DOI: 10.3745/KIPSTC.2009.16-C.3.325

강력한 보안성을 제공하는 RFID 상호 인증 프로토콜

안 해 순[†] · 부 기 동[††] · 윤 은 준[†††] · 남 인 길[††††]

요 약

본 논문에서는 기존에 제안된 RFID 인증 프로토콜이 임의의 RFID 태그로 위장한 공격자로부터 스푸핑 공격을 당할 수 있음을 증명하고, 이러한 보안 문제점을 해결한 새로운 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안한다. 제안한 RFID 상호 인증 프로토콜은 기존의 RFID 인증 메커니즘들이 가지고 있는 많은 보안 문제점들을 해결할 뿐만 아니라, 스푸핑 공격에 대한 취약점을 해결하고, 태그 측에서 수행하는 연산 오버헤드를 최대한 줄여줌으로써 신뢰할 만한 인증 시간을 보장하고 전방향 안전성을 만족하는 더욱 강력한 보안성과 효율성을 제공한다.

키워드 : 보안, 저비용 RFID, 상호 인증, 해쉬함수, 전방향 안전성, 스푸핑 공격

RFID Mutual Authentication Protocol Providing Stronger Security

Hae-Soon Ahn[†] · Ki-Dong Bu[††] · Eun-Jun Yoon[†††] · In-Gil Nam[††††]

ABSTRACT

This paper demonstrates that an attacker can impersonate a random RFID tag and then perform the spoofing attack in the previous RFID authentication protocol. To resolve such a security problem, we also propose a new secure and efficient RFID mutual authentication protocol. The proposed RFID mutual authentication protocol is not only to resolve many security problems with the existing RFID authentication mechanism and the vulnerability against spoofing attack, but also to guarantee reliable authentication time as reducing computational overhead performing by tag. As a result, the proposed RFID mutual authentication protocol provides stronger security including the forward secrecy and more efficiency.

Keywords : Security, Low-cost RFID, Mutual Authentication, Hash Function, Forward Secrecy, Spoofing Attack

1. 서 론

최근 유비쿼터스 컴퓨팅에 대한 연구와 관심이 증대됨에 따라, RFID(Radio Frequency IDentification) 시스템은 유비쿼터스 기반의 핵심 기술로 주목받고 있다. RFID 시스템은 무선 주파수를 이용하여 움직이는 물체를 인식, 추적, 분류 및 인식기 간의 데이터 통신을 수행하는 자동 데이터 수집 기술이다. 현재 국내에서는 교통카드, 출입구 보안 및 출결 카드 등 근접식 RFID가 주로 활용되고 있으며, 많은 연구로 인해 물류 및 유통 분야까지 빠르게 응용 및 확산되고 있는 추세이다[1-3].

그러나 물리적인 접촉 없이도 인식이 가능한 RFID 시스템의 특징과 객체를 유일하게 식별하기 위해 정보를 가지고 있는 RFID 태그는 시스템의 안전성과 개인의 정보 노출, 위치 추적 등의 프라이버시(Privacy) 침해를 유발할 수 있는 문제점을 가지고 있다[2-11]. 이러한 RFID의 프라이버시 침해 문제를 해결하기 위해 해쉬함수(Hash Function), 대칭키 및 공개키 시스템을 이용한 암호학적 알고리즘(Cryptography Algorithm) 또는 배타적 논리합(Exclusive-Or)과 같은 단순한 연산자를 사용한 다양한 기법들이 많은 연구자들에 의해 제안되었다[2-11].

최근 Kim-Ryoo는 기존의 RFID 인증 프로토콜 분석을 통하여 해쉬함수를 이용한 새로운 RFID 상호 인증 프로토콜을 제안하였다[11]. 또한 제안한 프로토콜이 위치 추적(Location Tracking), 재전송 공격(Repaly Attack), 스푸핑 공격(Spoofing Attack)에 안전할 뿐만 아니라 단순한 상호 인증방식에서 취약했던 반사 공격(Reflection Attack)에도 안전하다고 주장하였다.

