커니즘의 부재 등 연동장비의 설정오류 등을 통해 정상적으로 인가받지 않고 불법적으로 연동장비에 접속하는 것으로, 불법적인 서비스 이용, 연동장비 조작, 연동장비에 저장된 가입자 및 과금 등의 자료에 대한 정보유출 및 훼손, 제 3자 공격의 거점으로 악용 등을 초래할 수 있다.

○ **시스템 해킹**

- 연동구간에서 시그널링 및 미디어 변환/전송을 처리하는 소프트스위치, W-CDMA망의 IMS, MG, BcN 전달망 및 W-CDMA망의 에지 라우터 등의 연동장비에 대해 공격자가 보안패치 미비, 접근통제 및 인증기능 미비, 시스템 파라미터 설정 오류, 취약한 프로토콜 사용 등에 기인하는 시스템 운영체제 및 응용 프로그램의 취약점을 악용하여 연동장비에 침투하거나 연동장비 기능을 무력화, 연동장비에 저장된 가입자 및 과금 등의 정보유출 및 훼손, 악성 프로그램 삽입 또는 유포, 제 3자 공격의 거점으로 악용 등을 초래할 수 있다.

4. 연동시나리오의 보안위협에 대한 보안요구사항

위 협	공격기법	보안요구사항(환경, 보증, 기능)
도청	o 스니핑 o 세션 하이잭킹 o Proving o 악성코드 삽입 등	o 시그널링 데이터 암호화 o 미디어 데이터 암호화 o 악성코드, 비인가 프로세스 감사 및 조치
서비스 거부	o 과도한 세션연결 요청 o TCP SYN Flooding o UDP Flooding o 다량의 비정상 패킷 발송 o 대량의 불법 스팸 데이터 전송 o 과도한 DNS 쿼리 등	o 비인가 데이터 접근통제 o 시그널링 및 미디어 데이터 인증 o 자원 사용량 통제 o 네트워크, 시스템자원 모니터링 및 장애대응
메시지 위변조	o 세션 하이잭킹 o 스푸핑 o Proving o 시스템 해킹 o 악성코드 삽입 등	o 저장데이터 무결성 제공 o 전송데이터 무결성 제공 또는 암호화 o 악성코드, 비인가 프로세스 감사 및 조치
비인가 접속	o IP주소 등의 위장 o 세션 하이잭킹 o 인증우회 o Replay 공격 o IP 스푸핑 o 접근통제 우회 등	o 연동장비에 대한 물리적 보호 o 연동장비 접근에 대한 사용자 상호인증 o 단말기와 연동장비 상호인증 o 연동장비간 상호인증 o 비인가 데이터 접근통제
시스템 해킹	o 웜 · 바이러스 o 백도어 등의 악성코드 삽입 o 접근통제 우회 o 인증우회 o 프로토콜 취약점 악용 o S/W 결함 악용 o 운영체제 및 응용 S/W 결함 악용 등	o 시스템 접근통제 o 안전한 운영체제 사용 o 적절한 시스템 파라미터 구성 o 시스템 및 응용프로그램 보안패치 o 악성코드, 비인가 프로세스 감사 및 조치 o 시스템 모니터링 및 장애대응

위 표의 위협별로 보안요구사항은 해당 위협에 대응하기 위해 요구되는 항목들이다.

5. 보안대책

PSTN과 W-CDMA 서비스 제공을 위한 연동구간에 있어서 정보보호 대책은 연동구간에서 도출된 보안위협에 대해 연동장비 자체 및 연동장비에서 처리되는 프로토콜 및 미디어(시스템 보안), 연동장비와 연결되는 망(네트워크 보안)에 초점을 맞추고 있다. 이러한 보호대책은 앞 단락에서 나열한 5가지 위협에 대한 보안요구사항을 상세화 및 구체화하는 것으로 구성된다.

