사물지능통신망에서의 RFID/USN 기반 정보보호 기술동향

동서대학교 ▌이영실 · 박범수 · 임효택 · 이훈재

1. 서 론

미래의 인터넷은 급속도로 증가하는 사용자들의 수요에 대응하기 위해 통신 속도 및 다양한 접속 단말의 증가를 동시에 수용하면서, 센서 등 기존 인프라 및 ICT(Information & Communication Technology) 기술과 융합을 통해 진화하고 있다. 사물지능통신(O2N: Object-to-Object Intelligent Network)은 이러한 변화의 중심에 있으며 사람 對 사람, 사물 對 사물 간 지능 통신 서비스를 언제 어디서나 안전하고 편리하게 실시간으로 이용할 수 있는 미래 통신 융합 ICT 인프라로 부각되고 있다. 이러한 사물지능통신(O2N)은 좁은 의미로는, 기계 간 통신 및 사람이 사용하는 단말과 기계 간의 통신을 의미하며, 넓은 의미로는 통신과 ICT 기술의 결합을 통한 원격지의 사물정보를 확인할 수 있는 제반 솔루션을 뜻한다.

사물지능통신은 기존의 u-City, u-Health, u-교통, u-환경 사업 등을 통해 사회 현안 해결, 재난 · 재해방지, 에너지 절감, CO2 감축 등에 기여할 수 있는 필수적인 인프라로 활용되고 있다. 영국의 경우 올해 1월, 정부 부처와 기관이 업무를 수행하여 생산한 도로, 교통, 항만, 범죄, 재난 등에 관한 2,500여건의 사물정보 데이터를 개방하였다. 또한 중국은 올해 4월 초에 상하이 인근에 약 1,342억 원을 투입 사물지능통신 센터를 세계 최초로 구축했으며, 2010년 10대 유망기술로 선정하여 추진 중이다. 우리나라 역시 기존에 구축된 유 · 무선 통신망을 기반으로 하여 이동통신 사업자를 중심으로 사물지능통신(O2N) 서비스가 활성화되고 있다. 이로써 향후 초고속 유선망 기반의 저속 원격모니터링 분야에서 2G, 3G, Wibro 기술 등 광대역 무선망을 활용한 교통, 건물 · 시설물 관리 및 텔레매틱스 등으로 확대될 것으로 전망하고 있다.

이러한 사물지능통신(O2N)은 재난 · 재해 방지 등 기존의 인터넷과는 달리 매우 중요한 문제에 대한 IT 적용이란 생각을 가지고 있으며, 안전성을 우선순위로 뽑고 있다. 사물지능통신(O2N)을 위해 대부분 무선을 사용하고 있으나 사람들은 무선보다는 유선을 안정적으로 선호하는 입장이며, 이를 해결하기 위해서는 사물지능통신(O2N)의 정보보호 및 보안 분야, 데이터 신뢰성, 통신망의 안전성에 대한 실증적 데이터 확보와 대외에 알리고 인정받는 절차가 필요하다[1].

사물지능통신(O2N)을 이루는 기반기술은 USN, RFID, IPv6, 융합센서, 지능형 로봇, Baseband Modem chip 등이 있으며, 본 논문에서는 이 중 RFID/USN 기반 보안 기술에 중점을 맞추고 살펴보도록 하겠다.

RFID/USN은 주로 무선 통신 기술을 이용하고 여러 개의 디바이스/센서 노드들로 구성되어 있다. 여기에 더해 디바이스/센서 노드들 간의 타협, 또한 RFID/USN 망의 특성상 각 디바이스/센서 노드는 전력과 메모리, 그리고 계산 능력이 매우 제한되어 있다. 또한, 무선 통신 기술을 이용하기 때문에 무선망에서 발생하는 모든 유형의 위협이 그대로 상속되며, 대표적인 위협으로는 데이터 도청, 데이터 위 · 변조, 프라이버시 침해 등이 있다. 이러한 특성을 고려하고 다양한 위협에 대응하기 위해서는 세심한 보안 기술이 적용되어야 하며, 대규모 디바이스/센서 노드를 위해서는 기존의 유선망에서 적용된 보안 기능을 위한 키 관리 기술을 적용할 수 없다. 따라서 대규모 RFID/USN 망에서도 동작 가능한 효율적인 키 관리 기술이 필요하며, 이를 위해 키 관리 기술의 표준화는 매우 중요하다. 이러한 보안 기술은 주로 데이터를 수집하는 베이스스테이션과 디바이스/센서 노드에 적용되어야 한다. 그리고 RFID/USN 망의 구성요소에 유효한 보안 기술을 정의하고 구현 가능한 보안 기술의 적용이 요구된다[2].

이에 본 논문에서는 먼저 정보보호 국가 정책 동향과 RFID/USN의 분야별 주요 정보 기술 동향 및 표준화 동향에 대해서 보았다. 또한, RFID/USN의 보안 취약성 및 분석 사례에 대하여 기술하고 마지막 결론을 통해 서술한다.

2. 정보보호 국가정책 동향

2.1 국내 정보보호 국가정책 동향

2.1.1 개요

1987년 국가기간전산망 사업을 시작으로 u-Korea까지 정보화촉진계획을 수립·시행하면서 초고속정보통신망을 구축하였다. 이를 기반으로 구축된 초고속정보통신망을 기반으로, 유비쿼터스 사회 진입을 위해 광대역 통합망 구축사업을 시작하였다. 또한 행정서비스의 온라인화로 서비스형 정부를 구현, 행정서비스 체계를 일원화하고 공개함으로써 정부의 행정서비스 업무 효율성 향상과 투명도를 높이기 위해 노력하고 있다. 그러나 우리나라는 전 세계로부터 이상적인 IT 테스트베드로 평가받을 만큼 단기간에 IT 강국으로 급부상한 반면, 고도의 정보통신 인프라를 이용한 해킹이나 사이버테러 등 심각한 보안 위협에 노출되어 있는 실정이다[3]. 2003년 1.25 인터넷 대란, 2005년 전자정부 인터넷 민원서류의 위·변조 및 2007년 중국발 해킹 사건, 2009년 7월 미국과 한국의 주요 정부 사이트와 기업 및 금융 사이트에 대한 DDoS 공격, 2010년 5월 "천안함 사고 조사 결과"와 관련한 국가 전산망 해킹 시도 및 인터넷 서비스 사업자(ISP)를 대상으로 한 DDoS 공격과 지방자치단체를 직접적으로 공격한 사건 등을 대표적인 예로 들 수 있다.