본 논문에서는 Kim-Ryoo가 제안한 RFID 인증 프로토콜이 RFID 태그로 위장하여 공격자가 과거의 세션에서 사용된 인증 메시지들을 이용하여 스푸핑 공격[10]을 수행할 수

† 정 회 원 : 대구대학교 교양교직부 초빙교수
†† 종신회원 : 경일대학교 컴퓨터공학부 교수
††† 정 회 원 : 경북대학교 전자전기컴퓨터학부 연구교수
†††† 정 회 원 : 대구대학교 컴퓨터 · IT공학부 교수(교신저자)
논문접수 : 2008년 12월 15일
수 정 일 : 2009년 3월 18일
심사완료 : 2009년 4월 20일

있음을 증명하고, 이를 해결할 뿐만 아니라 백-엔드 데이터베이스(Database)와 태그가 상호인증 후 서로 공유된 비밀 값을 안전하게 갱신하게 하여 전방향 안전성(Forward Secrecy)을 만족하는 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안한다. 결론적으로 제안한 프로토콜은 Kim-Ryoo의 프로토콜과 비교하여 태그측에서 수행하는 해쉬함수 연산과 배타적 논리합 연산(XOR) 등을 최대한 줄여줌으로써 신뢰할 만한 인증 시간을 보장하게 하였고, 전방향 안전성을 제공케하여 태그 내에 저장된 비밀값의 유출로 인한 과거의 통신 메시지들에 대한 기밀성 침해 문제를 해결하여 줌으로써, 강력한 안전성을 제공할 뿐만 아니라 효율성 측면에서도 우수함을 보여준다.

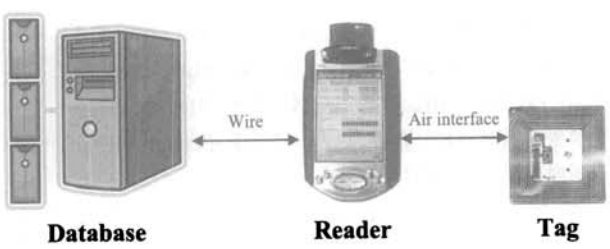
2. 연구 배경

본 장에서는 관련연구로서 RFID 시스템의 구성요소와 RFID 시스템이 갖추어야 하는 보안 고려사항에 대하여 알아본다.

2.1 RFID 시스템 구성요소

RFID 시스템은 태그(Tag), 리더(Reader), 그리고 백-엔드 데이터베이스(Back-end Database: DB)의 3가지 구성요소로 구성된다[1, 11]. (그림 1)은 기본적인 RFID 시스템의 네트워크 구조를 보여주며, 이들 각 구성요소의 기능은 다음과 같다.

1) 태그(Tag): 리더가 질의를 하면 태그는 저장된 식별정보를 무선 통신 채널을 통해 리더에게 전송한다. 태그는 무선 통신을 위한 안테나와 인증관련 연산을 수행하고 정보를 저장하는 마이크로 칩으로 구성되어 있다. 전원의 유무에 따라 전원이 있는 태그를 능동형 태그(Active Tag), 전원이 없는 태그를 수동형 태그(Passive Tag)로 구분한다.
2) 리더(Reader): 태그의 정보를 읽어내기 위해 태그와 송·수신하는 기기로서 태그에서 수집된 정보를 데이터베이스로 전송하는 기능을 한다. 리더는 무선 통신 채널을 통하여 태그에 정보를 요청한다.
3) 백-엔드 데이터베이스(Back-end Database: DB): 태그에 관련된 정보를 저장하며, 정당한 리더로부터 전송된 임의의 태그 정보를 수신하여 해당 태그의 정당성을 식별하는 기능을 수행한다. 또한, 연산 능력이 낮은 리더나 태그를 대신하여 복잡한 연산을 수행한다.



(그림 1) RFID 시스템의 네트워크 구조

2.2 RFID 시스템의 보안 고려사항

RFID 시스템은 다음과 같은 보안 문제들을 고려하여 설계되어야 한다[5, 10, 11].

(1) 상호 인증(Mutual Authentication): 통신하는 태그와 리더가 서로 합법적인지를 명시적인 인증을 통해 확인하는 것이다.

(2) 도청 공격(Eavesdropping Attack): 공격자가 리더와 태그 사이에 전송되는 메시지를 도청하여 정보를 얻게 된다.

(3) 재전송 공격(Replay Attack): 공격자는 특정 태그와 리더 사이의 통신 메시지들을 도청하고, 도청한 메시지를 임의의 태그에 저장한다. 이후 리더로부터 질의를 받으면 공격자는 임의의 태그에 저장된 메시지를 재전송함으로써 정당한 태그나 리더로 인증 받으려는 공격이다.

(4) 스푸핑 공격(Spoofing Attack): 공격자가 정당한 태그로 위장하여 리더로부터 인증에 필요한 정보를 획득하거나 정당한 리더로 위장하여 태그로부터 인증에 필요한 정보를 획득하고 이를 이용하여 정당한 태그 또는 리더로 인증 받는 공격이다.