□ 도청 위협 보안대책

○ 시그널링 및 미디어 데이터 암호화

- 연동구간 소프트스위치 ↔ W-CDMA망의 IMS 사이에서 H.323, SIP 등의 시그널링 데이터를 암호화 할 수 있어야 한다. 이는 연동장비에서 TLS, IPsec 등의 보안프로토콜 사용, 별도의 암호화 기능을 제공하는 VPN 솔루션 등의 사용을 통해 달성할 수 있다.
- 연동구간 소프트스위치 또는 IMS ↔ MG 사이에서 MGCP 등의 MG(Media Gateway) 제어 메시지를 암호화 할 수 있어야 하며, 이는 보안 기능이 향상된 Megaco/H.248 등을 사용함으로써 달성할 수 있다.
- 연동구간 ①MG ↔ W-CDMA망의 에지라우터 또는 W-CDMA망의 내부망 구간에서 음성, 영상 통화 등에 필요한 미디어 데이터를 암호화 할 수 있어야 한다. 이는 MG와 W-CDMA망 내부에 있는 장비가 SRTP (Secure Real-Time Transport Protocl) 등의 보안프로토콜 사용, 별도의 암호화 기능을 제공하는 암호화 솔루션 등의 사용을 통해 달성할 수 있다.

○ 악성코드, 비인가 프로세스 감사 및 조치

- 악성코드, 비인가 프로세스에 대한 전반적인 관리활동 계획이 수립 · 운영 되어야 한다.
- 연동구간의 소프트스위치, IMS, MG 등에 대해 정기적인 악성코드 검사, 활성화된 프로세스 검사를 실시하여 비인가된 프로그램의 활동여부를 확인하여야 한다.
- 악성코드 발견시 즉시 삭제하고, 비인가된 활성화된 프로그램 발견시 즉시 종료시키고 해당 프로그램이 시작된 시각 등을 조사하고,

절차에 따라 추가적인 자료유출 여부를 조사해야 한다.

□ **서비스 거부 위협 보안대책**

○ 비인가 데이터 접근통제
- 소프트스위치, MG, W-CDMA망의 IMS는 허가되지 않은 주소, 프로토콜, 비정상 패킷 등에 대해 필터링 등을 통해 차단할 수 있어야 한다.
- 소프트스위치, MG, W-CDMA망의 IMS는 호 사용자 정보, 진행중인 호 연결 상태와 관련없는 데이터에 대해서는 필터링 등을 통해 차단할 수 있어야 한다. 이는 Firewall, SBC(Session Board Controller) 등의 솔루션을 통해 구현할 수 있다.
- 소프트스위치, MG, W-CDMA망의 IMS는 가능한 사설망 등 네트워크 은닉 기법을 통해 외부 공격자가 주요 연동장비에 직접 접근할 수 없도록 해야 한다.

○ 시그널링 및 미디어 데이터 인증
- 소프트스위치, MG, W-CDMA망의 IMS는 새로 설립 되거나, 진행 중인 호에 대한 상태 정보를 유지하면서 유효성 확보를 위해 인증하고, 인증정보가 없는 데이터는 필터링 등을 통해 차단할 수 있어야 한다.

○ 자원 사용량 통제
- 소프트스위치, MG, W-CDMA망의 IMS는 정상 서비스를 유지할 수 있도록 시스템 성능, 대역폭 등을 고려하여 최대 세션수, 단위 시간당 호 발생량, 디스크 사용량, 프로세스 수, 기억공간에 대한 한계치 등을 정해 운영해야 한다.
- 소프트스위치, MG, W-CDMA망의 IMS는 원활한 서비스를 유지하기 위한 방법(예: 서비스별 우선순위에 따른 처리, 서비스별 Rate Limit 설정 등) 등의 운영을 고려하여야 한다.
- 소프트스위치, W-CDMA망의 IMS는 과도한 호를 발생시키는 단일 번호에 대한 추적 및 제한, 향후 책임관계를 조사할 수 있어야 한다.
- BcN 전달망의 에지 라우터, W-CDMA 망의 에지 라우터는 과도한 트래픽에도 적절히 처리하여 시스템 생존성을 보장할 수 있어야 한다.
- BcN 전달망의 에지 라우터, W-CDMA 망의 에지 라우터는 트래픽 집중시에도 중요 데이터는 최소한의 서비스가 유지될 수 있도록 운영하여야 한다.

