RFID 환경에서 보안 통신을 위한 안전한 인증 방안에 관한 연구

고 훈* · 김배현** · 권문택***

요 약

네트워크와 무선통신의 발달에 힘입어 유비쿼터스 시대가 도래하고 있다. 유비쿼터스 컴퓨팅에서의 시큐리티 문제는 인터넷 시대의 시큐리티 문제보다 복잡하며 공격이 용이하나 대책 수립은 현재로서는 굉장히 초보수준이다. 유비쿼터스 컴퓨팅 환경은 기존의 보안 기술로 적용하기에는 많은 다른점을 가지고 있다. Confidence level이 서로 다른 인증 방식이 필요하거나 또한 사용자의 위치에 대한 프라이버시도 만족해야 하는 인증 방식이 필요하다. 기존의 대표적인 인증 방식인 kerberos 인증 방식은 사용 범위가 지정 워크스테이션으로 국한되거나 클라이언트의 안전한 환경을 가정하여 이용되지만 유비쿼터스 컴퓨팅 환경에서는 이러한 조건을 제공하기가 어렵기 때문에 새로운 보안메커니즘이 필요하다. 또한 유비쿼터스 컴퓨팅 환경은 무선전송이나 이동통신에 크게 의존하게 되므로 이들 통신 구간에 대한 보안이 중요한 문제로 대두되고 있다. 이에 본 논문에서는 무선 인증서를 이용하여 사용자 인증 및 기밀성 제공을 위한 유비쿼터스 환경의 SSL을 적용 방안을 연구하여 실험을 통하여 결과를 증명하고자 한다. 즉, 유비쿼터스 환경에서 기밀성 및 인증을 제공하는 기법을 제안한다.

A Study on Safe Authentication Method for Security Communication in RFID Environment

Hoon Ko* · Baehyun Kim** · Moon Taek Kwon***

ABSTRACT

Ubiquitous computing environment has a lot of different things as for applying existing security technical. It needs authentication method which is different kinks of confidence level or which satisfies for privacy of user's position. Using range localizes appoint workstation or it uses assumption which is satify environment of client in Kerberos authentication method which is representation of existing authentication method but it needs new security mechanism because it is difficult to offer the condition in ubiquitous computing environment. This paper want to prove the result which is authentication method for user authentication and offering security which are using wireless certificate from experiment in ubiquitous environment. Then I propose method which is offering security and authentication in ubiquitous environment.

Key words : Ubiquitous, Authentication, Security

* 대진대학교 컴퓨터공학과

** 한신대학교 정보통신학과

*** 경희대학교 테크노경영대학원

1. 서 론

네트워크와 무선통신의 발달에 힘입어 유비쿼터스 시대가 도래하고 있다. 유비쿼터스 컴퓨팅에서의 시큐리티 문제는 인터넷시대의 시큐리티 문제보다 복잡하며 공격이 용이하나 대책 수립은 현재로서는 초보수준에 불과하다.

유비쿼터스 컴퓨팅 환경[1, 2]은 컴퓨터나 서로 이질적인 기기들이 일상생활 속에 스며들어 있어서 사용자가 자신이 인식하지 못하는 사이에 여러 기기들의 도움을 받을 수 있으며, 기존의 기기 조작의 혼란으로부터 벗어날 수 있게 해준다.

또한 응용은 사용자의 개입 없이도 사용자의 활동을 지원하기 위해 이용 가능한 자원과 서비스를 효과적으로 이용 할 수 있어야 한다. 그리고 컨텍스트 인식과 더불어 유비쿼터스 컴퓨팅 실현의 필수 요소는 보안이다. 유비쿼터스 환경에서 자원과 서비스는 응용이 실행되는 지역에 있을 수도 있지만 대게는 물리적으로 분산된 환경 안에 존재하게 된다. 따라서 유비쿼터스 환경은 응용이 실행되는 환경에서의 보안 뿐만 아니라 분산 환경에서의 자원과 서비스에 대한 보안이 필수적으로 고려되어야 한다.

결국, 유비쿼터스 환경의 보안기술은 기존의 보안기술로 적용하기에는 많은 다른 점을 가지고 있다. Confidence level이 서로 다른 인증 방식이 필요하거나 또한 사용자의 위치에 대한 프라이버시도 만족해야 하는 인증 방식이 필요하다. 유비쿼터스의 보안서비스에는 기밀성, 무결성, 가용성, 익명성, 부인방지 방지 등이 있다.

