RFID/USN에서 내부자공격에 대항하는 프라이버시 보호 프로토콜 설계

주태우○ 홍영식
동국대학교 컴퓨터공학과
{faldo○, hongys}@dongguk.edu

Design of Security and Privacy Protection Protocol Preventing Insider Attacks in RFID/USN

Tae-Woo Joo0, Young-Sik Hong
Department of Computer Engineering, Dongguk University

요 약

최근 급격히 발전하는 RFID(Radio Frequency Identification)나 USN(Ubiquitous Sensor Network)과 같은 무선환경은 태그(tag)와 리더(reader)간에 라디오 주파수를 이용하여 통신한다. 이러한 통신은 그 특성상 주파수 범위내의 다른 태그나 리더들 또한 이들의 통신내용을 들을 수 있다. 따라서 이렇게 도청된 정보는 악의적인 사용자에 의해 여러 가지 보안 공격을 야기할 수 있다. 반면 이러한 형태의 공격에 대해 대부분의 보안프로토콜은 외부의 공격에 주목하는 반면, 같은 알고리즘으로 통신하는 내부자의 공격, 특히 참여(entry)객체의 프라이버시정보는 이러한 프로토콜에서 보호되기 어렵다. 따라서 본 논문에서는 무선환경에서 최근 이슈가 되고 있는 불룸필터(bloom filter)를 이용하여 개인의 프라이버시 정보를 효과적으로 보호할 수 있는 기법을 제안하고 불룸필터를 확장 적용해서 그 성능을 개선하여 좀 더 효율적인 프라이버시 보호 기법을 설계하고자한다.

1. 서 론

'어디에나 존재한다.'와 '보이지 않는다.'는 개념을 중심 요소로 삼고 있는 유비쿼터스 컴퓨팅개념을 마크 와이저가 처음 제안하였다.[1] 그 이후, 유비쿼터스 컴퓨팅은 눈부신 발전을 거듭하여, 현재는 유선은 물론 적외선이나 초음파 또는 RFID와 같은 무선환경에서 사람이 장치를 인지하지 못하는 상황에서 실생활에 적용되고 있다.

유비쿼터스의 기본개념은 사용자가 컴퓨터나 네트워크를 인지하지 않은 상태에서도 장소에 구애받지 않고 자유롭게 네트워크에 접속하는 것을 의미한다. 의류, 가구, 자동차 등 일상생활 전반에 컴퓨터가 설비되어 이들이 서로 네트워크로 연결돼 연동하면서 인간이 가장 쾌적하게 생활할 수 있도록 지원하는 것이다.

유선과 무선을 통합한 유비쿼터스 컴퓨팅환경에서는 각 개인이나 장치들이 상호간 또는 새로운 장치와의 접속 시, ID나 비밀번호를 이용한 인증과정을 수반 하게 된다. 또한 필요에 따라 이러한 설비들은 많은 정보기술이 서로 융합되고 컨버전스(Convergence)하게 된다.

반면, 무선의 특성상 주파수범위 또는 통신영역 내에서는 누구나 주고받는 정보를 취득할 수 있다. 이런 맥락에서 비록 유비쿼터스 컴퓨팅이 인간생활을 편리하게 할 것으로 예상되고 있지만, 보호되지 않고 난무하는 정보들은 각 개인이나 장치의 프라이버시 또는 개별정보를 침해하여, 정보보호의 필요성을 부각시키는 사례가 발생하고 있다.

더욱이 최근에는 휴대폰과 개인정보단말기가 결합하여 스마트폰이라는 새로운 이동통신 수단으로 많이 사용되고 있어 더욱 개인의 프라이버시 등 정보보호가 요구되고 있다. 일부 특별한 스마트폰의 경우는 장치에 RFID칩이 추가되어 단거리 고대역폭(13.53MHz) 통신기술을 이용하고 NFC(Near Field Communication)를 지원하여 장치가 리더 또는 태그의 형태로 필요에 따라 자유롭게 이용할 수 있어 전자지불, 사용자 인증 등 다양한 분야에 이용되고 있다.[2]

이러한 모바일장치들은 기존의 RFID장비에 비해 높은 연산능력과 대용량의 저장장치들을 설비하고 있어 더욱 강력한 암호학적 보안 알고리즘을 적용할 수 있을 것으로 예상한다.