이에 국가정보원은 「국가 사이버안전 관리규정」을 제정하여 국가 사이버안전 관리체계를 확립하였다. 제정된 규정의 내용은 중앙행정기관의 장에게 사이버공격으로부터 소관 정보통신망의 안전성을 확보할 책임을 부여하였다. 또한 관계 중앙행정기관의 장은 지방자치단체 및 공공기관 정보통신망의 안전성 확보를 위한 제반조치를 강구하도록 하였다.

2.1.2 상용메일 차단, 정부기관 메일 사용 의무화

대부분의 국가·공공기관은 1대의 PC에서 업무와 인터넷 메일을 사용하고 있다. 이로 인해 업무 PC에서 이메일을 통한 악성코드의 감염으로 저장자료가 유출되어 그에 따른 대책강구가 시급하였다. 국가정보원에서 2008년 10월 1일부로 중앙행정기관 및 지자체 등의 상용메일 사용을 차단하였다. 문화체육관광부는 중앙행정기관 및 지자체에 ID·패스워드를 부여하여 공직자 통합이메일을 사용하도록 하고 있다. 2009년 3월 행정안전부의 인증 서버가 보강, 이후에는 행정전자서명(GPKI)으로만 접속할 수 있도록 보안을 강화하였다.

2.1.3 전자적 비밀관리시스템

현재 우리 정부는 모든 행정업무 수행방식이 네트워크에 의해 전자화되고 있다. 하지만 비밀문서는 여전히 암호화와 같은 별도의 보안대책 없이 과거의 종이 서류 방식으로 보관·관리되고 있다. 이로인해 비밀관련업무의 비효율성과 비밀유출 등 각종 보안사고가 발생하고 있는 실정이다. 이에 국가정보원은 2008년 6월 비밀의 생산·관리 등 비밀처리업무 전 과정에 보안 기술을 적용하였다. 전자화한 비밀관리시스템을 행정안전부와 공동으로 개발하여 통일부에 시험운용을 성공적으로 실시하였고, 비밀 관리업무에 대한 보안성을 강화하고 업무 효율성을 제고하였다.

국가정보원은 2009년 1월 외교통상부 및 방위사업청 등 현재 방송통신위원회까지 대상을 확대하였다. 국가용 보안장비와 행정전자서명을 적용하여 사용자 관리와 접근 제어를 통한 보안성 강화를 시도하였다. 시스템의 성능개선을 지속적으로 전개하여, 사용자의 PC에는 비밀작업내용이 저장되지 않도록 하여 비밀유출을 사전 차단하는 SBC(Server Based Computer) 방식 등 보안기술을 적용한 비밀의 생산·열람·관리 등 전 과정의 안전성과 편의성을 높이고 있다.

그리고 비밀문서에 RFID 기술을 적용하여 비밀문서 관련 업무를 전자적으로 처리할 수 있도록 업무를 개선하였다. 이러한 비밀관리시스템은 비밀업무 전 과정에 대한 보안기능 강화로 보안 사고를 사전에 예방할 수 있다. 또한 비밀업무처리의 표준화와 시스템화로 국가기밀 보호 역량을 강화시키고 있다[4].

2.1.4 국가 사이버안전 관리규정 개정

국가정보원은 「국가 사이버안전 관리규정」을 2005년에 제정하였다. 2008년에는 국가안보 및 국민생활에 직접적으로 영향을 끼치는 10대 국가 핵심 전산망(외교·행정·국방·금융·통신·과학연구·에너지·교통·교육·보건의료 등)에 대한 보안관제센터를 설립하였다. 또한 이를 관장하는 모든 중앙행정기관장이 국가 사이버안전에 관한 정책 결정에 참여할 필요성이 대두되어, 당년 8월에 「국가 사이버안전 관리규정」을 개정하였다. 개정된 내용으로 국가사이버 안전정책을 심의하는 국가 사이버안전 전략회의 위원에 기존에 미포함 되었던 교육과학기술부·지식경제부·보건복지가족부·국토해양부의 차관과 금융위원회 부위원장을 추가로 포함시켰다.

최근 국가정보원은 2009년 7월 발생한 분산서비스 거부(Distributed Denial of Services, 이하 DDoS) 공격 대응과정에서 나타난 문제점을 개선한 국가 사이버안전 관리규정(대통령 훈령) 개정안을 2010년 1월 법제처에 제출하여 2010년 3월 법령안 심사를 통과하고 4

월 16일 개정·공포되었다. 이 개정안은 국가·공공기관이 사이버공격 정보를 탐지·분석해 대응조치를 할 수 있는 보안 관제센터를 구축·운영한다. 그리고 보안관제 인력을 상시 배치, 필요시에는 보안관제 전문업체의 인력을 파견 받아 보안관제 업무를 수행할 수 있도록 명시되어 있다. 이와 함께 국가정보원장이 '주의' 수준 이상의 경보 발령 시 관계 중앙행정기관과 협의 하에 '범정부적 사이버 위기대책 본부'를 구성·운영한다. 또한 대책본부 내에 합동조사 및 복구지원팀 등도 설치할 수 있도록 하였다. 국가정보원은 각 정부기관들이 운영하는 정보를 수집하고 다시 전파하는 이른바 정보 컨트롤 타워 역할을 수행하며, 유사시 범정부 사이버 위기대책 본부에서도 주도적인 역할을 담당할 수 있을 것이다[5].

2.2 국외 정보보호 국가정책 동향

2.2.1 미국

미국 오바마 행정부의 '종합 사이버보안 구상(Comprehensive National Cybersecurity Initiative, 이하 CNCI)'은 사이버 침해사고에 대한 사후 대응 전략에서 사전 예방 중심으로 변환하였다. 이번 CNCI는 12개 핵심 전략으로 구성되었으며, 비밀로 분류된 국가 안보에 관한 대통령 명령 23(NSPD 54/HSPD23)을 근거로 하여 현재 내용의 일부 핵심기술만을 공개하였으며 그 내용은 다음과 같다.

- FDCC(Federal Desktop Core Configuration) : 연방기관내 업무용 PC 및 노트북 보안 강화
- TIC(Trusted Internet Connection) : 연방기관간 인터넷 경로 보안체제 강화
- Einstein 프로그램 : 연방기관간 인터넷 통신 감시체제 구축

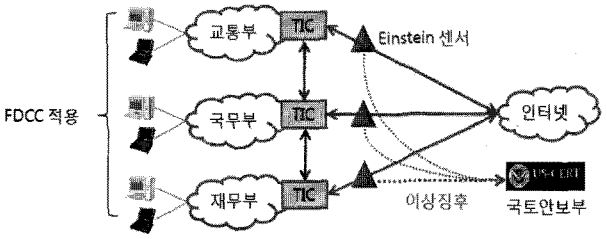


그림 1 CNCI 전략 구도

또한 2009년 10월 미국 정부는 사이버전 대비 향후 5년 동안의 프로그램 승인과 약 170억 달러로 확대 지원하여 사이버 전쟁의 능동적 수행 및 내부 데이터 보호를 위한 '사이버 사령부'를 창설, 2010년 10월 출범할 예정이다[6].