본 연구에서는 유비쿼터스 컴퓨팅을 위한 자원과 서비스 사용 자격을 부여하기 위해서 컴퓨터의 특정 값을 이용하여 전달하여 해당 값의 무결성을 판단하여 자원 및 서비스의 사용 허용 여부를 결정하도록 한다. 2장은 위협요소 및 보안 요구사항에 대해서 설명하고, 3장에서는 기존의 방법을 설명한다. 그리고 4장에서는 본 논문에서 제안하는 유비쿼터스 환경에서 안전한 인증방법을 설명하고, 5장에서는 2장에서 기술한 위협요소에 대해서 안전성을 분석한다. 마지막으로 6장에서는 결론을 맺도록 한다.

2. 위협요소 및 보안 요구사항

이 장에서는 유비쿼터스 컴퓨팅 환경에서 위협요소 및 보안요구사항을 기술한다[3].

유비쿼터스 컴퓨팅에서 발생할 수 있는 주요 공격방법은 아래와 같다.

- Eavesdropping(도청) : 태그와 리더간의 통신 방식은 무선이므로 공격자는 큰 노력 없이도 통신내용을 엿들을 수 있다.
- Traffic Analysis(통신 분석) : 공격자는 도청을 통하여 얻은 내용을 분석하여 리더의 질의에 대한 태그의 응답을 예측할 수 있다.
- Location Tracking(위치트래킹) : 공격자가 공격자 혹은 악의적인 리더가 태그의 위치변화를 감지함으로써 태그 소유자의 이동경로를 파악하는 방법으로 사용자의 프라이버시를 침해하는 유형이다.
- Spoofing(스푸핑) : 정당하지 않은 개체를 정당한 것처럼 속여 인증과정을 통과하는 방법이다.
- Message loss(메시지 유실) : 공격자의 고의 또는 시스템상의 문제로 인해 태그와 리더간에 주고받는 통신내용의 일부가 유실될 수 있다.
- Denial of Service(서비스 거부) : 시스템이 정상적으로 작동하지 못하도록 하기 위해 특정 주파수를 갖는 방해전파를 방출하는 공격방법이다.
- Physical Attack(물리적 공격) : 칩에 탬퍼 방어 패키지를 제거하여 직접 IC Chip에 프로브

를 해 중요정보를 해석하는 프로브 공격이나 통신장비 및 컴퓨터에서 방출되는 전자파를 분석하여 이들 사이에 송수신되는 내용을 도청할 수 있는 TEM PEST 공격에 취약하다.

위에서 설명한 위협요소들은 인증 처리를 하면 대부분 안전한 사용이 가능하나 Physical Attack 공격기법의 경우는 시스템의 특성상 불가능 하다.

아래에 설명하는 내용은 유비쿼터스 환경에서 인증시스템을 설계하기 위한 고려사항이다.

- 유비쿼터스 컴퓨팅 환경에서 사용자는 보안 시스템이 어떻게 동작하는지 신경 쓰지 않아도 되고, 보안 시스템에 의해 방해 받아서도 안된다.
- 보안 구조는 시스템 정책, 컨텍스트 정보, 환경 상황, 시간적 상황에 따라서 각각 다른 보안레벨을 제공할 수 있어야 한다.
- 컨텍스트와 결합하여 동적인 보안을 제공하여야 한다.
- 보안 시스템은 유연하고 적응가능하고, 특정 요구에 맞춤 가능해야 한다.
- 통신상의 내용을 인증 받지 않은 사용자는 내용을 볼 수 없어야 한다.
- 위치크래킹을 방지하기 위해서 데이터베이스와 리더이외의 개체에게는 태그의 이동경로를 파악할 수 있는 어떠한 정보도 제공해서는 안된다.
- 스푸핑 공격에 안전하기 위해 상대의 질의에 대한 인증을 처리해야 한다.
- 유비쿼터스 컴퓨팅의 특성상 인증에 필요한 계산 양과 저장 공간을 최소화해야 한다.

