Hotlisting과 Tracking 방지를 위한 RFID인증 프로토콜에 관한 연구

금준규*, 이희조
*고려대학교 컴퓨터정보통신대학원
e-mail:forjun@korea.ac.kr

An RFID Authentication Protocol for Hotlisting and Tracking Prevention

Jun-kyu Keum*, Heejo Lee
*Graduate School of Computer and Information Technology,
Korea University

요 약

RFID시스템은 태그와 리더, 백엔드DB로 구성되는 무선인식시스템으로 용도와 기능, 크기에 따라 다양하지만 가장 널리 사용될 것으로 예상되는 것은 저가 수동형 태그로 향후 바코드시스템을 대체할 것으로 기대된다. 이러한 RFID시스템은 적법한 리더와 태그에게 정보를 전달해서 도청자로부터 통신을 방해받지 않아야 하고, 원하지 않는 태그 정보의 노출로 인한 개인 프라이버시 침해를 방지할 수 있어야 한다. 본 논문에서는 불특정다수가 이용하는 많은 양의 아이템을 취급하는 공공도서관에서 RFID시스템을 도입함에 따라 예상되는 개인 프라이버시 침해를 방지하기 위해 보안 요구사항을 만족하면서 시스템 사용 환경에 맞는 프라이버시 보호 방식을 제안한다.

1. 서론

RFID(Radio Frequency IDentificatin)는 바코드와는 달리, 각 물품이 고유의 코드를 가지게 되어 물품 종류, 생산이력 등을 저장하여 다양하게 활용할 수 있다. 그러나 보안과 프라이버시 보호 측면에서 역기능을 유발하여 개인이 소유한 물품의 정보가 리더를 통해 유출될 수 있으며, 태그의 정보를 복사하여 위조될 우려가 있다[1].

RFID를 활용하는 여러 분야 중, 공공도서관 분야는 1990년 후반부터 전자기 바코드시스템을 대체하기 위해 RFID를 도입하기 시작하였다. 도서관 RFID 사용에 있어 RFID태그가 비인가된 리더에 쉽게 응답하는 static 데이터를 담고 있다는 점은 개인의 자료 이용습관을 프로파일화하여 악용하는 hotlisting과 특정 자료의 이용내역 및 이용자의 자료 이용을 추적하는 tracking 가능한 프라이버시 문제가 발생할 수 있는 환경이 된다[2].

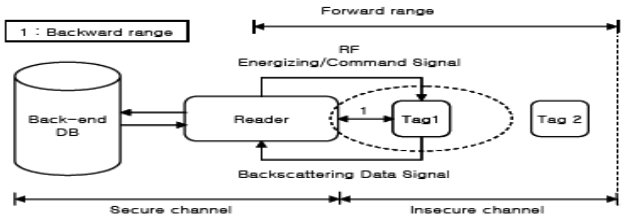
본 논문에서는 많은 양의 아이템을 취급하면서 불특정 다수를 대상으로 서비스하는 공공도서관 환경에서 RFID시스템을 도입함에 따라 제기되는 개인 프라이버시 위협 중, hotlisting과 tracking 가능한 프라이버시 문제를 해결할 수 있는 프라이버시 보호 방식을 제안하고자 하였다.

본 논문의 구조는 2장에서 RFID시스템 및 보안 요구사항을 서술하고 3장에서 프라이버시 문제와 관련한 기존연구 분석을 통해 문제를 제기하고 4장에서 본 논문에서 해결하고자 하는 hotlisting과 tracking 방지를 위한 프라이버시 보호 방식을 제안·분석하여 5장에서 결론을 맺도록 한다.

2. RFID시스템 및 보안 요구사항

2.1 RFID시스템

RFID시스템은 태그, 리더, 백엔드DB로 구성되며 작동형태는 그림 1과 같다[3]. 전방위영역(Forward range)은 리더가 RF신호를 태그로 전송할 수 있는 영역이며, 후방위 영역(Backward range)은 태그가 리더의 요청에 대하여 자신의 정보를 전송할 수 있는 영역이다.