RFID/USN과 같은 환경에서 지금까지의 대부분의 연구는 허가되지 않은 사용자의 접근(Access)을 방지하는 주로 외부자(outsider)의 보안에 집중되어있는 반면, 허가된 사용자 사이에서 누가 현재의 세션에 참여하고 있는지를 인지할 수 있는 주요 정보를 보호하는 연구는 매우 부족한 것이 현실이다.

따라서 본 논문에서는 같은 알고리즘을 사용하는 내부자(Insider)간에도 세션 참여자의 정보를 취득하여 개인의 프라이버시를 침해 할 수 있는 주요 정보를 모호하게 하여 이러한 정보를 유추 또는 추출을 방지하고, 궁극적으로 개인의 프라이버시 정보를 보호하여 안전하고 향상된 유비쿼터스 컴퓨팅 환경을 실현하고자한다.

본 논문의 2장은 RFID/USN 환경에서의 보안요구사항과 기존의 연구를 면밀히 조사하고 소개하며 3장에서 개인이나 장비의 프라이버시 정보를 보호하는 효과적인 기법을 제안한다. 4장에서는 필수적인 보안요구사항과 필요한 가정들을 정의하고 각각에 따른 보안평가를 하여 제안하는 기법이 효과적임을 보이고, 끝으로 5장에서 결론 및 향후 연구 과제를 기술한다.

2. 기존의 연구

2.1 암호기술에 기반을 둔 보안프로토콜

RFID/USN과 같은 무선환경에서의 프라이버시 보호와 관련된 분야의 연구는 대부분 두 가지 카테고리로 구분되어진다.[3]

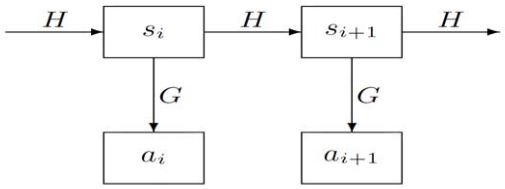
첫째는 물리적인 방법으로, 감추기(Hiding) 또는 차단(Blocking)하는 방법이다. 태그의 라디오채널을 방해하거나 아니면 정확히 해당되는 리더에게만 응답하는 방법으로 태그를 효과적으로 차단하는 방법이다.

두 번째는 소프트웨어적인 방법으로, 암호화(Encrypting) 또는 재기록(Rewriting)하는 방법이다. 태그 정보를 추적하는 것을 막기 위해 검증 안 된 리더에게는 전혀 의미가 없게 되는 값을 주거나 또는 그러한 데이터를 주기적으로 업데이트하는 방법이다.

본 논문에서는 후자의 방식에 초점을 맞춘다. 이렇게 소프트웨어적인 방법으로 Weis등은 암호학적으로 제어하는 간단한 형태의 프로토콜로서 "Hash lock"방식을 제안하였다.[4][6] 이것은 태그의 실제 값을 들어내지 않는 반면, 정적인 해쉬값이 추적가능하다는 문제를 안고 있다. 이러한 문제점으로 동 저자들이 대안으로 제안한 방법으로 "Randomized hash lock"이 있다.[5][6] 이 방식은 난수를 이용하여 리더의 추적을 효과적으로 차단하는 반면, 프로토콜단계에서 실제ID의 송출로 이전단계의 값을 유추할 수 있는 취약점을 갖는다.[3]

좀 더 발전된 형태의 프로토콜로 Hash-chain을 이용해서, 검증을 마치면 매번 결과를 상호 업데이트하는 방식이 Ohkobu등에 의해 제안되었다.[7]

기본구조는 그림1과 같이 두 개의 해쉬함수(G, H)를 이용하여 태그의 응답으로는 $a_i = G(s_i)$로 하고, 자신의 비밀을 새롭게 $s_{i+1} = H(s_i)$로 갱신하는 방식이다.

