모바일 RFID 프라이버시 보호 기법에 대한 취약성 분석†

함형민, 송주석
연세대학교 컴퓨터과학과
e-mail: {hmham, jssong}@emerald.yonsei.ac.kr

Vulnerability Analysis of Mobile RFID privacy protection scheme

Hyoungmin Ham, JooSeok Song
Department of Computer Science, Yonsei University

요 약

RFID는 무선 주파수를 이용해 사물이나 사람에 부착된 태그를 인식하고 태그에 담긴 정보를 주고받을 수 있도록 하는 비(非)접촉식 정보인식기술을 뜻하며 USN(Ubiquitous Sensor Network)의 핵심기술로 주목받으면서 다양한 분야에 걸쳐 연구되어 왔다. 기존 RFID와 이동통신 인프라를 융합한 모바일 RFID는 기존의 RFID 시스템과 모바일 네트워크의 장점을 동시에 지닌 개념으로써, RFID를 이용해 보다 다양한 서비스 제공이 가능할 것으로 기대되고 있다[1][2][3]. 2007년, Kim 등은 모바일 RFID 프라이버시 보호 기법에 관한 논문을 발표하였다[4]. Kim등은 논문에서 개인 사용자들이 각각 모바일 리더를 소지하고 이를 상품구매 시 이용하는 환경을 가정하고, 이 때 발생할 수 있는 위협과 이에 대한 해결책을 제시하였다. 그러나 주장과는 달리 제안된 기법은 위치추적에 대해 안전하지 못하며 사용자 프라이버시를 보장하지 못한다. 본 논문에서는 Kim등이 제안한 기법을 소개하고 실제 공격이 이루어지는 과정을 통해 제안된 기법의 취약성을 설명한다.

1. 서론

RFID 기술은 유비쿼터스 시대를 열어갈 최첨단 미래 기술로서 각광을 받고 있다. 모바일 RFID는 기존 RFID 기술과 모바일 네트워크를 융합한 개념으로 RFID 기술에 이동성을 더했다는 장점을 지니고 있어, 다양한 서비스 제공 및 기술발전이 가능할 것으로 기대되고 있다[1][2][3].

모바일 RFID에서 사용자는 개인용 모바일 리더를 소지하고 있으며, 특정 개체에 부착된 태그로부터 응답을 얻고 이것을 무선망을 통해 원거리에 있는 데이터베이스에 전송하여 인증이나 정보 제공 등의 서비스를 받게 된다. 모바일 리더는 데이터베이스와의 통신에 일반 사설망을 이용하게 되므로 기존 RFID와 달리 거리의 제약으로부터 비교적 자유로울 수 있으며, 여러 데이터베이스로부터 다양한 서비스를 제공 받을 수 있다는 장점이 있다. 2007년, Kim등은 개인 사용자들이 각각 모바일 리더를 소지하고 이를 상품구매 시 이용하는 환경을 가정하고, 이 때 발생할 수 있는 위협과 이에 대한 해결책에 관한 논문을 발표하였다[4].

그러나 Kim등이 제안한 기법은 사용자 프라이버시를 보장한다는 그들의 주장과는 달리 위치추적이 가능한 문제를 안고 있다. 본 논문의 구성은 다음과 같다. 우선 2절에서 Kim등의 논문에서 가정하고 있는 환경을 소개하고, 3절에서 제안된 기법을 소개한 후, 4절에서 공격이 이루어지는 과정을 설명함으로써 제안된 기법이 안전하지 못함을 보이고 끝으로 5절에서 결론을 맺는다.

2. 가정하는 환경

Kim 등은 모바일 리더를 소요한 사용자가 상품을 구매하려는 상황을 가정하고 이를 크게 구매 전과 구매 후로 나누었다. 구매 전과 구매 후는 각각 보안요구사항에 차이가 있으며 Kim 등은 각 상황별로 별도의 보안 기법들을 제안하였다[4]. 상품을 구매하기 전에는 누구나 상품에 부착된 태그를 통해 해당 상품에 대한 정보를 얻을 수 있고, 구매 후에는 특정 사용자의 소유가 된 상품의 정보를 보호함으로써 소유주의 프라이버시를 보호하고자 하였다.

3. Kim 등의 제안

Kim 등이 제안한 논문에서는 다음 세 가지 위협을 정의하고 있다.

-정보의 누출(Information Leakage)
-추적 가능성(Traceability)

† 이 논문은 2008년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. R01-2006-000-10614-0).

-위장(Impersonation)

여기서 Information Leakage는 특정 사용자가 상품을 구매한 후에 제 3자가 태그의 응답을 통해 사용자의 개인정보를 획득하는 것을 의미하며, Traceability는 특정 사용자가 상품을 구매한 후 태그의 응답을 추적할 수 있는지 여부를 말한다. 끝으로 Impersonation은 공격자가 도청한 메시지를 모바일 리더에게 전송하여 자신을 태그인 것처럼 위장하는 것을 의미한다.

Kim 등이 제안한 기법은 Identification phase, Initial setup phase 그리고 Privacy protection phase의 세 가지 상황으로 구성되어 있다. Identification phase는 사용자가 상품을 구매하기 전에 상품에 부착된 태그를 통해 특정 정보를 얻을 수 있도록 하고, Initial setup phase에서는 특정 사용자에게 태그의 비밀키 K를 전달하며, 마지막으로 Privacy protection phase에서는 태그가 매번 새로운 난수를 생성하여 항상 랜덤한 값을 응답함으로써 K를 알고 있는 모바일 리더 외에는 태그의 ID를 알 수 없게 하였다. <표 1>은 논문에서 사용되는 표기법이며, Privacy protection phase의 프로토콜의 흐름은 (그림 1)에 나타나 있다.

