RFID Access Control 보안 모델에 관한 연구

한동희*1, 김동진2, 김수홍1
1상명대학교, 2호서대학교
e-mail:towiz@smu.ac.kr

A Study of RFID Access Control Security Model

Donghee Han*1, Dong-Jin Kim2 and SooHong Kim1
1Sangmyung University, 2Hoseo University

요 약

RFID는 유비쿼터스 환경 구축에 있어 가장 큰 비중을 차지하고 있다. 하지만 이에 따른 RFID에 저장된 개인정보 유출과 이를 오남용하는 문제에 대해 많은 비판들이 쏟아져 나오고 있으며 이에 대한 보안기술에 많은 관심이 모아지고 있다. 본 논문에서는 이러한 RFID의 보안모델 중 Access Control 기존 모델과 이를 보안한 RFID 2중 Access Control 보안모델을 제안한다. 2중 Access control모델은 기존 Hash-lock Access나 Hash-chain Method모델과 비슷한 구조를 가지고 있으나 도청에 의한 키 값 노출에 대한 보안성을 가지고 있으며 Tag인증에 대한 값을 계속 변화 시켜 2중으로 Access Control에 대한 인증 정보를 보안하는 구조이다.

1. 서론

유비쿼터스에 대한 관심이 쏟아지면서 여러 가지 관련기술과 시스템이 구축되고 있다. 이는 개인화 모바일화 되어가는 시대의 조류와 맞물려 유비쿼터스라는 인간-사물-시스템의 연결된 시대의 도래를 의미한다. 유비쿼터스 환경에서의 사람/사물 등에 자동식별기술로 RFID 기술이 각광받고 있으며 지금은 성숙단계로 여러 분야로 보급되어 활용되고 있다.

RFID 기술은 바코드 기술과 비교하여 설명할 수 있으며, 바코드 방식의 시스템보다는 많은 장점을 가지고 있다. RFID도 바코드와 같이 일종의 태그 시스템이라는 점에서는 유사성을 가지고 있지만 바코드 방식은 태그를 레이저로 읽어 기존에 구축된 데이터베이스와 비교하여 처리한다. 하지만 RFID는 전자태그(Transponders)와 리더기로 구성되며 식별코드 외에 더 많은 정보를 전자태그에 저장할 수 있다. 이처럼 많은 정보를 저장하고 활용할 수 있다는 점은 RFID의 장점이라 할 수 있다. 하지만 RFID는 저장된 정보에 대한 보안의 필요성이 요구된다. RFID의 기본적인 구조가 무선으로 데이터를 주고받는 형태를 가지고 있기 때문에 모든 무선데이터가 가지는 보안상의 취약점을 가지고 있다. RFID 기술이 보편화됨에 따라서 RFID에 저장되는 데이터가 중요 정보 혹은 개인정보까지 포함됨에 따라 RFID의 데이터의 보안과 안전성에 대한 중요도가 더욱 높아지고 있다.

현재 RFID의 보안상의 취약점을 보완하기 위해 기술로 여러 가지 보안 기술이 제안되었다. 그러나 이러한 보안 기술에서도 여러 가지 문제점들이 발견되고 있다. 따라서 본 논문에서는 기존의 제안된 보안 기술들에 대해 연구하고, 기존의 보안 기술에서의 문제점 중의 하나인 RFID 접근에 대한 리더기와 태그의 도청 공격에 대해 해쉬 함수를 사용하여 인증키 교환 시 보다 더 안전한 RFID 2중 접근 제어 모델을 제안한다.

