情 報 保 護 學 會 誌
第 14 券 第 5 號, 2004. 10

RFID/USN 정보보호위협과 대응방안

주 학 수*, 권 현 조*, 강 달 천*, 윤 재 호*, 박 배 효*, 전 길 수*, 이 재 일*

요 약

RFID/USN 개념은 필요한 모든 것(곳)에 RFID 태그를 부착하고 이를 통하여 기본적인 사물의 인식정보는 물론 주변의 환경정보(온도, 습도, 오염정보, 균열정보 등)까지 센싱하여 이를 실시간으로 네트워크에 연결하고, 그 정보를 관리하는 것을 의미한다. 정보통신부는 국민소득 2만 달러 달성을 위한 IT389 정책을 적극적으로 추진하고 있는 가운데 국가차원의 RFID/USN 구축 실행을 위한 마스터플랜을 수립하여 기술개발, 표준화, 정보보호, 산업 적용 및 시범서비스 등의 정책을 실행할 예정이다. 프라이버시 침해문제가 RFID 서비스에서 더욱 이슈화되고 있어 정보보호 문제는 RFID 산업활성화를 위해 반드시 해결하여야 하는 문제이다. 따라서 초경량 암호알고리즘 등 정보보호 핵심기술 확보, RFID/USN 정보보호 인프라 구축, RFID/USN 정보보호 법제도 정비 등 RFID/USN 정보보호정책 추진방안 수립이 필요한 시점이다.

Ⅰ. 서 론

우리사회는 IT를 근간으로 한 과학기술의 급속한 발전과 더불어 유비쿼터스(Ubiquitous) 시대로 접어들고 있다. 유비쿼터스 환경에서는 자율컴퓨팅 기능을 갖는 기기 및 사물 등에 의하여 실시간 상황정보의 분석과 이를 통한 서비스가 이루어질 전망이다. 이를 가능하게 해주는 인프라가 USN(Ubiquitous Sensor Network)이다. 하지만 RFID 태그가 부착된 모든 기기 및 사물을 통해 정보를 수집·처리하는 과정에서 이들의 안전장치가 확보되지 않을 경우 중요한 개인정보가 유출될 수도 있고 개인정보의 과다수집 및 관리소홀 등의 프라이버시 문제를 일으킬 소지가 있다. 실제로 월마트와 질레트사가 RFID 시스템을 도입하려고 하였으나 개인정보 과다 수집 등 프라이버시 침해 논란으로 도입에 차질을 빚기도 하였다. 이러하듯 사생활 보호, 네트워크의 안전성 등 정보보호 문제가 USN 산업활성화에 중요한 변수로 작용할 것이 예상되므로 범국가차원의 RFID/USN 정보보호 방안 수립이 절실히 필요하며 USN은 산업기술이 아닌 정보통신망 인프라 구축기술이므로 RFID/USN 정보보호대책수립도 정보통신 인프라 측면에서 추진되어야 한다. RFID/USN 구축을 위한 정책추진 전략의 일환으로 정보통신부 장관을 포함하여 민·관 최고 의사결정권자가 참여하는 전략협의회에서 이러한 정보보호의 중요성을 지적하면서 RFID/USN 정보보호 대책 수립의 필요성을 제기하였다.

국외에서도 월마트, 베네통 등 RFID 시스템 도입 실패사례를 거울삼아 RFID로 인한 프라이버시 침해를 방지하는 법 제정이 추진되고 있다. 미국 캘리포니아에서는 개인 식별정보의 저장·사용 또는 공유하기 위해 RFID를 사용하는 자를 대상으로 하는 법안을 마련하였으며, 일본 총무성도 지난 6월에 RFID 개인정보보호 가이드라인(안)을 마련하여 발표한 바 있다. 또한 미국의 소비자단체인 CASPIAN(Consumers Against Supermarket Privacy Invasion and Numbering)은 RFID 사용제한을 주장하는 등 RFID/USN 환경에서의 프라이버시 보호운동에 앞장서고 있다. 또한 RFID 프라이버시 침해 방지를 위한 Blocker Tag, Kill Tag, Faraday Cage, Smart RFID 기술 등 기술적 대응방안이 지속적으로 나오고 있다. 각 기술의 주요 특징은 다음과 같다.

- Blocker Tag : RFID 태그에 저장된 정보의 접근을 선택적으로 차단하는 기술
- Kill Tag : 필요에 따라 RFID 태그의 기능을 제한하는 기술

* 한국정보보호진흥원({hsju, hckwon, dckang, jhyoon, parkbh, kschun, jilee}@kisa.or.kr)

- Faraday Cage : RFID 태그를 밀봉하여 전파를 차단시킴으로써 허가되지 않은 RFID 리더가 RFID 태그의 내용을 읽는 것을 방지하는 기술
- 전파방해 : 휴대용 소형기기가 전파 방해 신호를 보내 주변에 있는 RFID 리더의 동작을 차단/방해하는 기술
- Smart RFID : 해쉬알고리즘 등 암호기술을 활용하여 RFID 리더와 RFID 태그간의 정보를 인증/암호화하는 기술

RFID/USN 정보보호 위협에 대한 주제로 현재 많이 발표되고 있는 논문들은 대부분이 기술적 접근차원에서 이루어지고 있어 비기술자들이 실제로 RFID/USN의 정보보호 위협을 이해하는 데는 거리감이 있다. 따라서 본 고에서는 RFID/USN의 정보보호 위협에 대한 이해를 돕기 위해 단계별 USN 서비스에서 발생이 예상되는 정보보호 가상위협을 예시하고, RFID/USN 발전단계에 따른 정보보호 이슈를 제시함으로써 일반적인 차원에서 정보보호의 필요성을 제기하였다. 또한 정부가 추진하고 있는 RFID/USN 정보보호 추진방향에 대해 소개하고자 한다[1].

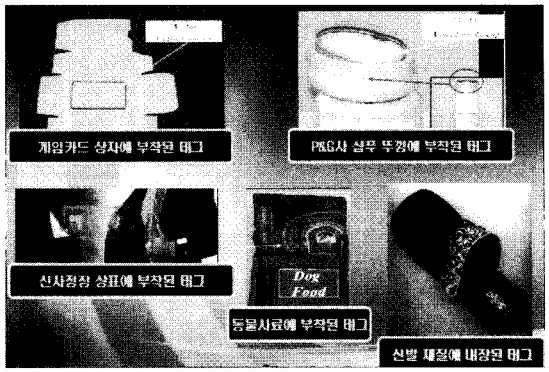
Ⅱ. RFID/USN 정보보호 위협

RFID/USN 기반 서비스는 놀랄만한 세상을 가져올 것이 틀림없지만 RFID의 특성상 반도체 칩에 수록된 정보는 당사자도 모르는 상태에서 쉽게 판독될 수 있으며, RFID 태그 정보와 연동된 방대한 데이터베이스가 무선 네트워크를 통해 순식간에 누출돼 악용될 소지가 있다. 본 절에서는 RFID 시스템 특성으로 인한 프라이버시 침해 위협 요인[3]을 제시하고, 단계별 USN 서비스에 따른 정보보호 가상 위협 시나리오를 기술한다.

