RFID/USN 미들웨어에서의 응용S/W 보안*

양석환○ 이기열 정목동

부경대학교

tigergal○@chol.com, zestgame@hanmail.net, mdchung@pknu.ac.kr

Computer Security for Application in the RFID/USN Middleware

Seokhwan Yang○, Kiyeal Lee and Mokdong Chung

Pukyung National University

요 약

최근 다양한 분야에서 안전한 RFID 애플리케이션 개발에 대한 필요성이 증가함에도 불구하고 초기의 많은 개발 비용과 전문적 보안 지식의 부재로 인해 중소 규모의 기업체에서는 안전한 애플리케이션 개발이 어려운 상황이다. 본 논문에서는 쉽고 효율적으로 RFID 미들웨어에 보안기능을 구현할 수 있는 Security Manager를 제안한다. Security Manager는 다양한 암/복호화 알고리즘을 제공하며 새로운 알고리즘을 구현할 경우 쉽게 Security Manager에 추가 및 확장이 가능하다. 또한 Security Manager는 Diffie-Hellman 키 일치 알고리즘, PKI 환경 구축 및 인증기능을 제공한다. Security Manager는 API형태로 제공되므로 적은 비용으로 쉽고, 효율적으로 RFID 미들웨어에 보안기능을 제공할 수 있으며 개발자가 보안 전문지식이 부족하더라도 API를 이용하여 쉽게 보안 애플리케이션 작성이 가능하다.

1. 서 론

RFID를 통해 업무의 효율성이 향상되고, 비즈니스의 효율성을 개선할 수 있어 국내외 여러 기업에서 많은 관심을 가지고 연구가 진행 중이지만, 비즈니스 프로세스, 표준 아키텍처, 통합 관련, 보안문제 등 여전히 많은 문제점을 가지고 있다. 특히 RFID 리더와 애플리케이션 사이의 중개역할을 하는 미들웨어는 민감한 데이터를 전달하는 경우가 많아 인증과 기밀성의 보장이 요구된다. 그러나 기술 전반에 걸쳐서 산발적인 연구개발이 이루어지고 있으나, 연구개발 투자의 규모가 미국과 일본의 10%도 안 되는 상황이어서 전반적인 기술연구가 어려운 상황이다.[8]

기존의 RFID 미들웨어 솔루션은 RFID 리더와의 통신 및 리더의 관리, 데이터 가공 등 기본적인 미들웨어의 기능지원에 제한되어 있으며, 미들웨어가 제공하는 태그 정보 보호 및 리더나 미들웨어 서비스 제어 권한 등을 보호하는 기술을 대부분 고려하고 있지 않다. 태그 정보, 리더 및 미들웨어 제어 권한 등은 비정상적으로 획득, 조작 및 악용될 경우, 전반적인 RFID 응용 서비스 체계에 큰 혼란을 초래할 수 있으므로 이와 같은 자원들을 안전하게 보호할 수 있는 기술이 필요하다. 그러나 많은 기업들은 보안에 대한 전문적인 지식 부족으로 인하여 안전한 미들웨어를 개발하는 데에 많은 어려움을 겪고 있다.

따라서 본 논문에서는 안전한 미들웨어와 RFID 애플리케이션 간의 데이터 전송에 대한 보안기능을 제공하는 Security Manager에 대한 연구를 제시하고자 한다.

Security Manager는 내부에 컨테이너 개념을 가지고 있는 프레임워크의 개발을 위해 Light 컨테이너 아키텍처의 개념을 활용하고 있다.

Security Manager는 BouncyCastle[9]을 이용하여 구현된 데이터 암/복호화 API를 제공함으로써 개발자는 보안에 대하여 자세히 알지 못하더라도 몇 개의 클래스만을 이용하여 데이터 암/복호화를 할 수 있다.

또한 Security Manager는 PKI 환경 구축[10]에 대한 API를 지원함으로써 손쉽게 PKI 환경을 구현할 수 있다는 장점을 가진다. 특히 PKI 환경의 효율성을 생각하여 OCSP[11]등과 같은 기능을 제공하며 이러한 아키텍처는 많은 데이터 처리를 안정적으로 수행할 수 있도록 도와준다. Security Manager는 암/복호화 및 PKI환경 등 다양한 보안기능을 구현한 API형태로 제공되므로 적은 비용으로 쉽고, 효율적으로 RFID 미들웨어에 보안기능을 제공할 수 있다. 이로 인해 제조업 및 유통업에서 많은 활용 가치가 있을 것이며, 특히 물류 자동화 부분에 많은 역할을 할 것으로 기대된다.

