情 報 保 護 學 會 誌
第 15 卷 第 3 號, 2005. 6

IT839 정보보호 기술의 현재와 미래

염 흥 열*

요 약

정보통신부에서 현재 추진 중인 IT839 프로젝트는 새로운 IT 서비스를 창출하여, 우리나라 IT 인프라를 강화하고 이를 근거로 국민소득 2만불 시대를 견인할 미래 신성장 산업으로 육성하고자 함에 있다. 본고에서는 IT839 분야에서 필요한 위협과 정보보호 요구사항을 도출하고, 현재 정보보호 기술의 현황을 살펴보며, 이를 근거로 추가로 개발되어야 할 정보보호 기술을 살펴본다.

Ⅰ. 서 론

정보통신부에서 추진하고 있는 IT839, 즉 IT 분야의 새로운 서비스와 신성장 동력산업을 찾고, 이를 지원할 IT 인프라를 찾는 것은 국민소득 2만불 시대를 대비하여 매우 중요하다고 볼 수 있다. 정보통신부에서 추진하고 있는 IT839 사업은 8대 정보통신 신규 서비스, 3대 기반 인프라, 그리고 9대 신성장 동력 산업으로서 서로 여러 서비스와 인프라가 가치 사슬 모델을 이루고 있으며, 이들은 서로 유기적으로 연결고리를 가지고 있어 새롭고 다양한 IT 사업을 창출할 것으로 예상된다. IT839를 자세히 살펴보면, 8대 서비스로 휴대인터넷(WiBro), DMB (Digital Multimedia Broadcasting), 홈 네트워크, 텔레매틱스(Telematics), RFID(Radio Frequency IDentification), W-CDMA (Wide-band Code division Multiple Access), 지상파 DTV(Digital TeleVision), 그리고 인터넷 전화 등이며, 3대 인프라는 광대역통합망(BcN: Broadband Convergence Network), USN(Ubiquitous Sensor Network), 그리고 IPv6 등이며, 9대 신성장 동력 산업은 차세대 이동통신, 디지털 TV, 홈 네트워크, IT SoC(System on Chip), 차세대 PC, 임베디드 S/W, 디지털 컨텐츠, 텔레매틱스, 지능형 로봇 분야이다.[1,7] 각 분야 별로 정보통신부에서는 2006년도에서 2010년도 까지 표준화, 기술개발, 서비스 활용 방안을 수립하고 의욕적으로 추진하고 있다. 그러나 이들 8대 서비스와 3대 인프라, 그리고 9대 신성장 동력 산업이 성공적으로 완성되기 위해서는 이에 따르는 정보보호 기술이 기반으로 지원되어야 한다.[2-6] 이들 분야의 정보보호 기술은 기존에 개발된 정보보호 기술을 기반으로 미래에 필요한 정보보호 기술이 어떤 것인지를 살펴보고, 기존의 기술과 향후 개발되어야 할 기술이 무엇인지를 정의하는 것은 매우 중요하다고 할 수 있다.

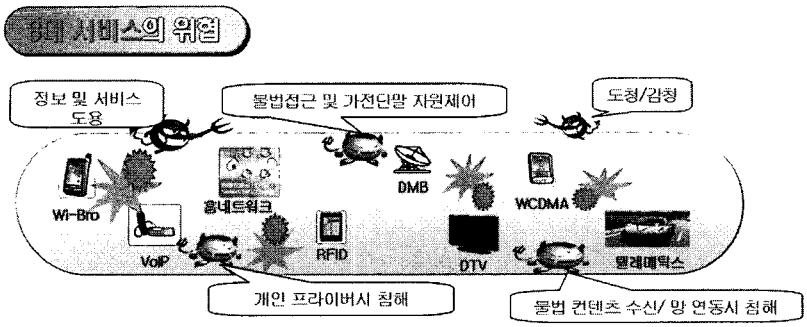
본 고는 IT839 관련 정보보호 기술 현황을 분석하고, 이를 근거로 앞으로 개발되어야 할 정보보호 기술을 제시함에 있다. 본고의 결과는 IT839 정보보호 정책 설정 및 연구 개발 시 유익하게 활용될 수 있기를 기대한다.

Ⅱ. 본 론

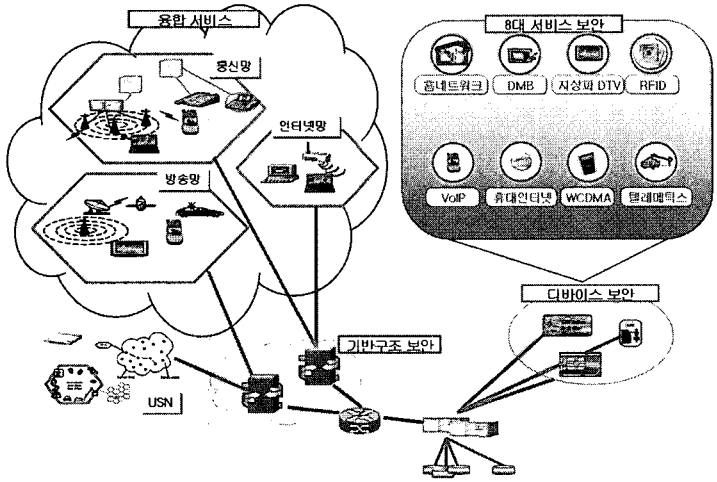
2.1 신규 서비스 및 신성장동력분야 정보보호

유·무선 고속 이동 통신망을 기반으로 하는 8대 정보통신 신규서비스를 이용하면, 우리의 생활양식에 큰 파급효과가 예상되며, 신규 서비스가 각 사용자의 금융정보, 위치정보, 의료정보 등 개인 정보를 많이 다루게 되어 이로 인한 유출 위험도 동시에 증가하게 될 것으로 예측된다.[5] 또한 이동 통신 네트워크를 주로 이용하게 됨으로 인하여 발생하는 네트워크에서 유통되는 정보의 도·감청 위험이 증가하게 된다. 그리고 휴대성

본 논문은 정통부 ITRC 사업에 의하여 수행되었음
* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)



〔그림 1〕 8대 서비스에 대한 보안 위협



〔그림 2〕 8대 서비스 보안 기술 적용 위치

이 용이한 이동 단말에 대한 분실 및 불법 접근, 홈네트워크에서 가전 단말의 불법 제어, DMB 서비스의 불법 컨텐츠 수신과 지적재산권 침범 등의 위협 요인이 존재한다. 이러한 과정에서 사이버 공간에서 제공되는 서비스에 대한 위험이 현실세계의 위협으로 전이될 가능성도 높아지고 있다. 안전하고 신뢰할 수 있는 신규 서비스의 보급을 위해서는 금융, 위치, 의료, 상황 정보 등 개인정보의 종합적인 보호체계를 정립할 필요가 있으며 이동통신 서비스의 보안 기밀성 강화를 위한 핵심 기술 및 8대 서비스의 장애로 인한 피해 및 안전 위협을 최소화할 수 있는 안전 관리 체계가 필요하다.[3,8] 그림 1은 이를 요약한 8대 서비스에 대한 보안 위협을 나타내고 있고, 그림 2는 8대 서비스에 대한 보안 기술 적용 위치를 나타내고 있다.