2.2.2 EU연합

EPCIP(European Programme for Critical Infra structure Protection)의 정책 전략은 다음과 같다.

- 주요 기반구조 보호 및 복구에 대한 국가 간 정책 차이 최소화
- 주요 기반구조 보호 및 복구에 대한 EU의 관리 능력 향상
- 유럽의 침해 사고 대응 능력 강화
- 국제적인 보호 및 복구 능력 향상

2.2.3 일본

일본은 사이버 공격 및 정보보호를 위한 정보보호센터(NISC : National Information Security Center)와 내각관방 산하의 정보보호정책회의(ISPC : Information Security Policy Council)에 의한 정부 차원의 정보보호 체계 수립하여 정보보호 표준에 의한 평가를 시행중에 있다. 그리고 사이버 공격에 대한 대응 능력의 향상을 위해 민관 공동 사이버 공격 대응 훈련 및 사이버 공격 분석 실시하고 있다. 또한 중대한 IT 장애

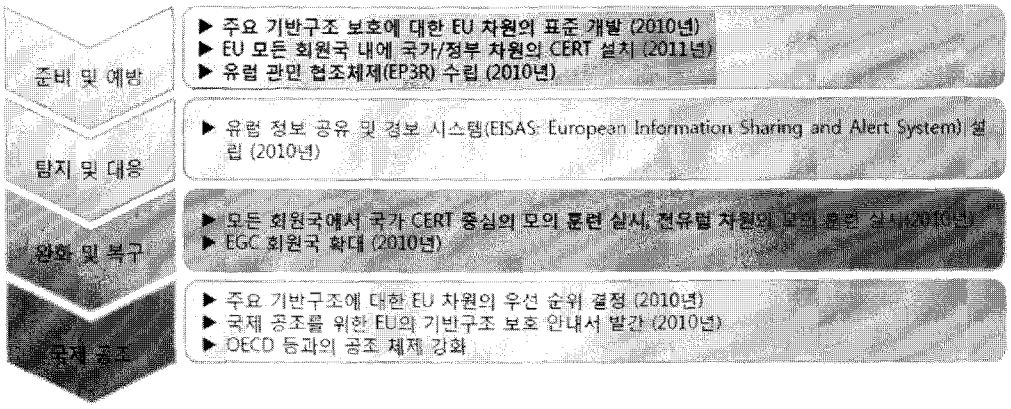


그림 2 EPCIP의 로드맵

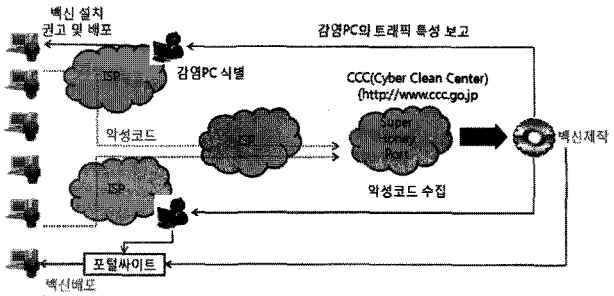


그림 3 CCC(Cyber Clean Center) 운영 체계

등의 긴급 정보를 일제히 통지하는 CEPTOAR(Capabilities for Engineering of Protection Technical Operations, Analysis, and Response)를 시작하면서 CII(Critical Information Infrastructure)에 대한 본격적인 보호 활동을 시작하였다. CII의 기능 마비/감소가 국민의 사회생활, 경제활동에 심각한 붕괴를 초래할 수 있는 대체 불가능한 서비스로 정의되고 있다. 또한 최근 급증하는 사이버 공격 봇넷, 악성코드 대응 등 예방 및 역기능방지에 대한 개발을 위해 CCC(Cyber Clean Center)를 설치 및 운영하고 있다[7].

2010년 5월 11일 일본 정보보호센터(NISC)의 제 23회 정보보호 정책회의가 개최되었다. 이 회의에서는 기존 제 2차 정보보호 기본계획(2009년 2월)을 포함하여 새로운 환경 변화에 적합하게 대응하고 실현하기 위한 포괄적인 새로운 정보보호 전략을 결정했다. 이것은 종래의 대응으로는 정보보호 확보가 곤란한 상황이 발생하고 있거나, 다른 국가에서도 동일한 전략적 대응이 행하여지고 있다는 것을 고려한 결정이다. 기본 전략에서 사이버공격 발생을 상정한 정책 강화 대처 체제 정비, 새로운 환경 변화에 대응한 정책 확립, 수동적인 대책에서 능동적인 대책으로 대응한다. 이로써 안전・안심할 수 있는 국민생활 실현, 사이버 공간상 일본의 안전 보장 위기관리 확보, 정보통신기술의 활용 촉진하여 일본 경제 성장에 기여를 하겠다는 계획이다[8].

3. 분야별 주요 정보보호 기술동향

3.1. RFID 정보보호 기술

RFID 응용 시스템은 태그, 리더, 디렉토리 서버, 그리고 정보 서버로 구성되며, 태그가 부착된 물품의 정보를 얻어오는 과정은 그림 4와 같다. 리더는 태그에게 태그의 ID를 요청하여 읽어 들인 후 태그의 ID에 대한 자세한 정보를 갖고 있는 정보 서버의 주소를 디렉토리 서버에 질의하여 알아오고, 그 후 정보 서버에 접속하여 태그의 ID와 관련한 물품의 자세한 정보

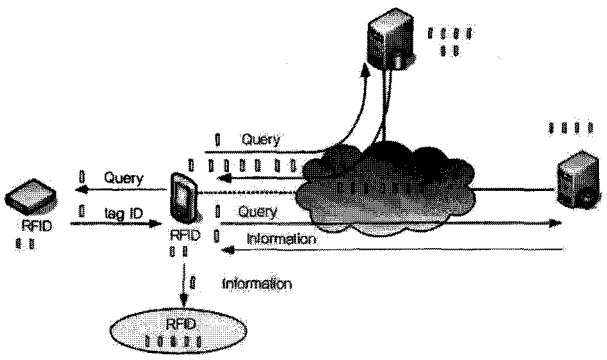


그림 4 RFID 응용 시스템 구조 및 정보 획득 과정

를 찾아낸다. 정보 서버는 모든 태그들의 정보를 저장하는 데이터베이스의 역할을 한다. 리더는 이 정보를 응용 프로그램에게 전달하여 관련 응용 서비스가 제공될 수 있도록 한다.