1. RFID 시스템 특성으로 인한 정보보호 위협

1.1 눈으로 쉽게 확인할 수 없도록 RFID 태그 부착

RFID 태그는 소형화, 지능화되는데 비하여 가격은 수 센트로 저가화가 실현되면서 물류, 유통분야 뿐만 아니라 동물 관리, 환경, 재해예방, 의료 관리, 식품 관리 등 실생활에서의 활용이 확대될 전망이다[2]. 실행활에 활용되어야 하는 만큼 RFID 태그 장착으로 인한 불편함을 최소화하기 위해 RFID 태그를 눈에 띄지 않도록 제작하여 부착하고 있다. 소비자에게 편리성을 가져다주는 반면, 이로 인해 소비자가 RFID 태그 부착 사실을 알 수 없도록 함으로써 프라이버시 침해 의혹을 가져다 줄 수도 있다. 그림 1은 실제 제품에 여러 형태의 RFID 태그가 부착된 모습이다.



〔그림 1〕 실제 제품에 부착된 RFID 태그 유형

1.2 모든 사물을 구별할 수 있는 고유번호 부여

RFID 태그를 이용하여 사물의 식별이 가능해야 하므로 용도에 따라서 단위 지역 또는 전 세계적으로 고유번호를 부여하기 위한 체계를 정립하고 있다. 현재 유럽과 북미의 경우 EAN(European Article Number)와 UCC(Uniform Code Council)에서 제안한 EPC (Electronic Product Code)와 일본에서 제안된 u-ID (Ubiquitous-ID) 체계가 있다[2]. 실제로 코카콜라 회사는 자사 재고관리 및 통제 목적으로 코카콜라 캔 한 개마다 고유번호를 부여한 RFID 태그를 부착시켜 유통시킬 계획이라고 발표한 바 있다[3]. IT 기술에서 편리성과 정보보호 문제는 상존하기 때문에 고유번호를 모든 사물에 부여하여 통제 관리의 편리성을 갖고 있지만 고유번호에 대한 정보만을 알아내면 이 제품에 연결된 상품이력정보, 고객정보 등 모든 정보를 알아낼 수 있게 된다. 주민등록번호제도가 우리나라 행정관리에 있어 상당히 많은 장점을 가져다 준 반면 주민등록번호를 악용한 범죄사례가 빈번히 발생하여 사회적인 문제가 된 바와 같이 모든 사물에 부여된 고유번호를 악용하게 되면 상상하지 못한 범죄 발생으로 사회적 혼란이 야기될 수도 있다.

1.3 개인정보 및 상품정보 등 대량의 데이터 수집

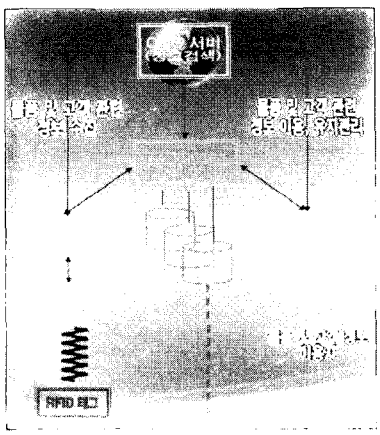
EPC Global에서 표준규격으로 제안하고 있는 EPC 네트워크는 사물의 정보를 관리하는 체계로 기본 동작 흐름은 다음과 같다.

① RFID 코드 생성 및 PML 서버에 물품정보 등록, ONS 서버에 PML위치(URL) 등록

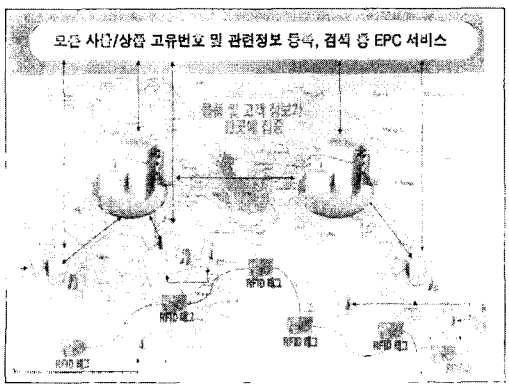
② RFID 코드를 RFID 태그에 입력시킨 후 물품에 부착

③ RFID 리더를 통해 RFID 태그의 RFID 코드 수집
④ RFID 리더가 수집한 RFID 코드를 Savant 서버로 전송
⑤ RFID 코드에 해당하는 물품의 정보를 얻기 위해 Savant 서버는 PML 서버의 URL을 ONS 서버에게 조회하고 ONS 서버는 PML 서버의 URL 정보를 전달
⑥ Savant 서버는 RFID 코드에 해당하는 물품정보를 PML 서버를 통해 수집
⑦ Savant 서버는 이벤트 발생조건이 충족되면 이에 따라 정보를 처리하여 응용서버로 전송

EPC 네트워크에서는 상품정보 및 고객정보를 하나의 DB에서 관리하게 됨으로써 다량의 데이터가 수집될 뿐만 아니라 하나의 지역의 데이터 관리가 아닌 전 세계로 퍼져있는 제품의 관리를 중앙 집중적으로 관리하고자 하기 때문에 그림 3에서와 같이 세계 곳곳에 퍼져 있는 물



〔그림 2〕 EPC 네트워크 기본 구성요소



〔그림 3〕 EPC 네트워크

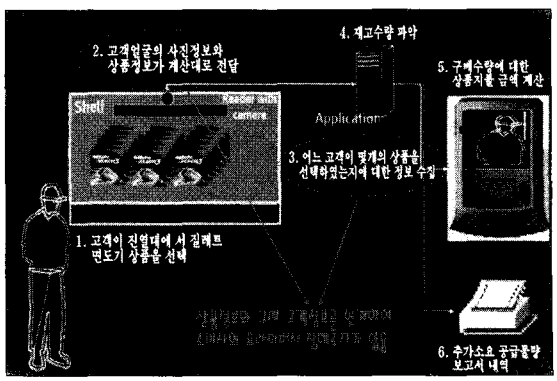
품에 관한 정보가 RFID 태그를 통해 한곳으로 집중될 우려가 있다. 또한 한번 수집된 정보는 파기되지 않고 수차의 분석을 통해 다양한 용도로 재활용될 수 있어, 고객 선호도 분석을 통한 고객 맞춤형 광고성 스팸메일 발송 및 고객정보 불법 거래 등의 역기능 발생이 예상된다.