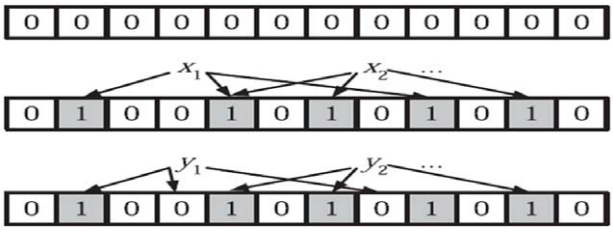


[그림1] Ohkobu's Hash-chain scheme

이 방식은 태그의 비밀을 유지하는 데 있어 논리적으로 가장 진보된 형태이고 태그의 전방향보안(forward security)을 효과적으로 지원한다. 반면 데이터베이스 서버에서 m개의 모든 태그에 대한 시드 값(1≤t≤m)과 hash-chain(1≤i≤n)에 대해 일치하는 $a_i^{'} = a_i$를 찾기 위해 통상적으로 $\frac{m \times n}{2}$번의 해쉬연산을 수행해야하는 overhead 문제점과 재전송공격(Replay Attack)에 취약성을 갖는 단점이 있다.[8]

2.2 불룸필터의 보안적용

불룸필터는 주어진 원소가 어떤 집합에 속하는지 여부를 검사하는데 사용할 수 있는 공간과 시간에 매우 효과적인 자료구조로 1970년에 Burton H. Bloom이 제안했다.[9] 이러한 불룸필터는 일방향성을 갖는 해쉬함수를 이용하기 때문에 항상 일정한 값을 가리키는 인덱스(index) 기능을 갖는다. 다만 여기서 잘못된 값이 대입되어도 참값을 가리키는 오류의 일종으로 긍정 오류(false positive) 특성을 가지고 있다.



[그림2] 불룸필터의 일반적 예

이러한 불룸필터의 기본 구조는 그림2와 같으며, 다음과 같이 정의된다.

- 불룸필터는 n개의 요소를 갖는 set S={x_1,x_2,..., x_n}을 표현 하기위해 m개의 bit 배열에 의해 기술되고 모든 배열은 초기 값을 0으로 한다.
- 불룸필터는 {1,2...,m}의 영역을 갖는 해쉬함수(h_1,2...,h_k) k개의 독립적인 해쉬함수를 사용한다.
- 수학적 편의를 위해, 이러한 해쉬함수들이 {1,2...,m}의 영역에 대해 랜덤하게 논리영역내의 각 아이템을 매핑 한다고 일반적 가정을 한다.

동작원리는 다음과 같다.

1. 각 요소 x ∈ S이며, $h_i(x)$의 결과 값은 임의의 배열에 1로 세트된다. (1≤i≤ k)
   - 하나의 배열에 여러 번 세트될 수 있는데, 오직 한번 1로 세트되면 더 이상 영향을 받지 않는다.
2. y 가 S에 속하는지를 검증하기 위해 모든 $h_i(y)$가 배열에 1로 세트되었는지를 검증한다.
   - 만약에 모든 $h_i(y)$ 가 1이 아니면, y 는 S의 멤버가 아니다.
   - 만약에 모든 $h_i(y)$ 가 1이면 비록 확률적으로 아닐 수 있지만 y 가 S에 있다고 가정한다(false positive).

이러한 불룸필터의 특성을 이용해서 프라이버시 보호 등 보안에 적용하려는 많은 시도들이 있어왔다. 특히 불룸필터에서 여러 개의 해쉬함수의 사용에 드는 비용을 줄이기 위한 노력의 일환으로 수학적으로 검증한 연구가 있다.[10]

수식을 살펴보면 표준 불룸필터에서 임의의 요소가 사이즈 m인 필터에 세트될 확률은 1/m이다. 따라서 n개의 요소가 k개의 해쉬함수를 통해 필터에 대입 후 1로 set 되지 않을 확률(P)은 식(1)이 된다.

$$P = (1 - \frac{1}{m})^{kn} \approx e^{-kn/m} \quad \text{----------} \quad (1)$$

따라서 이러한 조건에서의 False Positive일 확률(P_f)은 식(2)가 된다.

$$P_f = (1 - (1 - \frac{1}{m})^{kn})^k \quad \text{----------} \quad (2)$$

상기의 식(2)에 식(1)을 대입하면 식(2)는 다음의 식(3)으로 유도된다.

$$P_f = (1 - e^{-kn/m})^k \quad \text{----------} \quad (3)$$

만약 사이즈가 m인 필터에 k개의 해쉬함수를 통하지 않고 단순히 k개로 분해해서 필터에 대입한다고 가정하면 여전히 특별한 배열이 0으로 남을 확률(P')은 앞서의 식(1)에서 식(4)로 간단히 유추된다.

$$P' = (1 - \frac{k}{m})^n \approx e^{-kn/m} \quad \text{----------} \quad (4)$$

따라서 k≥1이면, $(1 - \frac{k}{m})^n \leq (1 - \frac{1}{m})^{kn}$이 성립되며, 이것은 본래의 불룸필터의 성능에 $O(\frac{1}{m})$로 근접한다.