본 논문의 구성은 다음과 같다. 2절에서는 관련 연구를 다루고, 3절에서는 Security Manager를 소개한다. 4절에서는 시스템 구현결과 및 평가를 다루고 마지막으로 5절에서는 결론 및 향후 연구 방향을 논한다.

2. 관련 연구

2.1 RFID 애플리케이션 보안 요구사항

* 이 논문은 (주)코리아컴퓨터의 산학 공동연구 개발과제 지원에 의하여 연구되었음.

RFID는 무선 전파(Radio Frequency)를 이용하여 사람이 개입하지 않고 자동으로 사물을 식별하는 기술을 말한다[1]. 사물에 대한 태그 정보와 태그 관련 상세 정보를 가지고 있는 EPCglobal network 구성요소에 대해 보안 기술을 적용해야 한다[2,4]. 또한 RFID 애플리케이션이 사용하는 네트워크상에서의 보안 역시 생각해야 한다. 이러한 보안 기술을 적용하지 않으면 공격자는 송수신 중인 데이터를 변형 할 수 있을 뿐만 아니라, EPCIS에 저장되어 있는 태그 관련 상세 데이터를 변경할 수 있다. 따라서 애플리케이션과 EPCIS등과 같은 외부시스템사이의 통신에서 주고받는 데이터에 대한 기밀성 및 무결성을 보장해야 할 것이다. 또한 위장과 같은 적극적인 공격에 대한 대처 방안으로 인증 서비스를 제공해야 하며, 애플리케이션 권한 및 EPCIS의 데이터의 무분별한 이용을 방지하기 위해서는 접근제어가 이루어 져야한다. RFID 애플리케이션에 적용되어야 하는 기술들은 표 1과 같다.

표 1. RFID 애플리케이션 보안 요구사항

보안 기술	RFID 환경 요소
Cryptography	ALE, EPCIS
WS-Security	RFID Application, ALE, EPCIS
Authentication	RFID Application, EPCIS
Authorization	RFID Application

2.2 모바일 RFID 기반 통합보안 기술

모바일 RFID 기술은 정보통신부에서 2005년 WiBro 및 DMB 기술에 이어, 2006년 핵심 개발기술로 선정한 제반 기술로 모바일 RFID 포럼에 의하면 모바일 RFID 기술은 약 3,000여 가지의 응용이 가능한 것으로 알려지고 있다.[7] 모바일 RFID 통합보안 프레임워크 기술은 센서와 결합하면 물리적인 침입감지 시스템에도 응용해 활용할 수 있다. ETRI 정보보호연구단 RFID/USN 보안연구팀에서 개발한 모바일 RFID 통합보안 프레임워크 기술은 기본적으로 모바일 RFID 환경에서 있을 수 있는 여러 가지 보안침해 문제를 해결하고 RFID의 시장 활성화에 가장 큰 걸림돌인 프라이버시 침해 문제를 해결하기 위한 모바일 RFID 기반 보안기술이다. 모바일 RFID 통합보안 프레임워크 기술의 주요 요소로는 모바일 RFID 암호 라이브러리, WIPI(Wireless Internet Platform for Interoperability, 한국형 표준 무선인터넷 플랫폼) 확장 보안 미들웨어, 보안 응용서비스 게이트웨이, 정책기반 RFID 개인 프라이버시 보호 시스템 기술이 있다.

2.3 EPCglobal Network

EAN인터내셔널과 UCC 합작으로 설립된 EPCglobal은 RFID의 핵심인 EPC와 이를 기반으로 한 네트워크를 국제적, 범 산업적으로 보급한다. 모든 기업들이 표준화된 통합 공급체인을 구축해 언제 어디서나 물류상태를 파악할 수 있도록 하는 것을 주요 범위로 하며 EPCglobal은 RFID분야의 국제 표준제정과 보급에 앞장서고 표준의 구현에 필요한 모든 정보를 지원한다. EPCglobal에서는 RFID 애플리케이션 개발에 필요한 다양한 환경을 EPCglobal Network를 통해서 제시하고 있다[4].

