情 報 保 護 學 會 誌
第18卷 第4號, 2008. 8

RFID 프라이버시 보호 기술 및 표준화 동향

이 향 진*, 신 동 휘*, 전 길 수*

요 약

RFID 기술은 기존 물류·유통, 항만 등 다양한 산업 분야에서 널리 활용되고 있을 뿐만 아니라 고속도로 요금징수, 차량 요일제 등에도 활용되는 등 일반 사용자의 생활 전반에 걸쳐 빠르게 확산되고 있다. 또한 국내에서는 이동통신 기술과 RFID 기술을 결합한 다양한 형태의 모바일 RFID 서비스가 추진되고 있어 RFID 기술이 일반 사용자들에게 미치는 영향력은 더욱 증대되고 있다. 그러나 RFID 기술은 태그정보의 유출이 쉬워 개인정보 유출 및 이로 인한 개인에 대한 프로파일링, 위치추적 등의 우려를 포함하고 있어 RFID 기술의 활용 분야를 제한하고 있다. 본 고에서는 이러한 우려를 최소화하기 위해 개발된 Kill 태그, 블로커 태그, Clipped 태그 등 다양한 RFID 프라이버시 보호 기술을 소개한다. 또한, ITU-T SG17에서 표준화 중인 RFID 서비스에서의 개인정보 및 프라이버시보호 관련 권고(안)의 주요 내용 및 표준화 추진현황을 소개한다.

Ⅰ. 서 론

RFID 기술은 기존 바코드 기술을 대신하여 사물에 대한 정보를 효율적으로 처리할 수 있도록 하여, 물류·유통·내부 재고관리·운송 등 다양한 분야에서 널리 활용되고 있는 기술이다. 그러나 RFID 기술은 바코드나 비접촉식 IC칩 등과 달리 직접 RFID 태그를 인식시키지 않아도 RFID 리더기의 인식영역 내에 있는 경우 RFID 태그에 저장된 정보가 쉽게 판독 가능함에 따라 개인에 대한 위치추적이나 개인의 구매패턴, 취향 등에 대한 프로파일링의 수단으로 이용될 수 있어 프라이버시 침해 우려가 존재한다. 소비자들의 이러한 프라이버시 침해 우려로 인해 RFID 기술 도입 초기에 국외 유명 유통업체 등에서는 소비자들의 반대에 부딪히기도 했다. 이러한 이유로 국내·외에서는 RFID 기술의 프라이버시 침해 우려를 최소화하기 위한 다양한 기술 개발 및 정책적 조치가 취해져 오고 있다. 본 고에서는 RFID 기술의 프라이버시 침해위협을 최소화하기 위해 개발 및 적용되고 있는 다양한 기술과 관련 표준화 현황을 소개한다.

Ⅱ. RFID 프라이버시보호 기술 동향

앞서 언급한 RFID 기술의 특징으로 인해 RFID 응용 서비스에서 발생하는 프라이버시 침해 위협은 RFID 태그 정보나 백엔드 시스템에 저장된 정보를 이용하여 사용자의 개인정보를 추출 혹은 유추하거나, 태그의 전송 정보를 지속적으로 도청 또는 불법 수집함으로써 사용자의 위치를 추적하는 등 크게 두 가지 위협으로 분류될 수 있다. 다음은 이러한 프라이버시 침해 위협을 최소화하기 위한 보안대책이다.

RFID 응용 서비스에서의 이러한 프라이버시 침해 위협을 최소화하기 위해 다양한 프라이버시보호 기술이 개발 및 적용되고 있다. 특히, RFID의 경우 가격에 대한

〔표 1〕 RFID 프라이버시 침해위협 및 보안대책

위협	보안대책
개인정보 노출	RFID 태그 저장 정보 최소화
	RFID 태그 부착 사실, 성질 및 기능, 기록정보, 기능제거 방법, 리더기 설치 장소 등의 표시
	RFID 태그 저장 및 전송 정보의 암호화
	RFID 리더기 인증
	RFID 태그 신호차단제 등의 물리적 대책 적용
위치 추적	RFID 태그 부착 사실, 성질 및 기능, 기록정보, 기능제거 방법, 리더기 설치 장소 등의 표시
	RFID 태그 전송 정보의 암호화
	RFID 태그 인식거리 조절
	RFID 태그 신호차단제 등의 물리적 대책 적용

* 한국정보보호진흥원 암호응용팀 선임연구원 (jiinii@kisa.or.kr, shindh@kisa.or.kr, kschun@kisa.or.kr)

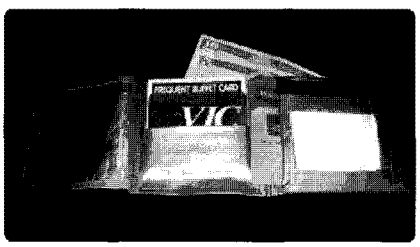
제약 및 계산량 제한으로 인해 프라이버시 보호를 위한 기존 암호화 및 인증 기술 등을 적용하기 어려움에 따라 다음과 같은 새로운 기술들이 개발되고 있다.