모든 정보가 한곳의 DB로 집중되게 되면 공격 목표도 한 곳으로 집중되므로 정보를 다른 곳으로 분산시키거나, DB 보안에 대한 기술적 대응방안을 강구하여야 할 것이다.

1.4 RFID 리더의 소형화 또는 통신기기에 내장되어 눈에 띄지 않음

RFID 리더의 형태는 바코드 스캐너와 같이 독립개체로 존재할 수 도 있지만 데이터를 바로 전송하여야 하는 응용분야에서는 PDA 등과 같은 휴대용 통신기기에 내장될 수도 있다. 또한 RFID 리더의 소형화로 인해 최근에는 동전크기로 제작된 RFID 리더가 판매되기도 한다. 앞서 설명하였듯이 미국 월마트와 질레트사가 RFID 시스템 도입을 실패한 원인은 RFID 부착사실을 고지하지 않았기 때문에 소비자 단체들에게 프라이버시 침해 의혹을 불러일으켰다. 미국 소비자 단체인 CASPIAN의 발표에 따르면 질레트 면도기 포장에 RFID 태그가 프린팅되어 있었으며 월마트의 진열대에 RFID 리더가 내장되도록 설치하였다. 그림 4는 월마트 RFID 시스템의 동작시나리오이다[3].

이외에도 유럽에서는 2005년부터 유로 지폐에 RFID 태그를 부착하여 유통시킬 계획을 가지고 있다. 유로 지폐를 가지고 다니는 사람은 언제나 강도의 표적이 될 수 있다. 예를 들어 강도는 RFID 리더를 숨기고 다니면서 지폐에 붙은 RFID 태그를 스캔하여 많은 지폐를 지갑에 넣어 다니는 행인의 정보를 획득함으로써 범죄대상으로



〔그림 4〕 월마트 RFID 시스템 동작시나리오

삼을 수 있다. 결국 100만원 뭉치 돈을 투명 비닐백에 넣어 다니는 것과 마찬가지 결과를 초래하게 될 수도 있다.

따라서 올바르지 않은 RFID 리더가 RFID 태그 정보를 수집할 수 없도록 하는 정보보호기술 개발이 시급한 실정이다.

2. 단계별 USN 서비스에 따른 정보보호 위협

RFID/USN 발전단계에 따라 USN 서비스의 유형도 다양해질 것으로 예상된다. 수동형 RFID 태그를 활용한 유통 분야의 재고관리 서비스, 센서를 활용한 원격진료 서비스, 통신 기능을 갖춘 센서를 활용한 텔레매틱스, 자율제어 기능을 갖춘 센서를 활용한 u-Commerce 서비스 등 RFID 활용서비스는 다른 IT 기술에 비해 우리 일상생활과 훨씬 가까운 곳에서 일어난다. 하지만 이러한 RFID 활용서비스에서의 정보보호 위협에 대한 대책을 마련하지 않은 경우 우리 생활에 바로 악영향을 미칠 수 있다. 다음은 RFID 활용 USN 서비스 유형별 [2] 로 가상 위협시나리오를 열거한 것이다.

(가) 동물 이력관리 서비스 : 가축에 RFID 태그를 부착하여 출생, 도축, 유통까지의 전 과정의 생산이력제로 관리함으로써 광우병과 같은 가축 질병 발생시, 성장과정을 역추적하여 정확한 원인을 파악하여 대처
-〉 (역기능) : 광우병이 걸린 가축의 이력을 담은 RFID 태그를 조작하여 폐기될 육류 등을 유통시킴으로써 소비자 피해 발생의 우려가 있음

(나) 홈네트워크와 연계된 환경정보 센싱 서비스 : 환경정보(온도, 습도, 압력 등)의 센싱기능을 가진 RFID 태그를 가전제품에 부착하여 홈네트워크로 연결하여 다양한 기능을 자동으로 수행케 함으로써 u-Life 실현
-〉 (역기능) : 가전제품들이 홈네트워크로 연결되어 이상 발생시 서비스센타에 자동으로 연락을 취하도록 설계되어 있으나 가전제품의 이상 발생을 탐지하지 못하거나 오작동으로 인한 오류정보 전송으로 적절히 대응하지 못하여 안전사고 발생 초래

(다) 의료 약품분야와 연계된 환경정보 센싱 서비스 : 사람의 신체 또는 주변장소에 혈압, 맥박 등을 측정할 수 있는 센서형 RFID 태그 설치, 원격 건강진료를 통한 환자 진료의 효율화 및 편리성 증대와 고령화 사회에 대비한 응급 서비스 체제 구축
-〉 (역기능) : 응급환자 발생시 환자의 의료정보를 즉시에 정확히 전달하지 못하도록 방해함으로써 환자의 생명에 위협을 가할 수 있음

(라) 자동차 교통 분야의 RFID 태그 간 통신 서비스 : 통신기능을 갖춘 태그를 타이어와 중요 부품에 장착하고 주행시 태그 간의 통신에 의해 교통사고를 회피하거나, 차량 이상을 사전에 감지하고 교통 상황 정보를 실시간 수집하여 최적화된 교통제어 수행
-〉 (역기능) : 차량 결함 및 열악한 도로 조건 등에 대한 정보전송에 오류가 발생하거나 고의로 정보를 변조/누락시키는 경우 교통대란 및 교통 사고 초래 가능

(마) 환경 관리 분야의 RFID 태그 간 통신 서비스 : 수온, 오염도, 강수량 등 자연 환경정보를 센싱할 수 있는 RFID 태그를 자연자원에 심고 댐 수위조절, 하천 관리, 대기 오염 모니터링 등 서비스 제공
-〉 (역기능) : 오염도를 잘못 감지하거나 오염 정보에 대한 정보를 잘못 전송하는 경우 대기오염으로 인한 적절한 대응조치를 취할 수 없음. 또한 강수량 등을 측정하는 센서의 오동작으로 댐 수위 조절을 못하는 경우 홍수, 범람의 자연재해로 이어질 수 있음