2.1.1 8대 서비스 분야 정보보호

가. 휴대 인터넷 정보보호

휴대인터넷 서비스(WiBro)는 사용자가 고속 이동 중에 휴대형 무선단말기로 고속전송속도로 인터넷에 접속하여 다양한 정보 및 컨텐츠를 얻거나 활용할 수 있도록 하는 통신서비스로써, 이동성 측면에서 기존의 무선 랜과 차별화되며, 고속성 측면에서 이동통신기반 무선인터넷과 차별되는 서비스이다. 무선랜이 지닌 고속 데이터 서비스의 장점을 살리고 이동성의 단점을 극복할 수 있도록 구성되어 있다. 휴대인터넷 시스템은 유선 인터넷에서 제공하는 다양한 형태의 IP 기반 무선 패킷 데이터의 고속 전송에 적합한 서비스 품질을 보장하는 것을 목표로 하고 있다. 또한 서비스 중단 없이 쎌(cell)간 이동성 보장, 휴대형 단말기에 대한 IP 어드레스의 동적 또는 정적 할당 및 인증 기능 수행, IP 기반 무선 데이터 서비스를 위한 비대칭 데이터 전송, 최대 반경 1km 정도의 서비스 영역 제공과 60 km/h 내외의 단말기 이동성 보장 등을 특징으로 하고 있다.

기존 휴대인터넷을 위한 무선 환경은 IEEE 802.16 보안 표준이 존재한다. IEEE 802.16에서 보안 기술은 MAC(Media Access Control) 계층에서의 Pri-

vacy 기능을 통해 제공된다. 즉, 인증 및 키 관리를 위한 PKM(Privacy Key Management) 프로토콜과 패킷 데이터 자체의 암호화 프로토콜을 사용하는 것이 제안되고 있다. PKM은 단말기를 기지국이 X.509 인증서 기반으로 장치를 인증하는 단방향 인증방식으로 단말기의 권한 부여 검증과 AK(Authorization Key) 교환 단계, 그리고 TEK(Traffic Encryption Key) 교환 단계로 구성된다. 패킷 데이터 암호화 프로토콜의 경우 AK 암호화는 RSA 알고리즘을 사용하며, TEK 암호화는 EDE(Encrypt-Decrypt-Encrypt) 방식의 Two-key 3 DES 알고리즘을 사용하고 있다. 그리고 트래픽 데이터 암호화의 경우는 CBC(Cipher Block Chaining) 모드의 DES 알고리즘을 사용하여 데이터를 보호하고자 제안되고 있다.

주요 위협은 무선 구간에서 발생하는 도청, 변조, 삽입, 삭제 등의 침해 위협, 휴대 단말기를 통한 웜·바이러스 공격, 불건전 정보의 유통 등도 매우 커다란 위협요인으로 대두될 것이다. 디지털 컨텐츠의 불법 복제와 유통 문제도 매우 심각한 역기능 현상이며, 특히 BcN을 통하여 여러 개별망이 통합된 환경에서는 이러한 지적재산권 침해나 유통 문제가 더욱더 손쉽게 발생될 가능성이 매우 높아질 것이다.

현재까지 개발된 기술은 무선 링크에서 적용될 수 있는 사용자 또는 단말 인증, 데이터의 기밀성, 무결성, 그리고 키관리 기술이다.

향후 개발되어야 할 정보보호 기술은 단말기와 사용자간에 사용자 인증을 위한 생체 인증기법, 단말기와 컨텐츠 서버 간의 EAP(Extensible Authentication Protocol) 기반의 단말 인증 기술, 단말기와 서버간의 안전한 정보 전달 기법, 단말기와 서버 간에 컨텐츠 보호 기술, 중앙 집중 인증/인가/계정관리를 위한 정보보호 프레임워크, 그리고 익명성 제공 및 프라이버시 보호 기술 등이다.

나. W-CDMA 서비스 정보보호

이동통신의 발전은 아날로그 방식에서 디지털 방식으로 발전하고 있다. 이러한 과정에서 멀티미디어 전송까지를 목적으로 하여, 고화질 화상 서비스, 빠른 데이터 전송률 등 많은 기존 시스템과의 차별성으로 높은 부가가치를 창출할 것으로 예상되는 3세대 이동통신 시스템, 즉 IMT-2000(International Mobile Telecommunications-2000)은 유럽/일본을 중심으로 한 GSM (Global System for Mobile communication)기반의 비동기 방식(W-CDMA: Wideband Code Division Multiple Access)과 미국을 중심으로 한 동기 방식(CDMA2000)의 양대 진영으로 나뉘어 기술 표준화 및 개발이 진행 중이다. 현재까지 개발된 보안 기술은 주로 W-CDMA에서 무선구간 데이터에서 사용자를 인증하고, 데이터에 대한 기밀성과 무결성을 보장하는 기술이 적용되었다. 특히, 단말을 위한 대부분의 암호 기능이 USIM (Universal Subscriber Identity Module)이라는 간섭이 불가능한 스마트카드에서 수행되도록 하였다.

W-CDMA에서 위협 요인은 복제 단말기에 의한 서비스 도용, 무선 링크에 대한 도청, 그리고 도청된 개인 정보를 이용한 프라이버시 침해 등이다.

이러한 위협을 방지하기 위하여 현재 개발된 정보보호 기술은 주로 제2세대와 제3세대 무선 링크에 대한 보호 기술, 익명성 기반 프라이버시 보호 기술, 도전-응답 인증 기법에 기반을 둔 사용자 또는 단말 인증 기술, 인증 기법 연관 키 분배 기술, 그리고 공유된 키를 이용하여 제공되는 기밀성 보호 기법 및 무결성 보장 기법 등이다. 또한, 유럽방식 제2세대에서 사용되고 있는 간섭이 불가능한 토큰인 USIM 카드에 기반을 둔 암호 구현 기술 등이 있다. 이를 요약하면, 무선 링크 계층에 적용 가능한 익명성 제공, 단말 인증기술, 기밀성 기술, 무결성 기술 등이다.

향후 개발되어야 할 요소 정보보호기술은 키 분실에 대비한 강화된 사용자/단말간에 생체 인증기법, 단말과 컨텐츠 서버 간의 EAP 기반 인증 기술, 유해 트래픽 차단을 위한 컨텐츠 필터링 기술, 단말간 AAA 서버 사이에 인증및 인가를 위한 보안 프레임워크, 응용 레벨에서 종단간 보안 기능, 단말에서 침해 상태를 판단하여 단말의 서비스 등급을 결정하는 긴급 대응 시스템, 그리고 사용자 익명성 보장 기술 등이다.

다. 지상파 DTV 서비스 정보보호

지상파 DTV는 대화면, 고화질, 입체음향의 고품질 방송을 제공할 수 있는 서비스이다. 지상파 DTV 전송 방식을 변경해야 한다는 주장이 있어 합리적 방법으로 조기에 논란을 종식하여 차세대 성장 동력으로 육성해야 한다. MPEG-4 기술의 도입으로 다양한 형태의 데이터 서비스 및 사용자의 Activity 제공, MPEG-7 기술의 도입으로 사용자의 요구에 따른 정보 제공, 그리고 3D 영상 및 실감 방송 기술 도입으로 현장감 있는 컨텐츠 제공이 가능할 것이다.

주요 위협은 유료서비스인 경우 시청 권한이 없는 사용자에 의한 불법 서비스 사용, 사용권한이 없는 사

용자에 의한 불법적인 서비스의 도용, 그리고 등급화된 방송 내용의 불법적인 이용 및 도용 등이 있다. 또한 방송 컨텐츠에 대한 저작권 침해 등을 들 수 있다.

현재까지 개발된 보안 기술은 영상 정보에 대한 워터마킹을 중심한 저작권 보호 기술, 한정수신접근기술에 의한 접근제어기술, 그리고 유해정보차단기술 등이다.

향후 개발되어야 할 정보보호 기술은 다양한 응용환경을 위한 디바이스 인증에 기반을 둔 한정수신접근기술 고도화 기술과, 영상뿐만 아니라 문자, 실감 방송 등에 대한 워터마킹에 기반을 둔 컨텐츠 보호 관리 기술, 그리고 잘 알려져 있지 않은 바이러스에 대한 유해정보 차단 기술의 고도화가 필요하다.

