모바일 RFID 네트워크 환경에서의 정보보호 모델 제안과 분석

박남제*,최두호*,김호원*,김장섭**,원동호**

*한국전자통신연구원 정보보호연구단 RFID/USN 보안연구팀

**성균관대학교 정보통신공학부

A Suggestion and Analysis of Security Model in Mobile RFID Network Environment

Namje Park*, Dooho Choi*, Howon Kim*, Jangsub Kim**, Dongho Won**

*Information Security Research Division, ETRI.

**School of Information and Communication Engineering, Sungkyunkwan University.

요 약

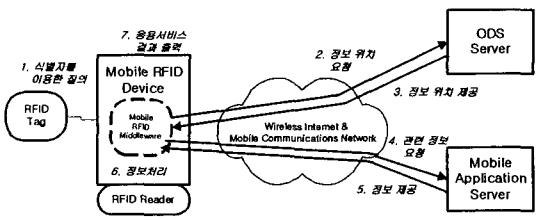
모바일 RFID는 휴대 단말에 RFID 리더를 장착하여 다양한 응용 서비스를 모바일 RFID 리더 사용자에게 제공하는 기술이다. 본 논문에서는 안전한 모바일 RFID 서비스 제공을 목표로, 도메인간 보안, 개인 프라이버시 보호, 인증, 단대단 보안, 위치 추적방지 등과 같은 다양한 보안 이슈들을 해결할 수 있는 모바일 RFID 정보보호 모델을 제안하고 분석한다.

I. 서론

본 논문에서는 최근 국내외에서 차세대 IT 환경인 유비쿼터스 환경을 실현하는 기술로 각광을 받고 있는 모바일 RFID 기술에 대한 보안 위협 및 프라이버시 이슈사항을 살펴보고 이를 막을 수 있는 보안 모델 및 보호 기술에 대해 살펴보기로 한다. 900MHz 대역 모바일 RFID 기술은 한국이 세계 최초로 개발하는 기술로서 우리나라가 경쟁력이 있는 이동통신 기술에 RFID를 결합하여 미래의 IT 시장을 선도할 기술이다. 본 고에서는 모바일 RFID 정보보호 모델을제안하고 분석하며, 함께 최근 한국전자통신연구원에서 개발한 모바일 RFID 보안 프레임워크 기술을 소개하도록 한다. 모바일 RFID 보안 환경에서의 정보보호는 법, 제도적인 차원에서의 적극적인 대응과 더불어, 기술적인 차원에서의 적극적인 대응을 통해서만, RFID 시장 활성화 및 관련 산업 육성을 도모할 수 있을 것으로 보인다.

II. 모바일 RFID 개요 및 보안 취약성

모바일 RFID 서비스란 모바일 단말기에 RFID 리더(칩)를 장착(내장)하여, 물품 또는 위치에 부착된 태그를 읽고, 무선 인터넷 상의 관련 정보를 검색하여 활용하는 서비스이다. (그림 1)은 모바일 RFID 서비스의 통신 인프라에 대한 연결 구조와 해당되는 시스템들의 종류와 일반적인 서비스 절차를 보여주고 있다.



(그림 1) 모바일 RFID 서비스 절차

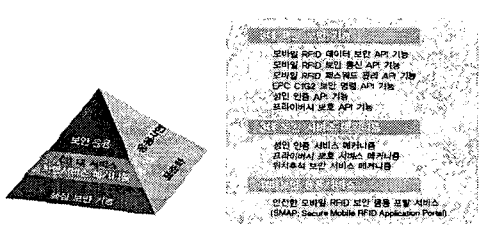
RFID 태그와 휴대폰 단말 사이에 RFID 무선접속 통신이 일어나고, 휴대폰과 BTS/ANTS 사이에 CDMA 이동통신이 일어나고, BTS/ANTS

와 모바일 RFID 응용 서버 사이에는 유선 통신으로 이루어진다.