(그림 1) RFID시스템 구성

▪ 태그는 리더의 요청에 대해 식별정보를 송신하는 것으로 무선통신을 위한 결합장치와 연산을 수행하고 정보를 저장하는 마이크로 칩으로 이루어져 있다.

▪ 리더는 태그가 송신한 식별정보를 수신하여 태그를

인식하는 장치이다. 리더는 태그에게 RF Signal을 전송하여 전력을 공급하고, 태그로부터 수신한 정보를 백엔드DB로 전송한다.

▪ 백엔드DB는 태그를 식별할 수 있는 정보를 저장하고 리더가 태그로부터 수집한 정보의 진위를 판별한다.

한편, 공공도서관에서 사용하는 수동형 RW태그는 도서관 아이템에 지속적으로 부착되어 바코드 넘버나 생산자 ID와 같은 static 데이터를 저장하고 이 데이터는 리더를 통해 도서관의 대출반납과 장서점검, 보안에 활용된다. RFID태그 사용으로 보안을 위한 추가 태그 구입없이 하나로 아이템 식별과 보안 유지를 할 수 있다[2]. 또한, 이용자가 도서관을 떠날 때 아이템의 대출여부 확인을 위해 태그가 판독되고, 도서관내에서 사서는 휴대용 리더기를 통해 분실되었거나 손실된 아이템을 확인한다.

2.2 보안 요구사항

RFID 사용으로 인한 프라이버시 침해유형에는 리더를 가진 누구에게나 태그 식별정보나 고유한 ID를 전송하는 정보유출과 태그마다 동일한 값을 송신하기 때문에 리더를 가진 공격자가 특정 태그 소유자의 위치를 추적하는 위치 추적이 있다. 이러한 정보유출과 위치추적을 해결하기 위해서는 아래의 보안요구사항을 만족해야 한다[4].

▪ 기밀성(confidentiality)

비밀리에 태그 정보가 전송되도록 기밀성을 보장하기 위해 태그가 식별정보를 리더에게 줄 때 리더가 적법한지 확인하는 인증 프로토콜을 거치거나, 적법한 리더만이 알 수 있도록 암호화해서 전송하는 방법을 사용해야 한다.

▪ 불구분성(indistinguishability)

태그는 리더가 정보를 요구할 때마다 다른 정보를 전송해주어야 하고, 이 정보는 리더측에서 예측이 불가능해야하며, 난수와도 구분이 불가능해야 한다. 불구분성은 태그 소유자의 위치 정보에 대한 프라이버시를 보호하기 위한 중요한 보안 요건이다.

▪ 전방 보안성(forward security)

태그가 현재 송신하는 정보를 알아내거나 태그 내부에 저장된 정보가 노출된 경우라도 그 정보를 가지고 과거의 송신 정보를 알아낼 수 없도록 해야 한다. 태그의 현재 정보를 이용해서 과거 송신정보를 알아낼 수 있다면 태그 소유자의 과거 정보를 파악할 수 있게 되어 프라이버시 침해가 발생한다.

한편, 미국의 프라이버시 권리 정보센터(Privacy Rights Clearing house)는 도서관 RFID시스템 가이드라인에서, 인가된 사용자의 RFID시스템 접근과 RFID 태그에 어떤 개인정보도 저장하지 말아야 하며, 태그 부착 아이템에 대한 기술은 데이터가 단지 바코드 넘버일지라도 암호화되어야 하고, 태그의 static 데이터에는 비인가된 리더에 판독될 수 있는 정보를 저장하지 않아야 하며 태그와 리더간의 통신은 고유한 암호키로 암호화되어야 한다고 제안했다[5].