라. DMB 서비스 정보보호

DMB 서비스는 국민들의 수요에 부응하는 고품질의 음성 및 영상 서비스를 언제 어디서나 제공할 수 있는 이동멀티미디어 방송 서비스이다. 세계 최초의 상용서비스 도입으로 디지털방송기기 산업과 컨텐츠 산업에 활력을 부여하고 있다. 고속이동 중에도 동영상 및 CD 수준의 오디오, 멀티미디어 데이터 서비스 안정적 수신이 가능한 이동멀티미디어방송 서비스이다. 2004년부터 차세대방송포럼에서 한정수신시스템 특별위원회를 결성하여 한정수신제한 시스템에 대한 표준규격 작업을 추진할 예정으로 있으나, 무료 서비스를 지향하고 있음으로 해서 그 필요성이 현재는 미미한 실정이다.

DMB 서비스 위협은 유료서비스인 경우 권한이 없는 사용자에 의한 서비스 도용, 전송 매체에서 발생 가능한 도청, 변조 등의 위협, 그리고 등급화된 컨텐츠의 불법 사용 등이다.

DMB를 위하여 현재 개발된 정보보호 기술은 거의 없다.

개발되어야 할 정보보호 기술은 이용자 신원 확인 서비스, 디바이스 인증 등의 DMB 서비스 서버에 대한 보안 기술, 한정수신기술 등의 DMB 단말 보안 기술, 그리고 내용 기반 유해 정보 차단 기술 등의 DMB 게이트웨이 보안 기술, 트래픽 상태 모니터링 제어 기술을 포함하는 인프라 보안 기술 등을 들 수 있다.

마. 홈네트워크 서비스 정보보호

홈네트워크 기술은 가정 내의 통신, 방송, 가전, 정보기기 등을 유무선 네트워크로 상호 연결하여 가정의 안팎에서 언제 어디서나 원하는 단말로 원하는 정보를 주고받을 수 있는 환경을 제공하는 것을 의미한다. 홈 네트워킹은 Ethernet을 비롯한 HomePNA, IEEE 1394, PLC, 무선LAN, WPAN, 등을 통해 구현되며, 네트워크화 된 가정 내 디지털 정보 기기들 간의 기능공유, 데이터 공유, 원격 제어 등을 가능하게 한다. 또한, 인터넷 액세스와 오디오/비디오 스트림, 홈 컨트롤 애플리케이션 및 서비스를 비롯하여 기타의 네트워크화 된 장비에 애플리케이션과 서비스를 분배해 주는 기능을 수행한다. 홈 네트워킹의 기본 구조는 내부와 외부 네트워크를 연결하는 홈 게이트웨이, 전화선, 전력선, 무선 등으로 내부망을 연결하는 홈네트워킹, 정보기기를 제어하며 상호 연동시키는 미들웨어, 홈 네트워킹 기능이 추가된 정보기기 등으로 구성 된다.

홈네트워크 서비스에서의 홈 디바이스에 대한 불법 제어와 홈 서버에서 제공하는 홈서비스에 대한 불법 도용 가능성이 매우 증대될 것이다. 홈네트워크 정보기기에 대한 불법적인 공격은 개인의 프라이버시 침해뿐 아니라 생명 및 재산까지 직접적인 피해를 줄 수 있어 보안 취약성이 존재한다.

현재 개발 중에 있거나 향후 개발되어야 할 정보보호 기술은 사용자 또는 홈네트워크 서비스를 위한 인증/인가 기술, 컨텐츠 보호기술, 홈게이트웨이 DoS 공격 탐지 및 침입 차단 기술, 콘텐츠 보호 기술, 디지털 저작권 보호 기술, 그리고 내외부 단말에 대한 프라이버시 보호 기술 등이 있다. 또한 홈네트워크 서비스를 위한 디바이스 인증을 위한 인증체계 고도화, 기존의 보안 기술의 홈네트워크로의 정합 기술, 그리고 보안기술을 위한 보안 가이드라인 등이 존재한다. 또한 홈 구성원이 편리하게 보안기능을 관리할 수 있게 하는 사용자 중심의 홈네트워크 보안관리 기술 개발도 수행되어야 한다.

바. 텔레메틱스 서비스 정보보호

텔레매틱스는 통신(Telecommunication) 과 정보과학(Informatics)이 결합된 용어로서, 차량의 위치 파악기술과 양방향 통신이 가능한 시스템을 이용하여 차량 내 정보단말을 통해 차량과 운전자에게 유용한 다양한 정보 및 서비스를 제공하기 위한 종합적인 정보서비스를 의미한다. 종래의 경우에는 무선통신과 GPS 기술을 이용하여 차량 운전자의 운전보조기능과 전통적인 교통시스템의 효율성을 확보하는 데 중점을 두어 왔으나, 이제 점차 버스, 기차, 승용차 등의 차량 탑승자를 위한 멀티미디어 서비스로 관심이 모아지고 있다. 따라서 텔레매틱스 기술을 통해 일반 탑승자들에게 일상생활의 상당부분을 차지하는 제한된 차량 공간 내에

서 보다 쾌적하고 향상된 운전환경을 제공함으로써 차내 공간이 비즈니스나 여가선용이 가능한 제 3의 공간으로 재조명 될 것으로 예측된다.

텔레매틱스 서비스의 경우, 서비스 임시 사용자에 의한 불법 서비스 도용 및 프라이버시 침해 가능성이 존재하고 있다. 또한 사용자의 위치 정보에 대한 침해 가능성도 있다. 이를 통하여 텔레매틱스 서비스 장애를 유발시키거나 불법 사용에 의한 금전적 피해가 우려되는 상황이다.

현재 개발되어 있는 정보보호 기술은 OSGi에서 개발되고 있는 객체 기반 정보보호 기술 등이 있다.

향후 개발되어야 할 정보보호 기술은 위치 정보에 대한 프라이버시 보호 기술, 무선 구간 암호화 기술, 게이트웨이 DoS 공격 방지 기술, 침입 탐지 기술, 그리고 컨텐츠 보호 기술 등을 들 수 있다.

사. VoIP 서비스 정보보호

VoIP(Voice over IP) 서비스는 인터넷의 IP 프로토콜을 이용하여 음성을 전송하는 기술을 말하는 것으로, 기존 IP 네트워크를 그대로 활용해 전화서비스를 구현함으로써 전화 사용자들이 저렴한 요금만으로 인터넷, 인트라넷 환경에서 시외 및 국제전화 서비스를 받을 수 있게 된다는 점이다.

적용되는 기술의 범위에 따라 웹투웹 서비스 또는 인터넷 텔레포니(Internet Telephony) 등의 서비스가 있다. 웹투웹 서비스는 사용자의 음성 신호를 디지털 신호로 변환한 후 IP 네트워크를 통해 수신자까지 전달하는 과정을 의미하며, 인터넷 텔레포니(Internet Telephony)는 IP 네트워크와 공중 전화망 (PSTN: Public Switched Telephony Network)이 연동되어 음성 서비스를 제공하는 것을 의미한다. 이 경우 저렴한 음성 서비스를 제공하기 위해 IP 네트워크를 이용하여 필요한 경로에만 기존 통신망을 사용하는 경우가 많다. 이 경우 국제전화나 시외 전화 같은 고비용의 PSTN 전화통화 서비스를 대체하여 저렴하게 이용할 수 있다.

주요 위협은 불법 사용자에 의한 서비스 도용, 게이트웨이에 대한 DoS 공격, 사용자에 대한 위치 정보 침해 등이 있다.