RFID 환경에서 해를 기칠 수 있는 방법은 여러 가지가 가능하며, 이는 더 이상 이론적으로만 가능한 것이 아니라 현실적인 문제이다. RFID 태그 및 리더에 대한 Passive signal interception 공격, 권한이 없는 리더에 의한 RFID 태그 읽기, Falsifying tag or reader identity, RFID 태그에 대한 공격 툴 사용, RFID 태그에 대한 무력화 공격, 암호학적인 해킹 기법을 동원한 정교한 RFID 태그 공격 등의 RFID 보안 취약성이 있으며, 모바일 RFID 환경에서도 유사한 보안 취약성과 프라이버시 침해 가능성이 존재하므로, 이에 대한 적절한 보안기술이 필요로 하다. 그리고, 현실적으로 기존의 RFID 규격 및 모바일 RFID 표준을 준수하며, 태그에서 암호 알고리즘을 사용하지 않는 상황에서 사업자 및 사업자에게 보안 기능 및 프라이버시 보호/ 관리 기능을 제공하는 정보보호 서비스 모델이 필요하다. 다음 장에서 이와 같은 여러 사항들을 고려한 모바일 RFID 정보보호 모델을 제안하고 분석한다.

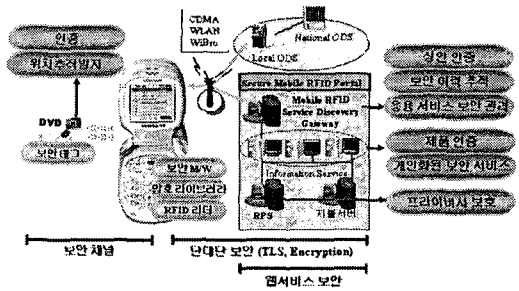
III. 모바일 RFID 정보보호 모델

안전한 모바일 RFID 서비스 제공을 위하여 MRF-Sec631로 명명된 모바일 RFID 보안 전략을 수립하여 모바일 RFID 정보보호 모델을 제시한다. 구체적으로 MRF-Sec631이란 모바일 RFID 단말 플랫폼에서 대표적인 6가지의 표준 보안 기능을 개발하고, 이를 기반으로 주요 3가지의 보안 서비스 메커니즘을 적용하여, 응용 포탈 서비스를 통해 안전한 모바일 RFID 서비스를 실현함을 의미한다.



(그림 2) 보안 기술 개발 631 전략

안전한 모바일 RFID 서비스가 제공되기 위해서는 도메인간 보안, 개인 프라이버시 보호, 인증, 단대단 보안, 위치 추적 방지 등과 같은 다양한 보안 이슈들을 해결할 수 있는 복합적인 보안 프레임워크를 필요로 한다. 앞 절에서 제시된 631 개발전략에 근거하여 서비스 프레임워크를 구성하면 다음과 같다.



(그림 3) 모바일 RFID 정보보호 서비스 모델

제안된 모바일 RFID 정보보호 모델의 주요 기능은 WIPI 기반의 모바일 보안 미들웨어 제공, 태그 인증 및 태그 불추적성 제공, 리더 인증, 메시지 보안 기능 제공, 프로파일 기반의 프라이버시 보호 제공 등이다.

IV. 모바일 RFID 보안 프레임워크 기술

다음은 최근 한국전자통신연구원 정보보호연구단에서 개발한 모바일 RFID 통합 보안 플랫폼기술을 소개한다. 본 기술은 기본적으로 모바일 RFID 환경에서 있을 수 있는 여러가지 보안 침해 문제를 해결하고 모바일 RFID 시장 활성화에 가장 큰 걸림돌인 프라이버시 침해 문제를 해결하기 위한 모바일 RFID 기반 보안기술이다. 휴대전화 같은 모바일 단말기에 900MHz 대역의 RFID 리더를 외장 형태로 장착, 안전한 RFID 서비스를 제공하는 보안 소프트웨어 기술과 기반 연동 기술로 구성되어있다.

4.1 EPC C1G2 리더 기술

EPC C1G2 모바일 RFID 리더는 이동형 900MHz RFID 리더이며, 스마트폰 혹은 PDA와 같은 이동기기의 주변장치로 사용 가능하다. 모바일 RFID 리더는 EPC C1G2 지원 및 무선

통신 기능 지원은 전자상거래, 개인 인증도구 등의 다양한 응용 서비스 출현을 가능하게 할 것이다. EPCglobal Class-1 Generation-2 (EPC C1G2) 및 ISO 18000-6 Type B/C, 모바일 RFID 포럼 표준 규격을 준수하며, 태그 잠그 및 32비트 패스워드 기반의 태그 킬링, 접근제어 기능을 지원한다.