3.1.1 RFID 정보보호 문제점 및 해결 방법

기존의 정보보호 기술들은 전통적인 클라이언트-서버 기반의 응용 서비스를 대상으로 하며, 사용자 이름, 암호 등과 같은 식별 정보가 개인에 대한 정보 접근의 직접적인 수단을 제공한다. 반면에, RFID 정보 시스템의 경우에 사용되는 태그 ID는 개인과는 무관한 물품 자체에 대한 것이고, 물품에 대한 정보는 정보 서버에 저장되어 있다. 이 정보가 여러 단계의 과정을 거친 후에 개인화 된 정보로 변화되어 지는 근본적인 차이를 가지고 있으므로, 기존의 정보보호 기술을 RFID에 그대로 적용하기에는 한계가 있다.

RFID에서의 두 가지 주요 위협은 RFID 응용을 위한 각 요소들(태그, 리더, 서버, 통신채널, 글로벌 RFID 네트워크, 바이러스)에 대한 공격과 도청, 추적, 개인정보의 악용의 위험성을 갖는 정보의 불법적인 유출이다. 또한, RFID 응용에서는 개인 신상 정보의 누출과 개인 위치 추적 등 프라이버시와 관련된 문제가 가장 크게 우려되고 있다. RFID 응용에서 프라이버시의

표 1 기존의 정보보호 기술 적용시의 문제점

기존 정보보호 해결 방안들	RFID에 적용시 문제점들
클라이언트와 서버간의 인증에 의한 정보 매개 요소의 도용 방지	정보 매개 요소 자체로는 개인 정보 수집 불가
클라이언트와 서버간에 교환되는 정보의 암호화	물품 또는 개인 정보의 교환이 여러 단계에 거쳐 이루어짐
정보 수집의 직접적인 동의를 위한 규제	개인의 직접 동의 환경의 부재
직접적인 개인 정보 수집 및 활용하는 명확한 주체에 대한 규제	정보 수집 주체의 모호성

표 2 RFID 정보보호 방법들

구간	위협요소	보호 방법들
태그	- 태그의 데이터 조작 - 태그의 복제 및 에뮬레이션	인증, Blocker Tage, Soft Blocking, 태그 접근 제어 등
태그-리더간	- 불법적인 도청 - 악의적인 리더의 불법 접근	- 태그 랜덤화, 해시 기반 태그 인식 - 키 분배 방식, 블로커 태그, 매스터 리더 적용 등
리더-로컬 서버간	- 무선 인터페이스의 교란 - 불법적인 도청	기본 무선랜 정보보호 방법들의 확장 적용 가능
디렉토리 서버	- 디렉토리 서버 공격 - 정보서버 주소의 불법 획득	DNS 보호를 위한 TSIG, DNSSEC, SSL 서버 인증과 같은 방법들의 확장 적용 가능
정보서버	- 정보서버 공격 - 정보서버 내용의 불법 획득	서버를 위한 기존 정보보호 방법들의 확장 적용 가능

문제가 심각히 대두되는 근본적인 이유는 RFID 태그가 부착된 물품의 소유주인 개인들이 태그의 존재를 인식하는 것이 불확실하며, RFID 태그는 모든 물체에 대한 유일한 식별자가 되므로, 프라이버시 문제의 시발점을 제공한다. 또한 RFID에서는 무작위로 대규모 정보를 수집하는 것이 가능하며, 이 중 리더는 노출되지 않고 접촉 없이 정보를 수집하는 것이 가능하다. 또한 RFID 응용에서는 개인 정보와 위치를 프로파일링한 서비스를 제공하기 때문이다[9].

3.1.2 RFID 표준화 동향

RFID 무선접속 규격의 국제 표준화를 담당하고 있는 대표적인 표준화 그룹인 ISO/IEC JTC1 SC31 WG4 SG3(이하 SG3)에서는 지난 2004년에 각 주파수 대역별로 RFID 태그와 리더의 통신을 위한 물리계층 특성과 데이터링크 계층 명령어 포맷을 규정하였다. 이후 각 주파수별 표준(ISO/IEC 18000-1,2,3,4,6,7)에서 센서 기능과 배터리 지원 기능을 포함시킨 규격으로 리비전을 추구하고 있는 상황이다.

RFID 보안기술의 국제표준화 논쟁이 급물살을 타게 된 시점은 2008년 8월에 미국 피츠버그에서 개최된 SG3 회의였다. 이 회의에서는 오스트리아 대표단이 RFID 파일관리 및 보안기술 표준화를 위한 신규작업화(NP: New Proposal) 내용을 소개하면서 RFID 보안기술의 표준화가 활발하게 논의되기 시작했다. 피츠버그 회의의 가장 큰 주요 이슈는 파일관리 및 보안기술 표준화를 제안한 오스트리아의 신규 작업화 제안에 대하여 향후 어떤 형태로 표준화를 접근할 것인가에 대한 논의였다. 당시 RFID 보안을 위한 요구사항 및 기술 소개의 시간이 끝난 후 의장의 제안에 따라 브레인스토밍(brainstorming)이 진행되었는데, 주요 파일관리 및 보안기술을 하나의 문서에서 처리하는 것이 바람직한지 아니면 구분하는 것이 바람직한지에 관한 의견 교환이 많았다. 이 과정에서 제안국인 오스트리아 대표단과 미국 대표단의 일부에서 상반된 주장을 보였고, 결론은 SG3 의장이 중재, RFID 보안기술 표준화 논의를 위하여 ISO/IEC JTC1 SC31 WG4 (이하 WG4)의 주도하에 관련된 표준화 그룹들(정확히는 WG4, SG1, WG4 SG3, WG4 SG5, WG5, WG6)이 참가하는 JWG(Joint Working Group)을 결성하여 본격적으로 논의해 보자는 것으로 매듭지어졌다. 피츠버그 회의 이후 2008년 10월에 오스트리아 대표단이 제안한 RFID 파일관리 및 보안기술 표준화 투표결과가 공지되었고 WG4에서는 RFID 보안기술을 표준화하기 위한 별도의 표준화 그룹을 구성할 것을 결정하였다. 그 결과 보안기술 논의를 전담하는 Ad hoc 그룹을 결성하였고, 그 최초 텔레컨퍼런스가 2008년 12월에 있었으며 한국에서는 ETRI가 참여하였다.