(5) 트래픽 분석 공격(Traffic Analysis Attack): 공격자가 리더와 태그간의 송수신 정보들을 도청한 후 도청된 내용을 분석하여 인증 프로토콜에 필요한 비밀정보 등을 분석 및 리더의 질의에 대한 태그의 응답 등을 예측하는 공격이다.

(6) 위치 트래킹 공격(Location Tracking Attack): 공격자가 태그의 위치변화를 감지함으로써 태그 소유자의 이동 경로를 파악하여 태그 소유자의 프라이버시를 침해하는 공격이다.

(7) 서비스 거부 공격(Denial of Service Attack): 리더와 태그가 정상적인 서비스와 기능을 수행 하지 못하도록 하는 공격이다. 상대방의 정당한 인증 요청임에도 불구하고 공격자에 의해 많은 계산이 요구되는 데이터 송신이나, 이전 세션에서 갱신되어져야 하는 값들을 올바른 값으로 갱신되지 못하도록 방해한다.

(8) 전방향 안전성(Forward Secrecy): 공격자에게 현재 세션에서 DB와 태그 간에 공유된 비밀키 값이 누출되더라도 해당 비밀 값을 이용하여 과거에 사용된 비밀 값 유도를 통하여, 과거 메시지들의 무결성을 저해하지 않아야 하는 보안성을 의미한다. 즉, RFID 태그는 폐기 되어질 수 있기에 공격자에 의해 쉽게 획득되어 부채널 공격(Side-Channel Attack) 등을 통해 태그 내에 저장된 비밀키 값이 유출될 수 있다.

따라서, DB와 태그는 상호인증을 수행 후 다음 세션을 위해 서로의 비밀 값을 안전하게 갱신하여 트래픽 분석 공격이나 위치 트래킹 공격 등을 방어할 수 있어야 한다.

2.3 관련 연구

RFID 시스템에서의 태그는 주위의 리더 신호에 반응하여 자신의 고유 정보를 무선 통신 채널을 통해서 리더에게 전송한다. 따라서 리더 주변의 공격자는 사용자의 개인 정보나 위치 정보를 쉽게 얻을 수 있으므로 심각한 프라이버시 침해 문제를 유발시킨다. 이러한 사용자의 프라이버시 보호를 위해 여러 가지 기법들이 제안되었다.

제안된 기법들은 크게 물리적 접근기법과 비트연산(XOR) 기반, 해쉬함수 기반, 재 암호화 등 암호학적 접근기법으로 분류된다. 물리적 접근기법의 가장 단순한 방법은 Auto-ID 센터에 의해 제안된 태그 무효화(Kill) 명령어 기법으로서 태그가 자신의 데이터 필드에 저장된 패스워드를 외부에서 받은 경우, 태그를 영구적으로 정지시켜 더 이상 리더의 질의에 응답하지 않게 하는 방법이다[13]. 이 방법은 명령이 수행된 이후, 완료되었는지 확인하기 어렵고, 한번 정지된 태그의 재사용이 불가능하다.

XOR 기반 접근기법으로는 Juels 기법과 Eunyoung 기법 등이 있다[14, 15]. Juels 기법은 단지 XOR 연산을 사용하므로 저가의 RFID 시스템에 적용이 가능하고, Eunyoung 기법은 Juels 기법을 기반으로 제안되었으나 태그와 DB에서 전송하는 비밀 값들을 분리하여 처리하였다는 점에서 차별성을 가지며, Juels 기법보다 태그와 DB에서 적은 저장 공간과 계산량을 보여주어 효율적이라 할 수 있다. 그러나 XOR 기반인 두 기법은 읽기와 쓰기가 가능한 저가형 RFID 태그에 적합하지만 읽기전용 RFID 태그에는 적용할 수 없다는 단점이 있다.

해쉬함수 기반의 대표적 기법인 해쉬락 기법은 해쉬함수를 사용하여 저가의 태그에 적용될 수 있지만, 리더와 태그 간에 동일한 해쉬 값인 metaID=h(key)를 사용하기 때문에 공격자가 태그의 위치를 추적할 수 있고, 재전송 공격, 스푸핑 공격 등이 가능한 단점을 가지고 있다[16]. 이러한 문제점을 해결하기 위해 제안된 바 있는 난수 값을 사용하는 랜덤 해쉬락 기법과 서로 다른 두개의 해쉬함수를 사용하는 해쉬체인 기법도 태그의 ID가 노출될 가능성과 재전송 공격 및 스푸핑 공격에 취약하다[3, 8]. 해쉬함수 이외의 암호학적 함수를 사용하는 방법으로 재 암호화 접근기법이 있다[4, 6]. 이 방법은 ElGamel 공개키 암호화 알고리즘을 기반으로 하여 유로화 지폐에 RFID 태그를 내장함으로써 사용자 프라이버시를 보호한다. 그러나 특정 리더만이 태그 정보의 정확성을 확인할 수 있다는 가정 하에 안전성이 보장되고, 공개키 암호화 알고리즘을 사용하므로 재 암호화 기법을 사용하기 위해서는 별도의 인프라가 필요하다는 단점을 가진다.