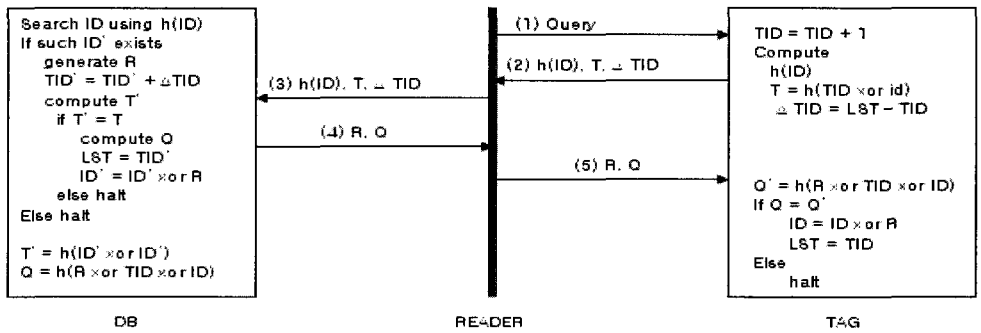
이러한 보안요구사항들이 설계시에 반영되어야만 위에서 설명한 위협요소로부터 안전한 유비쿼터스 컴퓨팅을 실현할 수 있다.

3. 기존의 인증 방법

기존에 제안된 인증 방법은 Henrici and Muller [4]가 제안한 해쉬기반 인증 방법이 있다(그림 1).

이 방법은 해쉬에 기반하여 ID를 갱신함으로써 위치트래킹 공격을 방지하는 프로토콜이다. 상품제조자는 h(ID), ID, TID, LST, AE를 저장할 수 있는 데이터베이스를 부착하고 태그에는 ID와 TID, LST를 저장한다. 질의를 받은 태그는 TID를 1 증가시키고 h(ID), T=h(TID xor ID), △TID를 계산하여 리더에게 전송한다.

데이터베이스는 h(ID)로 ID를 검색하여 해당 TID에 △TID를 더하여 T′를 계산한다.



(그림 1) 해쉬 기반의 인증 프로토콜

(그림 1)에서 (3)의 T와 T'가 일치하면 데이터베이스는 Q를 계산하여 전송하고 ID를 갱신하기 위해 랜덤하게 생성한 R과 xor 연산을 수행한다. (5)를 받은 태그 역시 Q'를 계산하여 Q와 일치할 경우 자신의 ID를 갱신하게 된다. AE는 이전 ID에 대한 정보를 가짐으로써 시스템상의 문제 또는 공격자의 고의로 인한 메시지의 유실에 안전하도록 하였다.

그러나 이 방법은 인증이 완료될 경우 ID가 갱신되므로 위치트래킹 공격에 안전한 듯 보이지만 태그와 데이터베이스 사이에 정상적이지 않은 인증의 경우, 즉 공격자가 공격의 목적으로 태그에게 질의를 하는 경우, 태그는 항상 동일한 h(ID)를 응답하므로 공격자는 태그의 위치를 트래킹 할 수 있다.

또한 스푸핑 공격에도 안전하지 못한데 공격자는 질의를 통해 (2)를 얻어낼 수 있으며 태그가 정상적인 인증세션을 열기 이전에 데이터베이스와의 세션에서 (2)를 전송하게 되면 데이터베이스는 공격자를 정당한 태그로 인증할 수밖에 없게 된다.

그리고 공격자가 세션 중간에서 리더가 태그에게 전송하는 (5)의 값에서 R을 연속된 0으로 이루어진 문자열로 주고 Q 대신 T를 전송하면 태그는 에러를 감지하지 못하며 ID를 ID xor 0으로 갱신하므로 다음 인증 시, 서버는 h(ID)로 기존 ID 정보는 찾을 수 있으나 태그와 데이터베이스에 저장된 기존 ID에 대한 LST가 일치하지 않으므로 태그는 인증을 받지 못하게 되는 단점이 있다.

다른 방법은 READER가 의사난수 생성기를 이용하여 랜덤값 S를 생성하여 태그에게 먼저 질의를 하는 방법이다[5]. 그러나 이러한 방법을 이용할 경우 제 3자가 마치 READER인 것처럼 태그에게 질의를 하면 태그는 이를 정당한 사용자인지 아닌지 파악 할 수 없는 단점이 있다.

