정형검증을 통한 RFID 보안프로토콜 분석 및 구현[1)]

김현석[o1] 김주배[1] 한근희[2] 최진영[1]
[1]고려대학교 컴퓨터학과
{hskim[o], jbkim, choi}@formal.korea.ac.kr

[2]행정자치부 전자정부 보안팀
keunhee@mogaha.go.kr

Analysis and Implementation of RFID Security Protocol using Formal Verification

Hyun-Seok Kim[o1] Ju-Bae Kim[1] Keun-Hee Han[2] Jin-Young Choi[1]
[1]Dept. of Computer Science and Engineering, Korea University
[2]e-Government Security Team, Ministry of Government Administration and Home Affairs

RFID(Radio Frequency Identification : 무선주파수식별) 기술은 유비쿼터스 구조 기술의 중요한 한 부분을 이루고 있다. 태그를 이용한 모든 제품들이 이러한 서비스의 대상이 되고 있지만 불행이도 다방면에 이용되는 이면에는 사용자의 사생활과 사용자 및 판매자 간의 인증문제를 이용한 서비스 공격 대상이 되고 있다. 현재 이러한 RFID 시스템의 보안 메커니즘들은 매우 중요하며 본 논문에서는 여러가지 메커니즘들 중 보안 프로토콜을 이용한 사생활과 인증문제 해결을 위해 정형검증을 통해 분석하고 새로운 프로토콜을 제안 및 구현가능성을 언급하고자 한다.

1. 서 론

RFID[1]를 위한 컴퓨팅 환경은 일반적인 인터넷 환경과는 달리 많은 제약사항을 갖는다. 이러한 제약사항은 Cellular Phone등을 이용한 무선 인터넷보다 더욱 자원 측면적 한계를 갖는다. 즉 유비쿼터스를 위한 RFID환경을 구축하기 위해서는 모든 상품이나 사람 등 객체에 설치되는 Tag가격은 5센트 이하로 구현되어져야 하며 대신에 Reader 장비나 Back End 시스템에서 많은 성능, 자원 측면에서 열악한 Tag장비의 자원적 한계를 극복할 수 있도록 설계 운영되어져야 한다. 이에 보안 기술 적용에 대한 부분도 이러한 운영, 환경 측면을 충분히 고려해야 한다. 본 논문에서는 물리적 레벨의 보호 기법이 아닌 암호 기술을 중심으로 한 RFID에서의 보안 프로토콜을 분석한다.

보안프로토콜을 구현하기 전에 설계단계에서부터 사용자와 개발자에게 안전성과 신뢰성을 제공하기 위한 기술이 요구되고 있다. 그러한 요구를 만족시키기 위해 진행되는 노력 중 대표적으로 정형 기법이라는 연구가 있으며 이는 정형 명세와 정형 검증의 두 가지 방법으로 구분된다.

본 논문에서는 정형검증 도구 중 FDR[2]이라는 모델체킹 도구를 이용, RFID 보안프로토콜인 해쉬기반 프로토콜들[3]의 취약성을 분석하여 보안 프로토콜의 안전성을 향상시키고자 한다.

2. RFID 시스템의 보안 요구사항

RFID 시스템의 RF태그와 리더 등 구성환경에 대해 다음과 같은 사항을 고려해 보안 요구사항을 설정할 수 있다. 특히 여러 가지 보안 요구사항 중 물리적인 방안을 통해 Tag 비용을 높이기 보다, 보안프로토콜과 같이 암호기술적 해결방안을 적용하기 위한 요구사항들로 아래와 같이 4가지를 제시하였다.

A. 인증이 되지 않은 리더에게 정보유출이 되지 않아야 하며, 태그와 그 소유자 사이에 긴 시간 동안의 추적(long-term tracking)이 불가능해야 한다.
B. 태그의 내용은 근제한기법 (access control)에 의해 질의채널 (interrogation channel)이 안전하지 않다고 예상되면 암호화되어야 한다.
C. 태그와 리더 사이에는 상호인증(mutual authentication)이 제공되어야 한다.
D. 태그와 리더 모두 재생공격(replay attack) 및 공격자 중간공격(man-in-the-middle attack)에 저항력이 있어야 한다.

3. Casper/FDR을 이용한 해쉬-언락킹 프로토콜 분석 및 수정된 프로토콜 제안

3.1 해쉬-언락킹 프로토콜 분석

태그는 해쉬 메커니즘을 처리할 수 있는 H/W 기반의 암호화 모듈로서 보안적 요구사항을 처리할 수

1) 본 연구는 산업자원부 성장동력기술개발사업(10016756)에 의해 지원되었음

있다. Tag에는 MetaID 정보만을 보관할 수 있는 저장 공간을 보유하고 있어야 하며 Lock과 Unlock 처리기능만 동작하면 된다. Unlock이 된 Tag만이 Tag Reader장비와 운영이 가능하다.