2007년에 Kim-Ryoo는 기존의 RFID 인증 프로토콜 분석을 통하여 해쉬함수를 이용한 새로운 RFID 상호 인증 프로토콜을 제안하였으나[11], 제안한 상호 인증 프로토콜은 RFID 태그로 위장한 공격자로부터 스푸핑 공격에 취약하다는 단점이 있다. 본 연구에서는 이러한 보안 문제점을 개선한 전방향 안전성(Forward Secrecy)을 만족하는 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안하고자 한다.

3. Kim-Ryoo의 RFID 상호 인증 프로토콜

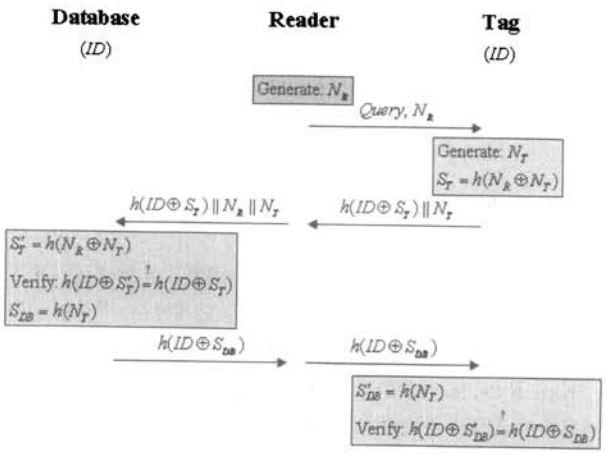
본 논문에서 사용할 용어들을 정의하고, Kim-Ryoo[11]가 제안한 RFID 상호 인증 프로토콜을 소개한다.

3.1 용어 정의

- $Query$: 태그의 응답을 요청하는 리더의 요청
- ID : 태그에 할당된 고유정보
- ID_{new} : ID의 새로운 갱신된 값
- ID_{old} : ID의 가장 최근 값
- DB : 백-엔드 데이터베이스(Back-end Database)
- $M_1 \| M_2$: M_1과 M_2의 연접
- $h(\cdot)$: 안전한 일방향 해쉬함수
- N_R : 리더가 생성한 난수
- N_T : 태그가 생성한 난수
- $\oplus$: 비트단위 배타적논리합(XOR) 연산
- S_T : $h(N_R \oplus N_T)$
- S_{DB} : $h(N_T)$
- $Info$: 인증된 태그에 관한 제품정보

3.2 Kim-Ryoo의 프로토콜

(그림 2)는 Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 아래와 같이 인증 프로토콜이 수행된다. (그림 2)에서 일반적인 RFID 시스템에서와 마찬가지로 리더와 백-엔드 데이터베이스 사이의 통신 채널은 공격자로부터 안전한 채널(Secure Channel)이며, 리더와 태그 사이의 통신 채널은 공격자가 개입하여



(그림 2) Kim-Ryoo의 RFID 상호 인증 프로토콜

2.2절에서 언급한 공격 등을 수행할 수 있는 공개된 채널(Open Channel)임을 가정한다.

Step 1. 리더 → 태그: *Query*, N_R

리더는 태그를 인증하기 위해 난수 N_R을 생성하여 *Query*와 함께 태그로 전송한다.

Step 2. 태그 → 리더: $h(ID \oplus S_T) \| N_T$

태그는 *Query*를 수신한 후, 리더를 인증하기 위한 난수 N_T를 생성한다. 그리고 태그는 N_R과 N_T를 이용하여 $S_T = h(N_R \oplus N_T)$와 $h(ID \oplus S_T)$를 계산하고, $h(ID \oplus S_T)$와 N_T를 리더에게 전송한다.

Step 3. 리더 → DB: $h(ID \oplus S_T) \| N_R \| N_T$

리더는 수신한 $h(ID \oplus S_T) \| N_T$ 메시지에 N_R을 연접하여 DB에게 전송한다.