(바) 물류/유통 분야의 RFID 태그 제어 서비스 : 자율컴퓨팅 기능(상황판단, 의사결정, 예측, 실행)을 가진 RFID 태그를 제품에 부착하여 식품 운송 중 주변 환경이 임계치를 초과하여 식품위생에 문제가 발생하면 자동으로 폐기처리 또는 고객의 구매 취향을 파악하여 고객이 원하는 최적의 물건을 선정 구매 지불을 자동으로 수행
-〉 (역기능) : 자동폐기 처리될 식품이 품질정보의 오류로 인하여 유통되는 경우 국민 건강에 위협이 되며 구매물건의 가격을 잘못 입력함으로써 부정확한 지불을 수행하여 고객의 재정에 손실

Ⅲ. 안전한 RFID/USN 기반조성을 위한 정보보호방안

1. 새로운 RFID/USN 환경의 특성

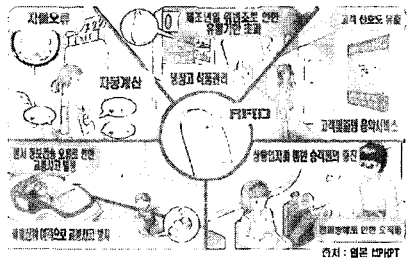
사물에 RFID 태그를 부착하여 궁극적으로 사물과 사물이 의사소통 할 수 있는 USN 환경에서는 정보화의 영역이 사람 중심에서 사물로 확대됨에 따라 기존의 인터넷 기반의 정보통신환경과는 다른 환경의 변화가 있을 것으로 예상되며 이에 따른 정보보호 위협도 지금과는 많이 달라질 것이라 예견할 수 있다. 즉, 인터넷에서 발생된

위협이 전체 위협요소로 이어질 수 있어 불법적 공격으로 인한 피해는 상상을 초월할 정도로 증가할 것이다.

전자상거래 서비스, 지불 서비스, 인터넷 뱅킹 등 현재 제공되고 있는 인터넷 기반 웹 서비스들의 대상 주체는 사람이나 USN이 구축되면 RFID 태그가 부착된 사물이 새로운 전자거래의 주체로 등장하면서 정보화 주체가 사람에서 사물로 확대될 것이다. 또한 TCP/IP 기반의 유선인터넷 망은 전화망과 같은 통신선로가 있는 고정망으로, 현재의 네트워크 보안기술은 인터넷 기반의 유선 네트워크 환경에 초점이 맞춰져 왔으나 USN 구축으로 정보가전, PDA, 자동차 등과 같은 단말이 기지국, 중계국과 같은 역할을 수행하면서 네트워크 구성 객체로 참여하므로, 이러한 단말의 빈번한 변화는 망형태의 동적인 변화에 대응하는 자율분산형 무선·이동망의 특성을 갖게 되므로 이에 대한 네트워크 보안기술이 요구 된다. 즉, RFID 태그에 통신기능을 부가함으로써 전자파를 통신 매개체로 하는 무선 네트워크 환경에 맞는 센서 네트워크 보안기술이 개발되어야 한다. 무선환경에서는 무선신호 범위 안에서는 누구나 접속이 가능하기 때문에 도청이나 신호방해 공격 등이 훨씬 쉬워질 수 있어 RFID 태그와 RFID 리더의 인증수단을 마련하여 도청의 위험요소를 제거하여야 한다. 통신형태는 PC-서버 간의 통신형태가 휴대 단말기-휴대 단말기, 정보가전-PDA 등의 P2P 형태로 변모할 것이다. 이러한 P2P 통신으로 이동기기가 네트워크 구성객체로 참여하면서 인터넷 공격대상이 인터넷에 연결되어 있는 PC, 서버 등에서 USN에 연결되어 있는 모든 자동차, 정보가전, 휴대기기 등으로 사이버 공격의 표적이 확대될 수 있다. 또한 이로 인하여 인터넷에 연결되어 통신을 하는 제한된 사람들만이 e-프라이버시 침해 대상이었지만 RFID 태그가 부착된 사물을 가지고 다니거나, 휴대기기를 지니고, 홈네트워크가 구축된 집에서 생활하게 되는 모든 국민이 프라이버시 침해 대상이 되어 향후에는 살아 숨쉬는 것만으로도 프라이버시 침해 위협에 노출될 가능성이 있다.

2. RFID/USN 발전단계에 따른 정보보호 이슈

USN은 우선 인식정보를 제공하는 RFID 태그를 중심으로 발전하고 이에 센싱 기능이 추가되면서 이들간의 네트워크가 구축되는 형태로 발전하는데 이러한 RFID 태그의 발전단계에 따라 정보보호 핵심 이슈도 달라지게 된다. 그림 5는 일본에서 발표한 RFID 활용서비스의 예에 대해 발생할 수 있는 위협을 나타내고 이러한 위협을 막을 수 있는 정보보호 기술을 표시하였다.



〔그림 5〕 RFID 활용서비스와 정보보호 기술

(가) 읽기전용 RFID 태그 : 현재 가장 많이 사용되고 있는 저가형 RFID 태그의 가장 큰 문제점은 개인정보의 과다노출이 발생한다는 것이다. 현재 이를 방지하는 기술로 태그 도청방지 기술, 특정 신호시 태그 정보를 비활성화시키는 기술, 태그 정보 블로킹 기술 등 주로 태그 정보 유출에 따른 문제점을 보완하기 위한 저가형 RFID 태그 프라이버시 보호 기술들이 개발되고 있다.

(나) 읽기/쓰기용 RFID 태그 : 쓰기 기능이 부가되는 RFID 태그에는 무결성, 기밀성 등 보안서비스가 제공되어야 하는데 현재 사용하고 있는 해쉬알고리즘, 블록암호알고리즘 등은 계산이 복잡하여 계산능력이 단순한 읽기/쓰기 RFID 태그에 탑재할 수 없다. 따라서 이들 태그의 계산능력, 저장공간, 소모전력 등의 특성을 고려한 새로운 차세대 초경량, 초전력 암호화 및 무결성 기술의 필요성이 대두되고 있다. 현재 RFID 태그 중 가장 값이 싸며 작은 태그는 Atmel TK5552 IC칩을 가지고 있다. 이 IC칩은 992비트의 저장공간을 갖고 있으며, 데이터 전송 비율은 약 초당 100kB이다.

또한, 메모리의 내용에 대한 읽기/쓰기를 허용하고 $1.0로 판매가 되고 있다. 그러나 향후 보편적으로 사용될 RFID 태그는 US$0.05~US$0.1의 가격범위에 있기 때문에 강인한 암호프리미티브를 사용하는 것은 현실적으로 가능하지 않다. 낮은 가격의 범위를 벗어나지 않으면서 보안 및 프라이버시 위험을 고려한 RFID 태그 및 RFID 리더의 설계가 중요한 문제가 되고 있다[4].