개발되어야 할 VoIP를 위한 보안 기술은 사용자 및 단말 인증 기술, VoIP 종단간에 암호 기술, 위치정보 보호기술, 보안 호환성을 위한 보안 알고리즘 표준화, 위치 식별 보호 기술, 단말기에 대한 인증 기술, 게이트웨이에 대한 DoS 공격 방지 기술, 그리고 통합 인증/인가/과금 기능 등이다.

아. 전파식별 서비스 정보보호

전파식별은 무선 통신 기술을 이용하여 사물을 식별하고 주변 상황에 대한 센싱 정보를 담고 있는 태그와 관련된 기술이다. 전파식별 태그는 기존의 바코드를 대체할 수 있다고 할 수 있으나, 기존의 바코드가 오직 사물을 식별하기 위한 정보만을 담고 있고 리더기와의 통신이 물리적인 접촉을 통하여 이루어지는 반면에 전자태그는 식별 및 센서를 포함할 뿐만 아니라 무선 통신 기술의 활용이 가능함으로써, 인터넷 등의 공개된 통신망에 연결되어 다양한 응용 서비스의 창출이 가능하다. 전파식별과 관련된 주요 시스템 구성 요소는 사물에 부착되어 사물에 대한 유일 식별 정보를 포함하는 전파식별 태그, 전파식별 태그와 무선으로 접촉하여 관련 정보를 읽어오거나 쓰는 리더기(reader), 리더기와 인터넷 등의 공개된 통신망으로 연결되어 특정 응용(상품 정보 관리 서버 포함)으로 구성되어 있다. 전파식별의 주요 특징은 무선 기술을 활용하므로 비접속 방식으로 동작할 수 있으며, 리더기와 전파식별 태그와의 거리가 수십 센티에서 수십 미터까지의 전송거리를 가지며, 인식속도도 기존 바코드(4초 정도)와는 비교할 수 없을 정도로 빠르고(0.1초 이내), 기존 IT 시스템과 실시간 처리가 가능하며, 재사용이 가능한 특징을 가지고 있다. 전파식별 태그는 전원 유무에 따라서 능동형 전파식별과 수동형 전파식별, 쓰기 기능 여부에 따라 읽기 전용 전파식별 태그와 읽기쓰기 공용 전파식별 태그, 상황을 인지하기 위한 센서와 리더가 아닌 이웃 노드 간에 통신을 위한 통신 기능을 부가한 센서/통신 부가형 전파식별 태그, 그리고 여기에 다양한 암호 기능이 부가된 스마트형 전파식별 태그 등으로 구분될 수 있다. 센서/통신 부가형 전파식별 태그와 스마트형 태그가 USN에서 활용될 수 있는 태그이다. 전파식별이 사용하는 주파수는 크게 저주파수(135KHz 이하), 고주파수(13.56Mhz), 극초단파(868-915MHz), 마이크로파(2.45Ghz)를 사용하며, 극초단파 대역을 사용하는 전파식별이 가장 저가로 구현 가능한 전파식별 태그이다. 전파식별 태그가 포함하고 있는 정보는 EPC (electronic product code)라 불리 우며, 64 비트와 94 비트 정보로 구성되며, 94 비트의 경우, 8 비트의 헤더, 28 비트의 제조업자 번호, 24비트의 상품 번호, 36 비트의 상품 일련번호로 구성되어 있다. EPC는 제조업자, 상품의 유형을 나타내는 상품 번호, 상품의 고유번호인 일련번호를 포함하고 있다.

전파식별에서 나타날 수 있는 위협의 원인은 전파식별 자체가 가지고 있는 취약성(정보의 위변조 용이성, 태그의 리더기 인증 부재 등), 무선 링크의 이용, 그리고 중앙 집중화된 전파식별 태그 정보 관리에 기인한다. 이러한 특성에 기인하여 전파식별에 나타날 수 있는 위협은 전자태그의 정보를 위조함으로써 나타날 수 있는 위협, 전자태그와 리더기간에 교환되는 정보를 도청함으로써 발생하는 위협, 그리고 불법의 리더기를 이용하여 전자태그에 대한 정보를 취득함으로써 발생하는 위협 등으로 분류될 수 있다.

전파식별을 위한 현재 개발되고 있는 간단한 정보보호 기술은 태그의 기능을 중지시키는 방식, 패러데이 보호망을 이용하는 방법, 방해 전파를 이용하는 방법 등 다양한 방법이 제안되고 있다.

향후 개발되어야 할 전파식별 관련 정보보호 기술은 리더기 인증, 태그 인증, 리더기와 태그간에 정보 유출 방지 기술, 그리고 개인정보보호 기술에 초점이 맞추어 수행되고 있다.

2.1.2 9대 신성장 분야 정보보호기술

9대 신성장 동력 분야는 주로 디바이스 차원의 정보보호가 요구된다. 다양한 서비스를 위한 이동 단말기기를 통한 개인정보의 다량 수집 및 유출 위협이 증가하고 있으며 다양한 유형과 기능의 무선 단말기기가 갖는 취약한 보안성은 시급한 과제로 부각되고 있다. 또한 디지털 컨텐츠에 대한 불법복제 및 유통량의 증가가 튼 문제가 되고 있다. 유비쿼터스가 제공할 키워드인 '언제, 어디서나, 누구나' 신뢰할 수 있는 디바이스가 제공되기 위해서는 개인정보의 사용제한이 가능한 능동형 프라이버시 보호기술이 절실하다. 임베디드 기술을 통한 보안 S/W 기술개발 및 보안기능 탑재(Security Embedded Device)가 필요하며 DRM 요소기술 및 기반구조 개발과 적용을 통한 안전한 컨텐츠 유통환경의 구축이 선행되어야 할 것이다.

가. 차세대 이동통신

가정, 사무실, 옥외 및 공중에서 정지 및 이동 중에 음성, 문자, 그림, 동영상 등과 같은 다양한 형태의 멀티미디어 정보를 안테나를 통해 인터넷 망과 연동하여 고속, 고품질로 송수신하는 통신방식이다. 주요 통신 방식은 이동 통신, 위성통신 등을 들 수 있다. 이 분야는 4세대이동통신, 휴대인터넷, Enhanced IMT-2000 및 초고속 무선 LAN을 포함하는 개념이다.

위협 요인은 주로 인증 부재로 인한 불법 단말기에 의한 서비스 도용과 불법 도청, 통합망 이동기기에 대한 웜 공격 및 스팸 등 보안 위협 증가와 단말기 불법 복제 증가 등을 들 수 있다.

현재 개발되어 있는 무선 LAN에 대한 표준은 IEEE 802.11i 위원회에서 개발된 EAP와 AAA (Authentication,. Authorization, Accoutability) 기반의 사용자 인증 기법, 인증의 부산물로 공유되는 키 관리 기법, 기밀성 및 무결성 보장 기법 등이 존재한다. 또한 제2세대 또는 제3세대 이동통신망을 위한 정보보호 기술, 위성망을 위한 정보보호 기술 등이다.

향후 개발되어야 할 정보보호 기술은 무선 링크 정보보호 기술과 이동성 지원을 위한 단말과 인프라의 디바이스 보안 기술, 그리고 다양한 이동망간의 연동 보안 기술 등이다. 또한 경량화 되고 저전력이 요구되는 무선 해킹방지 칩셋 기술, 생체기반 개인 인증/인가 통합 기술, 휴대 인터넷 인증/인가 기술, 그리고 휴대 인터넷 VPN 기술을 들 수 있다.