2.1 Kill 태그

Kill 태그는 리더기에서 패스워드(8bit)를 포함한 Kill 명령어를 전송하여 태그의 기능을 정지시키는 기법으로 사용자 프라이버시를 보호하는 가장 일반적인 방법이다. 그러나 Kill 태그의 경우, Kill 명령어가 적용된 후에는 더 이상 RFID 기술의 장점인 자동식별 기능을 이용할 수 없기 때문에 제한적인 환경에서만 이용이 가능하다.

2.2 페러데이 케이지(Faraday cages)

전파의 발산을 차단하는 특수물질로 만든 용기를 이용하여 리더기의 무선 신호 전송을 방해하여 정당하지 않은 RFID 리더기가 태그정보를 스캐닝 하지 못하도록 하는 기술로 금속성 호일 등을 이용하여 무선 신호를 차단한다. 패러데이 케이지는 일부 유용하게 사용되고 있지만 대체로 그 사용이 제한적이다.



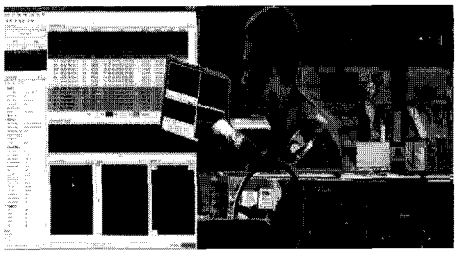
〔그림 1〕 알루미늄 포일 지갑

2.3 블로커 태그(Blocker tag)

블로커 태그는 의미 없는 신호를 발생하여 주변 RFID 태그의 통신을 방해하는 특수 RFID 태그로 정당하지 않은 리더기에 의한 태그 정보 유출을 차단할 수 있도록 2003년 RSA사에서 개발한 기술이다. 예를 들어, RFID 태그에는 'public' 또는 'private'으로 지정된 특수비트가 있는데, 이러한 태그가 부착된 의약품의 경우, 판매 전에는 'public'로 지정되어 있지만, 해당 의약품 구입 시 계산대에서 태그의 특수비트를 'private'으로 변경한다. 이렇게 태그의 특수비트가 변경된 의약품을 블로커 태그를 사용한 용기에 넣으면 블로커 태그에 의해 'private'으로 설정된 태그의 정보를 읽을 수 없도록 함으로써 의약품 구매자의 프라이버시를 보호할 수 있다.

2.4 Active Jamming

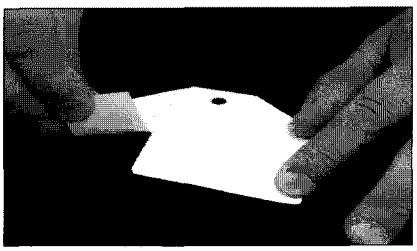
강력한 방해전파를 발산하는 기기를 이용하여 기기 근처에 있는 모든 RFID 리더기의 작동을 방해하는 기술로 RFID 태그 정보의 유출을 차단함으로써 개인정보 유출을 방지하는 기술이다.



〔그림 2〕 Active Jamming

2.5 Clipped Tag

태그 내부의 안테나 연결선을 일부 절단시킴으로써 태그의 통신거리를 줄이는 방법으로 Kill 태그 단점을 보완하기 위하여 IBM에서 개발한 기술이다. 태그의 정보저장 기능은 그대로 유지한 채 정보 송신거리를 대폭 줄임으로써 원거리에서 위치추적 등을 통한 프라이버시 침해 가능성을 줄일 수 있다.



〔그림 3〕 Clipped Tag

이 외에도 경량화된 암호학적 기술을 이용한 방법으로 해쉬함수를 이용한 Hash Lock 기법 및 Hash Lock

〔표 2〕 기타 RFID 프라이버시 보호 기술

기술	주요 내용
Hash Lock	경량의 해쉬 함수를 이용하여 백엔드 서버에게 인가 받은 리더에게만 데이터를 전송
Randomized Hash Lock	난수 생성기를 이용하여 인가된 리더에게만 데이터를 전송하도록 함으로써 Hash Lock 기법의 개인 추적 가능성 문제를 해소
Re-Encryption	정당한 리더기가 자신의 공개키로 태그정보를 암호화하여 생성된 정보를 태그에 저장함으로써 정당한 공개키를 가지는 리더기만 태그정보 수집 가능

기법을 보완한 Randomized Hash Lock, 공개키 암호화 기술을 이용한 Re-Encryption 등의 다양한 기술이 존재한다.