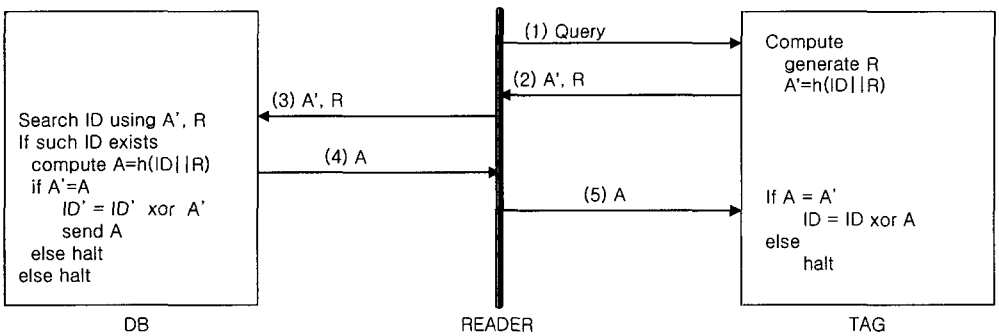
물론 이러한 단점을 해결하기 위한 몇 가지의 진보된 방법이 제안되었으나 원천적인 문제를 해결하지는 못하였다.

4. 안전한 인증 방법

제안하는 방법은 기존의 문제점인 스푸핑 공격에 대해 안전하고, 태그에서 수행하는 연산횟수, 즉 기존의 2번의 해쉬 함수 횟수를 1번으로 줄인 방법을 제안하였다(그림 2).

[Notation]

ID : 태그의 고유 식별자
h : 해쉬 함수
‖ : 문자열 연접 연산
xor : Exclusive or 연산
R : 랜덤값



(그림 2) 인증 방법

이 기법은 향상된 해쉬 기반 ID 변형 프로토콜 기법과 유사하다[5].

그러나 [5]에서 제안하는 READER가 인증을 위한 특정 값을 생성해서 전송한다는 것은 위에서 man in the middle attack에 취약하다.

그래서 랜덤값 R를 생성하는 주체가 READER가 아닌 TAG로 변경시켰다.

먼저 태그는 의사난수생성기를 이용하여 랜덤값 R를 생성한다. 그리고 A′=h(ID||R)를 생성한 다음 A′와 R를 READER를 통해 DB에 전송하게 된다.

DB는 A′와 R를 이용해서 ID를 검색하게 되고, A=h(ID||R)를 생성하게 된다. A와 A′를 비교하여 일치할 경우 정당한 태그로 인증하고 ID를 A′로 xor하여 갱신한 후, A를 태그에 전송한다.

태그는 A와 A′를 비교하여 일치할 경우 ID를 A와 xor를 수행한다.

이렇게 처리함으로써 서로간의 인증을 마치게 된다.

```
[STEP 1] query to TAG;                  /*Reader*/
[STEP 2] generate R;                    /*Tag*/
         compute A'=h(ID || R);
         send (A', R) to READER;
[STEP 3] bypass to DB;                  /*Reader*/
[STEP 4] search ID using (A', R);       /*DB */
         if such ID exist
         compute A=h(ID || R);
         if A'=A
         ID'=ID' xor A';
         send A to READER;
[STEP 5] bypass to TAG;                 /* Reader */
[STEP 6] if A=A' then ID=ID xor A;/* Tag */
```

5. 안전성 분석

지금까지 제안한 인증방법을 분석하면, 먼저 랜덤값 R을 READER가 생성하면서 발생될 수 있는 문제인 man in the middle attack에 안전하다. 그리고 TAG가 만드는 R을 이용하기 때문에 제 3자는 R을 생성할 수 없다. 따라서 [4]에서 발생할 수 있는 스푸핑 공격에 안전하며, 기존에 해쉬를 2번 혹은 3번 처리하는 방법에 비해 해쉬를 단 1번만 처리하기 때문에 효율적이라 할 수 있다.

〈표 1〉 인증방법 분석

구분	해쉬기반 인증방법 [4]	개선된 해쉬기반 인증방법 [5]	확장 해쉬기반 인증방법 [3]	제안방법
위치트래킹 공격의 안전성	×	×	○	△
스푸핑공격의 안전성	×	×	○	○
메시지 복구 가능여부	○	○	○	○
태그 메모리 사용량(L)	3L	1L	2L	1L
태그 계산량	해쉬 3회	해쉬 2회	해쉬 3회	해쉬 1회
데이터베이스 계산량	×	×	△	△
리더의 처리여부	×	○	○	×

본 장에서는 2장에서 설명한 위협요소에 대한 제안한 방법의 안전성을 설명한다.