Step 4. DB → 리더: $h(ID \oplus S_{DB})$

DB는 수신한 N_R과 N_T를 이용하여 $S_T' = h(N_R \oplus N_T)$을 계산한 후, 자신의 데이터베이스 내에 저장되어 있는 태그들의 ID를 이용하여 수신된 $h(ID \oplus S_T)$와 일치하는 값을 찾는다. 수신된 $h(ID \oplus S_T)$가 DB에서 계산된 $h(ID \oplus S_T')$ 값들과 일치하지 않는다면, DB는 Error 메시지를 리더에게 전송한다. 만약 수신된 $h(ID \oplus S_T)$와 DB에서 계산된 $h(ID \oplus S_T')$이 일치한다면 태그와 리더가 인증된다. 그리고 DB는 N_T를 이용하여 $S_{DB} = h(N_T)$를 계산한 후, 태그가 DB와 리더를 인증하기 위해 $h(ID \oplus S_{DB})$ 메시지를 리더에게 전송한다.

Step 5. 리더 → 태그: $h(ID \oplus S_{DB})$

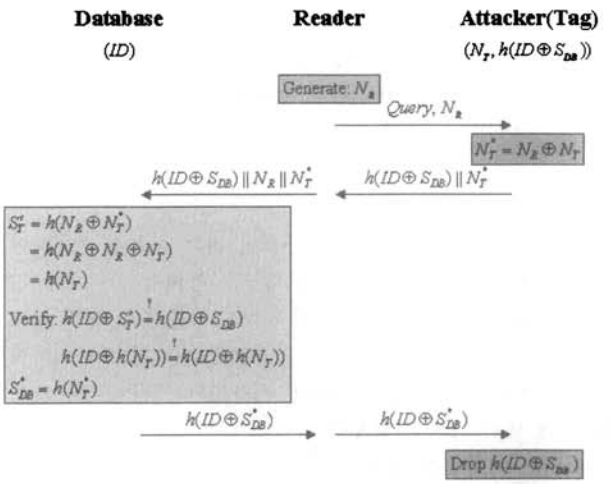
리더는 Error 메시지를 수신하면 태그와의 통신을 중단하고, $h(ID \oplus S_{DB})$ 메시지를 수신하게 되면 태그에게 수신한 메시지를 전송한다.

Step 6. 태그는 $h(ID \oplus S_{DB})$ 메시지를 수신하면, 자신이 저장하고 있는 N_T와 자신의 ID를 이용하여 $h(ID \oplus S_{DB}')$를 계산한다. 수신된 $h(ID \oplus S_{DB})$와 계산된 $h(ID \oplus S_{DB}')$이 일치하면, DB와 리더가 인증된다.

4. 스푸핑 공격

본 장에서는 Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜의 취약점을 지적한다. 즉, 인증 단계에서 이루어지는 스푸핑 공격(Spoofing attack)[7, 10, 11] 과정을 기술한다.

Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜은 임의의 세션에서 DB가 이전에 재전송된 태그의 인증 메시지를 쉽게 인증하는 스푸핑 공격에 취약하다. 임의의 세션에서 공



(그림 3) 스푸핑 공격

격자는 Step 2에서 태그가 리더에게 전송한 난수 N_T와 Step 5에서 리더가 태그에게 전송한 $h(ID \oplus S_{DB})$를 소유하고 있다고 가정하자. 그러면 다음과 같은 과정으로 공격자는 스푸핑 공격을 수행 할 수 있다. (그림 3)은 스푸핑 공격 과정을 보여준다.

Step 1. 리더 → 태그: *Query*, N_R

리더는 태그를 인증하기 위해 난수 N_R을 생성하여 *Query*와 함께 태그로 전송한다.

Step 2. 공격자 → 리더: $h(ID \oplus S_{DB}) \| N_T^*$

공격자는 *Query*와 N_R을 가로챈 후, 과거의 세션에서 사용된 난수 N_T와 현재 세션에서 가로챈 N_R을 이용하여 $N_T^* = N_R \oplus N_T$를 계산하여 과거 세션에서 도청한 $h(ID \oplus S_{DB})$와 함께 N_T^*를 리더에게 전송한다.

Step 3. 리더 → DB: $h(ID \oplus S_{DB}) \| N_R \| N_T^*$

리더는 수신한 $h(ID \oplus S_{DB}) \| N_T^*$ 메시지에 N_R을 연접하여 DB에게 전송한다.