EPCglobal Network에서 제시하는 Application Level Event(ALE)는 RFID 리더에서 읽히는 수많은 태그 데이터들을 이벤트 정보로 변환하여 상위 단에 넘겨주는 역할을 한다. 이러한 이벤트 정보는 EPC Capturing Application에 전달되어 EPCIS에 정보를 질의하는데 사용된다. EPCIS는 EPCglobal Network의 DB역할을 하는데, ALE로부터 올라오는 이벤트에 대한 태그의 실제 정보를 저장하고 있다[5].

3. Security Manager

3.1 Security Manager의 구성

Security Manager는 분산 미들웨어 환경을 위한 PKI 기반의 통합 인증 환경, 다양한 데이터 암/복호화, Diffie-Hellman을 통한 키 교환 및 안전한 데이터 통신을 지원하기 위한 보안 프레임워크를 구성하여 제공하며 JCA/JCE를 이용하였다.[3] 그림 1 은 Security Manager가 지원하는 암호화 기능의 규격을 나타낸다.

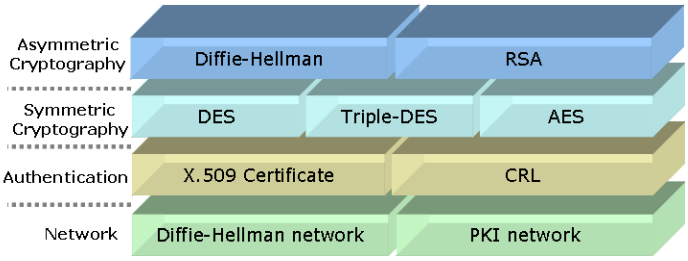

그림 1. Security Manager 1.0 규격

프레임워크는 크게 데이터 암/복호화, Diffie-Hellman 키 일치를 위한 서버와 클라이언트, 사용자 인증을 위한 PKI 환경 구축, PKI 인증서 생성 및 검증, 폐기를 위한 서버와 클라이언트로 구성된다. 또한 API를 이용하는 개발자에게 API의 내부 처리환경을 알지 못해도 쉽게 이용할 수 있도록 하기 위하여 Factory 및 Singletone 패턴을 이용하였고, 클라이언트의 요구사항을 서버가 원활하게 처리하기 위하여 명령어 수준의 클래스를 지원한

다.

그림 2는 Security Manager의 아키텍처를 나타낸다.

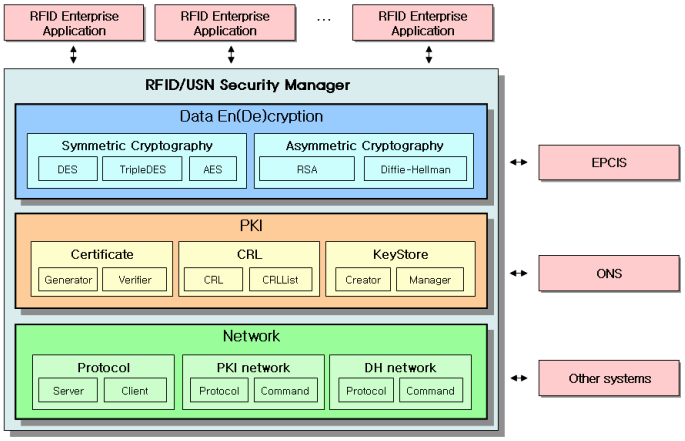

그림 2. Security Manager 아키텍처

그림 3은 Security Manager의 보안기능이 처리되는 과정을 보여주고 있다.

