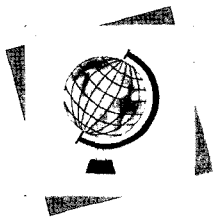
| 특집 07 |



RFID 정보보호 기술 동향

최은영 · 이동훈
(고려대학교)

목 차

1. 서 론

RFID 시스템은 사물에 부착된 태그(Tag)로부터 사물의 정보 및 주변 환경정보를 인식하여 실시간으로 정보를 관리하는 것이다. 즉, 각 사물의 정보를 수집, 저장, 가공 및 축적함으로써 사물에 대한 원격처리 · 관리 및 사물 간의 정보 교환 등 다양한 서비스를 제공한다[10]. 이러한 기술은 높은 인식률, 비 접촉형 인식 매체, 도달 거리, 다른 통신망과의 연결 및 통신 가능성 등의 확장성의 특성을 갖는다. 그러므로 RFID 시스템은 기존의 바코드를 대체하여 물류관리, 유통관리, 재고 관리를 할 수 있을 뿐만 아니라 정보의 실시간 처리 네트워크화 등의 특성으로 보안, 안전, 환경 관리 등에 혁신을 선도할 것으로 전망된다.

그러나 RFID 시스템의 특성상 리더(Reader)와 태그(Tag)는 비 접촉의 RF 통신을 이용하여 데이터를 주고받는다. 즉, 태그는 주위 리더가 정당한 리더인지에 대한 확인 없이 자신의 고유 정보를 리더로 전송한다. 이러한 RFID 시스템의 동작 원리는 리더 주변의 제 삼자가 손쉽게 사용자의 구매 이력이나 위치 정보 등을 얻을 수 있기 때문에 개인의 프라이버시 침해 문제를 야기시킨다. 따라서 RFID 시스템의 실생활 적용 측면에서 이러한 RFID 시스템의 문제점을 해결하기 위해 지속적인 연구가 이루어지고 있다.

2. RFID 정보보호 위협 요소

RFID 시스템은 리더(Reader)와 태그(Tag) 간에 RF 통신을 사용하여 태그의 고유 정보를 전송하는 형태로 동작한다. 이것은 RFID 시스템이 여러 위협에 노출되기 쉽다는 것을 의미한다. 이러한 취약점은 공격자가 기존의 시스템과 달리 적은 노력으로 원하는 정보를 얻을 수 있다는 것이다. RFID 시스템에서 공격자는 무선통신을 사용하는 RFID 시스템의 특성으로 인해 태그와 리더간의 RF 통신 도청이 가능하며, 이외에도 다음과 같은 공격을 수행할 수 있다.

- 도청 : 공격자는 도청을 통해서 쉽게 태그가 내장된 상품의 비밀 정보를 얻음으로써 사용자의 비밀 정보를 얻거나, 이후 설명되는 여러 가지 공격을 수행할 수 있다. 공격자는 이러한 공격을 통해서 사용자의 위치 정보나 사적인 정보를 얻을 수 있다. RFID 시스템은 무선 통신을 사용하기 때문에 공격자의 통신 도청을 막는 것은 불가능하다. 그러므로 도청이 불가능하게 하기 보다는 도청하는 것만으로 사용자의 비밀 정보를 얻을 수 없어야 한다.
- 위조 : 만약 공격자가 임의의 리더를 사용하여, 특정 태그에게 질의를 통해 고유 정보를 획득하는 경우, 공격자는 이 정보를 사용하여 특정 태그로 위장 가능하다. 이런 공격을 스푸핑 공격이라고 한다. 또한 공격자가 특정 태그와 리더 사이의 무선 통신을 도청하여 태그의 비밀 정보를 획득한다면 그 공격자는 이전에 통신에서 도청한 정보를 재사용하여 정당한 리더에게 전송함으로써 특정 태그로 위장할 수 있다. 이러한 공격을 재전송 공격이라고 한다. 이와 같은 위장 공격은 태그가 리더에게 대한 정당성 확인 없이 리더에게 정보를 전송하기 때문에 가능하다.

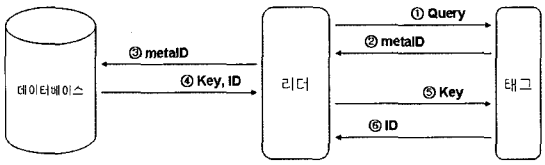
3. RFID 정보보호 기술 동향

RFID 시스템에서 사용자는 자신이 소유한 상품에 내장된 태그의 정보 유출로 인해서 사용자의 프라이버시 침해 문제가 발생한다. RFID 시스템에서의 사용자 프라이버시 문제를 해결하기 위해 다양한 기법들이 연구되고 있다. RFID 시스템에서의 정보보호 기술 기법은 크게 세 가지 형태, 해쉬 기반, 재-암호화 기반, XOR(exclusive-or) 기반으로 분류할 수 있다. 이 접근방식에 따라 RFID 시스템의 기술 동향을 정리한다.