3. 문제제기

공공도서관들이 RFID시스템을 사용하면서 단순 반복 업무에서 벗어나 업무 효율성 향상 및 도서관 보안과 장서점검에 드는 인적, 물적 비용 감소라는 잇점이 부각되었다. 그러나 불특정 다수를 대상으로 많은 양의 아이템 단위 태그를 사용하기 때문에 악의적인 의도를 가진 공격자에 의한 여러 유형의 프라이버시 침해문제도 제기되었다[5].

미국의 경우 1990년 이후 약 130여개의 공공도서관에서 RFID시스템을 사용하고 있지만, 우리나라의 경우 RFID를 도서관리시스템으로 사용한 기간이 짧아 프라이버시 침해 방지에 관한 연구가 미흡하다. 공공도서관이 RFID시스템을 사용하면서 제기되는 문제점은 다음과 같다.

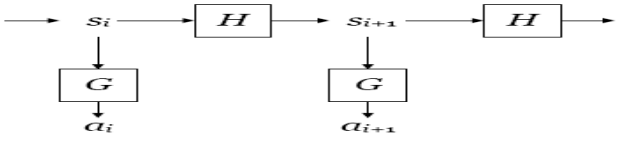
▪ 태그는 태그 데이터를 판독(read)하는데 별도의 접근제어를 하지 않고, 아이템이 속한 기관 확인용으로 태그내 고유한 prefix를 두는데 이것을 통해 공격자도 아이템의 소속을 확인할 수 있다. 또한, 태그의 static 데이터는 자료 추적(tracking)을 허용하고, 핫리스트를 작성(hotlisting)하여 특정 자료를 이용하는 이용자의 개인정보를 프로파일화함으로써 개인의 정보이용 습관을 수집하는 등 프라이버시를 침해하게 된다[2].

▪ RW태그를 사용함에 따라 쓰기 및 읽기 패스워드를 사용한다. 자가 대출시마다 사용되는 쓰기 패스워드와 도서관 출구 센서에서 인식되는 읽기 패스워드가 동일한 싱글 패스워드를 모든 태그에 사용할 경우, 패스워드가 일방향 커뮤니케이션으로 인해 도청자에게 이용가능하다. 반면, 태그마다 다른 패스워드를 사용하게 될 경우, 리더가 어떤 패스워드를 어떤 태그에 사용해야 하는지를 결정해야 하며, 각 태그가 지니게 될 고유한 ID는 태그의 hotlisting과 tracking을 가능하게 한다[2].

한편, 태그 내에 직접적인 식별정보가 들어있지 않더라도 태그 내 ID의 분류체계가 정해져 있어 분류체계에 대한 상세 정보를 가진 공격자에게 개인의 신상정보가 누출되면 프라이버시는 침해될 수 있다[7].

RFID 사용으로 인한 문제 해결을 위해 제안된 기법 중, 해쉬함수에 기반한 기법을 분석하여 각각의 문제점을 살펴보기로 한다[4][6].

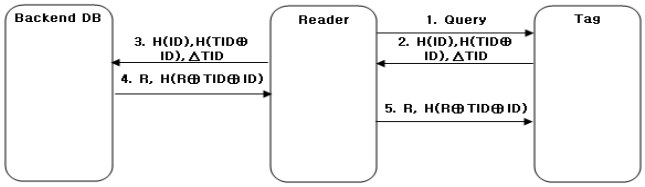
▪ 해쉬체인 기법



(그림 2) 해쉬 체인 기법

두 개의 서로 다른 해쉬함수를 이용하여 리더의 질의에 대해 항상 다른 응답을 하여 공격자에게 응답 메시지 간의 관계를 노출시키지 않도록 제안된 기법이다. 그러나 공격자가 태그의 응답을 재전송하는 경우 정당한 태그로 가장할 수 있어 재전송 공격과 Spoofing공격에 취약하고 백엔드DB는 모든 비밀정보에 대응하는 태그의 ID를 검색해야 한다.