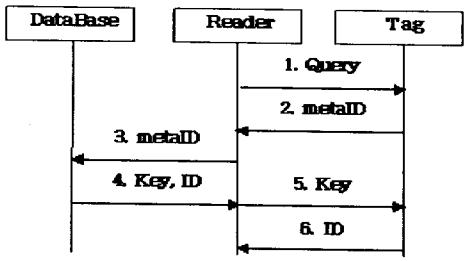

그림 1. 해쉬-언락킹 프로토콜

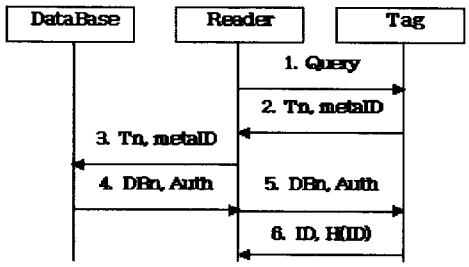

그림 2. 해쉬기반 제안프로토콜

2절에서 제시된 보안 요구사항에 대해 위 분석 결과를 토대로 다음과 같이 정리할 수 있다.

A. 인증 통한 long-term tracking 방지 : R입장에서 T로부터 정상적인 데이터를 전송받았다고 간주했으나, I_Tag나 I_DataBase와 같은 악의적인 개입이 가능했으며. metaID 정보는 tracking에 사용될 수 있다.

B. 암호화를 통한 채널 안전성 확보 : 위 반례에서 알 수 있듯이, 세번째 메시지의 Key와 ID는 암호화되지 않은 채 전송되어 노출되었다.

C. 상호 인증 : R입장에서 T로부터 정상적인 데이터를 전송받았다고 간주했으나, I_Tag나 I_DataBase와 같은 악의적인 개입이 가능했다.

D. Tag 정보의 유출방지를 통한 재생공격 및 중간자 공격 방지 : T가 R에게 정상적인 데이터 전송을 했다고 간주했으나 I_Reader에 의해 H(key)정보가 노출되었다. 결과적으로 T의 metaID 정보는 중간자 공격에 이용되었다

3.2 해쉬기반 프로토콜의 취약성을 수정한 제안프로토콜

이러한 해쉬-언락킹 프로토콜의 문제점으로 분석되었던 부분은 태그 내에 저장된 정보를 해쉬 기반기법으로 태깅할 수 있게 함으로써 발생되었으며 이는 태그의 정보를 인증된 리더기에 의해 데이터베이스에 접근함으로써 태그정보를 가져갈 수 있도록 하여 중간자 공격과 재생공격을 방지할 수 있었다. 즉 제안프로토콜은 다음 (그림 2)과 같은 절차로 인증이 이루어지며 앞서 언급된 취약성은 인증과정에서 도입된 3가지 기술에 의해 극복할 수 있다.

1. 첫번째로 태그의 난수와 데이터 베이스의 난수가 데이터 프라이버시와 태그 응답시의 악의적인 리더로부터의 재생공격을 막기 위해 도입된다. 따라서 태그는 난수재생기가 필요한데, 이는 장소추적을 막기 위해서 적어도 하나는 필요하다.
2. 통신참여자들간의 기밀성을 보장하기 위해 배타적 합 (Exclusive-or) 기술이 도입되었다.
3. 리더와 태그, 데이터 베이스와 리더간의 안전한 채널을 구축하기 위해 또 다른 metaID와 같은 타입의 데이터 베이스의 난수값과 리더의 원래 키값으로 이루어진 Auth라는 값이 사용되었다.

4. 제안 프로토콜 구현

현재 수동형태그에 대한 이슈는 단가가 낮은 보안 태그의 구현에 초점을 두고 있다. 따라서 공개키 기반 암호화 기술이나 대칭키 기반 암호화 기술이 적용되기도 하지만 최소 5센트 미만이라는 요구조건을 충족시키기에는 적합한 비용이 아니다[4]. 따라서 본 논문에서는 태그의 구현에 필요한 최소 게이트를 통한 보안 목표 달성을 하고자 한다. 제안된 프로토콜이 실질적으로 구현될 수 있는지를 검증하기 위해 ASICs 구현을 통해 총 게이트 수를 실험하였다.

5. 참고문헌

[1] S. Sarma, S. Weis, and D. Engels, "RFID systems and security and privacy implications", In Workshop onCryptographic Hardware and Embedded Systems (CHES) 2002, LNCS No. 2523, pp. 454-469, 2003

[2] Formal Systems Ltd. FDR2 User Manual, Aug. 1999.

[3] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", In 1st Intern. Conference on Security in Pervasive Computing (SPC), 2003.

[4] S. Weis., "Security and privacy in radio-frequency identification devices", Massachusetts Institute of Technology (MIT). Massachusetts, USA, 2003.