3.1 해쉬 기반 기법

해쉬 기반 기법은 해쉬 함수의 일방향성(One-Way Property)을 이용하여 태그의 정보를 보호하는 기법이다. 그러나 RFID 시스템에서는 공격자가 리더와 태그의 통신을 도청하기 쉽기 때문에 이 채널에서 얻은 정보를 이용하여 두 가지 공격, 재사용 공격과 스푸핑 공격을 수행할 수 있다. 이러한 공격에 RFID 시스템을 보호하기 위해서 해쉬 기반 기법에서는 상호 인증 방법을 사용한다.

■ Hash-Lock scheme



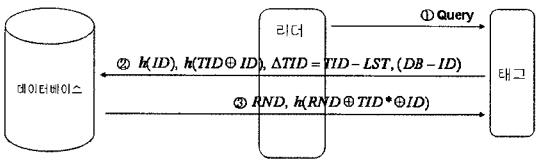
(그림 1) 해쉬 락(Lock) 기법

Weis 등이 제안한 기법[11]이며 제안된 기법은 (그림 1)과 같이 동작한다. 우선, 태그와 데이터베이스는 태그의 ID, key값을 저장한다. 리더는 태그에게 질의를 보내고, 태그는 리더의 질의에 자신의 key값을 해쉬 함수 h에 적용하여 생성한 metaID=h(key)값을 리더에게 전송한다. 리더는 데이터베이스(Database)에게 metaID를 전송하고 데이터베이스는 metaID에 대응되는 태그의 ID와 key를 찾아서 리더에게 전송한다. 리더는 key값을 태그에게 전송하고, 태그는 저장된 key와 받은 key가 동일할 경우 ID를 리더에게 전송한다.

그러나 이 기법에서는 태그가 고정된 값 metaID를 리더에게 전송하기 때문에 위치 추적이 가능하다. 이점을 보완하기 위해서 Randomized hash lock (RHLK)기법을 제안하였다. 이 기법에서 태그는 부가적으로 랜덤 생성기(Random Number Generator)를 사용하여 리더의 질의에 대하여 생성한 랜덤값 R과 자신의 임의의 여러 개의 ID

중에서 ID_K를 사용하여 생성한 $h(ID_K||R)$를 리더에게 전송한다. 개선된 기법에서 태그는 랜덤값을 사용하기 때문에 항상 다른 값을 리더에게 전송하므로 위치추적이 불가능하다.

■ Hash-based ID Variation



(그림 2) 해쉬 기반 ID 변형 기법

Dirk Henrici와 Paul Muller가 제안한 기법으로서, 전송되는 태그의 인증 데이터인 ID를 세션마다 갱신함으로써 태그의 위치 정보를 보호하는 기법이다[2]. 제안된 기법의 동작 과정은 (그림 2)와 같다.

- 태그는 리더의 질의에 대해서 TID(현재 세션의 횟수)의 값을 증가시키고, 해쉬 함수 h를 사용하여 생성한 해쉬 값 h(ID), h(TID⊕ID) 과 △TID=TID-LST, DB-ID 값을 리더에게 전송한다 (⊕ : XOR 비트 연산 연산자, LST : 마지막으로 정상 종료된 세션의 횟수, DB-ID : 태그의 정보가 저장된 데이터베이스의 정보, HID : h(ID) 값 저장 필드).
- 이 값을 받은 리더는 DB-ID에 해당하는 데이터베이스로 메시지를 전송하고 데이터베이스는 h(ID)에 저장된 행의 정보를 얻는다. 그리고 이전 LST값에 △TID를 더해서 TID^* 값을 계산한다. 데이터베이스는 TID^*값과 그 행의 ID를 XOR 하여 생성한 $h(TID^*⊕ID)$과 데이터베이스에게 전송된 h(TID⊕ID) 값을 비교한다. 만약 두 값이 다르면 받은 메시지를 무시하고, 두 값이 같으면 리더는 태그를 인증한다.
- 그 후 데이터베이스는 TID값에 TID^*을 저장하고, 랜덤값 RND을 이용하여 ID^*(=RND⊕ID)를 새롭게 갱신한 후, HID열에 새로운 $h(ID^*)$값을 저장한다. 기존 h(ID) 행의 AE (메시지 유실 복구 시 사용) 필드에 새로운 $h(ID^*)$값을 저장하고 새로 생성한 $h(ID^*)$ 행의 AE 필드에 기존의 h(ID)값을 저장한다. 이것은 메시지 유실 시에 사용한다.
- 마지막으로 LST의 값을 이전 세션에서 사용되었던 TID값으로 저장하고 (LST=TID), RND, $h(RND⊕TID^*⊕ID)$값을 태그에게 전송한다. 데이터를 전송받은 태그는 자신이 생성한 h(RND⊕TID⊕ID)값과 리더로부터 받은 $h(RND⊕TID^*⊕ID)$값을 비교하여, 두 값이 다르면 전송된 데이터가 조작되었거나, 잘못 전송되었다고 인식하여 작업을 중지한다. 그러나 두 값이 같으면, 태그는 리더를 인증하게 되고 랜덤값을 이용하여 ID를 새로운 ID^*로 갱신한다(ID^*=RND⊕ID). 마지막으로, 이 세션에서 사용되었던 TID값을 LST값으로 저장하여 (LST=TID), 데이터베이스와 LST값을 동기화 시킨다.