나. 디지털 TV

디지털 TV 기술은 아날로그 방식의 TV를 디지털 방식으로 변경한 것으로, 흑백시대·컬러시대를 거친, 이른바 제3세대 텔레비전이다. 디지털텔레비전은 여러 가지 기능을 더할 수 있는 별도의 IC를 부착, 방송국에서 보내는 아날로그신호를 디지털 신호로 바꾸어줌으로써 영상 및 음성신호의 열화를 방지해줄 뿐만 아니라, 그것을 정확히 복원시켜 주기 때문에 아날로그 전파의 반사로 생기는 이중화면도 볼 수 없고 잡음도 전혀 없다. 디지털텔레비전이 출현하게 된 것은 1982년에 독일의 인텔말사(社)가 아날로그신호를 디지털신호로 바꾸는 IC를 개발하여 이를 세계에 공급하면서부터인데, 한국에서는 인텔말사의 IC 샘플을 이용하여 디지털텔레비전 생산에 성공하고 이를 1983년 9월에 열린 '한국 전자쇼'에 출품한 바 있다. 디지털 TV를 위한 정보보호 기술은 한정 수신 시스템, 컨텐츠 보호 서비스를 위한 단말 보안 기술이다.

주요 위협 요인은 불법 사용자에 의한 불법 사용자 도용, 사용 권한이 없는 사용자의 컨텐츠 위변조 등이 존재한다.

향후 개발되어야 할 정보보호 기술은 유통되는 컨텐츠를 보호하기 위한 기기 및 사용자 인증 기술을 채택한 디바이스 보안 기술, 한정수신시스템을 위한 디바이스 보안 기술, 그리고 저작권 보호를 위한 디바이스 보호 기술 등을 들 수 있다.

다. 홈 네트워크

신뢰성 있는 홈네트워크 인프라 구축을 위해, 유효한 사용자를 구별하며 다양한 정보기기 간에 안전한 통신 및 제어를 가능하게 하는 홈네트워크 환경에 적합한 인증기술을 개발하고, 다양한 침입으로부터 홈네트워크 자원을 보호할 수 있도록 접근권한을 능동적으로 조절할 수 있게 하는 접근권한 제어기술을 개발이 필요하다.

주요 위협은 홈네트워크 정보기기에 대한 불법 접근으로 인한 홈 안전사고 우려 등이다.

주요 정보보호 기술은 홈네트워크 기기의 다양한 보안취약성을 분석하고 홈네트워크 환경에 적합한 디바이스 인증 및 접근제어 프레임워크, 사용자 중심의 보안 서비스 제공이 가능하도록 홈네트워크 환경에 적합한 경량화된 인증기술 및 암호기술 개발, 침해 발생시 자원에 대한 접근권한을 능동적으로 변경하여 홈네트워크 자원에 대한 안전성을 강화하게 하는 디바이스 보안 기술 등이다.

라. IT SoC

홈 네트워크 서비스의 안전한 제공을 위해 해킹 및 웜 등의 사이버 공격을 효과적으로 탐지 및 방지하는 침해방지 SoC 기술 개발이다. 주요 정보보호 기술은 각종 네트워크 서비스 제공을 위한 침해방지 SoC 기술 및 검증 플랫폼 개발, SoC기반의 IP개발을 통해 침해방지를 위한 핵심요소기술들을 Component화, 이를 기존의 상용 IP와 SoC공정에 의해 Chip화, 각종 플랫폼에 탑재하여 국가 또는 국제공인수준의 검증하는 기술 등이다.

주요 위협은 신규 서비스를 위한 고속 보안 SoC 기술 부재 및 경량화된 보안 기능 미비 이다.

주요 정보보호 기술은 사용자 식별 생체 인증 기술, 고속/고비도 하드웨어 기반 암호처리 연산 기술, 보안 SoC 기술 등이 있다.

마. 차세대 PC

차세대 PC 기술은 착용형 컴퓨터, 액세서리형 컴퓨터 등이 있으며, 여기서는 프라이버시 침해 위협에 노출될 가능성 높고, 네트워크 기반으로 정보 이용 환경에 맞는 서비스를 제공하기 때문에 자신도 모르는 사이에 데이터가 제3자에게 노출될 위험 있으며, 또한, 이러한 휴대형 장비에는 다양한 서비스 사용을 위한 보안 토큰, 비밀키 등을 저장하기 때문에 타인이 개인용 장비를 사용할 경우 서비스에 대한 불법사용 가능하다.

주요 정보보호 기술은 차세대 PC 자체 보호 기술, 착복형 컴퓨터 등의 차세대 PC에서 프라이버시 침해 방지를 위한 접근제어기술, 그리고 차세대 PC용 보안 핫키 기술 이다. 차세대 PC용 보안 핫키 기술은 일반 사용자 데스크톱 컴퓨터에서 OS 및 주요 보안 응용 소프트웨어에 대한 패치 등의 업데이트가 요구되는 경우 function key와 같은 역할을 하는 보안 핫-키를 스트로크 함으로써 편리하고 안전한 보안 업데이트 기능을 제공할 수 있다.

바. 임베디드 S/W

임베디드 SW는 모든 사물을 지능적으로 만드는 (Make Things Smart)핵심 솔루션으로 최근 디지털 융합에 따라 IT 제품의 지능·다기능·소형화가 가속화됨에 따라 휴대폰, 디지털 TV, 게임기, 항공기 등 다양한 제품에 내장되어 제품의 부가가치를 제고하는 기능을 수행한다. 현재의 포스트-PC 시대가 과거 IBM 주도의 메인프레임 시대가 PC의 등장에 따라 퇴조하고 시장의 주도권이 MS에게 넘어간 1990년대 초와 매우 유사한 것을 감안할 때, 임베디드 SW 산업은 세계최고의 초고속 인프라를 보유하고 가전, 휴대전화에서 자동차까지 HW 생산기술이 뛰어난 우리에게 포스트-PC 시대의 세계 IT시장에서 새로운 도약의 전기를 마련할 수 있는 분야이다.

임베디드 소프트웨어를 위한 정보보호 기술은 안전한 운영체제 보안 기술 및 생체 정보 기반 사용자 인증 기술 등이 존재한다.

사. 디지털 컨텐츠,

디지털 컨텐츠 보호 기술은 방송/통신망이 융합되고 홈 네트워크에서 방송 컨텐츠 소비가 이루어지는 차세대 방송 컨텐츠 서비스 환경에서 불법복제 방지 및 단말간의 컨텐츠 이동 및 공유를 지원하는 정보보호 기술이다. 방송·통신 융합 하에서 방송 컨텐츠를 소비하는 다양한 단말(DTV 셋톱박스, PC, Mobile 단말기)에서 컨텐츠 저작권 보호, 불법 복제/배포/유통 방지, 단말간 컨텐츠 이동 및 공유·사용제어를 지원하는 상호운용 가능한 적응형 방송 컨텐츠 보호관리 프레임워크 기술 개발이 요구된다.

주요 위협은 방송 컨텐츠 불법 복제 및 유통 증가, 유료 컨텐츠 과금 및 지불 방법 미비 이다.

주요 정보보호 기술은 단말간 방송 컨텐츠 이동 및 공유를 위한 방송 컨텐츠 보호관리 기술, 다양한 방송 컨텐츠 보호기술의 상호 운용성을 지원하는 프레임워크 기술 개발, 방송 컨텐츠 보호기술 국내/국제 표준 연

구, 멀티미디어 불건전 컨텐츠 차단기술 등을 들 수 있다. 특히 멀티미디어 컨텐츠 차단 기술은 인터넷 기술의 발전으로 다양한 유무선 인프라와 통신 단말들을 통해 유통되는 멀티미디어 형태의 음란/폭력/불법 등의 불건전 정보를, 컨텐츠의 내용별로 불건전 정도를 판단하고 분류 및 차단할 수 있는 기술 개발이며, 유무선 환경에서 주로 사용되는 온라인 응용 프로그램과, 멀티미디어 서비스를 통하여 전송되는 음란/폭력/불법 멀티미디어 컨텐츠에 대한 불건전 정도를 자동화되고 선별적으로 분류하고 차단할 수 있는 기술이다.