Step 4. DB → 리더: $h(ID \oplus S_{DB}^*)$

DB는 수신한 N_R과 N_T^*를 이용하여 $S_T' = h(N_R \oplus N_T^*)$을 계산하게 된다. 여기에서 $N_T^* = N_R \oplus N_T$ 이기 때문에, S_T'이 과거의 세션에서 사용된 $S_{DB} = h(N_T)$와 동일함을 아래 수식을 통해 쉽게 발견할 수 있다.

$$\begin{aligned} S_T' &= h(N_R \oplus N_T^*) \\ &= h(N_R \oplus N_R \oplus N_T) \\ &= h(N_T) \\ &= S_{DB} \end{aligned}$$

따라서 DB는 자신의 데이터베이스 내에 저장되어 있는 태그들의 ID를 이용하여 계산된 $h(ID \oplus S_T') = h(ID \oplus h(N_T))$는 공격자로부터 수신된 $h(ID \oplus S_{DB}) = h(ID \oplus h(N_T))$와 일치하는 값을 쉽게 찾을 수 있기 때문에, 공격자가 전송한 스푸핑 메시지를 인증하게 된다. 마지막으로 공격자를 인증한 DB는 N_T^*를 이용하여 $S_{DB}^* = h(N_T^*)$를 계산한 후, 태그가 DB와 리더를 인증하기 위한 $h(ID \oplus S_{DB}^*)$ 메시지를 리더에게 전송한다.

Step 5. 리더 → 태그: $h(ID \oplus S_{DB}^*)$

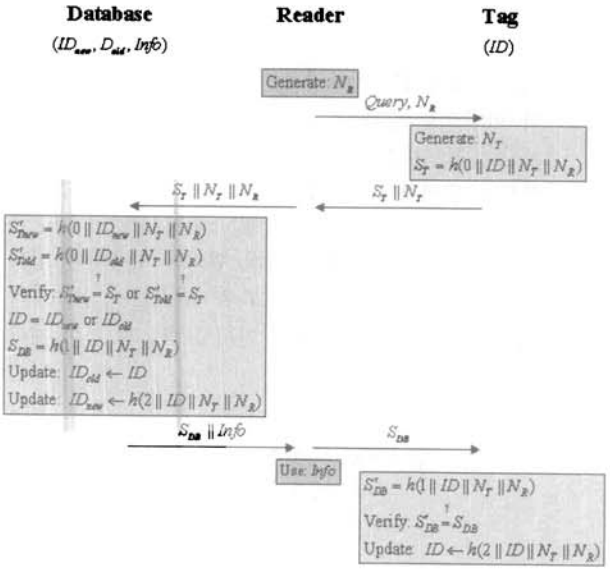
리더는 태그에게 $h(ID \oplus S_{DB}^*)$ 전송하게 된다.

Step 6. 공격자는 $h(ID \oplus S_{DB}^*)$ 메시지를 가로채어 스푸핑 공격을 마무리 하여 리더로부터 송신되는 중요한 정보를 가로채거나 악의적인 정보를 리더에게 송신할 수 있다.

결론적으로 Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜은 위 Step 1~6을 통하여 임의의 태그로 위장한 공격자를 쉽게 인증하는 스푸핑 공격에 취약하다.

5. 제안한 RFID 상호 인증 프로토콜

본 장에서는 4장에서 보여준 Kim-Ryoo가 제안한 프로토콜의 보안 취약점을 해결한 전방향 안전성을 제공하는 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안한다. Kim-Ryoo가 제안한 프로토콜과 달리 제안한 프로토콜은 동기화 문제 해결 및 전방향 안전성을 제공하기 위해 백-엔드 데이터베이스 내에 각 태그를 위한 기존 ID의 새로운 갱신된 값인 ID_{new}와 ID의 가장 최근 값인 ID_{old} 쌍을 가지



(그림 5) 제안한 RFID 상호 인증 프로토콜

고 있다. 이로 인해 제안한 프로토콜은 상호인증을 수행한 후에 DB와 태그 간에 공유된 비밀 값인 ID를 안전하게 갱신하여 전방향 안전성을 만족할 뿐만 아니라, 태그 측에서 수행하는 해쉬 연산량 및 XOR 연산량 등을 줄여주기 때문에 저비용 태그(Low-cost Tag) 기반의 RFID 인증 시스템에도 적합하다.

(그림 4)는 제안한 RFID 상호 인증 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 아래와 같이 인증 프로토콜이 수행된다. (그림 4)에서 일반적인 RFID 시스템에서와 마찬가지로 리더와 백-엔드 데이터베이스 사이의 통신 채널은 공격자로부터 안전한 채널(Secure Channel)이며, 리더와 태그 사이의 통신 채널은 공격자가 개입하여 2.2절에서 언급한 공격 등을 수행할 수 있는 공개된 채널(Open Channel)임을 가정한다.

Step 1. 리더 → 태그: $Query$, N_R

리더는 태그를 인증하기 위해 난수 N_R을 생성하여 $Query$와 함께 태그로 전송한다.