이후 2009년 2월에 미국 플로리다 보카라톤에서 개최된 보안 Ad hoc 그룹에서는 기술적인 논의가 있었던 것은 아니지만 중요한 결정 사항들이 있었다. 첫째는 보안 그룹이 처리할 범위가 SC31 산하의 무선 기술로 확장되어 RFID, RTLS, MIIM을 모두 고려한 보안기술 표준화로 커진 것이다. 이에 따라 SC31 산하의 WG7으로 결성하기로 결정하였고 SC31에게 그 승인을 요청하였다. 둘째는 ISO/IEC 29167 문서를 하나로 유지하고 여기서 파일 관리와 보안기술을 동시에 정의한다는 것이며, 이 문서의 에디터 권한을 오스트리아 제안자와 한국의 ETRI에서 함께 맡기로 했다. 파일관리와 보안기술이 함께 처리되다 보니 SG3 멤버들과 SG1 멤버들 모두 보안 Ad hoc 그룹의 논의에 크게 관심을 가졌으며, 향후에도 고용량 메모리 태그의 응용을 고려하는 곳에서는 보안기술 그룹의 논의에 큰 관심을 가질 것으로 예상된다. RFID 무선접속 규격 외에 네트워크 연동을 고려한 RFID 네트워크 표준화는 주로 ITU-T에서 추진되고 있는데, 2006년 9월에 캐나다 오타와에서 개최된 ITU-T SG17 Q.9 임시(Interim) 회

의에서 한국이 제안한 Networked RFID 보안을 위한 프라이버시 보호 프레임워크와 프라이버시 보호 가이드라인의 표준화 추진이 결정됐다. RFID를 이용한 정보 시스템은 자동화된 정보의 수집과 서버에 수집된 정보의 분석을 통하여 RFID 태그를 부착한 사용자의 위치나 전자 거래의 특성을 추적할 수 있기 때문에 이에 대한 프라이버시 문제가 제기되어 왔다. 또한 이를 법제도적으로 예방하기 위한 프라이버시 보호 가이드라인이 우리나라를 포함하여 일본, 미국 등에서 개발되어 적용되고 있지만, 이 프라이버시 보호 가이드라인은 나라마다 독자적으로 개발되어 범세계적 차원의 가이드라인 개발이 요구됐다. 이러한 문제를 해결하기 위한 국제표준이 Networked RFID 프라이버시 보호 프레임워크와 프라이버시 보호 가이드라인에 대한 표준이다. X.nidsec-1 드래프트로 시작된 프라이버시 보호 프레임워크 표준은 문서 번호 X.1171 표준이 되었으며 프라이버시 보호 가이드라인은 X.rfpg 드래프트가 작성중이다.

RFID 보안기술의 국내 표준화는 TTA(한국정보통신기술협회)에서 추진되고 있으며, 실질적으로 표준화를 담당하는 곳은 기술위원회이고, 그 중 RFID 보안기술의 표준화는 정보보호 기술위원회 산하의 PG504(응용보안 및 평가인증 프로젝트 그룹)에서 추진되고 있다. PG504에 제출한 표준안의 명칭은 "수동형 RFID 보안 태그와 리더의 인증 및 데이터 보호 프로토콜(Authentication and Data Protection Protocol of Passive RFID Security Tag and Reader)"이며 최종적으로는 2008년 12월 19일에 TTAI.KO-12.0091로 표준공고가 완료됐다. 최초 2008년 5월 15일에 과제제안이 되었으며 TTA 과제번호 2008-756으로 PG504에서 논의됐다. 제출된 표준안은 PG504에서의 논의를 거쳐 2008년 11월에 기술위원회를 통과, 12월에 운영위원회를 통과한 후 최종적으로 12월 19일에 표준총회에서 표준공고를 하였다. 본 표준은 TTA 임시표준으로 확정되었으며, 현재 PG504에서는 TTAI.KO-12.0091 표준의 개정안을 마련하기 위해 준비 중에 있다.

한편, 지식경제부 기술표준원 주최 "RFID 관련 국제표준화회의"가 3월 15일부터 26일까지 제주도에서 진행 중이며, 세계적으로 RFID 국제표준 68건이 제안돼 있고, 그 중 16%에 해당하는 11종을 우리나라가 제안, 미국이나 유럽의 선진국들과 대등한 기술경쟁을 펼치고 있다. 그동안 미국 및 유럽 기업들에 의해 RFID 관련 국제표준화가 주도돼 온 점을 감안하면, 우리 RFID 기술력은 정부와 관련업계 등이 합동으로 핵심기술 개발에 박차를 가해 짧은 기간에 비약적인 성장을 했으며, 세계시장 진출 전망도 밝은 편이다. 특히 우리가 선도적으로 핵심기술을 개발해 본격적 시장 출시를 앞두고 있는 모바일 RFID 및 RTLS(실시간위치추적시스템) 응용서비스 기술은 금년 중 국제표준으로 채택·완료될 것으로 보여 세계시장을 주도할 발판을 마련할 것으로 평가받고 있다[10].

3.2 USN 정보보호 기술

USN은 다수의 센서 노드로 구성된 무선 네트워크로써 다양한 위치에 설치된 센서 노드들로부터 사람과 사물, 그리고 환경 정보를 인식하고, 인식한 정보를 통합·가공해 언제, 어디서나, 안전하고 자유롭게 이용할 수 있게 하는 정보서비스 인프라를 뜻한다. 센서 네

표 3 우리나라가 제안한 RFID 관련 국제표준 목록 (11종)

분 야	국 제 표 준 명	진행단계
RTLS 기술	Real-time location systems(RTLS) - 2.4GHz air interface protocol	CD
모바일 RFID 리더 기술	Air interface specification for Mobile RFID interrogators	FCD
	Mobile RFID interrogator device protocol	CD
	Mobile RFID interrogator device protocol for ISO/IEC 18000-6 type B and type C	CD
모바일 RFID 정보보호	consumer privacy-protection protocol for Mobile RFID services	CD
모바일 RFID 서비스	Reference architecture for Mobile AIDC services	FCD
	UII scheme and encoding format for Mobile AIDC services	CD
	Application data structure encoding format for Mobile AIDC Services	CD
	Object Directory Service for Mobile AIDC services	CD
	Service broker for Mobile AIDC services	CD
모바일 RFID 응용인터페이스	Mobile AIDC application programming interface	CD

*국제표준 제정 절차 : 신규작업항목 제안(NP) → 국제표준초안(WD) → 위원회안(CD) → 최종 위원회안(FCD) → 최종 국제표준안(FDIS) → 국제표준(IS)

트워크는 다양한 환경에서 주변상황을 모니터링하고 필요한 정보를 센싱하는 용도로 사용되기 때문에 센서 노드의 정보 신뢰성이 매우 중요하다. USN의 보안 기능을 강화하기 위한 방법으로 내부적으로 센서 노드의 보안 기능을 추가하는 것 이외에도 외부적으로 보안 위협으로부터 전체 네트워크를 보호하기 위해 네트워크의 모든 부분에 보안 기능을 도입하는 계층적 보안이 관심을 모으고 있다.