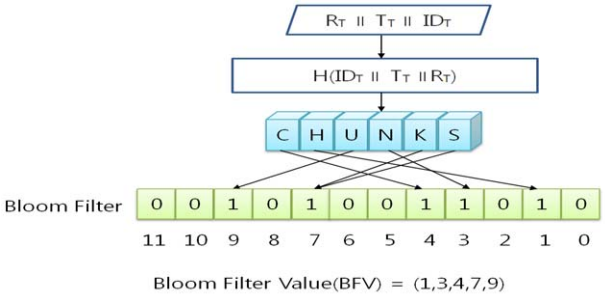
이렇게 k개의 해쉬함수대신 k개의 조각으로 분리해서 대입하는 기법은 여러 개의 장점을 갖는다.

첫째로, 이것은 해쉬함수의 저장 공간 및 거기에 따르는 연산을 줄여줌으로 인해 RFID태그의 부족한 메모리 공간과 연산능력에 여유를 줄 수 있다.

둘째로, 해쉬한 값을 여러 개의 조각으로 분리해서 대입하면, 추후에 고도의 능력을 가진 공격자가 설령 필터 값을 해석해 낸다 하더라도 결국 해쉬 값만을 얻을 수 있기에 본래의 비밀(secret)을 효과적으로 보호하게 되는 장점을 갖는다.

3. 제안하는 프라이버시 보호기법

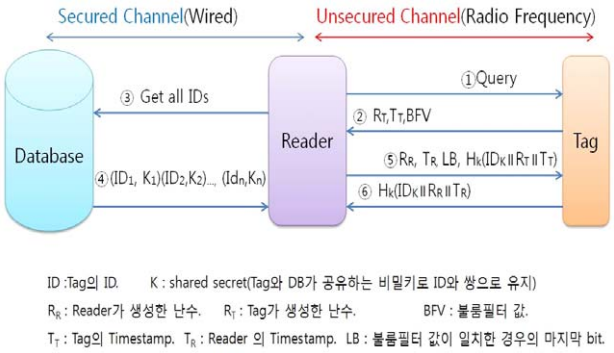
본 연구에 사용되는 불룸필터는 태그의 저장 공간 및 연산 효율성을 위해 여러 개의 해쉬함수를 이용하는 것을 피하고 하나의 해쉬함수를 사용한다. 또한 보안성을 강화하기위해 한번 해쉬 후 여러 개의 조각으로 분리하여 각각을 불룸필터에 대입하는 형태를 취한다. 연구에 사용되는 불룸필터구조는 그림 3과와 같다.



[그림3] Bloom Filter의 사용 예

불룸필터에서 나온 값(Bloom Filter Value : BFV)은 배열(1,3,4,7,9)을 가리키는 bit로 이것은 태그의 ID_T와 태그가 생성한 난수 R_T 그리고 태그의 Timestamp T_T를 연접하여 해쉬한 값을 여러 개의 조각으로 분할하여 각각을 불룸필터내의 배열에 1로 세트한 값이다.

본 연구에 이용되는 시스템의 프로토콜은 그림 4와 같다.



ID :Tag의 ID. K : shared secret(Tag와 DB가 공유하는 비밀키로 ID와 쌍으로 유지)
R_R : Reader가 생성한 난수. R_T : Tag가 생성한 난수. BFV : 불룸필터 값.
T_T : Tag의 Timestamp. T_R : Reader 의 Timestamp. LB : 불룸필터 값이 일치한 경우의 마지막 bit.