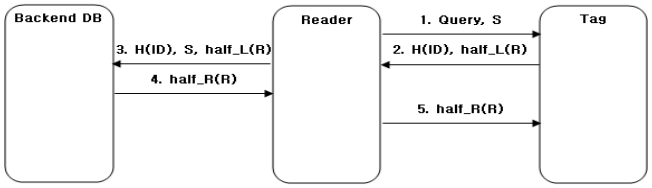
▪ 해쉬기반 ID변형 기법



(그림 3) 해쉬 기반 ID변형 기법

해쉬체인 기법과 유사하게 태그의 인증정보인 ID를 매 세션마다 바꾸는 기법이다. 매 세션마다 태그의 ID가 난수 R에 의해 갱신되고, TID와 LST가 갱신되므로 공격자의 재전송 공격에 안전하다. 그러나 공격자가 정당한 리더로 가장하여 태그로부터 H(ID), H(TID⊕ID), △TID를 획득하고, 정당한 태그가 다음 인증 세션을 수행하기 전에 이 정보를 리더의 질의에 대한 응답으로 이용하면 공격자는 정당한 태그로 인증받을 수 있다. 또한 정당한 세션이 이루어지기 전까지는 H(ID)은 항상 같으므로 위치 추적이 가능하다.

▪ 개선된 해쉬기반 ID변형 기법



(그림 4) 개선된 해쉬기반 ID변형 기법

이 기법은 Spoofing 공격을 개선하기 위해 제안되었으나 해쉬기반 ID변형 기법과 동일하게 인증 세션이 완전하게 종료된 이후에나 ID가 갱신되기 때문에 여러 개의 리더를 곳곳에 설치해 놓은 공격자가 정당한 리더로 가장하여 H(ID), half_L(R)을 획득하고 half_R(R)은 전송하지 않는다면 공격자는 태그가 정당한 리더와 인증 세션을 수행하여 H(ID)가 갱신되기 전까지 H(ID)를 통해 태그의 위치를 추적할 수 있다.

4. 제안방식

4.1 제안 방식

본 방식은 프라이버시 보호를 위한 보안 요구사항을 만족하고 불특정 다수를 대상으로 많은 양의 아이템에 저가의 수동형 RW태그를 사용하는 환경에 적합한 프라이버시 보호를 목표로 하였다. 메모리양과 해쉬 연산량을 줄여 저가의 태그에 유용하도록 하였고 재전송 공격이나 Spoofing공격 감지를 통해 공공도서관과 같이 취급하는 아이템의 특성상 예상되는 공격이 적은 환경에 적합한 인증 프로토콜로 활용하도록 하였다.

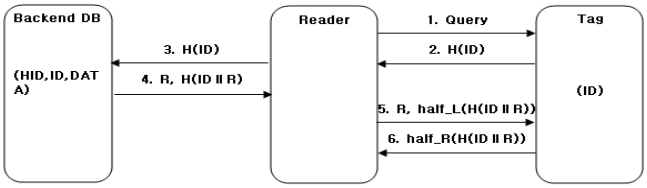
우선, 태그는 인증을 위한 랜덤값 ID만을 가지며, 백엔드DB는 태그 정보인 데이터와 ID의 해쉬값인 HID, ID를 갖는다. 이와 같은 입력은 사전에 RF통신이나 물리적인 접촉을 통해 안전하게 이루어짐을 가정한다.