2. RFID 시스템

RFID 장치는 식별될 정보를 가지는 전자태그와 식별데이터를 읽을 수 있는 리더기 및 수집된 데이터를 처리하기 위한 미들웨어로 구성된다. 이는 LF, HF, VHF, UHF의 국가별 지정 전파를 매개체로 하

여 송신국이 발신한 전파 신호 속에 들어 있는 고유 식별 질의 명령에 감응한 원격지 전자 회로가 내부의 고유 식별 부호를 출력하여 전파 신호로써 재발신하면, 송신국과 일체형의 수신국이 그 전파신호를 수신하며 고유 식별 부호를 추출, 분류, 저장, 비교, 인식하여 사용자가 원하는 형태로 데이터를 변환하여 사용하는 기술이다. 일반적으로 RFID 시스템은 RFIC, Antenna, 그리고 Packing하는 소재로 구성된다.[1]

2.1 RFID 시스템 위험요인

RFID는 편하고 바코드 시스템에 비하여 많은 장점이 있지만 시스템 설계 제약조건에 따른 위험요인을 가지고 있다. RFID 태그는 가격이 싸고, 저장공간 및 데이터 전송에 관해 매우 제약적이기 때문에 강력한 보안기법을 사용하는 것이 매우 어렵다. 따라서 이러한 제약사항을 고려한 태그 및 리더기의 설계가 중요시 되고 있다. 또한 RFID가 가지는 정보는 개인의 중요정보를 포함하는 경우가 많기 때문에 이에 따른 개인정보 침해 위험도가 높다.

NIST(National Institute of Standards and Technology : 미국국립기술표준원)의 “RFID 보안 가이드라인”[2]에서는 몇 가지 개인정보 위험요인을 다음과 같이 분석하였다.

○ 소유주의 의사와는 상관없이 원치 않는 태그를 개인사물 또는 문서 등에 내장하여 개인 사물들 또는 옷에 부착된 RFID 태그의 정보의 접근가능
○ 유일한 ID를 부여하여 전 세계에 존재하는 모든 사물 및 개인 등록, 파악으로 개인 사생활 침해 가능
○ 숨겨진 RFID 리더기를 사용하여 RFID 태그의 개인정보 누출위험
○ 개인정보의 대규모 데이터베이스 시스템과의 연계로 RFID 태그의 유일한 ID로 원치 않는 개인정보 및 신원확인 접근 가능
○ RFID 태그를 통한 개인위치 추적가능

2.3 RFID 시스템의 보안 취약성

RFID 시스템에 보호되지 않은 정보는 하드웨어의 한계에 의해 보안의 취약성을 갖는다. 또한 미들웨어와의 연동시 인터넷을 이용하는 경우 인터넷 보안 기술에 의존하게 된다. 이는 도청(Sniffing), 트래픽분석(Traffic analysis), 스푸핑(Spoofing), 서비스 거부 공격(Denial of Service), 세션가로채기(Hijack), 재생(Replaying) 및 중간자(Insertion) 공격 등 여러 가지 유형으로 나타난다.

○도청(Sniffing) : 태그가 보내는 신호를 도청하는 형태의 공격으로 리더기가 태그에게 질의를 보내는 범위에서 태그가 리더기에게 보내는 응답 신호를 도청한다.
○중간자공격(Insertion) : 쓰기 가능한 태그에 새로운 정보를 추가하거나 변형된 정보를 입력하여 잘못된 태그의 식별을 다르게 하는 공격
○서비스거부 공격(Denial of Service) : RFID 시스템에 가장 치명적 공격으로 무의미한 비트를 생성하여 공중에 뿌리면 리더가 태그의 정보를 무의미한 정보와의 충돌을 막기 위해 끝없이 데이터에 대해 질의를 반복하게 하여 RFID 시스템을 무력화 시킨다. 또는, RFID의 미들웨어에 연결된 인터넷 회선에 회선 용량을 초과하는 연결을 시도하여 RFID시스템의 호스트를 무력화 시키는 공격
○스푸핑(Spoofing) : 허가되지 않은 미들웨어 데이터베이스 및 호스트로부터 올바르지 않은 정보를 수용하거나 사용할 때 발생

3. RFID 보안 기술

현재 RFID 보안을 위해 여러 기술들이 제안되어 있다. 이들은 여러 형태의 공격에 대응하기 위해 설계되었는데 이중 태그의 접근 제어를 위해 설계된 방법은 Hash-lock Access Control, Random Access Control, Hash-chain Method 등이 있다.