[그림4] 제안프로토콜

① 리더의 query

② 태그는 난수(R_T)와 Timestamp(T_T)를 생성해서 자신의 ID와 연접 후 불룸필터 값[BFV = $H(R_T \| T_T \| ID_T)$]을 구하고 난수와 Timestamp를 불룸필터 값과 같이 리더에 보낸다. [R_T,T_T,BFV]

③ 리더는 수신된 태그의 정보들을 데이터베이스에 보내 일치하는 값을 보내줄 것을 요청한다.

④ 리더에게서 받은 태그의 정보로 자신이 보관하고 있는 모든 ID에 대해 수신된 R_T 와T_T를 이용 불룸필터에 대입하여 일치하는 값을 찾아 일치하는 ID_K와 쌍으로 보관한 키 값 K_K 그리고 일치한 BFV의 마지막비트 LB를 리더에 보낸다.

⑤ 키 값과 ID를 받은 리더는 태그가 생성한 이전의 난수 R_T와 Timestamp T_T 그리고 ID_K와 연접 후, 키 값K로 해쉬한 후 그 값과 같이 난수(R_R)와 Timestamp(T_R)를 생성하여 같이 LB와 함께 태그에 보낸다.[R_R, T_R, LB, $H_k(ID_K \| R_T \| T_T)$]

⑥ 정보를 수신한 태그는 자신이 ID의 실제 소유자임을 자신의 ID와 이전단계에서 리더가 생성한 난수(R_R)와 Timestamp(T_R)를 연접한 후 키 값 K로 해쉬하여 그 값을 보냄으로서 증명한다.

4. 보안 평가 및 분석

4.1 보안 요구사항 및 가정

RFID/USN에서의 프라이버시 보호를 위한 보안 요구사항은 다음과 같이 크게 3가지로 귀착되며, 이러한 사항들이 보장되어야한다.

-기밀성(Confidentiality) : 태그의 정보는 오직 정당한 사용자에 의해서만 읽혀져야 한다. 즉, 태그의 응답이 공격자에게 의미가 없어야한다. 도청이나 가로채기 공격에 대한 저항성으로 대부분의 경우 기밀성은 대칭키나 비 대칭키를 이용 보호하거나 메타정보를 이용한다.

-익명성(Anonymity) : 불구분성과 혼용되는 의미로 태그의 식별정보는 유추되거나 드러나서는 안 된다. 태그의 추적과 관련된 공격에 대한 저항으로 주로 해쉬함수나 난수를 이용 보호한다.

-내부자(Insider)보안 : 같은 멤버 또는 내부자간에는 태그의 식별정보를 유추하기가 쉽다. 이러한 내부자간의 추적에도 강하게 저항할 수 있어야한다.

제안된 프로토콜에서 리더와 태그사이에는 무선으로 통신이 이루어져 누구나 도청이 가능하다. 반면, 리더와 데이터베이스는 신뢰된(trusted) 객체로서 상호간에는 유선통신망으로 안전한 방법으로 통신한다고 가정한다.

4.2 제안프로토콜 보안분석

- 기밀성분석 : 기 제안된 프로토콜의 ② 단계에서 외부 공격자는 태그의 ID를 알지 못한다. 따라서 공격자는 불룸필터 값[BFV = $H(R_T \| T_T \| ID_T)$]을 생성할 수 없다. 만일 공격자가 정당한 태그의 전송정보를 저장한 후 재전송하는 재전송공격(Replay Attack)을 시도하는 경우 공격자는 합당한 Timestamp를 생성하여도 데이터베이스에서 일치되는 올바른 불룸필터 값을 생성할 수 없다. 따라서 기밀성을 보장받는다.
- 익명성 분석: 태그의 응답은 난수와 Timestamp 그리고 불룸필터의 사용으로 매 세션마다의 값이 변하여 누구의 것인지를 구별할 수 없다. 따라서 익명성을 보장받으며, 추적을 피한다.
- 내부자 보안 분석 : 내부자간에는 ID를 쉽게 유추 할 수도 있다. 이러한 경우 공격자는 남의 ID를 도용, 가장하여 리더에 응답할 수 있다. 반면, 데이터베이스와 태그가 공유하는 비밀(secret)은 드러나지 않는다. 따라서 이러한 위장의 경우 ⑤단계에서 리더의 응답 R -> T [R_R,T_R,LB, H_K(IDi || R_T||T_T)] 을 해석하지 못하며, 최종 ⑥단계에서 정당한 값 T -> R [R_R ,T_R, $H_K(ID_T \| R_R \| T_R)$]을 생성할 수 없어 검증을 통과할 수 없다. 따라서 제안한 프로토콜은 내부자의 공격에도 강하게 대항한다.