3.2.1 USN Cryptographicc Algorithm

USN의 안전한 서비스 제공 및 보안 응용 서비스의 실행을 위해서, 일반적인 보안 요구사항인 기밀성, 무결성, 인증, 부인방지를 구현하는 암호학적 방법이 적용되며, 자원제약성이라는 USN 환경에 적합한 경량의 저전력 특성을 가지는 암호 알고리즘이 필요하다.

USN 시스템은 작은 임베디드 기기상에서 구현되며, 이러한 임베디드 장치는 다양한 CPU 플랫폼을 가진다. CPU의 종류에 따라 연산은 8bit, 16bit, 32bit 단위로 수행된다. 현재 널리 쓰이고 있는 Atmega 103, Atmega 128, M16C/10, StrongARM SA-1110, XScals PXA250, UltraSPARC II 등의 플랫폼상에서, 보안에 폭넓게 사용되고 있는 암호 알고리즘은 RC4, IDEA, RC5, MD5, SHA-1이다. 그리고 TinyOS 기반 Mica2 센서 모트는 링크 레벨의 암호 및 기밀성 제공을 위해서 TinySec[11]을 사용한다. TinySec에서 사용되는 알고리즘은 64bit 블록 암호인 SkipJack과 RC5, 대칭키 암호 시스템이다. 상기 알고리즘은 저전력 동작을 위해서 선정되었으며, C 언어 단독 혹은 C와 어셈블리어를 함께 사용하여 소프트웨어로 구현되었다. 또한 USN 센서 노드의 통신에 가장 널리 사용되는 RF 통신 칩으로는 TI사의 CC2420[12], CC2430 등이 있으며, 상기 RF 칩에서는 AES-128 암호 알고리즘을 하드웨어 가속기로 제공하고, 이를 사용하여 센싱 데이터 통신에서의 기밀성을 보장받을 수 있다.

미국 매사추세스의 WPI에서는 경량 센서 노드에 탑재 가능한 저전력 공개키 암호로 Rabin, Ntru을 구현하였다. 상기 공개키 알고리즘은 RSA와 동일한 보안 안전성을 제공하면서도, ECC 연산의 다소 낮은 저전력 구현 특성을 보완할 수 있다. Rabin 기법은 RSA의 특별한 하나의 형태로써, 인수분해 문제의 어려움에 기반한 공개키 암호 시스템으로 1979년 Rabin이 제안하였으며, NtruEncrypt는 SVP의 어려움에 기반한 공개키 암호 시스템으로 1996년 Hoffstein, Pipher와 Silverman이 제안하였다. 표 4는 Rabin 기법과 Ntru 성능 특성을 보여주고 있다. 적절한 알고리즘과 구현 파라미

표 4 Rabin's Scheme과 Ntru 성능 특성[13]

	Rabin	Ntru (k=1)	Ntru (k=84)
Equivalent security	60 bits	57 bits	57 bits
Area [eqv.gates] combinational storage elements	16,726 8,875 7,851	2,850 523 2,327	16,200 7,000 9,200
Delay(avg. #cycles)	1,440	29,225	433
Avg.power@500 kHz static(%) dynamic(%) peak power	148.18 μW 117.58 μW (79.3%) 30.68 μW (20.7%) 169.8 μW	19.13 μW 15.10 μW (78.9%) 4.03 μW (21.1%) 20.22 μW	118.7 μW 103.06 μW (86.8%) 15.64 μW (13.2%) n/a
Energy per bit encrypted	426.76 nJ 833.5 pJ (512 bits)	1,118.15 nJ 4,235.41 pJ (264 bits)	102.79 nJ 389.4 pJ (264 bits)
Throughput	177.8 kbits/s	4.52 kbits/s	304.85 kbits/s

터를 선정하고 저전력 기술을 적용할 경우, 전력 소비를 20 μW 이하로 암호 연산을 수행할 수 있다. 이는 배터리 전지를 사용하는 센서노드 환경에서 충분히 사용할 수 있음을 보여준다.

노스캐롤라이나 주립 대학에서 타원 곡선 암호 알고리즘을 TinyOS 상에서 구현하여 키를 안전하게 분배하고 있으며, 실제 사용을 위해 타원 곡선 기반 암호화 프로토콜인 ECIES와 키 분배 프로토콜인 ECDH, 서명 기법인 ECDSA 프로토콜을 구현하였다[14,15]. 해당 기술은 MICAz와 Telosb, Tmote Sky에서 사용할 수 있으며, SECG에서 추천하는 128bit와 160bit, 192bit 타원곡선을 사용하고 있다.

한국의 ETRI에서는 2008년 보안 센서 노드에 필요한 키 분배 프로토콜 및 이에 필요한 ECC 연산 모듈을 TinyOS상에서 소프트웨어 구현 및 전용 하드웨어[16]를 개발하였다. 또한 설정 시간을 줄이기 위해 ECC 연산을 전용 하드웨어로 구현하였으며, ECC 연산은 사용 좌표에 따라 설계 구조 및 성능이 달라지며, 저면적/저전력 구현을 위해서 affine 좌표를 사용하여 설계하였다. 설계된 ECC 모듈은 0.25 μ 삼성 공정으로 하드웨어 합성 시 22k 게이트의 면적으로 구현되며, MSP430

표 5 ECC 연산 시간

Operation	Time
Scalar Multiplication(Np)	49 ms
ECC Addition(P+G)	220 μs

MCU 기반의 USN 보안 노드의 시스템 클럭인 4MHz로 동작 시 연산 성능은 표 5와 같다.

3.2.2 USN Network Protocol

센서 네트워크의 네트워크 계층은 다수의 노드로 구성되며, 이동성을 고려할 경우 네트워크의 토폴로지의 빈번한 변화로 라우팅 정보의 갱신을 필요로 한다. 무선 센서 네트워크의 전송거리 제약으로 센서 노드들의 통신은 멀티 홉 통신방식을 기본으로 라우팅을 하게 되며, 제한된 용량의 배터리를 사용하기 때문에 에너지 상태를 염두에 둔 통신 방법도 고려할 필요가 있다.

센서 네트워크의 보안을 위한 네트워크 계층에서의 프로토콜로는 SPINS가 제시되어 있으며, SPINS는 크게 두 가지 기술인 SNEP와 μTELSA로 나뉜다. SNEP는 데이터의 비밀성, 양단간의 데이터 인증, 재사용방지, 무결성 등을 제공하는 역할을 하고, μTELSA는 데이터 브로드캐스트에서의 인증을 담당한다.

3.2.3 USN 표준화 동향

해외의 USN 표준화 접근 방향이 기존의 기술로부터 USN으로의 기술을 접근하고 있다면, 국내의 경우 USN 기반 기술을 시범사업으로 활용하면서 기술과 응용서비스 모델의 표준화를 맞춰가고 있다. USN이 여러 기술의 결합인 만큼, 각각의 기술들이 적용되는 비즈니스 모델에 따라 요구하는 프로토콜이 모두 달라 개별적으로 표준을 갖춰가고 있다. USN과 관련된 주요 국제표준화 기구는 ITU-T, ISO/IEC JTC 1/SC 6, IETF, IEEE, 지그비 얼라이언스 등이 있으며, 각각의 전문분야에 대한 표준화를 추진하고 있다.