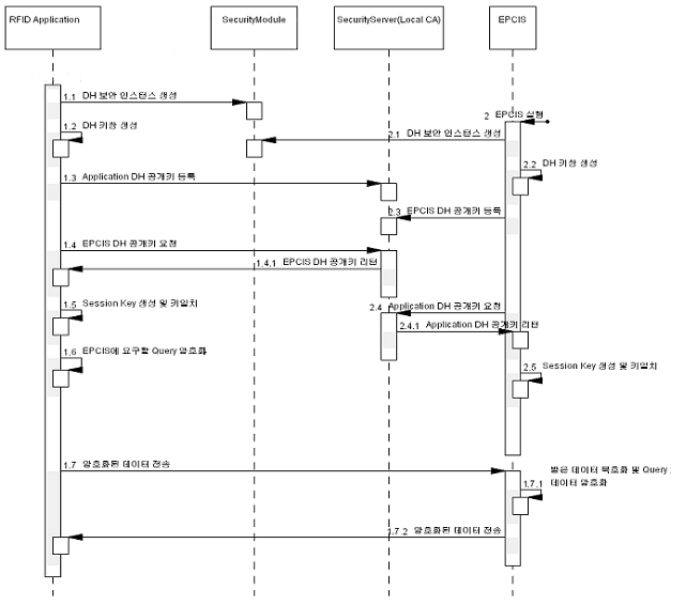

그림 3. 보안 처리 과정

① 사용자는 EPCIS와 안전한 통신을 하기 위해서 Diffie-Hellman 키 쌍을 생성한다.

② 사용자는 생성한 공개키를 Security Server에 등록하고 통신하려는 EPCIS의 공개키를 받는다. Security Server는 지역 CA로 사용한다.

③ 사용자는 자신의 비밀키와 EPCIS의 공개키를 이용하여 세션키를 생성하고 이를 이용하여 암호화를 위한 비밀키를 생성한다.

④ 사용자는 EPCIS에 질의할 Query를 ③에서 세션키를 통해서 생성한 비밀키를 이용하여 암호화하고 EPCIS에 전송한다.

⑤ EPCIS는 전송된 데이터를 복호화하고 Query에 대한 응답을 다시 암호화하여 사용자에게 전송한다.

⑥ 사용자는 받은 데이터를 복호화 하여 활용한다.

3.2 데이터 암/복호화

Security Manager는 데이터 암/복호화에서의 데이터의 기밀성, 무결성 제공을 위해 키 일치 방법을 사용하고 있다. 대칭키 방법은 데이터를 암호화 하는 시간은 짧은 반면 데이터를 주고받는 상호간의 비밀 키에 대한 비밀 유지가 어렵다. 그리고 비대칭키 방법은 암호화하는데 많은 시간이 걸려 효율적이지 못한 문제점을 지니고 있다[3,6]. 키 일치 방식은 이러한 단점들을 피하고 대칭키, 비대칭키 방식의 장점만을 이용하여 안전하고 빠른 데이터 송수신이 가능하게 한다[3,6]. 키 일치에는 Diffie-Hellman 알고리즘을 사용한다. 또한 Security Manager는 개발자가 다른 암호화 방법을 사용하고자 할 때를 대비하여, TripleDES, AES, RSA와 같은 여러 암호화 방법을 사용할 수 있는 API를 지원한다. 지원하는 API를 이용하여 새롭게 구현한 알고리즘을 Security Manager에 추가 및 사용할 수 있다. 그림 4는 데이터 암/복호화에 대한 아키텍처를 나타내고 있다. 암호화의 방법이 대칭키, 비대칭키로 구분되기 때문에 클래스가 크게 두 부분으로 나뉘어져 있다. 데이터 암/복호화 클래스들은 Factory 패턴을 적용하여 구현하였으며 이러한 패턴의 적용으로 인해 개발자는 암호화 관련 클래스가 어떤 식으로 구성되는지 알지 못하더라도 쉽게 애플리케이션을 구현할 수 있으며 유지보수가 쉬운 장점을 가진다.

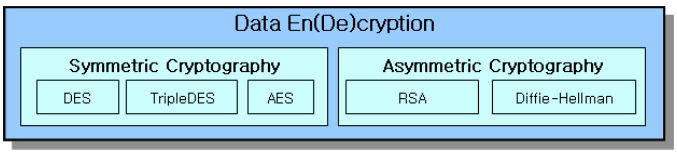

그림 4. 데이터 암/복호화 아키텍처

3.3 Diffie-Hellman 키 일치 서버-클라이언트 모델

Security Manager는 실무에서 가장 많이 사용되고 있는 Diffie-Hellman 방식을 구현한 서버-클라이언트 모델을 제공함으로써 개발자는 보다 쉽게 Diffie-Hellman 기능을 이용할 수 있다. 효율적인 키 일치를 수행하기 위해 상호간의 공개키를 공유할 수 있는 서버와 클라이언트를 쉽게 개발할 수 있도록 도와주는 API를 제공한다. 서버와 클라이언트 사이에 송수신되는 명령어는

Command 패턴을 적용하였고, 서버와 클라이언트 사이에 명령어를 전송하는 통신환경에 대한 Diffie-Hellman 관련 통신 프로토콜을 정의함으로써 효율적인 통신이 가능하도록 구현되었다. 그림 5는 Diffie-Hellman, PKI와 관련된 모든 프로토콜에 대한 Network 아키텍처를 나타낸다.