(다) 센서 : 주변환경의 정보를 수집하여 주변 상황을 인지하고 이에 따른 정보처리 능력을 가진 센싱형

RFID 태그에서는 스마트카드의 IC 칩과 같이 물리적 공격에 저항할 수 있는 보안칩 개발이 이루어져야 한다. 또한 RFID 태그가 부착된 u-디바이스가 정보 수집의 주체가 되면 네트워크에서 이들의 실체를 확인할 수 있는 u-디바이스 디지털 인증기술이 필요하게 된다.

(라) 통신기능을 갖춘 센서 : Ad-hoc 네트워크는 네트워크 토폴로지가 수시로 변하고, 네트워크를 구성하는 노드들의 참여/탈퇴가 수시로 일어나기 때문에 고정된 인프라를 대상으로 하였던 기존의 네트워크 보안기술로는 새로운 위협에 대처할 수 없다. 예를 들어 현재의 암호통신에 필요한 키를 관리하는 키관리프로토콜은 1:1 통신을 기본으로 하고 있으나 Ad-hoc 통신은 1:n, n:n 통신을 하기 때문에 통신에 참여하는 노드들의 참여/탈퇴에 따른 동적인 그룹 키관리 프로토콜의 개발이 필요하다. 또한 네트워크 토폴로지 변화 및 통신 노드의 동적인 참여로 인하여 라우팅 과정에서 노드가 바뀔 수 있으며 이러한 잦은 라우팅 변경은 보안서비스에 많은 오버헤드를 발생시킬 수 있는 문제점이 있다. 따라서 센서네트워크 특성을 고려한 효율적인 보안 라우팅 프로토콜 개발도 필요하다.

(마) 자율형 제어 기능(RFID 태그에 리더기능 포함) : 자율 컴퓨팅 기능(상황판단, 의사결정, 예측, 실행)을 가진 RFID 태그는 사람을 대신하여 판단하고 행동하기 때문에 P3P (Platform for Privacy Preferences) 기술과 같이 사람이 자신의 개인정보보호 수준을 결정할 수 있듯이 사람을 대신하여 RFID 태그가 개인정보보호 수준을 결정할 수 있는 자율형 센서 프라이버시 보호기술의 개발이 핵심 이슈가 될 전망이다. 또한 자율형 제어 기능을 갖춘 RFID 태그에 기반한 USN 서비스가 정착되면서 u-Commerce 시대가 도래 할 것이며 이에 따라 지불 보안기술 개발에 대한 수요도 새로 생길 것이다.

3. RFID/USN 정보보호 추진방안

앞서 설명하였듯이 다양한 경로로 센서와 개인단말을 통해 수집되는 개인의 위치정보, 서비스 사용패턴, 신상정보 등 민감한 정보는 개인화된 서비스를 제공하지만, 역으로 심각한 프라이버시 침해와 감시도구로 사용될 수 있다. 정보보호가 전제되지 않을 경우, 개인단말기의 식별번호를 통한 이용자의 노출, 추적 기능 등은 개인 사생활의 해체로까지 이어질 수 있다. 따라서 무엇보다 사용자가 믿고 이용할 수 있는 안전한 USN 서비스를 제공하고 프라이버시를 보호하기 위한 준비가 필요하다. 실례로 외국에서는 RFID 판독기가 건물 바닥 타일에 심어져 소비자들을 스캔하는 사례가 보고된 바 있다.

이에 정부는 안전한 RFID/USN 환경조성을 위하여 다음과 같은 정보보호 정책방안을 마련하여야 한다.

3.1 RFID/USN 프라이버시 보장을 위한 법제도 정비

개인프라이버시 보장을 위한 제도정비를 통한 RFID/USN 정보보호 관련 법제도 기반을 조성하여야 한다. 현재 법제도 정비의 일환으로 한국정보보호진흥원은 년내에 RFID 프라이버시보호가이드라인(안)을 마련할 계획이다. RFID 프라이버시보호가이드라인(안)의 목적은 RFID 시스템을 도입한 사업자나 RFID 태그 부착 물품을 취급하는 자가 준수하여야 할 기본적인 사항을 정함으로써 RFID 활용서비스를 안전하게 제공할 수 있는 환경 조성을 통해 소비자의 권리와 이익을 보호하기 위함이다. 이외에도 지금의 개인정보보호와 관련한 법들은 개인정보 수집에 대한 명시적 동의, 사실 고지 등 자기정보통제권을 보호하기 위한 최소한의 원칙들을 규정하고 있다. 그러나 RFID/ USN에서의 정보유통환경은 정보수집 방법· 경로의 상이함 및 동의획득의 곤란함, 정보주체에 대한 고지의 어려움 등의 이유로 현재의 법체계에 적용하기 어렵다. 기존의 법제의 개선 등을 모색하면서, 이러한 법·정책적 대안들이 RFID/USN 환경에서의 개인정보 침해 문제를 충분히 해결할 수 있는지 아니면 새로운 환경에 타당한 새로운 입법을 추진할 필요가 있는지에 대한 제도적 연구가 선행되어야 한다[5]. 향후 전자거래의 대상주체가 사물로 까지 확대되는 RFID/USN 환경에서 지금의 전자서명법체제 내에서 전자거래 주체인 사람의 신원확인을 위한 인증제도가 유효할 수 있는지 검토해야 한다. 현재의 전자서명법 체계내에서는 사물이 전자서명의 주체가 되어 인증서를 발급받을 수 없다. 그리고 USN 기반 RFID 활용서비스인 원격진료서비스에서 환자의 건강상태를 센싱하여 이러한 정보를 의사에게 전달하면 의사는 검진소견 또는 처방전을 발급하여 이를 환자에게 전송해주게 되는데 이때 처방전을 발급한 의사가 정말로 의사자격을 갖춘 의사인지를 확인하기 위해서는 자격 증명을 위한 속성인증서가 필요하다. 하지만 이 역시도 현재 전자서명법 체계내에서는 사람의 신원확인을 위한 인증서 발급만을 대상으로 하고 있어 속성 증명을 위한 인증서 발급을 포함할 수 없다. 따라서 현재의 법제도

내에서 USN 기반 RFID 활용서비스가 공정하고 안전하게 이루어질 수 있는지 서비스별로 분석하여 개선책을 제시하여야 할 것이다.

