유비쿼터스 사회에서 프라이버시 보호 가이드라인 분석

노선식*, 이동은**

*광주대학교 정보통신학과, **청운대학교 인터넷컴퓨터학과

A Study on RFID Privacy Protection Guidelines In Ubiquitous Society

Sun-Sik Roh*, Dong-Eun Lee**

* Dept. of Information & Communication Engineering. Gwangju Univ.

** Dept. of Internet Computer. Chungwoon Univ.

E-mail : ssroh@gwangju.ac.kr

요 약

본 논문에서는 RFID를 기반으로 하는 유비쿼터스 사회에서 개인 프라이버시 침해 요인을 분석하고 RFID 프라이버시 보호를 위한 요구 사항을 도출한다. 또한 세계 각국 및 국제 단체에서 RFID 프라이버시 보호를 위한 세계 각구의 법제 동향 및 가이드라인 제정 동향에 대하여 분석한다. 이를 기반으로 국내의 RFID 프라이버시 보호 가이드라인을 분석하여 적용방안을 제시한다. 최종적으로 RFID 기술 구현에 따른 RFID 프라이버시 보호 방안을 제시한다.

Ⅰ. 서 론

유비쿼터스 사회에서는 자율 컴퓨팅 기능을 갖는 기기 및 사물 등에 의하여 인식 정보 및 상황 정보가 실시간으로 분석되며, 이를 통한 서비스가 이루어질 전망이다. RFID(Radio Frequency IDentification)는 유비쿼터스 사회를 구현하기 위한 핵심기술이다. RFID 기술은 최근 급격한 속도로 성장하고 있으며, 산업·문화·경제 등 모든 분야에서 RFID 기술을 적용하려는 노력을 하고 있다.

기본 바코드에 비해 다양한 정보를 저장할 수 있는 RFID는 사물에 대한 정보를 효율적으로 처리할 수 있는 기술이다. 이로 물류·운송·유통·재고 관리 등에 획기적인 개선을 가져올 것으로 예상된다. 하지만 RFID는 개인이 휴대하는 사물 정보에 대한 판독 또는 위치 파악에 악용되는 등 개인 프라이버시의 침해 우려가 있다. 특히 RFID를 이용하여 개인 신상 정보를 저장할 겨우 RFID 판독기만을 통해서 간단히 개인 정보를 습득할 수 있어 개인 프라이버시 침해의 위험도가 높다. 따라서 RFID를 확산하기 위해서는 사업자는 안정적으로 RFID 사업을 추진할 수 있도록 하며, 개인에게는 프라이버시 침해에 대한 우려에서 벗어날 수 있도록 기준을 제시하는 것이 필수적이다.

본 논문에서는 RFID를 기반으로 하는 유비쿼터스 사회에서 개인 프라이버시 침해 요인을 분석하고 RFID 프라이버시 보호를 위한 요구 사항을 도출한다. 또한 세계 각국 및 국제 단체에서 RFID 프라이버시 보호를 위한 세계 각국의 법제 동향 및 가이드라인 제정 동향에 대하여 분석한다. 이를 기반으로 국내의 RFID 프라이버시 보호 가이드라인을 비교 분석한다. 최종적으로 RFID 기술 구현에 따른 RFID 프라이버시 보호 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 RFID 적용에 따른 프라이버시 침해 요인 및 프라이버시 보호 요구 사항에 대하여 기술하고, 3장에서 국내외 프라이버시 보호 법제 현황에 대하여 기술한다. 4장에서는 프라이버시 보호 가이드라인의 적용방안을 제시한다.