Eavesdropping(도청)은 태그에게 질의를 하여 얻은 응답을 분석하는 공격기법이지만, ID의 해쉬값과 랜덤값을 DB에 전송하여 TAG에서 처리하여 생성된 값과 비교한다. 그리고 값이 같으면 인증 처리를 하게 된다. 그러나 공격자는 이 값을 모르기 때문에 TAG의 ID를 알 수가 없다.

Location Tracking(위치 트래킹)은 태그 소유자의 이동경로를 파악하는 방법이지만, TAG가 이동하면서 랜덤값 R은 계속 변하기 때문에 공격자는 위치를 트래킹 할 수 없다.

Spoofing(스푸핑)은 정당하지 않은 개체를 정당한 것처럼 속여서 인증 받는 과정이지만 ID를 모르기 때문에 스푸핑은 불가능하다.

6. 결 론

유비쿼터스 컴퓨팅을 구축하기 위해서 많은 요소들이 필요하다. 본 논문에서는 이러한 요소 중에서 RFID의 인증 방법에 대해서 분석하고 설명하였다. 기존에도 많은 인증 방법이 제안되었고 그들의 단점을 분석하고 문제점을 해결하는 방법을 제안하였다.

특히 본 논문에서는 기존의 문제점 중에서 Location Tracking 및 Spoofing에 취약함을 인지하고 이를 보완하여 위치 프라이버시를 보장하도록 설계하였다.

또한 인증을 위해서 반드시 처리해야 하는 해쉬를 기존의 2~3번에서 단 1번으로 줄임으로써 인증의 효율성 적인 측면에서도 향상된 방법을 제시하였다. 따라서 본 논문에서 제안한 인증방법을 이용한다면 각 요소들의 부하를 줄임으로써, 안전하고 효율적인 유비쿼터스 인증을 실현할 것으로 기대된다.

그러나, 인증을 받기 위해서 랜덤값을 계속적으로 생성한다라면, 만약 인증이 빈번히 발생된다면 인증빈도수 만큼 랜덤값 생성도 비례해서 증가할 것이다. 이는 TAG의 부하증가로 이어질 수 있다. 따라서 향후 이러한 문제점을 해결하기 위한 방법이 연구가 진행되어야 하겠다.

참 고 문 헌

[1] Mark Weiser, "Some Computer Science Problems in Ubiquitous Computing", Communications of the ACM, July 1993.

[2] Mark Weiser, "Ubiquitous Computing", Nikkei Electronics, pp. 137-143, December 1993.

[3] Sungho Yoo, Kihyun Kim, Yongho Hwang, and Piljoong Lee, H., "Satus-Based RFID Authentication Protocol", Journal of The Korean Institute of Information Security and Cryptology, Vol. 14, No. 6, pp. 57-67, December 2004.

[4] Dirk Henrici and Paul Muller, "Hash based enhancement of location privacy for radio frequency identification devices using varying identifiers", PerSec'04, pp. 149-153, March 2004.

[5] Youngjoo Hwang, Misoo Lee, Donghoon Lee, and Jongin Lim, "Low-Cost RFID Authentication Protocol on Ubiquatous", CISC'S04, pp. 120-122, June 2004.

[6] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, "Security and Privacy aspects of low-cost radio frequency identification system", SPC'03, pp. 457-469, March 2003.

[7] Alastair Beresford and Frank Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing 2003, pp. 46-55, 2003.

[8] F. Stajano, "Security fot Ubiquitous Computing", Halsted Press, 2002.

[9] M. Langheinrich, "Privacy by Design Principles of Privacy-Aware Ubiquitous System", presented at ACM UbiComp 2001, Atlanta, GA, 2001.

고 훈

1992년 호원대학교 전자계산학과 (이학사)

2000년 숭실대학교 컴퓨터학과 (공학석사)

2004년 숭실대학교 컴퓨터학부 (공학박사)

2002년~현재 대진대학교 컴퓨터공학과 초빙교수

김 배 현

1995년 호원대학교 전자계산학과 (이학사)
1997년 수원대학교 전자계산학과 (이학석사)
2003년 경희대학교 컴퓨터공학과 (박사 수료)
2004년~현재 한신대학교 정보통신학과 겸임교수

권 문 택

1970년 육군사관학교(이학사)
1981년 미국 University of Iowa (공학석사)
1987년 University of Wisconsin (경영정보학박사)
경희대학교 테크노경영대학원 종신교수
경희대학교 정보처리처장
경희사이버대학교 학장