제안된 해쉬 기반 ID 변형 기법은 ID를 변형하여 RFID의 프라이버시 문제점을 해결하였으나 세션마다 ID 값이 변경되므로 하나의 데이터베이스에 의존적인 환경에만 적용가능하다.

■ Hash Chain based RFID scheme

Ohkubo 등이 제안한 기법으로 두 개의 해쉬 함수를 이용하여 태그의 정보를 보호하는 방법으로 EPC 코드에 적용하기 쉬운 기법이다[9]. 태그에 두 개의 해쉬 함수 G, $H:\{0,1\}^* \rightarrow \{0,1\}^L$가 사용된다. 우선, 태그 T는 초기 비밀값 $S_{T,1}$을 저장하고 있다. 태그 T는 리더의 질의에 해쉬 함수 H의 입력값으로 비밀 값 $S_{T,1}$값을 사용하여 다음 세션의 비밀 값을 생성한다. 그 후 그 비밀값에 G 함수를 적용한 결과 값을 리더에게 전송한다. 예를 들어 설명하면 다음과 같다.

- 만약 i번째 태그와 리더가 통신하는 경우, 이전 세션의 비밀값 $S_{T,i-1}$을 사용하여 해당 세션의 비밀값 $S_{T,i}=H(S_{T,i-1})$값을 생성한 후, G 해쉬 함수를 적용한 값 $a_{T,i}=G(S_{T,i})$을 전송한다. 그 이후 세션에서 태그는 리더의 질의에 대해서 $S_{T,i+1}=H(S_{T,i})$, $a_{T,i+1}=G(S_{T,i+1})$을 생성하여 전송한다.
- 데이터베이스는 전송한 값에 대응되는 태그를 찾기 위해서 저장된 태그의 ID와 비밀값 $S_{T,1}$에 해쉬 함수 H, G를 취하여 동일한 해쉬 값이 생성되는 ID를 찾아서 리더에게 전송한다. 리더는 전송 받은 값을 통해서 태그의 정보에 대해 알 수 있다.

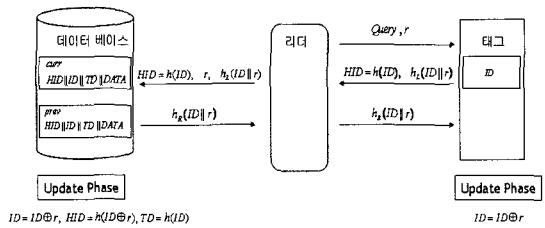
이 기법에서는 그 세션에서 해쉬 함수의 값이 노출 되더라도 해쉬 함수의 일방향 성질에 의해서 이전의 세션에 대한 정보를 얻을 수 없다. 이러한 성질로 인해 사용자의 프라이버시를 보호할 뿐만 아니라 사용자의 위치 정보를 보호할 수 있다. 반면, 이 기법에서는 데이터베이스의 해쉬 연산량이 태그의 수에 비례한다는 취약점을 갖는다.

■ Low cost RFID Authentication protocol (LCAP)

이수미 등에 의해 제안된 기법으로서 기존의 해쉬 기반 기법보다 더 안전하고, 저가형의 태그에 적합한 효율적인 기법이다[7]. 이 기법은 기존에 제안된 Randomized hash lock (RHLK) 기법에 비해 더 안전하며, HIDV (Hash based ID variation) 기법보다 적은 두 번의 해쉬 연산을 수행하기 때문에 효율적인 기법이다. 제안된 기법은 초기화 단계와 LCAP (low-cost authentication protocol) 단계로 구성되어 있다.

- 초기화 단계에서 태그와 리더는 데이터 필드에 HID, ID, TD, DATA에 대응되는 값들을 저장한다. HID는 데이터베이스에서 태그를 찾는데 사용할 값이고, TD는 메시지 유실 시에 이전의 메시지를 찾기 위해 사용될 것이다. ID는 태그 인증을 위한 정보이고 DATA에는 접근 가능한 태그의 정보가 저장되어 있다.