3.1 Hash-lock Access Control

태그에 대한 접근제어 기술로서 접근이 허가된 사용자만이 태그에 접근할 수 있는 방법이다. 난수 형태의 키를 해쉬하여 데이터베이스에 정장한 리더는 이를 태그의 메타ID로 사용한다. 메타ID를 리더가 태그에게 전송 하면 Tag는 잠긴 상태가 된다. 태그를 읽을 경우 리더기가 Tag에 메타ID를 요구하고 태그는 리더기에게 메타ID전송한다. 리더기는 태그로부터 전송받은 메타ID를 발생 시 저장한 데이터베이스의 값과 비교하여 메타ID에 대한 키 값을 읽어 태그에 전송한다. 키 값을 전송받은 태그는 이 키 값을 해쉬하여 자신의 메타ID와 동일하면 잠긴 상태를 해제하고 사용가능한 상태로 전환한다.

3.2 Random Access Control

Hash-lock access Control과 유사한 방법으로 태그를 잠금 상태로 바꿀 때는 Hash-lock access control과 같이 난수형태의 키를 해쉬하여 메타ID를 태그에 전송하고 데이터베이스에 저장한다. 메타ID를 받은 태그는 잠금 상태가 된다. 태그를 잠금을 풀고 사용하기 위해서 리더가 태그에게 사용을 요청하면 태그는 자신의 메타ID와 랜덤한 nonce R을 해쉬하여 R과 함께 메타ID를 해쉬한 값을 리더에게 보내면 리더는 데이터베이스에 저장된 모든 메타ID값을 R과 해쉬하여 태그에서 보낸 해쉬된 메타ID값과 비교하여 일치하는 메타ID를 태그에 전송하면 태그는 자신의 메타ID와 비교하여 일치할 경우 잠금을 풀고 사용가능한 상태로 전환한다. 이는 데이터베이스에 저장된 메타ID가 많으면 많을수록 수행속도가 느려지고 해쉬를 계산할 수 있는 태그의 경우에만 사용가능하다.

3.3 Hash-Chain Method

NTT사에서 제안하였으며 태그의 정보가 향후 템퍼링 등에 의해 노출되었어도 이전 전송된 데이터는 안전성인 순방향 안전성을 보장하는 방법이다.

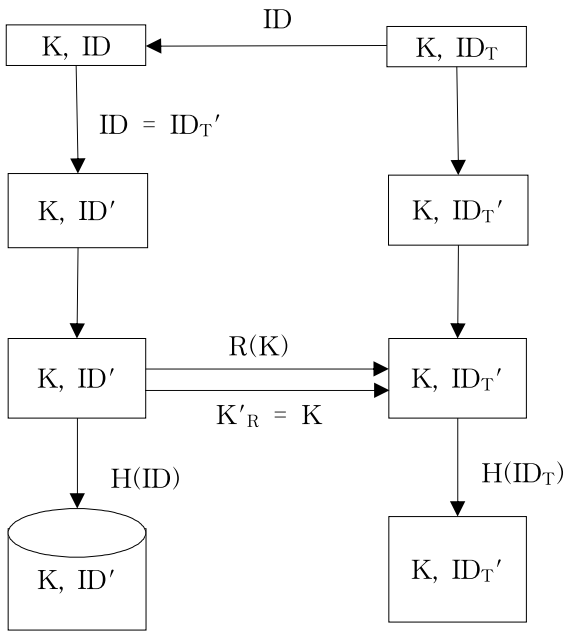
단방향 해쉬함수를 H, G라 하고 태그 초기 정보를 s1이라 하고 데이터베이스에는 태그의 ID인 ID와 S1을 저장하여 보관하고 있다.(ID와 s_1은 유일한 값이다.) i번째 거래에 태그는 리더에게 $a_i=G(s_i)$를 보내고 s_i를 새로운 값 s_{i+1} = H(si)로 갱신한다. 리더는 받은 a_i를 데이터베이스에 보내어 저장된 s1에 대해 $a_i'=G(H_i(s_1))$를 계산하여 ai와 비교하여 a_i = a_i'일 경우 저장된 ID를 출력한다.