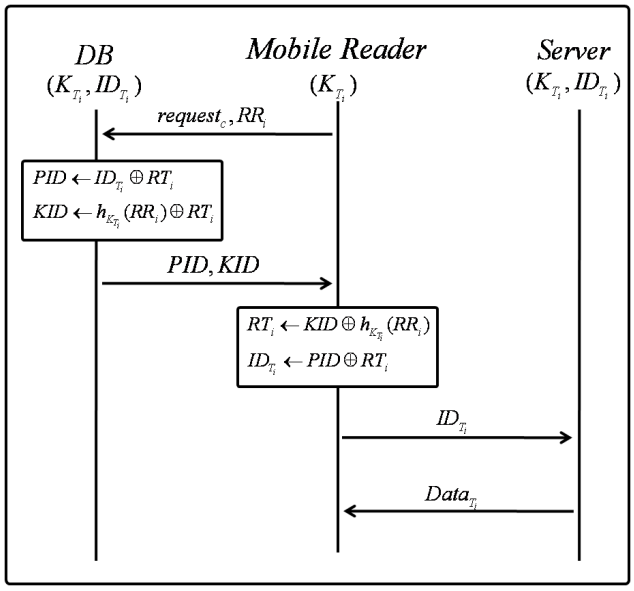
<표 1> 표기법

용 어	정 의
$request_c$	Pravacy protection phase에서의 요청 메시지
ID	태그의 ID(EPC)
K	태그의 키 값
r_i	모바일 리더가 생성한 난수
r_t	태그가 생성한 난수
$h_{k(.)}$	keyed hash function
$\oplus$	XOR 연산

Km등은 태그가 모바일 리더에게 항상 랜덤한 값을 응답하기 때문에 제 삼자가 이것을 도청하더라도 상품의 정보를 알아낼 수 없고, 결과적으로 구별불가능성을 만족하게 되므로 추적이 불가능하다고 주장하였다.

4. 취약성 분석

Kim등은 태그가 자체 생성하는 난수를 통해 매 세션마다 새로운 TID와 PID를 응답하므로, 만일 공격자가 같은 요청을 반복하더라도 추적이 불가능하다고 주장하였다. 그러나 다음과 같은 방법을 통해 공격자는 도청과 재전송을 통해 태그를 추적할 수 있다.



(그림 1) Kim등이 제안한 Privacy protection phase

1. 공격자 M은 모바일 리더와 태그의 통신을 도청한다. 도청으로 얻을 수 있는 메시지들은 다음과 같다.

$$M : RR_i, PID, KID$$

2. 이전세션에서 수집한 RR_i^M을 요청과 함께 태그에게 보낸다.

$$M \rightarrow Tag : request, RR_i^M$$

3. 공격자 M은 RR_i^M이 포함된 태그의 응답을 얻는다.

$$Tag \rightarrow M : PID, KID$$

$$PID = ID_{T_i} \oplus RT_i$$

$$KID = h_{K_{T_i}}(RR_i^M) \oplus RT_i$$

4. 이전 세션에 얻은 KID, PID를 KID_1, PID_1이라고 하고, 현재 세션에서 얻은 KID, PID를 KID_2, PID_2라고 하자. 공격자 M은 KID_1과 PID_1, 그리고 KID_2와 PID_2를 각각 XOR하여 각각의 $ID \oplus h_{K_{T_i}}(RR_i^M)$를 구하고 이를 비교한다.

$$PID \oplus KID = ID_{T_i} \oplus h_{K_{T_i}}(RR_i^M)$$

만일 KID_1, PID_1과 KID_2, PID_2 대한 결과가 같다면 공격자는 두 메시지가 동일한 태그로부터 온 것임을 알 수 있다.

5. 공격자 M은 요청 시 동일한 RR_i^M을 사용하고, 1에서 4까지의 과정을 반복함으로써 특정 태그의 응답을 구분할 수 있다.

5. 결론

2007년, Kim등은 모바일 RFID에서의 프라이버시 보호 기법에 관한 논문을 발표하였다. Kim등은 논문에서 개인 사용자들이 각각 모바일 리더를 소지하고 이를 상품구매 시 이용하는 환경을 가정하였고, 이 때 발생할 수 있는 위협에 대한 해결책을 제시하였다. 그러나 Kim등의 기법은 공격자가

몇 차례 XOR 연산만으로 특정 태그의 응답을 구별할 수 있으므로 실제 주장과는 달리 위치프라이버시를 보장하지 못한다. 이에 모바일 RFID에서 사용자 프라이버시를 보장하기 위한 추가적인 연구가 필요할 것으로 보인다.

참고문헌

[1] Hyangjin Lee, Jeeyeon Kim, "Privacy threats and issues in mobile RFID," Availability, Reliability and Security, 2006, ARES 2006, pp.5, 20-22 April 2006.

[2] 한국RFID/USN협회, "RFID (GL) 기술자격검정," 한국RFID/USN협회, pp.372, 2008.04.18.

[3] Divyan M. Konidala, Kwangjo Kim, "Mobile RFID Security Issues," The 2006 Symposium on Cryptography and Information Security, SCIS 2006, Hiroshima, Japan, Jan. 17-20, 2006.

[4] Il Jung Kim, Eun Young Choi, Dong Hoon Lee, "Secure Mobile RFID system against privacy and security problems," Security, Privacy and Trust in Pervasive and Ubiquitous Computing 2007, SECPerU 2007, pp.67-72, 19-19 July 2007.