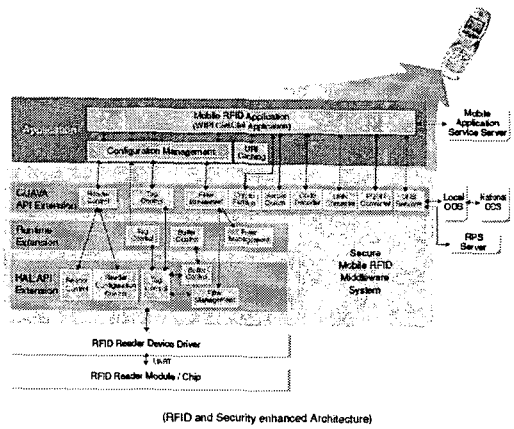
4.2 모바일 RFID 보안 라이브러리 기술

모바일 RFID 보안 라이브러리는 WIPI 환경 기반의 모바일 RFID 응용 보안 수행을 위한 WIPI/C-JAVA 언어로 작성된 모바일 RFID 단말 플랫폼 암호 처리용 API 기술로서, 이 기술은 서비스 업체 및 콘텐츠 업체, 정보보호 업체 등에서 단기간에 저렴한 비용으로 미들웨어 단말 플랫폼의 정보보호 서비스를 지원할 수 있도록 개발되었다. 주요 지원 기능은 경량형 무선 암호 연산 컴포넌트, 대칭키/공개키, 메시지 다이제스트 및 서명, 고성능 타원곡선 고속 연산 및 암호, 국산 KCDSA 전자서명, SEED 대칭암호, ARIA, AES 표준형 경량 알고리즘, 표준 보안통신 프로토콜 (SSL/TLS), ASN.1 및 PKCS #5/8, 이통 3사별 표준 인터페이스 컴포넌트 등이 있다.

4.3 WIPI 확장 보안 미들웨어 기술

WIPI 확장 보안 미들웨어는 사용자가 이통망에서 UHF 대역의 리더기가 장착된 단말기를 사용하여 안전하게 응용서비스를 이용하도록 지원하는 모바일 RFID 미들웨어 기술로서, RFID 리더제어 및 Tag 정보 연산과 필터링 기능, ODS 질의 처리 기능 등을 지원하며, 모바일 RFID 보안 라이브러리를 이식 및 확장하여 리더로부터 응용 서버까지 모든 데이터 이동 경로에 대한 보안을 보장한다.

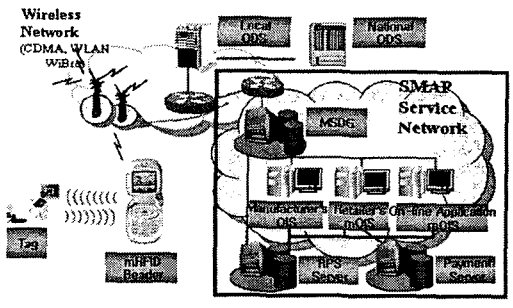
이 보안 미들웨어는 모바일 RFID 리더를 위한 WIPI-C/JAVA API 및 HAL API 표준 규격 지원, WIPI 기반의 모바일 RFID 네트워크 APIs, 접근권한 관리 API 및 보안 등급 규격, 리더 제어 프로토콜 규격 등 모바일 RFID 포럼의 표준 규격을 지원한다. 또한 패스워드(보안키) 관리, 성인인증, 프라이버시 보호, Gen2 보안 명령(Kill/Lock/Unlock) 등과 같은 모바일 RFID 보안 API 기능을 제공한다.



(그림 4) 모바일 RFID 보안미들웨어 구조

4.4 보안 응용 포탈 게이트웨이 기술

보안 응용 포탈 게이트웨이 서비스 기술은 다양한 모바일 RFID 응용 서비스 구축을 위한 참조 모델이다. 다양한 모바일 RFID 응용을 제공하기 위한 정보 포탈 서비스 보안 기술로서 응용 포탈 게이트웨이, 정보서비스 서버, 단말 보안 응용, 지불서버, 프라이버시 보호 서버 등으로 구성되어 어느 누구나 쉽게 모바일 RFID 보안 응용 서비스를 구축할 수 있는 통합 환경을 제공한다. SMAP을 사용하면, 모바일 RFID 서비스 제공자는 보안 안전성과 프라이버시 보호를 보장하는 다양한 응용 서비스 손쉽게 구축할 수 있게 된다. 개방형 모바일 RFID 보안 응용 서비스 플랫폼 기술은 다음과 같이 서비스 구축한다.