아. 텔레메틱스

텔레매틱스 센터의 강력한 서버 시스템을 통신을 매개로 하여 차량내에 Virtually Embeded되어 다양한 서비스 제공하며, 이동통신서비스, 초고속 인터넷 인프라와 GIS/LBS/ITS 등 다양한 정보시스템을 기반으로 제공되는 종합적인 서비스이다.

주요 위협은 사이버 공격에 의한 서비스 장애 및 단말기 불법 접근으로 사고 피해 우려 이다.

정보보호 기술은 텔레매틱스 서비스 통합 보안 미들웨어 개발, 텔레매틱스를 위한 인증 및 접근권한 제어 기술 개발, 상황인지 기반 지능형 보안 에이전트 기술 개발, 위치정보에 대한 개인 프라이버시 보호 기술, 대용량 교통정보 데이터베이스 보호 기술 및 디바이스 Jamming 방지 기술, 텔레메틱스 서비스용 게이트웨이에 대한 침입탐지 및 방어기술, 유해 트래픽으로 게이트웨이를 공격하는 것을 탐지하고 방어하는 기술 등이다.

자. 지능형 로봇

기존의 로봇에 네트워크를 부가한 URC 개념을 도입함으로써 다양한 고도의 기능이나 서비스 제공이 가능하고 이동성과 휴먼 인터페이스가 향상된 로봇 시스템으로 진화하고 있다. URC(Ubiquitous Robotic Companion)의 범위에는 네트워크 인프라에 연결되고 지능을 갖추고 있어야 하되 이동성 측면에서 기구적 이동뿐만 아니라 제어 소프트웨어에 대한 이동까지도 포함하고 있다. 지능형 서비스 로봇 기술은 모션 등을 제어하는 메카트로닉스 기술, 인식 등 지능화 기술, 인터페이스 기술 등과 이들 각각을 통합하는 통합 시스템 기술로 분류한다.

주요 위협은 지능형 로봇에 대한 불법 접근으로 서비스 중단 및 제어 서버 및 로봇을 해킹하여 얻을 수 있는 개인정보 유출 피해 우려이다.

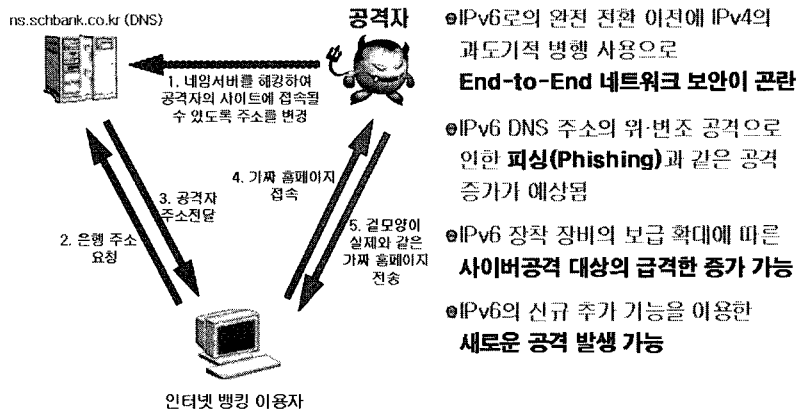
이를 위한 정보보호 요구사항은 로봇 외부의 부정한 디바이스나 부정한 사용자에 의하여 로봇의 이용을 방지하는 고도의 인증기술과, 네트워크기반 지능형로봇에 다양한 형태로 명령을 주는 경우, 이에 대한 인증프로토콜, 불특정 제3자가 네트워크에 연결된 로봇을 부정하게 동작시키거나, 로봇이 네트워크에 연결하여 취득한 정보를 부정하게 읽어내거나 고치거나 혹은 도청을 방지하기 위한 간섭 불가(Tamper Resistant) 기술 및 이를 위한 경량 암호화방식의 기술, 소프트웨어 로봇 에이전트를 인증, 허가하는 프로토콜의 제정이 필요, 향후에는 정보의 안전성 및 비밀정보를 안전하게 관리하는 프라이버시 정보관리 등을 위한 고도의 정보보호 기술, 네트워크에 연결된 로봇간의 시큐리티에 관련된 프로토콜 개발 및 Multi Modal 생체 센싱 정보의 통합화를 위한 기술 필요하다.

현재 개발을 고려중인 기술개발 항목은 URC용 임베디드 소프트웨어 보안 플랫폼 및 미들웨어 개발, 지능형 로봇 플랫폼을 위한 차세대 암호 시스템 개발, 인증 및 기밀성을 포함하는 무선 링크를 위한 URC 기반 무선통신 보안 기술 등이다.

2.2 인프라 분야 정보보호

IT839 전략에서 3대 인프라는 유·무선 인터넷 및 방송과 통신이 융합되는 광대역통합망(BcN), 모든 사물에 전자태그를 부착하고 인터넷에 연결하여 정보를 인식하고 관리하는 유비쿼터스 센서 네트워크(USN) 그리고 인터넷 주소 고갈 문제를 해결해 줄 차세대 인터넷 프로토콜인 IPv6 등이 있다.[2,9]

그러나 3대 인프라 도입 및 통신·방송의 융합으로 인하여 사이버 위협의 대상은 IP를 사용한 특정 망에서 통합된 망으로 확대되어질 예정이며, 피해 확산 속도가 기존망보다 훨씬 빠르며, 피해 규모 역시 확대될 것으로 예상되고 있다. 이러한 인프라 측면에 있어서 새롭게 대두되고 있는 위협요소들은 아래와 같다. 첫째, 침해로 인한 피해정도가 대규모로 발생한다는 것이다. 둘째, 기존의 개별 통신망들이 상호 통합되고 융합되는 환경에서 개별망의 피해가 BcN으로 연결된 모든 구성 네트워크로 확산될 소지가 매우 높다는 것이다. 셋째, IPv6 망을 기반으로 하기 때문에 IPv4 망에서 발생되었던 기존의 위협과 동시에 IPv6에서 새롭게 발생될 수 있는 취약점이 있다는 점과, IPv4/ IPv6 망 혼재에 따른 취약점 발생 가능성이 증가하게 될 가능성이 높다는 것이다. 넷째, 초경량, 저전력의 RFID/USN 자체의 특성에 따른 서비스거부공격(DoS)과 프라이버시 침해가 확대될 가능성이 매우 높다는 점이다.



〔그림 3〕 IPv6 보안 위협

이는 USN에서는 도처에 설치된 여러 가지 센서를 통하여 사용자의 위치, 쇼핑정보, 뱅킹정보 등을 수집하기 때문이다.

2.2.1 IPv6

IPv6은 프로토콜은 설계 시 메시지 인증 구조, 암호화된 채널의 도입 등 보안에 대하여 고려되었지만, 주로 기밀성의 위협에 대한 대응으로 초점이 맞추어져 있었다. 그러나 기밀성의 보장 이외에 IPv6 환경에서 예상되는 보안위협은 다른 여러 분야에서 나타날 수 있다. 첫째, 기존 IPv4에서 IPv6로 전환하는 단계에서 발생할 수 있는 관리자의 설정 오류 등 운영 미숙, 공격 발생 시 차단 미숙 등 인적 요인과, 장치들이 IPv4와 IPv6 동시지원에 따라 생기는 전환상의 위협을 예측할 수 있다. 둘째, IPv6 대상 해킹도구 개발 및 유포 그리고 공격자가 기밀성이 보장되는 IPv6 망을 악용하여 비밀통신 수단으로 이용하는 위협이 예측된다. 다시 말해, 기존의 IPv4에서 침입 탐지가 가능한 공격이 IPv6에서 암호 채널의 사용으로 인하여 이의 탐지가 불가능하게 되는 문제가 발생하게 된다. 셋째, 자동 환경 설정, 이동 IP 지원 등 IPv6에서 강화된 이동 컴퓨팅 환경 으로 인한 위협이 예측된다. 넷째, 이동환경에서 Home Address Option (HAO)을 사용한 DoS 공격, 라우팅 헤더를 이용한 공격 등 Mobile IPv6 프로토콜을 악용하여 발생하는 위협이 예측된다. 그림 3은 IPv6 관련 주요 보안 위협이다.