Ⅱ. 프라이버시 침해

유비쿼터스 사회에서 RFID의 사용은 생활의 편리성을 증가시키게 된다. 하지만 RFID 기술을 이용하여 정보를 처리할 때 사용자 정보에 대한 추적·접근이 용이한 RFID의 특성은 프라이버시 침해의 위험은 갖고 있다. RFID의 사용으로 인한 프라이버시 침해 위험 요인은 다음과 같다[1]

· 은닉성(눈으로 쉽게 확인할 수 없도록 RFID 태그 부착):RFID 태그들이 소유주인 개인들이 알지 못한 상황에서 사물들과 문서에 내장되어질 수 있다. 무선전파는 섬유, 플라스틱, 다른 물질들을 쉽게 조용하게 통과할 수 있기 때문에 지갑, 쇼핑 백, 옷가방 등에 들어있는 사물 또는 옷에

부착된 RFID 태그들을 읽을 수 있다.

· 유일성(모든 사물을 구별할 수 있는 고유번호 부여):전자제품코드(EPC)는 지구상에 있는 모든 사물에 유일한 ID를 가지게 할 수 있다. 유일한 ID 번호의 사용으로 개별 물리적인 사물이 판매 또는 이전 시점에서 신원이 확인되고 구매자 또는 소유자와 연결될 수 있는 전 세계적인 사물 등록 시스템의 창조가 가능하다.

· 대량성(개인정보 및 상품정보 등 대량의 데이터 수집):RFID 배치는 유일한 태그 데이터를 포함하고 있는 대량 데이터베이스의 개발을 요구한다. 이들 기록들은 특히 컴퓨터 메모리와 프로세스 능력이 확장되면서, 개인의 신원확인 데이터와 연결될 수 있다.

· 소형화(RFID 리더의 소형화):인간 또는 사물이 모여져 있는 어떤 환경에서도 보이지 않게 섞여 질 수 있는 리더들에 의해 태그들은 시야의 제한없이 멀리서 읽혀질 수 있다. RFID 리더들은 이미 실제로 바닥 타일들에 내재되어 소비자들이 언제 또는 스캔되고 있는지 없는지에 대한 인식을 불가능하게 하고 있다.

· 추적성(개인추적과 개인정보프로파일):개인적인 신원이 유일한 RFID 태그 넘버와 연결되어 있다면 개인들이 인식하지 못하는 사이에 프로파일 되고 추적당할 수 있다

· 접근용이성(RFID 리더와 태그의 정보 전송의 용이성): RFID 태그를 사용하게 되면 RFID 리더를 이용하여 쉽게 RFID 태그의 정보를 알아낼 수 있다. 이는 은닉성과 함께 인식하지 못한 채 태그 정보가 유출될 수 있다.

프라이버시 침해에 대해 프라이버시 보호를 위한 요구 사항은 다음과 같다[2].

· RFID 소유자의 개인정보는 노출되지 않아야 한다. RFID 태그와 리더간의 정보교환을 제3자의 의해 도청되지 않아야 한다. 개인 정보가 노출되더라도 개인 정보의 내용은 허가된 자들에 의해서만 판독되어야 한다.

· 허가되지 않은 RFID 리더에 의해 RFID 태그 정보가 노출되어서는 안된다. RFID 리더의 사용은 신뢰할 수 있는 기관에 의해 허락되거나 RFID 리더가 사용되고 있음을 공지해야 한다.

· RFID와 RFID 소유자 사이 장기간 유지되는 추적 관련 정보(위치 정보포함)를 만드는 것은 불가능해야 한다. 추적 관련 정보를 생산할 때는 사전에 보고되어야 하며, 필요시에는 사용자가 정보를 삭제하거나 삭제요청을 할 수 있어야 한다.

· RFID 소유자는 작동중인 RFID를 탐지할 수 있어야 하고 그 RFID의 작동을 정지시킬 수 있어야 한다. 소유자가 RFID 태그를 선택적으로 제거할 수 있어야 하며, 자신 소유의 태그를 제어할 수 있어야 한다.

· 공개적으로 이용 가능한 RFID와 그 소유자간의 장기간 연결을 피하기 위해 랜덤화가 가능해야 하고 쉽게 변경 가능해야 한다.

· 개인 RFID에 저장된 데이터는 접근권한 부여 및 암호화 기법 등으로 보호되어야 한다. 제3자의 접근을 원천적으로 봉쇄할 수 있어야 한다.