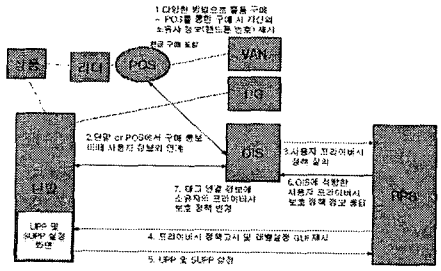


(그림 5) 보안 응용 포탈 서비스 플랫폼

4.5 정책 기반 프라이버시 보호 기술

정책 기반 모바일 RFID 프라이버시 보호 기술은 모바일 RFID 환경에서 개인화된 태그에 연결된 정보에 대한 개인 프라이버시를 보호하는 서비스 기술이다. 모바일 RFID 사용자가 태그가 부착된 상품을 소유하는 순간부터 태그에 연결된 각종 정보를 소유자 개인이 보안 서비스를 통해 직접 통제할 수 있다.

본 서비스 기술은 프로파일을 기반으로 하여, RFID 태그 부착 상품을 구매한 사용자들이 자신이 구매한 상품 및 이와 연관된 정보에 대해 누구에게 어느 정도의 정보를 제공할지 여부를 설정하고, 이에 따라 접근 제어를 수행하는 메커니즘을 제공한다. 이러한 메커니즘의 가장 큰 장점은 사용자 정보에 따른 무조건적인 정보에 대한 접근을 막는 것이 아니라, 필요한 경우에 권한을 부여받은 사람에게 적절한 정보를 제공할 수 있도록 함으로써 모바일 RFID 응용서비스를 활성화할 수 있다는 점이다. 또한 사용자에게 사용자 정의 프로파일 집행에 따른 의무사항 준수에 대한 여부를 무선 인터넷 메시지를 사용하여 통보하며, 프라이버시가 강화된 감사 기능을 통하여 시스템 로그 분석에 따른 프라이버시 침해 문제를 최소화하면서, 사후 문제 발생 시 이에 대한 귀책 여부를 판단할 수 있는 기능을 제공한다. 이를 위한 서비스의 기본적인 주요 기능으로는 소유자의 프라이버시 보호 정책 설정 및 관리 기능, 소유자의 프라이버시 정책에 따른 개인화된 태그에 연결된 정보 접근 제어 기능, 소유자가 설정한 의무사항 집행 결과 통지 기능, 감사 로그 관리를 통한 프라이버시 감사 기능 등이 있다.



(그림 6) 프라이버시 보호 적용 메커니즘

위의 그림은 서비스 적용 메커니즘을 나타내고 있으며, 사용자의 UPP(User Privacy Policy) 정보 없으면 사용자에게 프라이버시 보호 정책 고시 및 레벨설정 요청 (단계 4,5). 사용자의 UPP(User Privacy Policy) 정보 있으면 사용자의 UPP를 OIS 맞게 가공하여 전달하는 순서로 동작된다.

V. 결론

본 논문에서는 최근 각광을 받고 있는 모바일 RFID 기술의 활성화를 위해 있을 수 있는 보안 취약성을 살펴보고, 이를 위한 정보보호 서비스 모델의 제안과 그 기술에 대해 살펴보았다. 특히 본 고에서는 세계 최초로 개발된 UHF 900MHz 모바일 RFID 서비스 환경에 대한 보안 기술과 프라이버시 보호 기술도 소개했다.

모바일 RFID 기술은 현재 국내외적으로 관련 제반 기술 개발이 활발히 진행되고 있으며 관련 서비스 기술 개발에도 많은 노력을 기울이고 있다. 서비스 활성화를 위한 법/제도 차원에서 보안기술 및 프라이버시 보호를 위한 노력을 해야 하지만, 이와 더불어, 기술적인 차원에서의 기술을 개발해야 한다. 보안 기술과 프라이버시 보호 기술에 있어서 완벽한 기술이란 존재하지 않지만, 본 고에서 제안한 기술들이 안전하고 신뢰할 수 있는 네트워크 RFID 환경 개발에 도움이 되어 국내외의 모바일 RFID 시장 활성화에 도움이 될 수 있을 것으로 보인다.

[참고문헌]

[1] MRF Forum: WIPI C API Standard for Mobile RFID Reader (2005)

[2] MRF Forum: WIPI Network APIs for Mobile RFID Services (2005)

[3] Wung Park, Byoungnam Lee: Proposal for participating in the Correspondence Group on RFID in ITU-T. Information Paper. ASTAP Forum (2004)