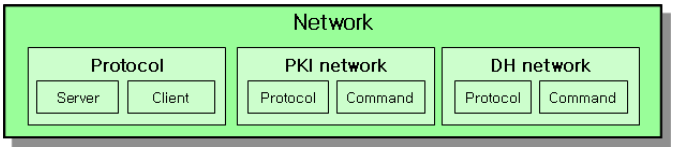

그림 5. Network 아키텍처

3.4 PKI

Security Manager는 분산 미들웨어 환경을 위해 PKI 기반 통합 인증환경을 제공한다. 사용자는 Security Manager에서 제공하는 PKI 인증서 기능을 이용하여 사용자 인증을 하게 되고 애플리케이션은 사용자의 인증서가 Security Manager에서 발급한 인증서인지 아닌지를 확인하여 만약 인증서가 검증된 인증서라면 사용자를 인증하게 된다. Security Manager는 효율적인 인증 처리 기반을 제공하기 위하여 PKI를 제공한다. 개발자는 PKI의 이론 및 구현에 대해 자세히 알지 못하더라도 Security Manager에서 제공하는 PKI 관련 API를 이용함으로써 쉽게 PKI 환경을 구축할 수 있다. Security Manager는 X509. CertificateFactory를 이용하여 X509 버전1, 3에 대한 인증서를 생성할 수 있다. 또한 CertificateVerifier와 CRL을 통해서 인증서의 검증 서비스를 제공한다. 그림 6은 PKI 처리에 대한 아키텍처를 나타낸다. PKI 역시 인터넷 상에서 인증서 생성, 검증, 폐기에 대한 기능을 제공하기 위하여 서버-클라이언트 모델로 구현하였고 효율적인 통신을 위해서 Diffie-Hellman 통신 환경과 같이 서버와 클라이언트를 쉽게 개발할 수 있도록 도와주는 API를 제공한다. Diffie-Hellman 통신환경과 마찬가지로 서버와 클라이언트 사이에 송수신 되는 명령어는 Command 패턴을 적용하여 효율적인 명령어 송수신을 가능하게 하였다.

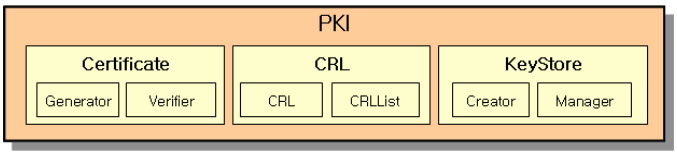

그림 6. PKI 아키텍처

4. 시스템 구현결과 및 평가

그림 7은 Security Manager를 이용해서 개발한 Demo Application의 한 부분이다. Demo Application을 통해서 키 생성, 키 등록, 세션 키 생성 및 암/복호화의 기능을 확인할 수 있다. API 형태로 제공되는 Security Manager의 특징으로 인해 기본적인 서버-클라이언트의 인터페이스를 제외하면 API를 호출하는 것만으로 원하는 기능의 구현이 가능하다. 또한 다양한 암/복호화 기능을 추가할 수 있는 API 설계에 의해 기본적으로 제공되는 알고리즘 외의 암/복호화 알고리즘의 추가도 간단하게 적용 가능하다. Security Manager를 구현함으로써 다양한 암/복호화 기능을 활용하여 기존 시스템의 데이터에 대한 기밀성과 무결성을 향상시킬 수 있으며, PKI 환경구축을 활용한 인증기능의 지원이 가능하다.