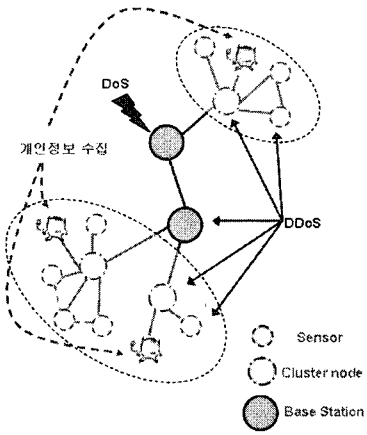
요구되는 정보보호 기술은 IPv4/6 변환을 위한 변환 노드(게이트웨이) 정보보호 기술, IPv6 게이트웨이 보안 기술, 이동 IP 지원 정보보호 기술, IPv6를 위한 침입 차단 및 탐지 기술, IPv6용 P2P 보안 기술 개발, 그리고 이동성 지원에 이용되는 인증/인가/과금 시스템을 위한 정보보호 기술을 들 수 있다.

현재 개발이 고려되고 있는 정보보호 기술은 (1) IPv6용 라우터 및 게이트웨이에 적용 가능한 멀티플랫폼 침해 방지 기술 개발, (2) DNS의 주소정보 위·변조 방지를 위한 DNSSEC 기술 개발, (3) P2P 오버레이 네트워크 구축기술 개발, P2P 자원 및 정보관리(유출방지) 기술 개발 등으로 구성된 유·무선 IPv6 환경에서 안전한 P2P 환경 구축 기술 개발, (4) 다양한 기기(홈서버, 통신기기, 정보통신장비)에 탑재된 보안 프로토콜의 기능 검증을 위한 IPsec 표준적합성 시험 기술 개발, (5) IPv6를 위한 멀티캐스트 보호기술 등이다.

2.2.2 USN

USN은 여러 개의 센서노드들로 구성되며, 통신 인프라와 연결하기 위한 하나의 기지국이 존재한다. 통신과 센싱 기능을 갖는 전파식별 태그를 이용하므로, 기본적으로 전파식별에서 발생하는 모든 위협에 더하여 다음과 같은 위협들이 추가로 발생하게 된다. 유비쿼터스 네트워크에서 주요 위협은 장치의 도난과 분실, 노드간의 통신 내용의 노출 가능성 증가, 사용자 신원 정보와 위치 정보의 노출 가능성 증대, 불법 기지국 설치, 위조 메시지의 전송, 노드에 대한 DoS 공격, 밧테리 쇠진 공격 등을 들 수 있다. 이러한 공격을 효율적으로 막기 위하여 요구되는 보안 기술은 기밀성, 멀티캐스트 인증을 포함하는 인증 및 무결성, 그리고 신성성(freshness) 기술이다.

USN 환경에서의 보안위협은 다음과 같다. 첫째, 보안위협 대상이 모든 USN에 의하여 연동되는 모든 장



- 사용자 위치, 쇼핑정보 등의 **프라이버시 침해 위험이 증가**
- **Ad-hoc 네트워크 구조**로 인한 **사이버 공격 취약성 증대**
- 소형 USN 장치의 **보유자원을 집중 소모시키는 공격으로 전체서비스가 중단될 위험이 있음**
- RFID ODS의 분산 구성으로 어느 한 **정보의 위·변조는 연쇄적인 보안 위협 초래**

※ ODS : Object Directory System

〔그림 4〕 USN 보안 위협

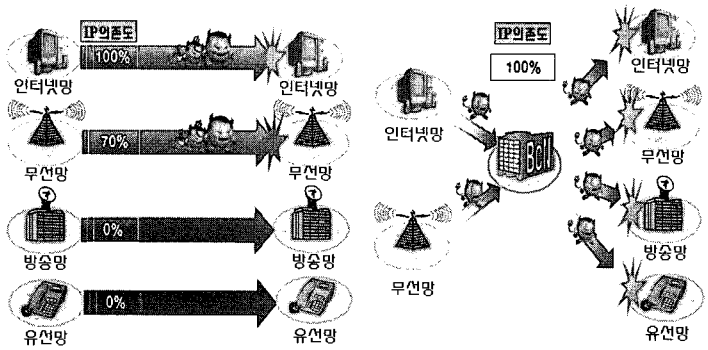
치로 범위가 확대될 것으로 예상되며, 이런 경우 센서 노드에 의하여 검출된 환경에 대한 센서 정보 전달이 단절되거나 잘못된 정보로 인식되는 등의 사고가 발생하고, 환경에 대한 신뢰성을 보장할 수 없게 된다. 둘째, 사물에 부착된 전자태그와 판독기 사이의 정보 흐름에 대한 도청으로 인하여 전자태그에 저장된 정보와 소유자의 개인정보의 노출 등 기밀성을 침해하는 위협이 크게 증가할 것으로 예측된다. 셋째, 비정상적 정보를 포함한 불법적인 복제태그의 대량 유통과 이를 악용하여 비정상적인 트래픽을 발생시켜 네트워크를 마비시키는 등 가용성을 침해하는 위협이 늘어날 것으로 예측된다. 마지막으로, 전파식별 등에 수록된 정보를 변조시키거나 위조하는 등의 위협도 증가할 것으로 예측된다. 그림 4는 USN 관련 주요 보안 위협을 나타내고 있다.

요구되는 정보보호 기술은 센서 태그에 대한 인증 기술, 센서 태그와 리더기간에 무선 링크상의 도청 방지 기술, 센서 노드에서 시작하여 정보 종단점까지의 기밀성 및 무결성 보장 기술, 센서 노드간 정보흐름에 대한 기밀성 보장 기술, USN과 BcN을 연결하는 기지국에 대한 서비스 거부공격 방지 기술, 그리고 센서 노드에 대한 재밍 방지 기술 등이다.

향후 개발되어야 할 정보보호 기술은 (1) 사용자 개인 정보 관리를 위한 주문형 프라이버시보호 기술, (2) 사용 환경에 따라 가변적으로 적응하는 상황 인지형 프라이버시 보호 기술 개발, (3) 센서 정보의 위·변조 등을 차단할 수 있는 초경량 보안칩/센서 노드 기술 개발, (4) 도청, 위·변조 등의 공격에 대응하기 위한 USN 침입탐지 및 대응 기술 개발, (5) DNS-SEC (Domain Name Server-Security) 기반의 ODS (Object Directory Server) 위·변조 방지 기술 개발, (6) 핵심 미들웨어 및 경량 객체보안(Light-weight Object oriented embedded Security) 플랫폼 기술 개발, (7) 애드혹 연동 동적 네트워크 보안 기술 등이다.