○ 네트워크, 시스템 자원 모니터링 및 장애대응
- 연동장비의 자원사용량(최대 세션수, CPU/디스크/메모리 사용량, 프로세스 수, 대역폭 사용량 등) 모니터링을 통해 적절한 서비스가 유지될 수 있도록 망관리 시스템, 보안시스템 등을 활용하여 모니터링 등을 수행하여야 한다.
- 연동장비 자원 고갈로 서비스 제공이 어려울 경우, 서비스 회복을 위한 절차에 따라 신속히 장애분석 및 대응 절차가 수행되어야 한다.
- 연동장비에 유입되는 트래픽에 대해 침입을 탐지할수 있어야 하며, 침입탐지시에는 서비스 장애 방지를 위해 망 분리 등의 적절한 조치를 취할 수 있어야 한다.
- 원활한 서비스 제공 및 신속한 장애 대응을 위해, 연동장비에 관계된 사업자간 긴밀한 연계 또는 공동 대응 체계를 구축운영 하여야 한다.

□ 메시지 위변조 위협 보안대책

○ 저장데이터 무결성 제공
- 소프트스위치, MG, W-CDMA망의 IMS는 필요시 Keyed 해쉬 방법 등을 활용하여 호처리에 필요한 저장된 데이터의 무결성을 확인할 수 있어야 한다.

○ 전송데이터 무결성 제공 또는 암호화
- 연동구간 소프트스위치 ↔ W-CDMA망의 IMS 사이에서 H.323, SIP 등의 시그널링 데이터의 무결성을 제공해야 한다. 이는 연동장비에서 PKI 기술, TLS, IPsec 등의 보안프로토콜 사용, 별도의 암호화 기능을 제공하는 VPN 솔루션 등의 사용을 통해 달성할 수 있다.
- 연동구간 소프트스위치 또는 IMS ↔ MG 사이에서 MGCP 등의 MG(Media Gateway) 제어 메시지에 대한 무결성 또한 제공할 수 있어야 한다.
- 연동구간 ①MG ↔ W-CDMA망의 에지라우터 또는 W-CDMA망의 내부망 구간에서 음성, 영상 통화 등에 필요한 미디어 데이터에 대한 무결성을 제공할 수 있어야 한다. 이는 MG와 W-CDMA망 내부에 있는 장비가 SRTP(Secure Real-Time Transport Protocl) 등의 보안프로토콜 사용, 별도의 무결성 기능을 제공하는 솔루션 등의 사용을 통해 달성할 수 있다.

○ 악성코드, 비인가 프로세스 감사 및 조치
- 악성코드, 비인가 프로세스에 대한 전반적인 관리활동 계획이 수립 · 운영 되어야 한다.
- 연동구간의 소프트스위치, IMS, MG 등에 대해 정기적인 악성코드 검사, 활성화된 프로세스 검사를 실시하여 비인가된 프로그램의 활동여부를 확인하여야 한다.
- 악성코드 발견시 즉시 삭제하고, 비인가된 활성화된 프로그램 발견시 즉시 종료시키고 해당 프로그램이 시작된 시각 등을 조사하고, 절차에 따라 추가적인 자료유출 여부를 조사해야 한다.

□ 비인가 접속 위협 보안대책

○ 연동장비에 대한 물리적 보호
- 연동장비는 설치된 공간은 인가된 자에 한해 출입할 수 있도록 물리적으로 출입 · 통제를 실시하고, 출입통제 사항에 대해서는 그 내역을 기록하여야 한다.