3.2 RFID/USN 정보보호 인프라 구축

USN 서비스 이용자 환경의 안전성을 향상 킬 수 있도록 RFID/USN 기반 정보통신기기의 안전성 검증제도 및 u-디바이스의 인증 및 속성 인증 등 다양한 인증유형을 수용할 수 있는 디지털 통합인증제도 등 안전한 RFID/USN 정보보호 인프라 구축을 추진하여야 할 것이다.

정보보호기술/보안모듈을 탑재한 RFID/USN 기반 정보통신기기의 안전성을 제작단계에서부터 확보할 수 있도록 이에 대한 안전기준 마련 및 검증체계가 구축되어야 한다. RFID 태그 및 리더 등에 탑재 가능한 정보보호 자원의 공동 활용과 재사용을 위하여 RFID/USN 기반 정보통신기기용 정보보호기술 아키텍쳐 및 보안프레임워크를 개발하여 이를 표준화하여야 한다. 또한 Ad-hoc 네트워크 등 자율분산형 네트워크의 취약성으로 인한 다양한 위협에 예방 및 대응할 수 있도록 안전한 기기 등의 설계 및 구현 가이드라인을 개발·보급할 필요가 있다. 이외에도 인터넷 기반의 정보통신환경에 초점을 맞춘 기존의 정보보호시스템 평가체계를 확대·개편하여 RFID/USN 환경에 적합한 새로운 정보보호의 안전성을 검증할 수 있는 제도로 개선하기 위하여 RFID 태그에 탑재 가능한 초경량 암호기술, 자율형 네트워크에 적합한 능동형 접근제어기술 및 키관리 기술, RFID 태그의 개인정보보호기술 등 새로운 RFID/USN 정보보호기술의 안전성 검증 기준을 마련하고 이 기준에 따라 기기의 안전성을 검증할 수 있는 검증방법론 개발도 병행되어야 한다.

RFID/USN 환경의 구축으로 RFID 태그가 부착된 사물이 새로운 전자거래 주체로 등장함에 따라 사람의 신원확인을 목적으로 하는 기존 전자서명관리체계를 RFID/USN 환경에 맞게 변환할 필요가 있다. RFID/USN 환경에서는 RFID 태그를 이용하여 사물의 식별이 가능해야 하므로 용도에 따라 식별번호 를 부여하는데 이를 기반으로 RFID 태그가 부착된 사물이 정보의 주체가 되어 네트워크 통신/전자거래에 참여하게 된다. 이러한 환경에서 참여개체의 정당성을 확인하는 인증절차를 수행하지 않는다면 사회적·경제적 피해를 발생시키는 RFID/USN 정보화 역기능이 발생할 수도 있다. 예를 들어, 회사의 불만을 품은 직원이 회사의 RFID 리더를 이용하여 회사제품에 부착된 모든 RFID 태그 정보를 삭제, 변조하고 회사 고객관리 및 상품관리 DB 정보를 파괴함으로써 노조파업시 RFID 시스템 악용이 예상되며, 경쟁회사가 RFID 리더를 이용한 불법 감청을 통해 어떤 유형의 제품을 얼마나 생산· 선적하는 지 등에 대한 정보를 빼내는 등 산업스파이 활동에 악용될 소지도 있다. 제품의 식별·인증 정보를 담고 있는 RFID 태그의 정보를 읽거나 가로채기 하는 경우 이를 이용하여 RFID 태그를 위조할 수 있어 이러한 위조 RFID 태그를 모조품에 부착시켜 불법 유통시킬 수 있는 등 RFID/USN 기반 통신참여 개체에 대한 인증수단의 부재로 나타날 수 있는 문제점이 있다[6]. 따라서 RFID 시스템 개체에 대한 인증을 수용할 수 있는 체계마련이 반드시 이루어져야 한다. 하지만 PKI 모델은 계산능력이 좋은 PC와 서버를 대상으로 설계하였기 때문에 상대적으로 계산능력이 떨어지는 RFID 태그 및 RFID 리더의 인증기능을 수용하기에는 문제가 있다. PKI 모델은 인증서 경로검색, 인증서 폐지목록 유지관리 등 부하가 많이 걸리는 작업을 CA 서버를 통해서 하는데 USN 네트워크에서는 CA 서버의 역할을 수행할 수 있는 안정적인 참여개체가 없다. 그러므로, 사람의 신원확인을 위한 인증기능은 PKI 모델을 그대로 RFID/USN 환경으로 가져올 수 있지만, RFID 태그와 리더, 센서 등의 인증기능은 기존 PKI 모델에서 수용할 수 없어 PKI 모델을 경량화하거나 또 다른 RFID/USN 인증모델 개발이 요구된다. 또한 앞서 설명한 바와 같이 USN 기반 RFID 활용서비스가 제대로 이루어지기 위해서는 자격증명을 위한 속성 인증서 발급체계도 갖추어져야 하며, 신원정보 및 위치정보 노출을 최소화하면서 개인화된 RFID 활용서비스가 가능하도록 익명 인증서 발급에 대한 연구도 진행되어야 한다.

3.3 RFID/USN 정보보호 핵심기술 확보

눈으로 쉽게 확인할 수 없도록 RFID태그를 부착하거나 RFID 리더의 소형화 또는 통신기기에 내장되고 이들을 통해 개인정보 및 상품정보 등 대량의 데이터를 수집하는 등의 RFID 시스템 특성으로 인하여 개인정보보호의 중요성이 더욱 부각되고 있다. RFID 리더가 소형화되어 눈에 뛰지 않기 때문에 RFID태그의 정보를 당사자 모르게 얻을 수 있는 문제점이 있다. 따라서 재밍공격 등을 통해 RFID태그로부터의 정보가 유출되지 않도록 Blocker Tag기술, Kill Tag기술 등과 같은 RFID프라이버시보호기술 등을 개발하여야 하며, 정당한 RFID리더만이 RFID태그 정보를 읽을 수 있도록 RFID태그와 RFID리더간의 상호인증기술이 필요하다. 그러나 암호기술을 활용한 기존의 상호인증, 무결성, 기밀성 등 정보보호기술들은 계산처리 능력이 좋은 환경에서 고려된 방식