2.2.3 광대역 통합망

광대역통합망(BcN)의 구축은 이종망간에 끊김 없는 멀티미디어 서비스 제공이 가능해짐에 따라 언제, 어디서나, 누구든지 편리하게 이용할 수 있는 환경으로 진화하고 있다. 광대역통합망 환경에서는 기존 인터넷망에 잠재된 취약점에 추가적으로 융합망의 특징이 반영된 신규 보안 위협이 나타날 것으로 예측된다. 첫째, 네트워크의 광대역화로 악성코드의 전파 역시 급속하게 진행되어 취약한 네트워크 기반을 마비시킬 수 있다. 둘째, 기존 IP망과 분리되어 운영되고 있는 방송·전화망 등이 유무선 인터넷망과 통합되어 운영되므로 공격에서 상대적으로 안전했던 전화망, 방송망으로 공격이 전이되어 피해 범위 확산이 우려된다. 셋째, 휴대폰, PDA등 기능이 융합된 휴대 단말기와 유비쿼터스 환경을 구성하는 전파식별 등 내장형 장치들을 대상으로 한 해킹 및 웜·바이러스가 발생할 것으로 예측되며, 이들이 네트워크 기반을 공격하는 경우 현재의 개인용 PC에 의한 공격보다 매우 넓은 범위에서 공격이 이루어져 더욱 위협적일 것으로 예측된다. 그림 5는 단일 망의 침해가 모든 다른 구성망(예를 들어, 인터넷망, 무선망, 방송망, 그리고 유선망) 으로 확산되는 것을 나타내는 BcN 관련 주요 보안 위협을 나타내고 있다.



〔그림 5〕 BcN 보안 위협

요구되는 정보보호 기술은 (1) 신호 등을 위한 제어 및 응용계층에서 요구되는 정보보호플랫폼 구조 개발 및 관련 기술 표준화, BcN 기반 서비스의 안전한 제공을 위한 보안기술 참조모델 개발 등으로 구성된 안전한 접속환경 구현을 위한 정보보호플랫폼 구조 개발, (2) 무선 액세스망을 위한 링크레벨 보안 기술, (3) 이동성 지원을 위한 보안 기술, (4) 신뢰성 있는 DNS 서비스 제공을 위한 차세대 DNS 보안관리 체계 구축, 장애발생 망에 대한 분리가 용이하도록 그룹별 IPv6 주소 할당체계 수립, 침해사고의 확산을 방지하기 위한 망분리 메커니즘 개발 등으로 구성된 BcN 안전관리 체계 구축, (5) 정보보호 장비간 연동을 위한 BcN 통합정보보호시스템 구축, (6) 초고속 네트워크 정보보호 기술 개발, (7) 정보보호 정책기반의 보안관리기술 개발, (8) 침해사고 분석 및 대응기술 개발, (9) 다양한 접속환경을 지원하는 망간 상호인증기술 개발정보보호 관련기술 개발 등이다.

2.2.4 3대 인프라 정보보호 추진 전략

3대 인프라의 보안위협에 대응하기 위한 정보보호 전략을 제시하면 다음과 같다.[2]

첫째, 망 융합에 따른 트래픽 모니터링 영역 확대 등 침해사고 발생 시 사전 감지 및 피해를 최소화할 수 있도록 사이버공격 예방 및 고도화 전략이 마련되어야 한다. 즉, 방송망 등에 대한 공격의 발생이나, 지능형 홈을 위한 제어센터 등에 대한 공격은 그 피해가 단순히 개인에 한정되지 않고 불특정 다수에게 피해가 예상되기 때문에, 이와 같은 피해를 예방하기 위하여 공격을 조기에 탐지하고 피해를 예방하기 위한 대책이 필요하다. 둘째, 3대 인프라 환경에 적용 가능한 고성능 정보보호 요소기술 확보가 필요하다. 또한 이러한 정보보호 요소 기술들을 사물에 내장된 초소형 내장형 시스템들과 연계하여 능동적으로 공격에 대응할 수 있는 능동적 통합보안기술과, IPv4 환경에서 IPv6로 안전하게 전환하기 위한 기술의 확보도 필요하다. 셋째, IPv6 또는 RFID/USN 등에 적용하기 위한 정보보호제품의 안전성 검증 및 정보보호 제품 간 상호 연동성 보장을 위한 표준 제정 및 표준적합성 인증 등을 위한 제도가 필요하다. IPv6가 적용된 환경에서는 매우 많은 정보기기들이 서로 연동되어 작동하고, 각각이 서로 다른 특성을 가지고 있으므로 각 기기들에 내장된 정보보호 기능들을 연동할 수 있도록 관련된 표준이 필수적으로 마련되어야 한다. 넷째, 방송망에 대한 사이버공격의 발생 등 망 융합에 따른 정보보호 환경의 변화를 수용할 수 있고, 온·오프라인 상에서 개인의 프라이버시를 보장할 수 있도록 정보보호 관련 법·제도 정비가 필요하다. 기존의 방송망, 통신망 등이 분리된 환경에서는 각각의 영역에 따라 관련 법규가 존재하여 왔으나, 통합망 환경에서는 각 망의 영역을 특성에 따라 분리하기 어려우므로, 이와 같은 환경에서 발생하는 역기능에 대응할 수 있는 법규가 필요하다. 또한 전파식별, 내장시스템 등이 보편화됨에 따라 개인정보가 누출될 수 있는 가능성이 확대되므로, 이러한 환경에서 개인정보를 보호해 줄 수 있는 제도의 확립이 필수적이다.

Ⅲ. 결 론

지금 정보통신부에서는 IT839 정보보호를 위한 종합적인 로드맵을 발표하고, 신뢰성 있는 IT 인프라를 개발하고 있다. IT839 정보보호를 위한 지금까지 수행된 정보보호 기술과 향후 개발되어야 할 정보보호 기술을 살펴보는 것은 매우 중요하다. 본 고에서는 지금까지 발표된 각종 자료 및 논문을 바탕으로 하여, IT839 각 분야의 기술 및 서비스 개요, 각 분야에서 발생하는

주요 위협, 현재 개발된 관련 정보보호 기술, 그리고 향후 개발되어야 할 주요 요소 정보보호 기술을 중심으로 기술하였다. 본고의 결과는 IT839 정보보호 기술 개발 계획 수립 및 관련 정책 수립시 유용하게 활용되기를 기대한다.

참 고 문 헌

[1] 송정희, "IT839 전략과 정보보호과제," Information Security Review, 한국정보보호진흥원, 제1권 3호, 2004년 9월

[2] 이홍섭, "IT839 3대 인프라 보호를 위한 사이버공격 예방 및 대응체계 고도화," Information Security Review, 한국정보보호진흥원, 제1권 3호, 2004년 9월

[3] 임주환, "성공적인 IT839 전략 추진을 위한 정보보호의 필요성," Information Security Review, 한국정보보호진흥원, 제1권 3호, 2004년 9월

[4] 정보통신부, "정보보호 중장기 기술개발 계획(안)," 2004. 12. 6.

[5] 한국전자통신연구원, "8대 서비스의 정보보호 요구사항, 2004.

[6] 염흥열, "IT839 정보보호 기술", 한국정보보호학회, NETSEC-KR'2005, 2005.4.

[7] 정보통신부, 안전한 U-Korea 구현을 위한 중장기 정보보호 로드맵, 공청회 발표 자료, 2005.3.

[8] 정보통신부, 안전한 U-Korea 구현을 위한 IT 서비스 및 디바이스 안전성 확보, 공청회 발표 자료, 2005. 3.

[9] 정보통신부, 안전한 U-Korea 구현을 위한 IT 네트워크 인프라 보호, 공청회 발표 자료, 2005.3.

〈著 者 紹 介〉

염 흥 열 (Heung Youl Youm)

1981년 2월 : 한양대학교 전자공학과 졸업(학사)
1983년 2월 : 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월 : 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~현재 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2004년 1월~현재 : OSIA 이사
2003년 9월~2004년 3월 : ITU-T SG17/Q10, Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
〈관심분야〉 네트워크보안, 전자상거래보안, 공개키 기반구조, 부호이론, 이동통신보안