<표 1> 제안방식 구성요소 및 연산도구

	필요한 메모리	연산도구
태그	H()	H(), ⊕
리더	-	-
백엔드DB	HID, H(), DATA	H(), R.N.G,⊕

ID : 인증을 위한 랜덤값, 인증 성공시 변화
HID : ID의 해쉬값, (=H(ID))
DATA : 사용자정보, 실질적인 데이터
H() : 일방향 해쉬함수
R.N.G : 난수발생기
⊕ : XOR 연산(exclusive-or function)
‖ : 연결 연산(concatenate function)
half_L() : 입력되는 값의 왼쪽 반을 출력하는 함수
half_R() : 입력되는 값의 오른쪽 반을 출력하는 함수

▪ 인증과정



(그림 5) 제안방식

1. 리더 : 태그에게 질의한다.
2. 태그 : 자신이 가진 ID를 해쉬한 값 H(ID)를 리더에 전송한다.
3. 리더 : 2번 과정에서 받은 정보를 백엔드DB에 전송한다.
4. 백엔드DB : H(ID)를 통해 태그의 정보를 찾아 확인하고, ID를 갱신하기 위한 랜덤값 R을 생성한다. 그리고 R과 함께 리더나 공격자가 R을 조작하는 것을 방지하기 위해 H(ID‖R)을 생성해 같이 보낸다.
5. 리더 : 태그에게 R과 H(ID‖R)의 왼쪽 반인 half_L(H(ID‖R))을 전송한다.
6. 태그 : 5번 과정에서 받은 정보가 자신이 만들 수 있는 H(ID‖R)의 왼쪽과 일치한다면, 자신이 받은 정보가 타당함을 확인하고 자신도 리더에게 H(ID‖R)의 오른쪽인 half_R(H(ID‖R))을 제대로 받았음을 알린다.

세션이 정상적으로 완료되면 태그는 인증되고, 백엔드DB와 태그의 ID는 ID=ID⊕R로 갱신한다.

4.2 제안 방식 분석

도서관 사용 태그는 해당 식별정보가 직접 들어있는 대신 백엔드DB에서 식별정보를 찾을 수 있도록 하는 ID를 사용한다. 이 경우에도 태그 내 static데이터로 인

해 적법하지 않은 리더나 도청자가 사전에 다수의 태그 ID에 대한 정보를 축적한 상태(hotlist)라면, 직접적인 식별정보를 얻은 경우만큼이나 프라이버시에 문제가 된다. 따라서 본 방식은 태그는 랜덤값만을 가지도록 하고 백엔드DB에 태그의 정보 데이터가 저장되어 백엔드DB는 안전하다 가정하므로 개인정보 프라이버시를 만족한다. 백엔드DB가 생성한 랜덤값 R에 의해서 ID가 갱신되므로 위치 프라이버시를 보장하도록 하였다.

▪ 인증프로토콜 구성

도서관 RFID시스템 중 리더의 역할을 수행하는 장치로는 각 기능에 따라 자가대출기, 장서점검기, 도난방지 안테나 등을 들 수 있는데 이처럼 다양한 리더 장치와 인증프로토콜을 구현하는데 따른 어려움을 극복하기 위해 리더는 단지 전달 기능만을 수행하도록 하도록 하였다.

▪ 인증프로토콜 메모리 및 연산량

본 방식은 해쉬기반 ID변형 기법에 비해 태그에게 요구되는 메모리양은 1/3로 적으며 해쉬연산을 두 번 수행한다. 현재 태그 단가에서 큰 비중을 차지하는 해쉬함수 연산량을 감소하여 태그 비용 감소를 시도하였으며 개선된 해쉬 기반 ID변형기법과는 달리 리더가 아닌 백엔드DB에서 난수를 발생하도록 했다.

<표 2> 제안방식 분석

구분	태그메모리(bit)	연산량(회)		
		태그	리더	백엔드DB
해쉬체인 기법	L	해쉬함수 2	-	해쉬함수(태그수/2) *i
해쉬기반ID 변형기법	3L	해쉬함수 3	-	난수생성1 해쉬함수3
개선된 해쉬기반ID 변형기법	L	해쉬함수 2	난수생성 1	해쉬함수2
제안방식	L	해쉬함수 2	-	해쉬함수 2

▪ 보안 요구사항 만족여부

프라이버시 권리정보센터[5]의 제안대로 태그에 개인정보를 수록하지 않았고 태그의 고유한 ID도 매번 갱신하도록 하였다. 또한, 태그가 항상 동일한 정보를 송신하지 않도록 난수 생성기 모듈을 백엔드DB에 구현하여 백엔드DB가 태그에서 송신하는 값에 대해 정상적인 식별을 수행하도록 하였다. 또한, 해쉬함수를 사용하여 태그의 현재 송신 정보를 가지고 과거 정보를 알아낼 수 없도록 보장하여 전방 보안성을 만족하도록 하였다.