  데이터베이스는 전송되는 메시지의 유실 시 데이터 복구를 위해서 항상 두 개의 행 Curr, Prev을 유지하며 Prev행에는 이전의 세션의 HID와 ID가 저장되어 있으며, Curr행에서 현재 세션의 HID와 ID를 저장한다. 반면, Prev행에서의 TD에는 현재의 HaID, Curr행의 TD에는 이전의 HID를 저장한다. 만약 메시지가 유실된다면, 태그가 전송하는 값을 TD필드에서 찾아서 이전의 행을 찾아 간다.



h:해쉬, ⊕: XOR 비트 연산자, ||:메시지 연접, $h_{L(R)}(\ )$: 해쉬 함수 값의 1/2비트의 왼쪽(오른쪽) 비트

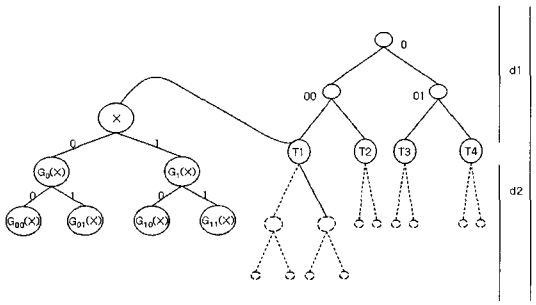
(그림 3) LCAP 프로토콜

- LCAP(low-cost authentication protocol)단계에서는 데이터베이스와 태그가 공유하고 있는 HID를 사용하여 태그의 정보를 인식하고 세션마다 새로운 랜덤값 r을 이용하여 생성한 값 $h(ID||r)$이 정확한지 확인함으로써 서로를 인증한다. 제안된 기법은 (그림 3)을 통해서 자세히 볼 수 있다.

■ Tree based RFID Authentication protocol

David에 의해 제안된 기법으로 태그 인증을 위해 Tree 형태의 인증 기법을 제안하였다[8]. 이 기법에서는 태그의 인증 가능한 트리의 높이 d 를 d1+d2로 설정한다. d1은 태그가 저장하고 있는 비밀값의 높이이고 d2 는 의사 난수에 의해서 생성될 값을 의미한다. 아래의 (그림 4)와

같이 태그 T1은 d1까지의 노드의 값을 저장하고 있으며, 그 이후의 d2에 해당하는 노드 값은 의사 난수 생성기를 통해서 유도해 낸다.



(그림 4) 트리 기반의 인증 프로토콜

제안된 기법에서 태그는 카운터를 비밀 값으로 유지하며 자신이 속한 높이에 해당하는 값을 전송하게 된다. 태그의 카운터가 d1보다 적은 경우에는 랜덤값 r을 생성하고 자신이 속한 높이까지의 해당 노드의 값과 의사 난수 함수를 이용하여 값을 전송한다.

만약 태그 T1이 카운터가 2라면 랜덤값 r을 선택하고 F(의사 난수) 함수를 사용하여 $F_{node0}(r)$, $F_{node00}(r)$을 생성한다. 태그는 리더에게 $(r, P) = (r, F_{node0}(r), F_{node00}(r))$을 전송하며, 리더는 그 값을 데이터베이스에 전송하고 그 값이 정확한 값인지에 대한 응답을 받는다. d2에 해당하는 노드 값들은 의사 난수 생성기 G를 사용하여 생성한다. 생성한 값들은 이전과 동일한 방법으로 F 함수에 결과 값을 전송한다. 이 기법은 이전의 기법들과 달리 리더는 데이터베이스로부터 비밀 값을 받고 그것을 사용하여 일정 기간 동안 데이터베이스에 접근 없이 자체적으로 태그를 인증 할 수도 있다는 점에서 권한 위임 기능을 제공한다.

3.2 재 암호화 기반 기법

RFID 시스템에서 리더의 질의에 태그가 매번 다른 값을 전송함으로써 사용자의 위치 정보가 노출되는 것을 막을 수 있다. 재-암호화 기법이란, 태그의 정보를 재-암호화하여, 리더의 질의에 대해서 항상 다른 값으로 응답하는 기법이다. 재-암호화 기법은 많은 연산량을 필요로 하기 때문에, 제한된 자원을 가진 태그가 수행하기 어렵다. 따라서 태그를 대신하여 데이터베이스나 리더 등을 사용하여 재-암호화 과정이 이루어진다.

■ Universal Re-encryption with a check and using one-time random values

Satio 등에 의해서 제안한 기법[6]으로 Universal 재-암호화 기법을 사용한다. Universal 재-암호화 기법이란, 재-암호화 과정이 일어날 때 공개키 없이 임의의 랜덤값을 사용하여 재-암호화가 이루어지는 기법이다. 하지만, 태그의 정보에 재-암호화 과정이 여러 번 일어나더라도, 단 한 번의 복호화 과정으로 원래의 메시지를 복원할 수 있다. 이 기법은 다음의 재-암호화 기법에 기반하며 그 과정은 키 생성, 암호화, 복호화, 재-암호화 4단계로 이루어진다.