4.3 False Positive에 의한 Overhead 분석

앞서 기술한 바와 같이 본 논문에 이용된 Bloom Filter의 False Positive는 각각의 요소를 k개로 분할하여 필터에 대입함으로 식(5)로 유도된다.

$$P' = (1-(1-\frac{k}{m})^n)^k \approx (1-e^{-kn/m})^k \text{ ------ } (5)$$

이러한 에러는 불룸필터의 사용으로 인한 불가결한

일이다.

물론 이러한 에러는 프로토콜 ⑤와 ⑥의 단계에서 걸러져서 초기상태로 되돌아가질 것이나, 통신상의 부하를 야기하게 된다. 따라서 이러한 에러를 최소화할 필요가 있다.

상기 식(5)의 우변을 최소화할 수 있는 k값은 식(6)과 같다.

$$k = \ln 2 \times m/n \quad \text{----------} \quad (6)$$

상기 식(6)을 만족하는 경우의 False Positive는 식(7)이된다.

$$P_f^{'} = (1-\frac{1}{2})^k = 2^{-k} \quad \text{----------} \quad (7)$$

따라서 필터에 대입되는 요소의 수를 필터크기의 1/2로 하고 분할되는 수(k)를 증가 시키는 경우 식(7)에서와 같이 $P_f^{'} = 2^{-k}$에 의해 현저히 줄일 수 있다.

5. 결론

본 논문에서 기여하는 바는 단순히 ID를 해쉬해서 사용하는 meta ID에서 발전하여, False Positive가 있는 Bloom Filter라는 자료구조를 이용하는 데 있다. 이러한 구조는 태그의 응답을 모호하게 만든다. 따라서 ID를 유추할 수 있는 내부자의 공격에 대해서도 추적을 피하여, 프라이버시를 보장한다.

또한 제안한 프로토콜에 대해 기밀성 및 익명성 그리고 내부자 보안에 대해 각각의 경우에 대한 공격모델을 산정하고 검증하여 제안한 프로토콜이 효과적이고 안전함을 보였다.

비록 데이터베이스에서 리스트내의 모든 ID와 키 쌍을 연산해야하는 과부하 문제가 존재하며, 연산 효율성을 개선해야하는 문제가 있지만 이러한 문제들은 향후 RFID/USN 환경에서 모바일 RFID로의 발전으로 이동장치의 연산능력 향상과 기억공간 확대로 점 차 줄어들 것으로 예상한다.

6. 참고문헌

[1] Weiser, M. “The computer for the 21st century”, Scientific American 265. pp. 94-104. September 1991.

[2] http://www.nokia.com/nokia/0,,55738,00.html

[3] Marc Langheinrich. "A survey of RFID privacy approaches", Personal and Ubiquitous Computing, October 2008. Online First Edition, available from http://www.springerlink.com/content/p71246k75029v715/.

[4] S.E. Sarma. Weis, and D.W. Engels, "RFID systems, Seucrity and Privacy Implications", White Paper MIT-AUTOID-WH-014, AUTO-ID CENTER, 2002

[5] S.A. Weis, "Security and Privacy in Radio Frequency Identification Devices", MS Thesis, MIT, May 2003

[6] S. Weis et al., “Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems,”Security and Pervasive Computing 2003, LNCS 2802, pp.201-212. 2003.

[7] M. Ohkobu et al., “Cryptographic Approach to “Privacy-Friendly Tags””, *RFID Privacy Workshop*, MIT, MA, USA, November 2003.

[8] G. Avoine, E. Dysli, and P. Oechslin. Reducing time complexity in RFID systems. In B. Preneel and S. Tavares, editors, *Selected Areas in Cryptography — SAC 2005*, Lecture Notes in Computer Science Springer-Verlag, 2005.

[9] B. Bloom, "Space/Time Trade-offs in Hash Coding with Allowable Errors," Communications of ACM, pp. 422-426, 1970.

[10] A. Broder and M. Mitzenmacher, "Network Applications of Bloom Filters: A Survey," Internet Mathematics, vol. 1, 2005.