Ⅲ. RFID 프라이버시보호 국제표준화 동향

RFID 기술에 대한 표준화는 국제 표준화 기구인 ISO/IEC와 사실상의 표준화 규격을 제시하고 있는 EPC-global 등에서 지속적으로 추진해 오고 있다. 다만, 두 기관에서는 RFID 기술 자체 및 코드체계, Air Interface 등에 대한 표준화를 추진하고 있으며, 프라이버시보호 기술에 대한 국제표준화는 ITU-T의 보안기술 표준화 그룹인 SG17에서 주로 진행되고 있다. 한국을 중심으로 SG17 Q6(Cyber Security) 및 Q9 (Secure Communication Service)에서 RFID 응용에서 개인식별정보[1](이하, 개인정보) 보호를 위한 필요한 기술적·관리적 보안 요구사항에 대한 표준화가 진행 중에 있다.

3.1 RFID 응용에서 개인식별정보 보호를 위한 가이드라인 표준화 동향

2006년 9월 SG17 WP2 오타와 회의에서 한국이 표준 제안한 "RFID 응용에서 개인식별정보 보호를 위한 가이드라인"은 국내 "RFID 프라이버시보호 가이드라인"을 기반으로 RFID 취급사업자가 사용자의 개인정보 보호를 위해 취해야 하는 기술적·관리적 보호조치에 대한 권고사항을 제시하고 있다. 본 권고(안)은 사용자들의 RFID에 대한 프라이버시 침해 우려로 서비스 운영상의 차질이 발생하지 않도록 RFID 서비스 구축 과정에서 RFID 사업자 및 시스템 개발자들이 참고할 수 있는 모범사례를 제시하는 것을 목표로 하고 있다.

권고(안)은 RFID를 통한 데이터 수집, 프로파일링, 사용자 추적 등 RFID 기술 특징으로 인한 프라이버시 위협과 RFID 기술을 이용한 재고관리, 고속도로 요금 자동징수 시스템, 스마트 포스터 서비스 등 다양한 RFID 서비스 형태에 따라 발생되는 프라이버시 위협을 소개하고 있다. 또한, 권고(안)은 이러한 위협으로부터 사용자 개인정보를 보호하기 위해 OECD 프라이버시 원칙에 따라 RFID 서비스 제공자가 사용자 개인정보를 보호하기 위해 제공해야 하는 기술적·관리적 보호조치에 대한 모범사례를 권고의 형태로 제시하고 있다.

권고(안) 주요내용

o RFID 응용에서의 프라이버시 위협
- RFID 태그 소유자 몰래 태그 정보 수집이 가능함에 따라 불법적 정보수집 가능
- RFID 태그가 부착된 물품 정보 수집을 통해 이용자의 구매패턴, 성향 등에 대해 프로파일링 가능
- RFID 태그 추적을 통해 태그 소유자의 위치추적 가능

o RFID 응용에서의 개인정보보호를 위한 조치사항
- 개인정보보호 정책·절차 수립 및 RFID 태그에 개인정보 기록 금지
- RFID 태그에 기록된 개인정보의 수집 및 기록된 물품정보와 개인정보 연계 시, 적절한 인증절차 제공 및 사용자에게 고지
- RFID 태그 및 리더기 설치 위치에 대한 사전 고지
- RFID 기능 제거방법에 대한 사용자 고지 및 그 외 개인정보보호를 위한 관리적·기술적 조취

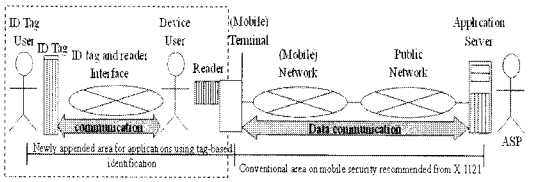
권고(안)은 2008년 4월 ITU-T SG17 회의에서 대부분의 내용이 확정되었으며, 2009년 최종(안)이 개발·확정될 것으로 예상된다.

3.2 RFID 응용에서의 개인정보에 대한 위협 및 개인식별정보 보호를 위한 요구사항 표준화 동향

2006년 12월 ITU-T SG17 제네바 회의에서 한국이 표준 제안한 "RFID 응용에서의 개인정보에 대한 위협 및 개인식별정보 보호를 위한 요구사항"은 RFID를 이용한 B2C(Business-to-Customer) 응용 서비스에서 발생 가능한 개인정보 침해위협과 개인정보를 보호하기 위한 요구사항을 제시하고 있다. 본 권고(안)은 사용자가

1) ITU-T는 'Privacy'라는 용어 대신 'Protection for Personally Identifiable Information(개인식별정보보호)'라는 용어 사용

RFID 리더가 탑재된 모바일 디바이스를 이용해 RFID 태그가 부착된 물품의 정보를 확인할 수 있는 국내 모바일 RFID 기술 및 표준을 기반으로 하고 있다.