- 키 생성 : 데이터베이스는 비밀키 x, 공개키 y ($y=g^x$)를 생성한다.
- 암호화 : 정당한 데이터베이스는 다음과 같이 태그의 정보(m)를 암호화하여 태그의 메모리에 안전하게 저장한다.
  $(C = [(\alpha_0, \beta_0); (\alpha_1, \beta_1)] = [(my^{k_0}, g^{k_0}); (y^{k_1}, g^{k_1})])$
- 복호화 : 리더의 질의를 받은 태그는 자신의 암호문 C를 데이터베이스에게 전송한다. 데이터베이스는 암호문 C에서 $m_1(m_1 = \alpha_1/\beta_1^x)$을 확인하고, m_1이 1이면, $m_0(m_0 = \alpha_0/\beta_0^x)$을 메시지로 받아들인다.
- 재-암호화 : 재-암호화 과정은 외부기기가 대신 수행하며, 태그로부터 전송받은 암호문을 변경하여 태그에게 전송한다. 태그는 데이터베이스로 저장하고 있는 one-time 랜덤값 $\triangle = \{(\alpha_1^{m_1}, \beta_1^{m_1}), (\alpha_1^{m_2}, \beta_1^{m_2}), ... (\alpha_1^{m_{2n}}, \beta_1^{m_{2n}})\}$ 과

자신의 암호문 C를 사용하여 다음과 같이 재- 암호화 값을 리더에게 전송한다.

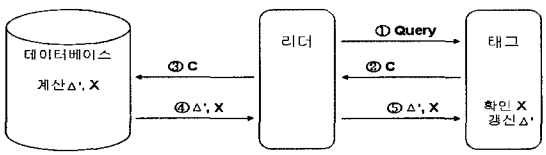
$$C' = [(\alpha_0', \beta_0'); (\alpha_1', \beta_1')] = [(\alpha_0\alpha_1^{m_1}, \beta_0\beta_1^{m_1}); (\alpha_1\alpha_1^{m_2}, \beta_1\beta_1^{m_2})]$$

- one-time 랜덤값 갱신 : 태그는 리더로부터 받은 one-time 랜덤값에 대해 다음과 같은 과정을 통해서 기존의 값을 갱신한다. 우선, 태그와 리더는 비밀 정보 S를 공유한다. 데이터베이스는 태그에게 새로운 one-time 랜덤값 Δ'과 X를 다음과 같이 생성하여 태그에 전송한다.

$\Delta' = \{(\alpha_1^{m_1'}, \beta_1^{m_1'}), (\alpha_1^{m_2'}, \beta_1^{m_2'}), \cdots, (\alpha_1^{m_{2n}'}, \beta_1^{m_{2n}'})\}$

, X=h(S, I, Δ')

태그는 새로 받은 값들을 이용하여 h(S, i, Δ')를 계산하고, 이 값이 데이터베이스로부터 받은 값 X와 동일한지 비교한다. 두 값이 같으면, 태그는 전송된 메시지가 공격자에 의해서 변조되지 않고, 정확하게 전송되었다고 인식하게 된다. 그래서 새로운 one-time 랜덤값 Δ'으로 기존의 랜덤값들을 갱신한다. One-time 랜덤값을 사용하는 프로토콜은 다음 (그림 5)와 같다.



(그림 5) one-time 랜덤값 사용하는 기법의 프로토콜

■ Privacy Protection in RFID-enabled Banknotes

이 기법은 Euro 화폐에 태그를 적용하여 불법 거래 시 화폐의 흐름을 추적하기 위해 제안된 기법이다[3]. 이 기법은 불법 거래 이외에는 재-암호화 기법을 이용하여 사용자의 프라이버시도 보호가 가능하다. Euro 화폐는 사용자의 프라이버시 보호를 위해 두 개의 계층(RF, Optical)으로 나뉜다. RF 계층은 어떤 리더라도 접근하여 데이터를 읽을 수 있다. Optical 계층은 중앙은행에서 보급하는 리더를 가진 상인만이 접근 가능하며 이 부분에 데이터를 읽은 리더만이 RF 계층에 재-암호화 과정을 수행할 수 있는 접근 권한 키를 얻게 된다.