본 방식에서 공격자는 도청에 의해 얻은 2번 과정을 재전송할 수 있지만, 이미 전 단계에서 백엔드DB가 저장하는 HID값이 바뀌었으므로 공격은 성공하지 못한다. 또한, 공격자가 임의의 태그에게 질의를 하여 H(ID)를 획득한 후, 정당한 리더에게 인증을 요구하고 정당한 태그가 다음 인증 세션을 요청하지 않았다면, 리더는 공격자를 정당하다고 판단하고 5번 과정을 전송하므로 적극적으로 Spoofing 공격을 예방하지 못할 수 있으나 공격자가 6번 과정을 보내지 않으므로 리더는 Spoofing 공격을 감지할 수 있고 리더와 태그가 5, 6번 과정을 서로 주고받는 것은 메시지 유실에 대한 감지 기능도 수행한다. 따라서, 공공도서관과 같이 Spoofing공격이나 메시지유실 가능성 및 예상 공격이 적은 시스템에서 활용할 수 있을 것이다.

5. 결론

본 논문에서는 저가형 RW태그를 사용하는 RFID시스템 환경의 프라이버시 침해 중, hotlisting과 tracking 위협을 방지하는 방식을 제안하였다.

공공도서관과 같은 환경의 RFID시스템은 실제로 태그에 개인정보를 수록하지 않거나 또한, 수록된 정보의 크기가 매우 작기 때문에 고속 암호가 필요하지 않으므로 재고관리 및 물류 유통분야의 보안 설계 요구조건과는 차별화되어야 한다. 즉, RFID 적용 환경과 제공되는 서비스의 종류에 따라 암호와 설계사상이 다른 보안 방식 연구가 필요하다.

향후 불안전한 통신채널인 리더와 태그간 통신에서 태그의 고유한 ID가 충돌방지 프로토콜 정보 및 식별정보로 이용됨에 따라 예상되는 보안 위협과 RFID가 다양한 환경에 적용됨에 따라 각 적용환경의 특성을 반영한 보다 구체적인 프라이버시 보호방안에 대한 연구가 있어야 할 것이다.

참고문헌

[1] 오길영, “개인정보보호를 위한 RFID 규제에 관한 연구”, 정보통신정책 제12권제2호, 2005

[2] D. Molnar, D. Wagner, “Privacy and Security in Library RFID: Issues, Practices, and Architectures”, ACM CCS, October, 2004

[3] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, “분산데이터베이스 환경에 적합한 Challenge-Response기반의 안전한 RFID 인증 프로토콜”, 한국정보처리학회논문지 제12-C권 3호, 2005

[4] M. Ohkubo, K. Suzuki and S. Kinoshita, “Efficient Hash-Chain Based RFID Privacy Protection Scheme”, In Ubicamp 2004, 2004.

[5] Privacy Rights Clearinghouse, “RFID Position Statement of Consumer Privacy and Civil Libraries Organizations”, November, 2003
http://www.privacyrights.org/ar/RFIDposition.htm

[6] M. Ohkubo, P. Oechslin, “A Scalable and Provably Secure Hash-based RFID Protocol Protection Scheme”, In Ubicamp 2004, 2004.

[7] 이재일, 조규범, 이용필, “RFID의 발전에 따른 정보프라이버시 보호에 관한 법적 연구”, 한국정보보호진흥원 연구보고서, 2004