Step 2. 태그 → 리더: $S_T \| N_T$

태그는 $Query$와 N_R을 수신한 후, 리더를 인증하기 위한 난수 N_T를 생성한다. 계속해서 태그는 수신한 N_R과 생성한 N_T 그리고 저장된 비밀 값 ID를 이용하여 $S_T = h(0 \| ID \| N_T \| N_R)$를 계산하고, S_T와 N_T를 리더에게 전송한다.

Step 3. 리더 → DB: $S_T \| N_T \| N_R$

리더는 수신한 $S_T \| N_T$ 메시지에 N_R을 연접하여 DB에게 전송한다.

Step 4. DB → 리더: $S_{DB} \| Info$

DB는 자신의 데이터베이스 내에 저장되어 있는 태그들의 ID_{old}와 ID_{new} 그리고 리더로 부터 수신한 N_T와 N_R을 이용하여 $S_{Told}' = h(0 \| ID_{old} \| N_T \| N_R)$와 $S_{Tnew}' = h(0 \| ID_{new} \| N_T \| N_R)$를 각각 계산한 후, 수신된 S_T와 일치하는 값을 찾는다. 수신된 S_T가 DB에서 계산된 S_{Told}' 또는 S_{Tnew}'값들과 일치하지 않는다면, DB는 Error 메시지를 리더에게 전송한다. 만약 수신된 S_T와 DB에서 계산된 S_{Told}' 또는 S_{Tnew}'와 일치한다면 태그와 리더가 인증된다. 그리고 DB는 검증에 사용된 해당 ID_{old} 또는 ID_{new}를 ID로 두고 수신한 N_T와 N_R을 이용하여 $S_{DB} = h(1 \| ID \| N_T \| N_R)$를 계산한 후, 태그가 DB와 리더를 인증하기 위한 S_{DB} 메시지와 리더가 필요로 하는 태그에 관한 정보를 담고 있는 $Info$를 함께 리더에게 전송한다. 마지막으로 전방향 안전성을 제공하기 위해 DB는 현재의 태그의 비밀 값인 ID를 다음 세션을 위해 사용될 새로운 비밀 값 쌍인 $ID_{old} = ID$와 $ID_{new} = h(2 \| ID \| N_T \| N_R)$로 각각 갱신하여 저장한다.

Step 5. 리더 → 태그: S_{DB}

리더는 Error 메시지를 수신한 경우, 태그와의 통신을 중단하고, $S_{DB} \| Info$ 메시지를 수신한 경우는 태그에 관한 정보를 담고 있는 $Info$를 정보로 활용하며, S_{DB}는 태그에게 전송한다.

Step 6. 태그는 S_{DB} 메시지를 리더로부터 수신하면, 자신의 메모리 내에 저장하고 있는 ID와 난수 N_T와 N_R을 이용하여 $S_{DB}' = h(1 \| ID \| N_T \| N_R)$를 계산한다. 수신된 S_{DB}와 계산된 S_{DB}'이 일치하면, DB와 리더가 인증된다. 마지막으로 전방향 안전성을 제공하기 위해 DB는 현재의 태그의 비밀 값인 ID를 다음 세션을 위해 사용될 새로운 비밀 값인 $ID = h(2 \| ID \| N_T \| N_R)$로 갱신하여 저장한다.

6. 안전성과 효율성 분석

본 장에서는 제안한 RFID 상호 인증 프로토콜에 대한 안전성과 효율성을 분석한다.

6.1 안전성 분석

제안한 RFID 인증 프로토콜은 다음과 같이 상호인증을 명시적으로 제공하며, 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전하며 전방향 안전성을 제공한다.

(1) 상호인증(Mutual Authentication): 제안한 프로토콜의 Step 4에서 DB는 태그로부터 수신한 $S_T = h(0 \| ID \| N_T \| N_R)$가 DB에 저장된 ID_{old}와 ID_{new}로 계산한 $S_{Told}' = h(0 \| ID_{old} \| N_T \| N_R)$ 또는 $S_{Tnew}' = h(0 \| ID_{new} \| N_T \| N_R)$와 동일한지를 검증하며, Step 6에서 태그는 리더로부터 수신한 $S_{DB} = h(1 \| ID \| N_T \| N_R)$가 태그 자신이 계산한 $S_{DB}' = h(1 \| ID \| N_T \| N_R)$와 동일한지를 검증한다. 태그와 DB 사이에 공유된 비밀키 값 역할을 하는 ID를 모르는 공격자는 태그 또는 리더로 위장하여 스푸핑 공격 등을 수행할 수 없게 된다. 따라서 제안한 프로토콜은 안전한 상호인증을 제공한다.