중앙은행은 화폐의 고유번호 S를 선택하고 자신의 개인키로 서명값 ($\Sigma \leftarrow Sig(SK_B, [S \| den])$), 접근 권한 키 D(= $h(\Sigma)$)를 생성한다. 화폐에 S와 서명값 Σ를 태그의 Optical 계층에 쓴다. 태그는 리더로부터 질의를 받을 때마다, RF 계층의 C(= $Enc(PK_L, [S \| \Sigma], r)$)와 랜덤값 r을 전송한다. 정당한 리더는 Optical 계층에도 접근 가능하기 때문에 Optical 계층에서 얻은 S, Σ과 RF 계층에서 태그로부터 받은 r값과 화폐 위치 추적 기관의 공개키 PK_L을 사용하여 C를 생성한다. 상인은 생성한 C값과 태그로부터 받은 C값이 동일한지를 확인함으로써 위조지폐인지 아닌지를 판단한다. 만약 두 값이 동일하지 않을 경우, 상인은 화폐위치 추적 기관에 신고한다. 만약 리더가 생성한 값 C와 받은 값이 동일한 경우, 리더는 재-암호화 과정을 수행한다. 리더는 새로운 랜덤값 r'을 선택하고 새로운 C' (= $Enc(PK_L, [S \| \Sigma], r')$)을 생성하여 접근 가능한 키 값 D를 이용하여, RF 계층에 C'와 r'을 쓴다. 이러한 재-암호화 과정을 통해서 태그는 세션 마다 다른 값을 전송하며 사용자의 위치 정보를 보호한다. 그러나 만약 악의적인 상인이 화폐에 재-암호화 과정을 수행하지 않거나 시스템의 오류로 재-암호화 과정이 수행되기 전에 리더와 태그 사이의 통신이 끊길 경우, 태그는 일정한 기간 동안 고정된 값을 리더에게 전송하게 되고 사용자의 위치 추적이 가능하다는 문제점이 있다.

3.3 XOR 기반 기법

해쉬 기반과 재-암호화 기반의 기법들은 최소한의 연산만을 수행하는 태그가 사용되는 환경에 적용하기에는 적합하지 않다. XOR 기반의

기법은 해쉬 기반의 기법보다 더 단순한 비트 연산을 사용하여 RFID의 프라이버시를 보호하는 기법으로 최저가의 RFID 태그에 적용 가능한 기법이다.

■ Minimalist Cryptography (XOR based scheme)

Juels는 사용자의 프라이버시를 보호하며 최소한의 암호학적 함수를 사용하는 기법을 제안하였다[4]. 제안된 기법은 간단한 비트 연산인 XOR 연산을 사용한다. 제안된 기법은 XOR 연산을 사용하며, 리더로부터 랜덤한 값들을 받아서 그것을 이용하여 다음 세션에 사용될 값들을 갱신한다. 그것이 공격자가 태그를 추적하지 못하도록 하기 위한 방법이다.

우선, 태그와 데이터베이스는 동일한 랜덤값 테이블을 저장하고 있다. 그 값들의 변경된 값들을 확인함으로써 태그는 리더를 인증하고 리더는 태그를 인증하게 된다. 이 기법에서는 태그와 리더 사이의 통신을 공격자가 도청할 수 있는 횟수 m에 의존하여 제안된 기법의 안전성이 보장된다. 이 기법에서는 공격자가 리더로부터 전송되는 값을 2m보다 적게 도청 가능하다고 가정한다.

Juels 기법에서 태그는 비밀 값 k개를 저장한다. 비밀값은 $(\alpha_i, \beta_i, \gamma_i), 1 \leq i \leq k$로 구성되어 있다. 태그와 데이터베이스가 저장하고 있는 랜덤 값 테이블은 m개의 $\triangle_i = \{\delta_i^{(1)} (= (\triangle\alpha_i^{(1)}, \triangle\beta_i^{(1)}, \triangle\gamma_i^{(1)})), \ldots, \delta_i^{(m)}\}$, $1 \leq i \leq k$로 구성되어 있다. 태그는 리더의 질의에 α_d, $d \leftarrow (c \bmod k) + 1$ (c : 카운터, 처음에 0으로 초기화 되어 있는 값)에 대응되는 값을 리더에게 전송하고 리더는 데이터베이스에게 전송하며 데이터베이스는 받은 값과 관련된 β_d를 리더에게 전송한다. 리더는 β_d을 태그에게 전송하고 γ_d을 받고 데이터베이스에게 전송한다. 데이터베이스는 받은 값을 데이터베이스 테이블에서 확인한 후 리더가 태그에게 전송할 새로운 랜덤 값 테이블을 생성하여 전송하며 새로 생성된 랜덤 값 테이블은 $\widetilde{\triangle_i} = \{\tilde{\delta}_i^{(1)} (= (\triangle\tilde{\alpha}_i^{(1)}, \triangle\tilde{\beta}_i^{(1)}, \triangle\tilde{\gamma}_i^{(1)})), \ldots, \tilde{\delta}_i^{(m)}\}$, $1 \leq i \leq k$로 구성된다. 이 랜덤 값 테이블을 받아서 태그는 기존의 랜덤 값 테이블 갱신에 필요한 값을 생성한다. 우선 기존의 $\triangle_i = \{\delta_i^{(1)}, \ldots, \delta_i^{(m)}\}, 1 \leq i \leq k$ 값의 원소에 $\delta_i^{(j)} = \delta_i^{(j+1)}$, $1 \leq j \leq m-1$을 적용하고, 마지막 값은 $\delta_i^{(m)} = 0^{3\ell}$로 갱신한다. 리더로부터 받은 $\widetilde{\triangle_i} = \{\tilde{\delta}_i^{(1)} (= (\triangle\tilde{\alpha}_i^{(1)}, \triangle\tilde{\beta}_i^{(1)}, \triangle\tilde{\gamma}_i^{(1)})), \ldots, \tilde{\delta}_i^{(m)}\}$과 위의 과정에서 생성한 $\triangle_i = \{\delta_i^{(1)}, \ldots, \delta_i^{(m)}\}$, $1 \leq i \leq k$을 XOR 한다. 즉, $\delta_i^{(j)} = \delta_i^{(j)} \oplus \tilde{\delta}_i^{(j)}$, $1 \leq i \leq k, 1 \leq j \leq m$을 생성한다. 태그는 다음 세션에 이전 세션의 비밀 값 $(\alpha_i, \beta_i, \gamma_i)$에 $\delta_i^{(1)}$을 XOR 하여 새로운 랜덤 값 테이블을 생성한다. 이 랜덤 값 테이블의 값은 다음 세션에 사용된다.