○ 연동장비 접근에 대한 사용자 상호인증
- 연동구간의 소프트스위치, IMS, MG는 시스템에 직접 또는 네트워크로 접근하는 사용자를 시도-응답(challenge-response) 프로토콜 기반으로 반드시 상호인증하여 신원을 확인 후 서비스를 제공하여야 한다. 이 경우 인증을 연동장비가 직접 처리하거나, DIAMETER, RADIUS 등의 인증 서버를 활용하여 구현할 수 있다.
- 소프트스위치, IMS 등의 호처리 연동장비에 최소 설치시 디폴트로 설정된 사용자 인증정보는 반드시 바꾸고, 암호는 숫자, 특수문자, 알파벳 등을 혼용하여 8자 이상으로 설정하고, 주기적으로 암호를 바꾸어야 한다.
- 가능한 연동장비는 원격관리를 최소로 허용하여야 하며, 원격 관리시 접근 사용자에 대한 접근통제, 신분확인을 엄격하게 수행하여

야 한다.

○ 단말기와 연동장비 상호인증
- 연동구간의 소프트스위치, IMS, MG는 서비스 제공을 위해 접근하는 단말기를 시도-응답(challenge-response) 프로토콜 기반으로 반드시 상호인증하여 신원을 확인 후 서비스를 제공하여야 한다.
- 소프트스위치, IMS 등의 호처리 연동장비는 악의적인 사용자가 복사, 도난 등의 방법을 통해 비정상적으로 사용할 수 없도록 적절한 상호인증 메커니즘을 운영해야 한다.

○ 연동장비간 상호인증
- 연동구간의 소프트스위치, IMS, MG는 서비스 제공을 위해 연계되는 상대방 연동장비를 시도-응답(challenge-response) 프로토콜 기반으로 반드시 상호인증하여 신원을 확인 후 서비스를 제공하여야 한다.

○ 비인가 데이터 접근통제
- 소프트스위치, MG, W-CDMA망의 IMS는 허가되지 않은 주소, 프로토콜, 비정상 패킷 등에 대해 필터링 등을 통해 차단할 수 있어야 한다.
- 소프트스위치, MG, W-CDMA망의 IMS는 호 사용자 정보, 진행중인 호 연결 상태와 관련없는 데이터에 대해서는 필터링 등을 통해 차단할 수 있어야 한다. 이는 Firewall, SBC(Session Board Controller) 등의 솔루션을 통해 구현할 수 있다.
- 소프트스위치, MG, W-CDMA망의 IMS는 가능한 사설망 등 네트워크 은닉 기법을 통해 외부 공격자가 주요 연동장비에 직접 접근할 수 없도록 해야 한다.

□ 시스템 해킹 위협 보안대책

○ 시스템 접근통제
- 소프트스위치, MG, IMS, 에지 라우터는 허가되지 않은 주소, 프로토콜, 비정상 패킷 등으로 접근하는 데이터에 대해 필터링 등을 통해 차단할 수 있어야 한다. 이는 Firewall, SBC(Session Board Controller) 등의 솔루션을 통해 구현할 수 있다.
- 소프트스위치, MG, IMS, 에지 라우터는 자신을 통해 허가되지 않은 곳으로 전송하는 데이터는 필터링 등을 통해 차단할 수 있어야 한다.
- 소프트스위치, MG, W-CDMA망의 IMS는 가능한 사설망 등 네트워크 은닉 기법을 통해 외부 공격자가 주요 연동장비에 직접 접근할 수 없도록 해야 한다.

○ 안전한 운영체제 사용
- 연동장비의 운영체제는 보안이 강화된 안전한 운영체제를 탑재하고 있어야 한다.

○ 적절한 시스템 파라미터 구성
- 연동장비 관련 운영체제의 보안속성 등과 관계된 디폴트 파라미터 설정 값들을 조사하여 용도에 맞게 적절하게 설정하여야 한다.

○ 시스템 및 응용프로그램 보안패치
- 소프트스위치, MG, IMS, 에지 라우터는 정기적으로 시스템 및 응용프로그램에 대한 보안패치 여부를 확인하여 최신 자료로 업데이트해야 한다.