으로, 읽기전용 RFID태그, 읽기/쓰기 RFID태그와 같은 저가형 RFID태그는 아주 작은 소형 프로세서와 소량의 메모리 등 구조적 제약조건을 가지고 있기 때문에 계산능력의 한계가 있어 현재의 정보보호기술을 그대로 적용할 수 없다. 따라서 RFID/USN 환경에 적합한 정보보호기술을 제공하기 위한 암호원천기술 개발이 먼저 이루어져야 한다. 즉, 5센트 이하의 저렴한 RFID 태가 사용할 수 있는 전력, 처리시간, 저장공간, 게이트 수 등의 자원이 제한된다. 또한 이러한 RFID태그용 IC 칩 비용은 2센트를 넘으면 안되기 때문에 IC 칩을 구성하는 게이트 수가 7,500~15,000개로 제한된다. 따라서 보안기능을 제공하기 위해 사용할 수 있는 게이트의 수는 2,500~5,000개로 제한된다[7]. 하지만 현재 사용하고 있는 AES, DES, SEED 알고리즘들은 앞서 설명한 저가의 RFID 태그에 적용하기에는 이들 RFID 태그가 가진 메모리, CPU 등의 자원을 훨씬 더 많이 요구한다. 예를 들어 앞에서 설명했듯이 5센트 정도의 저가의 전자태그는 안전성 측면에서 요구되는 게이트의 수가 2,500~5,000개를 넘어서면 안되지만, 일반적으로 AES와 같은 블록암호알고리즘을 하드웨어로 구현하는 경우에 20,000 ~ 30,000개의 게이트를 필요로 한다[8]. 따라서 RFID태그, RFID 리더 또는 센서 등과 같이 초경량, 저전력 계산환경에서 고속의 암호연산이 가능한 암호기술 개발이 반드시 필요하다. 이를 위해 초경량, 저전력 등 RFID/USN 환경에 적합한 암호알고리즘의 사양을 도출하기 위한 연구가 선행되어야 한다. 미국의 경우 2003년 북캘리포니아 주립대학의 임베디드 시스템 연구센터(Center for Embedded Systems Research)에서는 RFID태그의 계산환경과 유사한 플랫폼에서 MD5, SHA1(이상 해쉬함수), RC5, IDEA(이상 블록암호), RC4(스트림 암호) 등 암호알고리즘의 수행 속도 및 코드 길이 등을 비교한 결과를 제시하는 등 RFID/USN 환경에 적합한 암호알고리즘의 사양을 찾기 위한 연구를 진행하고 있다.

또한 EPC 체계에서는 고객의 정보 및 상품정보를 DB에서 집중적으로 수집 관리하기 때문에 DB보안에 대한 기술개발도 이루어져야 한다. 현재 대부분의 웹서버 운영자들은 가입자 또는 고객의 정보 DB의 보안을 위해 관리자 인증 및 접근제어 등과 같은 기본적인 정보보호기술을 적용하고 있고 DB 정보 자체를 암호화하여 보관하는 곳은 드물다. 이용자의 민감한 개인정보를 안전하게 관리하기 위해 정보를 저장한 DB를 암호화하여 보관한다 하더라도, 현재의 DB 암호화 기술로는 웹 운영에 필요한 통계수치를 파악하기 위해 DB 전체를 복호화해야 하기 때문에 필요 이상의 개인정보가 노출 될 수 있다. 대량의 정보를 가진 DB 자체를 빠르게 암호화하여 보관할 수 있는 기술개발이 필요하며, 특히 암호화된 개인정보 DB를 복호화하지 않고도 필요한 통계수치를 산출해 낼 수 있는 DB 암호화 기술 개발이 꼭 필요하다. 이외에도 센싱형 RFID 간의 통신이 가능해지고, RFID가 자율제어 기능까지 갖추게 되는 궁극적인 RFID/USN 환경에서는 지금보다도 더 고도의 정보보호기술이 요구된다.

USN은 여러 종류의 센서노드들이 무작위로 배치되며 센서노드들의 토폴로지와 라우팅 경로의 변화가 수시로 일어나 각 센서노드를 관리하기 어렵기 때문에 위장 센서노드가 정상 센서노드 사이에 위치하기가 용이하다. 따라서 USN을 구성하는 이동 센서노드들은 수시로 가입/탈퇴를 하기 때문에 이러한 특성을 고려하여 키관리 및 보안 라우팅 프로토콜 등 네트워크 보안메커니즘을 동적으로 설계하여야 한다. 또한 센서노드는 레이저 에칭(etching), 탐침, TEMPEST 공격 등 물리적 공격에도 취약성을 가지고 있기 때문에 센서노드에 탑재되어 있는 암호키를 노출시킬 수도 있다. 따라서 이러한 위협을 고려하여 USN환경에 적합한 키관리 기술이 개발되어야 안전한 센서네트워크 환경을 구축할 수 있다. USN 통신에 참여하는 송수신 개체들은 보안서비스를 제공받기 위해서는 통신이 개시되기 이전에 암호키를 생성할 수 있는 비밀정보를 사전에 공유하여야 하는데 USN환경의 특성으로 인하여 이를 해결하기가 쉽지 않다. 또한 USN의 이동 센서노드들은 End-to-End 암호화방식을 사용하지 않고 Hop-by-Hop 암호화 방식을 주로 사용한다. 즉, 각 센서노드는 이웃 센서노드와의 암호키만을 공유한다. 이 경우 하나의 센서노드를 제어하고 있는 공격자가 자신의 노드를 통한 암호문을 복호화할 수 있는 문제가 있다. 이러한 문제는 공격자가 수많은 통신이 자신의 노드를 경유하도록 조작하는 경우 정보유출 등 심각한 문제가 될 수 있다[9]. 그리고 공격자는 위장 센서노드를 통신개체로 참여시켜 거짓 라우팅 정보를 네트워크에 주입함으로써 라우팅 프로토콜에 대해 DoS 공격을 가해 통신을 단절시킬 수 있는 문제점이 있다. 이러한 문제를 해결할 수 있는 자율분산형 Ad-hoc 네트워크 환경에 적합한 동적 라우팅 보안프로토콜의 개발이 필요하다. 이외에도 RFID태그 부착 제품의 소유자가 노출되는 자신의 정보 수위를 조절하여 원치 않는 정보의 유출을 방지할 수 있는 주문형 프라이버시 보호기술, RFID태그의 정보를 읽고 쓰는 주체의 세부권한 관리를 위한 역할기반 접근통제 기술, RFID/USN, BcN, IPv6의 3대 인프라의 연동환

경에서 새롭게 등장하는 보안위협을 능동적으로 모니터링, 탐지 및 대응할 수 있는 통합보안관리기술 개발 등 새로운 정보보호기술이 필요하다.