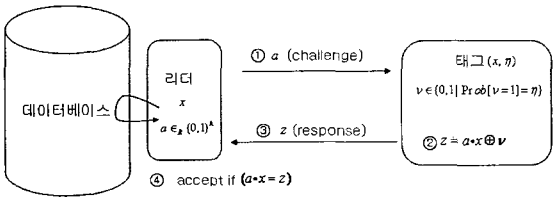
■ HB Authentication protocol(XOR based cheme)

최근에 Crypto 학회에 RFID 시스템의 프라이버시 보호에 대한 기법이 제안되었다[5]. 이 기법은 Juels에 의해 제안된 기법으로 1 비트로 상대방을 인증하는 기법이다. 제안된 기법은 HB 프로토콜이라 표기하며 과정은 다음과 같다.

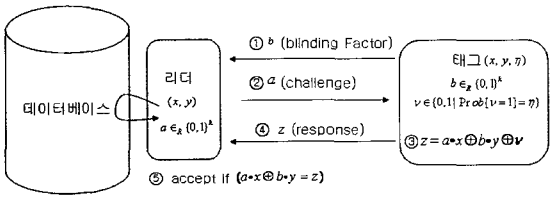
우선, RFID 태그와 리더 간에 비밀값 x를 공유한 상태에서 리더가 태그를 인증하게 된다. 태그가 리더에게 a 값을 전송하고 태그는 $z = a \cdot x$ 값을 생성하여 전송한다. 이 값을 생성하는 과정은 내적을 사용한다. 즉, $z = a_1 \cdots a_k \cdot x_1 \cdots x_k = a_1 \cdot x_1 + \cdots + a_k \cdot x_k$이다. 리더는 그 값을 받고 자신이 저장하고 있는 x값과 a값을 이용하여 생성한 $a \cdot x$값을 받은 z값과 같은지를 확인한다. 1 비트로 인증을 하기 때문에 r번 반복하여 정확성을 높인다. 하지만 이러한 경우에도 공격자가 a의 비트 길이 k번만큼 세션을 도청할 경우 비밀값 x에 대해 알 수 있

기 때문에 $\eta \in (0, \frac{1}{2})$라는 확률로 ν값을 XOR 하여 전송한다. 그 과정은 (그림 6)과 같다. 이 과정에서는 리더는 태그로부터 받은 $z = a \cdot x \oplus \nu$ 값의 정확성은 r번 반복하여 그 값이 $\eta \cdot r$보다 적게 틀린 경우 정당한 태그로 받아들인다.

위에 제안된 기법은 수동적인 공격자에 대해서 안전할 수 있으나 공격자가 a값을 자신에 유리한 값으로 선택하여 리더에게 전송한다면 응답값 z에서 x에 대한 값을 알아 낼 수 있다. 따라서 Jules는 능동적인 공격에 안전한 HB$^+$기법을 제안하였다. 이 기법은 리더와 태그 간에 추가적으로 y라고 하는 비밀값을 서로 저장하고 이전 기법과 달리 b라는 랜덤값을 태그가 전송하는 기법이다. 그 과정은 아래 (그림 7)과 같다.



(그림 6) HB 프로토콜



(그림 7) HB+ 인증 프로토콜

제안된 HB$^+$기법은 능동적인 공격에 안전하게 설계하기 위해서 b라고 하는 값을 태그가 선택하여 전송하도록 하였다. 그러므로 공격자가 자신에게 유리한 값 a를 생성하여 공격을 시도할지라도 b 값으로 인해 비밀값 y에 대한 정보를 얻을 수 없기 때문에 안전하다고 저자는 주장하고 있다. 하지만 제안된 기법은 1비트의 값으로 태그를 인증하는 것이기 때문에 다수의 태그를 관리하는 환경에서는 오류 발생의 확률이 많다. 그러므로 다수의 태그의 정보를 다루는 환경에서 사용하기에는 부적합하며 이 기법은 안전성 측면에서 취약성을 갖는다[1].