국내 표준의 경우 PG504에 제출한 USN 보안기술 표준안의 명칭은 "USN에서의 센서 노드 간 인증 및 키 분배 프로토콜(USN Sensor Node Authentication and Key Distribution Protocol)"이다. 최종적으로는 2008년 12월 19일에 TTAK.KO-12.0092의 표준번호로 공고가 완료됐다. 최초 2008년 5월 15일에 과제제안이 되었으며 TTA 과제번호 200-757로 PG504 응용보안 및 평가인증 프로젝트 그룹에서 논의됐다. 제출된 표준안은 PG504에서의 논의를 거쳐 2008년 11월에 기술위원회를 통과하고 12월에 운영위원회를 통과한 후 최종적으로 12월 19일에 표준총회에서 표준공고를 했다[17].

4. 취약성 및 분석 사례

지난 3월 15일, MBC 뉴스에서 전국적으로 수천만 장이 발행돼 사용 중인 교통카드 해킹이 가능하다는 것이 시연을 통해 보도되면서 많은 사람들을 놀라게 했다[18].

이는 2008년 네덜란드에서 크게 이슈가 된 사실로, 독일의 Karsten Nohl과 Henryk Plotz라는 연구원들이 Mifare 칩의 해킹 기술개발[19]과 독일 Radbaud 대학의 Bart jacobs 교수팀[20]이 Mifare Classic의 Crypto-1 암호 알고리즘을 해독하는 시연 동영상을 공개함으로써 Mifare가 해킹에 노출될 우려가 있음을 공식 발표하였었다. Mifare는 필립스사가 개발한 비접촉식 카드로서 교통카드, 신분증, 금융서비스 등의 응용분야에 전 세계적으로 사용되고 있으며, 현재는 NXP 반도체 사에서 개발한다.

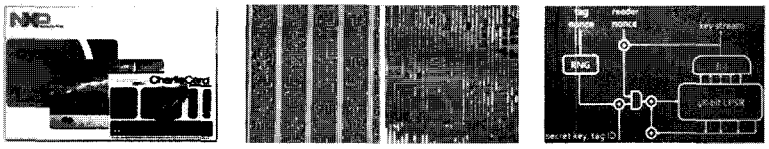
Jacobs 교수팀의 Mifare Classic의 Crypot-1 알고리즘 분석결과 카드의 UID와 암호키 사이에 상관관계가 존재하여 암호의 통계적 특성과 난수 발생기의 약점 분석이 가능해졌으며 PC를 이용해 수분만에 위조카드의 제작이 가능함을 보였다.

실제로 Mifare를 이용한 영국 런던의 Oyster 교통카드의 경우 단 1회의 수동적 도청으로 수 분만에 비밀키를 복원하여 카드를 복제할 수 있어 현실적인 공격이 될 수 있음을 경고하고 있다.

그리고 Mifare Classic 카드의 위험성에 대한 논문 발표에 대해 제조사인 NXP가 논문 발표자를 상대로 제기한 소송도 이미 NXP의 패소로 결론이 났다.

현재 사용되고 있는 전자여권 역시 보안상의 문제가 있는 것으로 밝혀졌다. 지난 2008년 8월 외교통상부가 도입한 RFID 방식의 전자 여권은 도입된 지 불과 한달 뒤 진보네트워크센터에서 보안상의 문제가 있음을 입증하는 시연 행사를 개최하였다. 진보네트워크에서는 데스크탑 컴퓨터 1대와 인터넷을 통해 산 저가의 RFID 리더기 그리고 웹 상에서 다운받은 전자여권 리딩 프로그램을 사용하여 여권 내 칩에 담겨있던 개인정보가 해킹됨을 시연해보였다[21].

또한, 전자여권은 위변조에 대한 가능성도 제기되었었다. 전자여권은 기존 여권이 위변조에 취약해서



Mifare 내장 카드 H/W 역공학 로직 Crypto-1 알고리즘

그림 5 H/W 역공학 로직과 Crypto-1 알고리즘 구성

위변조가 불가능한 최첨단의 여권이라며 도입되었다. 전자여권은 개인정보를 내장하고 있으며, 이를 전자서명을 통해 위변조를 막는다.

이 전자서명은 DS인증서라는 인증서를 통해 위변조 여부를 검증하는데, DS인증서가 전자여권 내에 저장돼 마치 자물쇠와 열쇠가 같이 있는 격이라는 주장이다. DS 인증서 자체는 각국이 저장하고 있는 CSCA라는 인증서를 통해 다시 한번 인증과정을 거치게 된다. 하지만 모든 나라에서 반드시 인증절차를 거치고 있는 것이 아니며, CSCA인증서를 보호하기 위한 공개키디렉토리(PKD) 코드 시스템을 도입한 나라는 전자여권 도입 40여 개국 중 5개 나라밖에 되지 않는다.

하지만, 전자여권 안에 전자서명과 이를 복호화하는 키가 같이 담겨있다는 것은 신용카드위에 비밀번호까지 올려놓은 격으로 사실상 이것은 해킹이라 할 수 없으며, 현재 칩을 망가뜨려도 출입국 심사에는 아무런 지장이 없다는 것만 봐도 문제가 많다는 주장이 대두되었다[22].

한편, 해외에서는 RFID 스키밍(Skimming)을 통해 신용카드의 마그네틱 정보나 IC카드의 RFID 정보 등을 무단으로 복제하는 범죄가 만연하고 우리나라 역시 최근의 카드 복제 범죄가 빈번히 발생하며 더이상 복제 범죄에서 안전하지 않다. 스키밍(Skimming)은 카드 소지자의 허락 없이 카드상의 정보를 전자적으로 복사해 가는 부정행위를 말한다.

5. 결 론

이상으로 본 논문에서는 현재 국내·외의 정보보호 관련 정책 동향과 사물지능통신망에서의 RFID/USN 기반 보안 기술 및 표준화 동향, 그리고 RFID/USN의 보안 취약성 및 분석 사례에 대하여 기술하였다.