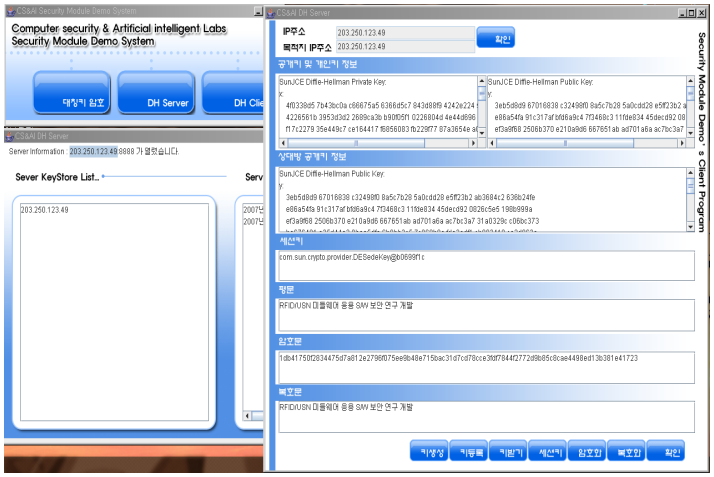

그림 7. Security Manager를 이용한 Demo Application

5. 결론 및 향후 연구

RFID/USN 기술은 다양한 분야에서 사용될 기술임에도 불구하고 초기 개발에 드는 고비용과 부족한 전문적인 지식으로 인해 중소 규모의 기업체에서 선뜻 개발을 시작하기 어렵기 때문에 API 형태로 제공되는 Security Manager를 설계, 구현하였다.

Security Manager는 다양한 암/복호화 알고리즘을 제공하며 새로운 알고리즘을 구현할 경우 쉽게 Security Manager에 추가 및 확장이 가능하다. 또한 Security Manager는 Diffie-Hellman 키 일치 알고리즘, PKI 환경구축 및 인증기능을 제공하며 구현된 기능들을 API 형태로 제공한다. Security Manager는 다양한 보안기능을 구현, 통합하여 API형태로 제공되므로 쉽게 미들웨어 또는 응용 S/W에 적용이 가능하고 이로 인해 중소규모의 기업체는 보안기능 제공에 대한 연구 및 비용 부담으로

부터 벗어날 수 있으며 보다 안전한 제품의 개발이 가능할 것이다.

그러나 RFID/USN 환경에서의 보안문제는 미들웨어와 애플리케이션 간의 보안뿐만이 아니라 RFID 태그와 리더 간의 보안, 센서와 센서, 센서와 미들웨어 간의 보안 또한 중요한 문제로 남아있으며 하드웨어를 비롯한 RFID/USN 환경의 특성상 보편적인 소프트웨어로는 적절한 적용이 어려운 것이 사실이다. 따라서 이러한 문제점을 해결하기 위해서는 RFID 리더 및 태그와 같이 제한된 하드웨어 환경에서도 적용 가능한 초경량 암호기술에 대한 연구가 필요하며 다양한 상황에서의 적절한 대응을 위하여 상황인식에 의한 동적 보안기술이 연구되어야 한다. RFID는 이용자에게 어디서나 유용한 정보를 제공할 수 있는 모바일 RFID 서비스로 발전해 가고 있으며 이에 따라 모바일 RFID 리더기의 이동성으로 인한 개인정보보호 침해와 이동통신 및 무선 인터넷 환경으로 인한 정보노출의 위협이 예상되므로 모바일 환경에서의 보안기술의 연구가 필요하다.

[참고문헌]

[1] Auto-ID Center, EPC Information Service, Whitepaper, 2004

[2] Auto-ID Labs, http://www.autoidlabs.org.

[3] David Hook, Beginning Cryptography with Java, Wiley, 2005

[4] EPCglobal, EPCglobal Architecture Framework, EPCglobal Final Version of 1 July 2005.

[5] EPCglobal, http://www.epcglobalinc.org.

[6] Jess Garms, Daniel Somerfield, Professional Java Security, Wiley, 2002

[7] 정보통신부, http://mic.news.go.kr

[8] 과학기술부, 한국과학기술기획평가원, 2005년도 기술수준평가 기술동향 조사서

[9] Bouncy Castle, http://www.bouncycastle.org

[10] Carlisle Adams, Steve Lloyd, Understanding PKI, Addison-Wesley, 2006

[11] RFC2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, http://www.ietf.org/rfc/rfc2560.txt