4. 결 론

RFID 기술은 비접촉식이라는 장점으로 바코드를 대체하여 사용될 수 있지만 사물 인식 과정에서 비접촉 RF 통신으로 데이터를 주고받을 수 있다는 점에서 사용자의 프라이버시 침해의 가능성을 갖는다. 이러한 RFID 기술의 프라이버시 침해에 대한 문제점은 RFID 기술을 실생활에 적용하는데 걸림돌이 되고 있다. 구체적인 예로, 미국의 세계 최대의 유통업체 월마트는 2004년에 월마트 매장에서 RFID 기술을 이용하여 판매현황 및 절도피해 등을 실시간으로 파악하는 매장관리시스템을 시험할 계획이라고 발표하였으나, 소비자 단체의 프라이버시 침해우려 등으로 인해 시험계획이 취소되었으며, 현재는 매장 내에서의 RFID 태그의 상품 적용 범위를 축소하여 시행할 계획이다.

이러한 문제점을 해결하기 위해 앞에서 언급한 것과 같이 RFID 정보보호를 위한 다양한 기법들이 제안되었다. 최근에 RFID 시스템에 관련되어서 발표되는 논문들의 내용은 RFID 태그의 분류에 따라 프라이버시 보호를 위해 적용 가능한 기법들을 제안하고 있다. RFID 태그는 전원 공급 방식에 따라서 크게 수동형과 능동형으로 나눌 수 있다. 능동형 RFID 태그는 내부에 암호화 알고리즘과 같은 복잡한 연산을 수행 가능한 반면, 수동형 RFID 태그는 태그 내부에 제한된 연산만 수행 가능하기 때문에 XOR 비트 연산과 같은 단순한 연산 수행이 가능하다. 현재는 RFID 태그를 바코드를 대체할 수 있을 만큼 저가형의 것으로 생산하여 실생활에 적용 가능하며 프라이버시를 보호하는 기법들에 대

해 관심을 갖고 활발히 연구하고 있다. 또한 미래의 유비쿼터스 환경에서도 적용 가능한 초소형의 RFID 시스템에 적합한 기법도 연구되어야 할 것이다.

참고문헌

[1] H. Gilbert, M. Robshaw and H. Sibert. An Active Attack Against HB^{+}-A provably Secure Lightweigh Authentication Prtocol. http://eprint.iacr.org/2005/237.

[2] D. Henrici and Paul Muller. Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. PerSec'04 at IEEE PerCom. pp. 149~153, 2004.

[3] A. Juels and R. Pappu. Squealing euros : Privacy protection in RFID-enabled banknotes, In proceedings of Financial Cryptography -FC'03, vol.2742 LNCS, pp.103-121, Sep 2003.

[4] A. Juels. Minimalist cryptography for Low-Cost RFID Tag, In The Fourth Internationl Conferecne on Security in Communication Networks-SCN 2004, vol. 3352 LNCS, pp. 149~164, Sep 2004.

[5] A. Juels. Authentication Pervasive Devices with Human Protocols. To appear Crypto 2005, Aug 2005.

[6] S. Junichiro, R. Jae-Cheol and S. Kouichi, Enhancing privacy of Universal Re-encryption scheme for RFID Tags, EUC 2004, Vol. 3207 LNCS, pp.879~890, Dec 2004.

[7] L. Su Mi, H. Young Ju, L. Dong Hoon and L. Jong In. Efficient Authentication for Low-Cost RFID systems. ICCSA05, vol. 3480 LNCS, pp.619~629, May 2005.

[8] D. Molnar, Andrea Soppera and David Wagner. A Scalabe, Delegatable Pseudonym protocol Enabling Ownership Transfer of RFID Tags. To appear SAC 2005, Aug 2005.

[9] M. Ohkubo, K. Suxuki and S. Kinoshita. Efficient Hash-Chain Based RFID Privacy Protection Scheme, Ubcomp2004 workshop.

[10] 표철식, 채종석, RFID 기술 및 표준화 동향, TTA저널, 제 95호. pp.37~47. 2004년.10월

[11] S. A. Weis, S. E. Sarma, S. A. Weis and D. W. Engels. Security and privacy Aspects of Low-Cost Radio Frequency Identification Systems. First International Conference on Security in Pervasive Computing, 2003. http://theory.lcs.mit.edu/sweis/spc-rfid.pdf.

저자약력

최 은 영

2001년 고려대학교 수학과 학사
2003년 고려대학교 정보보호대학원 공학석사
2004년~현재 고려대학교 정보보호대학원 박사과정
관심분야 : 암호 이론, 정보보호 프로토콜, RFID 정보보호

이 동 훈

1983년 고려대학교 경제학사
1987년 Oklahoma University 전산학 석사
1992년 Oklahoma University 전산학 박사
1993년~1997년 고려대학교 전산학과 조교수
1997년~2001년 고려대학교 전산학과 부교수
2001년~현재 고려대학교 정보보호대학원 교수
관심분야 : 정보보호 프로토콜, 계산이론, 암호이론, 네트워크 보안