· RFID 시스템에서 보호되지 않는 RFID는 도청, 트래픽 분석, 스푸핑 및 DOS 등의 공격에 안전해야 한다.

· 공격자가 태그 정보를 수정하거나 제거할 수 없어야 한다.

· 리더와 RFID 태그사이의 상호인증을 위한 인증프로토콜 수행 시 발생할 수 있는 공격에 대한 안전해야 한다.

III. 프라이버시 보호 법제 동향

RFID 프라이버시 보호를 위해 RFID를 규제하는 방법에는 법률에 의한 방법과 가이드라인에 의한 방법이 있다. 법률에 의한 방법은 RFID 사용에 대한 규제 내용을 입법기관에 의해 법으로 제정하는 것으로 규제 내용에 강제성이 부여된다. 반면 가이드라인은 법률적 강제성을 지니지 않고 있으나 향후 법제화에 대한 사전 예고적 성격을 지닌다. 이는 가이드라인을 제시하기 이전에 법제화를 추진하는 경우 RFID 산업 확산을 방해 할 수 있으며 법제화를 위해서 장시간을 요구함으로써 빠른 RFID 산업 정착을 방해하게 된다. 또한 가이드라인은 새로운 상황에 보다 유연한 대응이 가능하고 향후 법제화하는 경우 발생할 수 있는 문제점을 방지할 수 있다. 따라서 RFID 프라이버시 보호 가이드라인은 새로운 기수발전에 따른 법적 규율 이전에 자율적 가이드라인을 제시함으로써 제도적으로 미비한 부분을 보완하고 개인의 프라이버시를 보호하기 위해 제시되어야 한다.

25회 International conference of Data Protection and Privacy Commissioners에서의 RFID 사용에 대한 결의문을 체결하였다. RFID가 긍정적이고 효율적인 기술이라고 하더라고 RFID에서 개인정보의 활용에는 프라이버시 문제를 갖고 있다. 즉 생상 제품의 정보와 소비자의 개인정보를 연결하는 것과 태그가 부착된 제품을 처리함에 있어서 개인 위치 및 정보를 수집하는 것은 프라이버시 침해의 문제가 있다고 지적하였다.

2005년 4월 개최된 ASTAP 포럼 회의에서는 RFID에서의 개인정보보호를 위한 가이드라인 권고안을 작성하자는 한국측 기고서가 참가자들의 전체 동의를 얻어 다음 ASTAP 포럼 회의나 ITU-T SG17 회의에서 기고하기로 결정되었다. 제안된 가이드라인에서는 RFID 태그를 직접 또는 간접적으로 개인정보의 수집, 이용 및 제3자 제공에 사용하는 사업자에 대하여 적용하며, RFID 태그가 부착된 물품 및 그와 관련된 것을 취급하는 자가 준수하여야 할 기본적인 사항을 정의하고 있다.

CASPIN(Consumer Against Supermarket Invasion And Numbering)에서는 RFID를 사회전반에 도입하는 것과 개인 프라이버시 침해에 대한 우려를 하면서 2003년 6월 2003RFID 알권리

법안(RFID Right to Know Act of 2003) 제안[3] 하였다. RFID가 내장된 제품과 사용자의 프라이버시 보호에 대한 표시를 하도록 규정한 법안으로 제안되었다. 이 법안에서는 법안의 제목을 규정, 공정 포장 및 라벨링 프로그램에 대한 내용으로 RFID 태그를 포함하는 사용자 제품이나 패키지는 RFID 태그의 포함내용을 구분되게 표시하여야 함, 연방 식품, 약품, 화장품, 연방 주류, 담배와 관련된 법에 대한 내용으로 RFID 태그를 포함하게 될 경우 RFID 태그 정보를 표시하여한다는 것에 대한 규정, 소비자의 프라이버시를 보호하기 위한 조항들과 소비자와 사업자 교육에 대한 내용을 포함하고 있다.