해쉬함수 G와 H가 단방향 해쉬 함수이기 때문에 태그의 전송값 a_i나 새로운 태그의 비밀값 s_{i+1}이 노출되더라도 공격자는 a_i를 a_{i+1}과 연결이 불가능하고 s_i값을 추적할 수 없다. 이 방법은 적은 연산이 가능한 RFID 시스템에서도 사용할 수 있기 때문에 가격면에서 저렴하며 템퍼링이 발생하는 경우에도 프라이버시를 보호할 수 있다. 또한 ID 자체를 출력하지 않아 익명성을 보호한다. 하지만 데이터베이스 서버에 고가용성을 요구하며 서비스거부공격에 취약할 수 있다.

4. 2중 Access Control 모델

이 연구에서 제안하고자 하는 모델은 2중 Access Control 모델로서 RFID Access에 대한 리더기와 태그의 도청공격에 대해 해쉬 함수를 통해 인증 키 교환 시 좀 더 안전한 2중 Access Control로 보안을 강화한 모델이다.

4.1 2중 Access Control 모델 구조



[그림 1] 2중 Access Control 모델

리더는 키 값 K, 태그인증을 위한 난수형태의 값 ID를 가지고 있다. 태그를 리더기에 등록할 때 리더기는 태그에게 키 값 K와 ID를 전송한다. 태그는 이 두 값을 전송 후 태그를 사용 불가한 상태로 전환한다. (이 때 태그의 ID값은 ID_T라 한다.)

태그사용 시 리더기가 태그에 인증을 요청하면 태그는 자신의 ID_T 값을 리더에게 전송한다. 리더기는 태그로부터 전송 받은 ID_T 값을 데이터베이스에 저장된 ID값과 비교하여 일치하는 값을 찾는다. 리더기는 일치하는 ID값을 데이터베이스에서 찾게 되면 쌍으로 저장된 키 값 K를 불러내고 이를 양방향 해쉬 함수인 R을 사용해 R(K)값 K′을 생성한다. 생성된 K′값을 리더기는 태그에게 전송하게 된다. K′값을 전송받은 태그는 이를 역방향 해쉬 함수인 R′을 통해 R′(K′)값 K_T를 생성한 후 처음 리더기로부터 전송받은 K값과 비교한다. K_T값과 K값이 일치하면 태그는 잠금 상태에서 사용가능상태로 전환한다. 이때 리더기는 사용된 ID값을 태그는 사용된 ID_T값을 값은 단방향 함수H를 사용하여 ID′과 ID_T'을 생성한 후 ID'은 데이터베이스에 ID_T'은 태그에 저장한다. 다음번 사용요청이 오게 되면 새로 생성

되어 저장된 ID′값과 ID_T′값을 사용한다.