○ 악성코드, 비인가 프로세스 감사 및 조치
- 악성코드, 비인가 프로세스에 대한 전반적인 관리활동 계획이 수립 · 운영 되어야 한다.
- 연동구간의 소프트스위치, IMS, MG 등에 대해 정기적인 악성코드 검사, 활성화된 프로세스 검사를 실시하여 비인가된 프로그램의 활동여부를 확인하여야 한다.
- 악성코드 발견시 즉시 삭제하고, 비인가된 활성화된 프로그램 발견시 즉시 종료시키고 해당 프로그램이 시작된 시각 등을 조사하고, 절차에 따라 추가적인 자료유출 여부를 조사해야 한다.

○ 시스템 모니터링 및 장애대응
- 연동장비의 자원사용량(최대 세션수, CPU/디스크/메모리 사용량, 프로세스 수, 대역폭 사용량 등) 모니터링을 통해 적절한 서비스가 유지될 수 있도록 망관리 시스템, 보안시스템 등을 활용하여 모니터링 등을 수행하여야 한다.
- 연동장비 자원 고갈로 서비스 제공이 어려울 경우, 서비스 회복을 위한 절차에 따라 신속히 장애분석 및 대응 절차가 수행되어야 한다.
- 연동장비에 유입되는 트래픽에 대해 침입을 탐지할수 있어야 하며, 침입탐지시에는 서비스 장애 방지를 위해 망 분리, 백업시스템 가동 등의 적절한 조치를 취할 수 있어야 한다.
- 원활한 서비스 제공 및 신속한 장애 대응을 위해, 연동장비에 관계된 사업자간 긴밀한 연계 또는 공동 대응 체계를 구축운영 하여야 한다.
- 시스템 및 네트워크에 대한 주기적인 취약점 점검 및 웜 · 바이러스 검사를 통해 침해사고 발생 여부를 즉시 파악하고 대처할 수 있어야 한다.

V. 결 론

이상으로 PSTN과 W-CDMA망간의 연동 시나리오를 중심으로 BcN의 보안위협 및 보안대책을 설명하였다.

기존의 개별망 서비스 중심에서 제공되는 음성, 데이터, 방송 등의 통신서비스가 BcN을 통해 융합되면서 사용자, 사업자 모두에게 다양한 사업영역과 기회를 제공하고 있으며, 이러한 BcN 기반의 사업 활성화는 BcN의 성패에 중요한 관건이 될 것이다. BcN의 사업 활성화를 위해서는 원활하고 안정정인 서비스 제공과 더불어 BcN 환경의 정보화 역기능에 대해 사용자로부터 BcN에 대한 안전 · 신뢰성 확보가 필수로 요구된다 할것이다. 이를 위해 본 기고문에서는 BcN 환경에서 다양한 망과 사업자들이 연동되는 경우에서 PSTN과 WCDMA 망간 연동 시나리오에 대한 위협과 보안대책들을 살펴보았다. 여기서 제시되고 있는 네트워크 환경은 실제 BcN 망을 구축하는 사업자들의 환경과 범위를 추후에 세밀히 반영할 필요가 있으며, 이에 따라 위협과 대책들 또한 보완하여야 할 필요가 있을 것이다. 또한 추가적인 연동 시나리오들의 도출이 필요하고, 제시하고 있는 대책들은 좀더 효과적이고 현실성이 있기 위해서 다양한 분야로부터 추후 좀더 많은 검토과정을 통해 보완될 필요가 있다.

이강신

1987년 한양대학교 졸업(학사)
1989년 한양대학교 수학과 졸업(석사)
1990년 ~ 1992년 (주)데이콤 종합연구소
2002년 ~ 2005년 고려대학교 정보보호대학원 졸업(박사)
2000년 ~ 현재 한국정보보호진흥원 팀장
관심분야 : BcN, Network Security, Security Management

김호성

1994년 한양대학교 졸업(학사)
2000년 포항공대 정보통신공학과 졸업(석사)
2001년 ~ 현재 한국정보보호진흥원 선임연구원
관심분야 : BcN, Network Security, Network QoS

신동훈

2001년 충남대학교 졸업(학사)
2003년 충남대학교 컴퓨터공학과 졸업(석사)
2003년 ~ 현재 한국정보보호진흥원 연구원
관심분야 : BcN, Network Security, Wireless Network