미국의 소비자단체들은 RFID의 기술 특성상 프라이버시 침해 위험이 높은 현실과 이에 대한 보호방안이 불투명한 상태에서 RFID의 전면적인 도입에 대한 우려속에 소비자 제품에 RFID를 사용하는 것에 대한 사용자 프라이버시 성명서를 발표하였다[4]. 성명서는 RFID에 대한 간단한 소개와 RFID의 특성이 프라이버시와 자유에 대해 위협을 주는 요인을 설명하고 있으며, RFID를 사용하는데 있어서의 권리와 책임의 기반 구조를 제안하고 있다.

EPIC(Electronic Privacy Information Centre)에서는 2004년 6월 사업적인 관심과 소비자의 프라이버시에 대한 관심의 균형을 유지하기 위해 RFID 기술의 사용에 대한 가이드라인 초안을 작성하였다[5]. EPIC 가이드라인은 RFID 기술의 적용을 금지할 수는 없다는 전제속에서 RFID의 상업적인 적용을 바코드의 대체와 RFID 데이터와 미리 저장된 데이터의 대조 수단이란 두가지 영역으로 정의하고 있다. 가이드라인은 라벨, 로고 또는 다른 수단을 통해 RFID 태그가 존재하고 있음을 소비자에게 공지해야 됨을 요구하고 있다. 소비자의 쇼핑 유형 등을 파악하기 위해 판매자가 소비자의 이동을 추적하는 것을 금지하고 있다. RFID 시스템을 통해 수집된 데이터와 다른 소비자의 정보를 연결하는 부분에서 EPIC의 가이드라인은 우선적으로 소비자의 사전 동의를 요구하고 있다. 또한 소비자의 권리를 명시하고 있다.

미국 캘리포니아주 상원의원인 데브라 보웬(Debra Bowen)은 RFID 상용화와 소비자 사생활 보호 등을 주장한 법안 SB 1834(California Senate Bill, No.1834)를 제안하였다. 하지만 상원 위원회를 22-9로 통과했던 보웬의 법안은 상임위원회에서 8-0으로 거부되었다. 보웬의 법안이 거부된 이유는 이 법안은 아직 기술적으로 성숙되지 않는 RFID의 사용을 규제함으로써 향후 핵심적인 기술로 자리잡게 될 RFID의 기술 개발을 저해하게 되며, 현재로서는 RFID가 어떻게 활용될 것인지에 대한 정확한 방법이 제시되지 않은 상황에서 RFID의 사용을 규제하는 것은 옳지 않다고 판단하였기 때문이다. 이후 미국 캘리포니아주 상원의원인 죠 시미티안(Joe Simitian)은 캘리포니아주에서 발급하는 신분증 등에 RFID 적용을 금지하는 '신원정보보호법 (Identity Information Protection Act)'를 제안하였으며 캘리포니아 상원에서 29-7로 통과시켰다. 반면 캘리포니아 상공회의소, EDS, EPC글로벌, 오라클, 필립스 반도체, Texas Instrument 등으로 구성된 High-Tech Trust Coalition은 신원정보보호법은 내용이 엉망으로 기술되었을 뿐만 아니라 연방정보처리표준(Federal Information Processing Standard)나 ISO 14443과 같이 국제적으로 통용되고 있는 일반적인 보안 표준을 무시하고 있다고 주장하면서 법 발의자인 죠 시미티안 상원에게 서면의견을 제출하였다. 이에 따라 죠 시미티안은 '신원정보보호법'을 일부수정하여 보안요소를 충족시킬 경우 일부 신분증 발급의 경우 RFID 적용을 허용하는 수정안을 2005년 6월 제출하였다.

미국에서는 캘리포니아주이외에도 미조리주, 메사츄세츠주, 유타주, 로드아일랜드주에서 RFID 사용에 대한 법안을 제시하였다.