〔그림 4〕 RFID를 이용한 B2C 응용에 대한 레퍼런스 모델

권고(안)은 일반적인 RFID 응용서비스가 아니라 RFID를 이용한 B2C 응용서비스, 즉 모바일 디바이스에 RFID 리더기를 부착한 사용자가 직접 비즈니스에 참여하는 응용서비스에서 발생 가능한 개인정보 침해위협과 개인정보 보호를 위한 기술적 요구사항을 제시하고 있다.

권고(안) 주요내용

o RFID를 이용한 B2C 응용에서의 개인정보 침해위협
- RFID 태그정보 유출로 인해 RFID 부착 물품의 구입 시기, 장소, 위치추적 등이 가능함에 따른 개인정보 침해위협
- 지속적인 RFID 태그정보 유출로 해당 사용자의 성향, 관심사항 등에 대한 프로파일링 가능

o RFID를 이용한 B2C 응용에서의 개인정보보호를 위한 기술적 요구사항
- RFID 태그 소유자는 자신의 개인정보에 대한 관리·수정 등 제어기능 제공
- 응용서버에서 RFID 태그 및 리더기 소유자에 대한 인증 기능 제공
- 응용서버에 저장된 사용자 개인정보에 접근 시 적절한 접근제어 제공
- RFID 태그에 관련된 정보에 대한 기밀성 보장
- RFID 리더 소유자와 관련된 로그 데이터 수집에 대한 동의 절차 제공

또한, 부록에 국내 표준으로 채택된 개인정보보호 정책 프로파일 기반의 개인정보보호 서비스 구조를 제시하고 있다.

권고(안)은 2008년 4월 ITU-T SG17 회의에서 최종(안)이 개발·확정되어 현재 최종안에 대해 ITU-T 회원국을 대상으로 한 투표가 진행되고 있어 연내 표준 채택될 것으로 확실시 된다.

Ⅳ. 결 론

RFID 기술을 이용한 응용 서비스는 단순 물류·유통 분야에서부터 최근 환자 병력관리, 전자여권, 모바일 RFID 서비스까지 활용 분야와 적용대상이 확대됨에 따라 프라이버시 침해에 대한 다양한 기술적 대책이 개발되고 있다. 그러나 프라이버시 문제는 국가 및 지역적 특징에 따라 기술적 조치만으로는 해결이 어려운 경우가 많아 정책적·관리적 조치와 함께 추진되어야 실효성을 획득할 수 있다. 이러한 관점에서 현재 ITU-T에서 표준화 추진 중인 기술적·정책적 요구사항에 대한 권고(안)이 가지는 의미는 특정 기술에 대한 표준화 못지않게 중요하며, 향후에도 지속적으로 정책과 기술을 병행할 수 있는 다양한 프라이버시보호 기술이 개발 및 표준화될 수 있기를 기대한다.

참고문헌

[1] Simson Garfinkel and Beth Rosenberg, RFID Applications, Security, and Privacy, 2005.

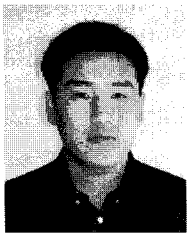
[2] TD 4034Rev.2, Revised working document of X.rfpg: Guidelilne on protection for personally identifiable information in RFID application, 2008.

[3] Draft ITU-T Recommendation X.1171 (X.nidsec -1), Threats and Requirements for Protection of Personally Identifiable Information in Applications using Tag-based Identification, 2008

〈著者紹介〉

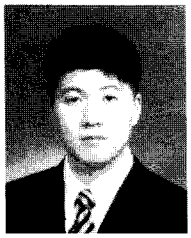
이 향 진 (Hyangjin Lee)

2000년 2월 : 성균관대학교 전기전자컴퓨터공학부 공학사
2002년 2월 : 성균관대학교 전기전자컴퓨터공학과 공학석사
2002년 3월~현재 : 한국정보보호진흥원 선임연구원
<관심분야> 정보보호, 프라이버시 보호, ID관리



신 동 휘 (Donghwi Shin)

2002년 2월 : 성균관대학교 전기전자컴퓨터공학부 공학사
2008년 2월 : 성균관대학교 전기전자컴퓨터공학과 공학석사
2007년 12월~현재 : 한국정보보호진흥원 연구원
<관심분야> 네트워크 보안, 침투테스트, 정보보호 응용



전 길 수 (Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호응용팀장
<관심분야> 암호학, PET, ID관리