전 세계적으로 직면한 글로벌 금융위기, 기후 변화 대응 등 사회·경제적 과제들에 대한 해결책으로 ICT (Information & Communication Technology)의 중요성이 부각되고 있다. 우리나라 또한 최근 국가 주요 정책과제의 해결책으로 ICT의 중요성이 부각되면서, ICT를 선도하는 사물지능통신기술은 지능화된 사물들이 정보 교환을 통해 변화된 패러다임의 중심 역할 및 국가 정책 실현에 있어 가장 중요한 인프라로서 미래 방송통신 산업시장에 크게 성장할 것으로 기대되고 있다. 미래 사물지능통신망의 새로운 서비스 모델은 지금 앞에 있는 사회 현안, 특히 저탄소 녹색성장, 기후변화 대응, 에너지 절감, 재난·재해 방지 등에 대한 것들이 주로 개발될 것으로 예상된다. 더 나아가 인간의 모든 활동과 생활에 있어 필요한 정보 가치를 높이고 불확실성을 줄이는 인간의 삶에서 없어서는 안 될 필수 인프라가 될 것이라 기대한다.

사물지능통신(O2N)을 이루는 기반기술은 USN, RFID, IPv6, 융합센서, 지능형 로봇, Baseband Modem chip 등이 있으며 이 중 RFID/USN 기술은 단순한 바코드의 대체 수준을 넘어서 오늘날 통신, 물류, 국방, 소방, 금융, 의료, 환경, 교육, 정보가전, 도로, 건설 등 다양한 인간의 생활 전반에 활용되고 있다. 이로써 무한한 부가가치를 창출 가능하고 전 세계적인 산업구조, 시장구조의 변화뿐만 아니라 이제는 인간의 삶의 형태까지 변화시키고 있다. 그러나 RFID/USN 기술이 인간의 삶의 전반에 걸쳐 긍정적인 효과를 제공할 지라도 개인이 인식하지 못하는 중에 노출되는 개인정보의 침해와 같은 역기능은 RFID/USN 보급의 가장 큰 장애가 되고 있다.

이러한 문제점을 해결하기 위하여 사용자의 프라이버시보호, 등록자의 인식제고를 위한 교육 및 홍보 강화, 정보의 법제도 및 추진체계 정비, 국제기준 및 그 협력 강화, 정부 차원의 개인정보보호에 대한 노력이 필요할 것으로 보인다.

참고문헌

[1] 남동규, "사물지능통신의 발전과 미래 서비스 모델", 한국통신학회지(정보와통신), 제27권 제7호, 2010.06.

[2] 염흥열, "글로벌 USN 보안 표준화 동향", 2009.

[3] 국가정보원 국가사이버안전센터, http://wervice1.nis.go.kr

[4] 국가정보원, 방송통신위원회, 행정안전부 그리고 지식경제부, "2009 국가정보보호백서", 2009.04

[5] 국가정보원, "대통령훈령 제222호", 2008.08, http://www.nis.go.kr/app/intro/law/list

[6] 박춘식, "미국 사이버 보안 정책동향", 한국 사이버테러 정보전학회, 제10회 사이버테러 정보전 컨퍼런스 - 국가 산업기술 유출 대응, 2010.01.08

[7] 인터넷 침해 대응 기술 연구센터, 류재철, "국내·외 침해사고 대응 정책 동향", 2009.10

[8] 길민권, "日, 세계 최첨단 정보보호 선진국 만들겠다 발표", 보안뉴스, http://www.boannews.com/media/view.asp?idx=21060&kind=3, 2010.05.17.

[9] 월간 자동인식&보안, 노병희, "RFID 정보보호와 프라이버시", 2008.02

[10] 지식경제부 기술표준원, "우리 RFID 기술, 세계 표준으로 대거 진입", 2010.03.12 http://www.kats.go.kr/

[11] Chris Karlof et al., "TinySec: A Link Layer Security

Architecture for Wireless Sensor Networks", SenSys'04, Nov. 2004.
[12] CC2420 DataSheet, "CC240, 2.4GHz IEEE 802.15.4/ ZigBee-ready RF Transciever", Chip-con, 2006.
[13] Deukjo Hong et al., "HIGHT: A New Block Cipher Suitable for Low-Resource Device", CHES'06, LNCS 4249, 2006.
[14] 김호원, 이석준, 오경희, "센서네트워크 보안 기술 개발 동향", 정보보호학회지, 제 18권 제2호, 2008.04
[15] TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wiress Sensor Networks, Ver 1.0, http://discovery.csc.ncsu.edu/software/TinyECC, 2007.02.11
[16] 최용제, 김호원, "센서 네트워크용 타원곡선 암호 프로세서 구현", IEEK, 2007.
[17] ETRI, 전자통신동향분석, 제23권, 제4호, "안전한 USN을 위한 정보보호 기술 동향", 2008.08
[18] MBCNews, 해킹 무방비 "교통카드", http://imnews.imbc.com/replay/nwdesk/article/2587138_5780.html
[19] Karsten Nohl, Starbug, Henryk Plötz, "MIFARE SECURITY", CCC'07 Chaos Communication Congress, http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html
[20] Digital Security - RFID, http://www.ru.nl/ds/research/rfid
[21] 보안뉴스, "전자여권, 보안 허술.. 개인정보 술술~", http://www.boannews.com/media/view.asp?idx=11589&kind=0
[22] 이티뉴스, "전자여권 위변조 가능성 제기...개인정보 유출 위험성", http://www.etnews.co.kr/news/detail.html? id=200809290268

약 력

이 영 실

2006 동서대학교 정보네트워크과 졸업(학사)
2010 동서대학교 디자인&IT 전문대학원 유비쿼터스IT학과 졸업(석사)
2005~2006 (주)오토닉스 HMI팀 연구원
관심분야 : 암호이론, 정보보호, 네트워크보안
E-mail : youngsil.lee0113@gmail.com

박 범 수

2009 동서대학교 정보네트워크과 졸업(학사)
2010~현재 동서대학교 일반대학원 유비쿼터스IT학과 석사과정
관심분야 : 암호이론, 정보보호, 네트워크보안
E-mail : redcorona7@gmail.com

임 효 택

1988 홍익대학교 전자계산과 졸업(이학사)
1992 포항공과대학교 대학원 전자계산과 졸업(공학석사)
1997 연세대학교 컴퓨터공학과 졸업(박사)
1988~1994 한국전자통신연구소 연구원
2000~2002 Univ. of Minnesota(미) 컴퓨터공학과 연구교수
1994~현재 동서대학교 컴퓨터정보공학부 교수
관심분야 : Computer Network, Storage Networking, Mobile Application
E-mail : htlim@dongseo.ac.kr

이 훈 재

1985 경북대학교 전자공학과 졸업(학사)
1987 경북대학교 전자공학과 졸업(석사)
1998 경북대학교 전자공학과 졸업(박사)
1997~1998 국방과학연구소 선임연구원
1998~2002 경운대학교 조교수
2002~현재 동서대학교 컴퓨터정보공학부 부교수
관심분야 : 암호이론, 네트워크보안, 부채널공격
E-mail : hjlee@dongseo.ac.kr