EU에서는 Article 29 Data Protection Working Party에서 RFID 기술에 대하여 다루었으며, RFID 사용에 대한 가이드라인이 포함된 협약서를 2005년 1월에 발표하였다[6]. 미국의 각 주의 법들이 RFID 프라이버시 보호에 대한 책임을 소매 상인에게 부여한 것과는 달리, EU의 협약서에서는 RFID 프라이버시 보호에 대한 책임 주체 선정에 있어서 데이터 제어자가 그들의 의무를 수행하고 개개인의 권리를 보장해 줄 수 있도록 도울 수 있는 프라이버스 보호 기술을 보장하는데 있어서 직접적인 책임은 생산자에게 있다고 정의하였다.

일본은 경제산업성이 주도하여 2003년 12월 22일에 "RFID 기술에 관한 프라이버시 보호 가이드라인(안)"을 정리하였고, 2004년 1월 21일에 이를 발표하였다. 총무성에서도 2004년 2월 23일 「RFID 개인정보보호 가이드라인」의 제정 필요성과 기본내용을 발표하였으며, 이를 기반으로 총무성과 경제산업성이 협력하여 2004년 6월 8일 "전자태그(IC태그)에 관한 프라이버시 보호 가이드라인"을 발표하였다.

국외 각국의 다양한 법제 및 가이드라인에 대한 시도와 더불어 우리나라에서도 정부에서 RFID 기술을 적용함에 있어서 가이드라인의 필요성을 인식하였다. 이에 따라 2004년 11월 RFID 프라이버시 보호 가이드라인을 제안하였다. 가이드라인 초안은 11월과 2005년 5월 두 번의 공청회를 거쳐 2005년 7월 최종적인 RFID 프라이버시 보호 가이드라인을 제시하였다[7]. 한편 우리나라의 함께하는시민행동에서는 RFID 태그가 부착된 상품이 매장에 진입되는 것에 대해 반대를 하였으며, 소비자의 물품에 직접적으로 이용되는 RFID 태그가 매장에 들어온다면 '보이콧캠페인' 등을 할 수 있음을 표명하면서, RFID에서의 프라이버시 보호를 위한 10가지 최소 가이드라인을 제안하였다.

IV. 가이드라인 적용 방안

RFID 프라이버시 보호 가이드라인은 사용자에게 안심하고 RFID 관련 제품 및 RFID 환경에서 생활할 수 있는 방법을 제시하고, 사업자에게는 사용자의 수요를 증가시켜 안전하게 사업을 활성화시키는 목적이 있다.

사업자 측면에서 RFID 제품을 생산함에 있어서 프라이버시 보호 가이드라인을 적용하기 위한 방안은 다음과 같다.

RFID 태그 생산단계서의 규제 내용은 RFID관련 기술 표준에 맞추어 생산하는지에 대한 확인이며, 이 단계에서는 사용자의 요구에 따라 RFID의 기능을 중지시키거나 필요시 저장하고 있는 정보의 일부정보를 제거할 수 있는 기술을 적용하여 생산해야 한다. 태그 생산단계에서는 개인정보가 기록되기 이전이므로 개인정보와 관련된 직접적인 규제는 없다.

RFID 태그에 정보를 기록하는 과정은 물품정보기록과 개인정보기록으로 나눌 수 있다. 물품정보기록은 RFID 생산자가 RFID 태그 구매자의 요청에 따라 관련 물품정보를 기록(또는 물품을 생산/유통하는 자가 기록)하는 것이며, 개인정보기록은 RFID 생산자가 RFID 태그를 정보가 기록되지 않은 상태로 판매하면, 사용자가 개인정보를 기록하는 것이다. 물품정보기록시에는 CODE 표준에 맞추어 물품정보 기록해야 하며, 이때는 개인정보와 관련하여 규제할 필요는 없다. 하지만 물품정보가 구매자와 관련된 정보를 추적할 가능성이 있을 경우는 사전에 공공기관으로 부터의 허락이 필요하다. 개인정보기록에서는 RFID태그에 개인정보 기록을 엄격하게 제한해야 하는데, 법률규정 또는 정보주체의 명시적 동의 없는 개인정보의 기록을 금지해야 하고, 정보 주체로부터 개인정보 기록에 대한 동의를 획득할 때에는 기록목적 등을 미리 정보 주체에게 고지해야 한다.