V. 결 론

RFID활용 서비스는 우리의 실생활과 아주 밀접한 IT 기반 서비스이다. 지금까지의 인터넷기반 서비스는 인터넷 이용자를 대상으로 제공되어왔기 때문에 소외계층이 있었다. 하지만 RFID활용 서비스는 모든 사물을 대상으로 제공될 수 있기 때문에 물건을 사고 팔고 하는 경제생활에 참여하는 우리 모두가 RFID활용 서비스 대상자이다. 하지만 IT 기술이 편리함을 가져다 준 반면 이에 대한 역기능이 발생하였듯이 RFID활용 서비스가 살기 좋은 U-Life 실현에 초석이 될 것임이 분명하지만 RFID로 인한 역기능 발생도 예견된다. 월마트와 베네통의 RFID시스템 도입 사례에서 알 수 있듯이 RFID활용 서비스 초기단계인 지금부터도 프라이버시 침해논란으로 서비스 보급에 차질이 생기고 있다. 과거 인터넷 서비스가 보급되기 이전에는 정보화의 역기능에 대한 국민들의 인식이 낮아 정보보호를 고려하지 않은 인터넷 서비스 보급이 가능하였으나, 지금은 인터넷, 휴대폰 등을 통한 개인정보 유출의 심각성을 누구나 인식하고 있어 정보보호 대책을 마련하지 않는 인터넷 서비스는 고객들로부터 외면받기 시작하고 있다. 더군다나 RFID활용 서비스의 대부분은 고객 정보를 기반으로 하는 맞춤형 서비스를 지향하고 있어 프라이버시 보호 등 정보보호 대책을 마련하지 않는다면 RFID활용 서비스는 보급되기 이전인 초기단계부터 고객들에게 외면을 받을 수도 있다. 살기좋은 유비쿼터스 사회를 구현하는 핵심요소로 RFID/USN을 구축하기 위해서는 정보보호에 대한 대책마련도 반드시 병행되어야 한다. 본 고에서는 RFID/USN 환경에서의 정보보호의 필요성을 제시하고자 정보보호 위협을 좀 더 구체화하였다. 기존의 논문들은 정보보호기술 측면에서 RFID/USN 환경의 정보보호 위협을 다루고 있어 일반인들이 이해하기에는 조금 어려운 점이 있었다. 따라서 본 고에서는 RFID 시스템의 실제적인 구현형태에 따른 위협을 제시하였으며, USN기반 RFID활용 서비스에서 예견될 수 있는 위협을 가상시나리오로 제시함으로써 RFID/USN 정보보호의 필요성에 대한 일반인의 인식제고의 기회가 될 것이다. 이와 더불어 정부는 RFID/USN 구축에 따른 정보보호 추진방안을 마련함으로써 안전한 RFID/USN 환경을 구축할 것이다.

참 고 문 헌

[1] 정보통신부, "RFID/USN 정보보호대책 로드맵", 전략협의회 2차 회의, June. 2004

[2] 정보통신부, "u-센서 네트워크 구축 기본계획(안)", Feb. 2004.

[3] Katherine Albrecht, "Privacy and Societal Implications of RFID," CASPIAN, 2003.

[4] 주학수, 권현조, "센서네트워크 정보보호 동향", KISA 정보보호표준동향, June. 2004

[5] 강달천,"유비쿼터스 시대의 개인정보보호법제", 중앙법학 제6집 제2호, 2004

[6] LARAN, "A Basic Introduction to RFID Technology and Its Use in the Supply Chain", Jan. 2004

[7] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, ""Cryptographic Approach to "Privacy-Friendly" Tags", submitted 2003.

[8] S. A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identication systems." In First International Conference on Security in Pervasive Computing, 2003.

[9] 박종욱, 주학수, 이재일, 이동훈, "유비쿼터스 센서 네트워크의 정보보호 이슈와 동향", 한국통신학회지, 21(6), Jun. 2004

〈著 者 紹 介〉

주 학 수 (Juhak Soo)
정회원

1997년 8월 : 고려대학교 수학과 학사

1999년 8월 : 고려대학교 수학과 석사

2001년 8월 : 고려대학교 수학과 박사과정 수료

2001년 9월~현재 : 한국정보보호진흥원 연구원

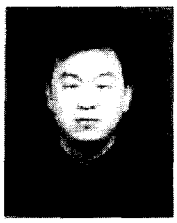
〈관심분야〉 암호학, 공개키암호, 응용보안프로토콜, RFID/UNS 정보보호

권 현 조 (Hyun Joe Kwon)
정회원

1997년 2월 : 성균관대학교 정보공학과 학사
2000년 8월 : 성균관대학교 정보통신대학원 석사
1997년 1월~1997년 7월 : (주)나라계전기술연구소 연구원
1997년 7월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 키관리, 암호프로토콜, RFID/USN 정보보호

강 달 천 (Kang, Dal-cheon)
정회원

1987년 2월 : 중앙대학교 법과대학 법학과 학사
1989년 2월 : 중앙대학교 법과대학 법학과 석사
1998년 5월 : 미국 미네소타 대학교 법학 석사
2001년 2월 : 중앙대학교 법학과 박사
2002년 1월~현재 : 한국정보보호진흥원 선임연구원
2002년 9월~현재 : 중앙대학교 법학과 강사
〈관심분야〉 개인정보보호 관련 법제도, 유비쿼터스 관련 법제도



윤 재 호 (Jaeho, Yoon)
정회원

1997년 02월 : 인하대학교 전자공학과 학사
1999년 09월~2000년 11월 : MSc IT Security in University of Westminster(London) 수료
2002년 09월~2004년 08월 : 세종대학교 소프트웨어공학과 석사
1997년 02월~1998년 12월 : (주)현대엔지니어링 FA Sensor 설계팀
2000년 12월~현재 : 한국정보보호진흥원(KISA) 암호인증기술팀 연구원
〈관심분야〉 RFID/USN 정보보호, PKI, 암호프로토콜

박 배 효 (Park, BaeHyo)
정회원

1997년 2월 : 한국과학기술원(KAIST) 전기 및 전자공학과 학사
2002년 8월 : 광주과학기술원(GIST) 기전공학과 석사
2002년 7월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 RFID/USN 정보보호, 암호프로토콜, 통합 인증기술

전 길 수 (Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호인증기술팀장
〈관심분야〉 암호학, 정보보호, RFID/USN 정보보호

이 재 일 (Jae-il Lee)
종신회원

1986년 2월 : 서울대학교 계산통계학과 학사
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월~1996년 6월 : 한국 IBM
1996년 7월~현재 : 한국정보보호진흥원 전자거래보호단장
관심분야 : 정보보호, 유·무선PKI, 유비쿼터스 보안