4.2 2중 Access Control 모델의 특징

제안하는 2중Access Control은 다른 Access Control 보안 모델과 같이 sniffing과 같이 리더와 RFID간 정보 교환 시 도청 유형의 보안 취약점을 보안하고자 제시된 모델이다. 2중 Access Control 모델은 기본적으로 Hash-lock Access Control 모델과 같이 접근 제어를 위해 태그의 사용권한을 잠금으로 인증되지 않은 리더로 부터의 사용에 제한을 둔다. 하지만 Hash-lock Access Control 모델의 경우 리더기로부터 키 값이 태그로 전송될시 도청이 이루어진다면 공격자는 임의에 리더기에서 태그에 사용요청 후 어떤 ID값이 오던지 도청된 키 값을 전송하게 되면 도청공격당한 태그는 정상적으로 작동하게 될 것이다. 이처럼 Hash-lock Access Control 모델의 키 값 전송에 대한 방어 장치가 없다. 하지만 본 연구에서 제안한 2중 Access Control모델에서는 키 값이 직접 전송되지는 않는다. 때문에 리더기와 태그간 인증정보 전송 시 도청이 가능하게 되더라도 이를 사용하여 태그사용 인증을 할 수 없다. 또한 인증을 위해 미들웨어에서 키 값을 찾기 위한 키 값과 쌍으로 대응하는 ID값이 사용 후 계속 단방향 함수 H를 통해 변하기 때문에 ID값을 알게 되더라도 다음번 인증 시 사용할 수 없게 된다. 이처럼 인증에 필요한 정보를 2중으로 변환시켜 교환 하므로 다른 Access Control모델에 비해 2중 Access Control 모델은 도청에 상대적인 강점을 가지게 된다. 또한 ID의 해쉬 변환은 인증이 모두 이루어진 이후 수행되기 때문에 Jamming Attack으로 인한 Tag의 인증 실패 시 ID값의 변환이 이루어지지 않아 ID값을 잃어버리지 않아 인증 시도를 통해 태그의 사용요청 작업을 무사히 완료 할 수 있다.

5. 결론

유비쿼터스 시대에서 RFID가 차지하는 비중은 매우 크다. 현재 RFID는 많이 활용되어지는 편리한 기술이지만 무선을 통한 데이터 전송으로 많은 보안상의 취약점을 가지고 있다. 하지만 RFID의 저렴한 가격 및 사용의 편리성을 대체할 기술이 아직 없는 것이 사실이다. 따라서 중요한 정보 및 개인 사생활 침해를 최대한 줄일 수 있는 보안 기술이 절실히 필요할 때이다. 이러한 보안상의 취약점을 해결하기 위해 본 연구에서는 RFID 2중 접근 제어모델을 제안하였다. 제안된 방법은 단방향 해쉬 함수를 이용해 태그에 접근 제어를 설정하기 때문에 도청공격에 효과적이며 매번 Access Control값이 갱신되어 사용할 때마다 요청 값이 달라져 이전 값을 알게 된다 하더라고 이에 대한 보호가 가능하다. 하지만 키 값인 K 도출시 데이터베이스에 참조해야할 자료가 많으면 수행속도에 제약이 따른다. 또한 해쉬 계산을 위해 RFID 회로에 많은 게이트가 필요하게 되는 단점이 있다. 따라서 RFID의 하드웨어적, 시스템적 제약점을 극복할 수 있는 보안모델로의 연구가 계속되어져야 한다.

참고문헌

[1] 박승창, 남상엽, 류영달, 이기혁, 김완석, “유비쿼터스 센서 네트워크 기술” Jinhan M&B, 2005

[2] Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Phillips, "Guidelines for Securing Radio Frequency Identification(RFID) System" Recomandation paper, National Institute of Standards and Technology

[3] David Molnar, David Wagner, "Privacy and Security in Library RFID Issues, Practices, and Architectures" ACM Conference on Communications and Computer Security, 210-219, ACM Press , 2004

[4] EPGglobal Web Page, www.EPCglobalinc.org

[5] Istv´an Vajda, Levente Butty´an, "Lightweight Authentication Protocols for Low-Cost RFID Tags" In Second Workshop on Security in Ubiquitous Computing-Ubicomp 2003, 2003

[6] Shucheng Yu, Kui Ren, Wenjing Lou, "A Privacy-preserving Lightweight Authentication Protocol for Low-Cost RFID Tags" IEEE Military Communication Conference-MILCOM 2007, 2007

[7] Chiu C. Tan, Bo Sheng, Qun Li, "Serverless Search and Authentication Protocols for RFID" IEEE Conference on Pervasive Computing and Communications-PerCom2007, 2007

[8] Frank Thornton, Brad Haines, Anand M. Das, Hersh Bhargava, Anita Campbell, John Kleinschmidt, "RFID Security" Syngress, 2006