물품생산자가 물품에 RFID태그를 부착하는 단계에서는 RFID태그 부착사실 등을 이용자가 용이하게 알아볼 수 있도록 설명하거나 표시해야 하며, RFID 태그 기능을 제거할 수 있는 방법을 설명하거나 표시해야 한다. 또한 물품의 유통단계에서 물품에 RFID 태그가 부착되었음을 알고 소매업자로 하여금 사용자에게 공지할 수 있도록 인지되어야 한다.

물품의 유통관리 및 재고관리에 RFID 태그를 사용하는 단계에서는 RFID가 내부업무처리에 활용될 뿐 이용자와 연계되지 않을 경우 개인정보와 관련한 규제가 필요하지 않다. 하지만 유통중에 개인정보 유출의 가능성에 대해서는 명시되어야 하며, 개인정보 유출시 유통 담당자와 생산자에게 모두 책임이 있다.

RFID 태그가 부착된 물품을 판매하는 단계로 RFID 리더기를 이용하여 물품정보를 판독할 수 있다. 물품 판매시 RFID 태그가 제거되지 않고 이용자에게 교부되는 경우만 규제해야 하는데, 물품정보와 개인정보의 연계에 대한 주의 및 경고를 해야 하고, RFID 태그정보를 판독하기 위해리더기를 설치하는 경우 리더기가 설치되어 있다는 것을 표시해야한다. 또한 RFID 태그 부착 사실 등을 이용자가 용이하게 알아볼 수 있도록 설명하거나 표시해야 하고, RFID 태그기능을 제거할 수 있는 방법을 설명하거나 표시해야 한다. RFID 태그의 물품정보와 개인정보를 연계하는 경우에는 이용자에게 통지하거나 표시해야 한다.

RFID태그가 부착된 상태로 물품을 이용하는 단계에서는 개인정보가 기록된 태그가 휴대된다. RFID 태그 정보를 판독하기 위해 리더기를 설치하는 경우 리더기가 설치되었음을 표시해야 하고, RFID태그에 기록된 개인정보를 수집하는 경우에는 이용자에게 통지하거나 표시해야 한다. 또한 이용자가 개인정보의 수집을 거부할 경우 수집된 개인정보는 파기되어야 한다.

RFID 태그가 부착된 물품을 폐기할때는 RFID 태그도 탈착/파기해야 하며, 이를 위해 RFID 태그 기능을 제거할 수 있는 방법을 설명 또는 표시해야 한다.

V. 결론

이더넷을 구내 기본 망으로 사용하는 이용기관 안 설정 강화 및 보안 관리 방안을 강화해야 한다.

Acknowledgement

본 연구는 한국전산원의 지원으로 수행되었습니다.

참고문헌

[1] Electronic Privacy Information Center, Radio Frequency Identification (RFID) Systems, Washington, D.C., August 11, 2003, p. 2. www.epic.org/privacy/rfid/

[2] 강달천, "프라이버시보호가이드라인(안)" 프라이버시보호가이드라인공청회 자료집, 2004.11

[3] CASPIAN, "RFID Right to Know Act of 2003," http://www.nocards.org/rfid/rfidbill.shtml, 2003

[4] CASPIAN, et. al., " RFID Position Statement of Consumer Privacy and Civil Liberties Organizations " http://www.privacyrights.org/ar/RFIDposition.htm, 11. 2003.

[5] http://www.epic.org

[6] Article 29 Data Protection Working Party, "Working document on data protection issues related to RFID technology," 10107/05/EN WP105, Jan. 2005.

[7] 정보통신부, "RFID 프라이버시보호 가이드라인," 2005.7.