(2) 도청 공격(Eavesdropping Attack): 제안한 프로토콜에서 공격자는 송수신되는 통신 메시지 $Query$, N_R, S_T , N_T, S_{DB}를 도청할 수 있다. 하지만 도청한 내용으로부터 공격자는 태그와 리더의 DB 간에 공유된 비밀키 값 역할을 하는 ID를 구할 수 없다. 즉, ID를 얻기 위해서는 공격자가 도청한 메시지 $S_T = h(0 \| ID \| N_T \| N_R)$ 또는 $S_{DB} = h(1 \| ID \| N_T \| N_R)$로부터 ID를 구할 수 있어야 한다. 하지만 안전한 일방향 해쉬 함수의 성질과 충분한 보안 강도를 만족하는 비트 길이를 가지는 비밀키 값인 ID에 의해 공격자는 S_T와 S_{DB}로부터 ID를 얻는 것은 불가능하다. 또한 비밀 값인 ID는 태그와 DB측에서 내부적으로 활용되어 지며 공개된 통신 채널로 전송되어 지지 않기에 공격자는 ID를 직접적으로 구할 수 없다. 따라서 제안한 프로토콜은 도청 공격에 안전하다.

(3) 재전송 공격(Replay Attack): 제안한 프로토콜에서는 매 세션마다 리더가 생성하는 새로운 난수 N_R 그리고 태그가 생성하는 새로운 난수 N_T를 이용하여 상호인증을 수행하기 때문에 과거에 공격자에 의해 재전송된 난수 값들은 태그와 리더의 DB간의 상호인증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

(4) 스푸핑 공격(Spoofing Attack): 제안한 프로토콜에서 공격자가 리더의 DB와 태그 간에 공유된 비밀키 값인 ID를 얻을 수 있으면, 스푸핑 공격을 수행할 수 있다. 하지만 공격자는 리더의 DB와 태그 내에 각각 안전하게 저장하고 있는 비밀키 값인 ID를 직접적으로 얻을 수 있는 방법이 없다. 또한 송수신되는 통신 메시지 S_T와 S_{DB} 내의 비밀키 값인 ID는 난수 N_T와 N_R과 안전한 일방향 해쉬함수에 의해 보호되어져 있다. 따라서 제안한 프로토콜은 일반적인 스푸핑 공격에 안전하다. 또한 제안한 인증 프로토콜이 Kim-Ryoo가 언급한 반사 공격(Reflection Attack)에 대해서도 안전하도록 하기 위해, 태그가 리더에게 전송하는 $S_T = h(0 \| ID \| N_T \| N_R)$ 메시지와 리더가 태그에게 전송하는 메시지인 $S_{DB} = h(1 \| ID \| N_T \| N_R)$에 0과 1의 각각 서로 다른 시드(Seed) 값을 이용하여 비밀키 값인 ID와 리더와 태그가 생성한 난수들을 이용한 해쉬 결과 값들을 생성하였다. 즉, 안전한 시도-응답(Challenge-Response) 방식의 RFID 상호 인증 프로토콜 기반[12]으로 리더와 태그가 생성한 난수들을 사용하여 서로 다른 값을 가지는 S_T와 S_{DB}를 생성하여 사용함으로 S_T와 S_{DB}가 동일한 값이 아님으로 반사 공격을 막을 수 있다. 더 나아가 제안한 프로토콜은 4장에서 소개한 스푸핑 공격에 대해서도 안전하다. 즉, Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜에서 제안한 스푸핑 공격이 가능한 이유는 배타적 논리합 연산의 원리를 이용하여 임의의 세션에서 도청한 난수 N_T와 $h(ID \oplus S_{DB})$로부터 S_{DB}와 동일한 S_T'을 DB로 하여금 다음과 같이 계산할 수 있었기에 가능하였다.

$$\begin{aligned} S_T' &= h(N_R \oplus N_T^*) \\ &= h(N_R \oplus N_R \oplus N_T) \\ &= h(N_T) \\ &= S_{DB} \end{aligned}$$

하지만 Kim-Ryoo의 프로토콜과 달리 제안한 RFID 인증 프로토콜에서는 태그와 DB가 각각 $S_T = h(0 \| ID \| N_T \| N_R)$와 이에 대응되는 값인 $S_{DB} = h(1 \| ID \| N_T \| N_R)$를 계산할 때 배타적 논리합 연산을 전혀 필요로 하지 않기에 S_{DB}와 동일한 S_{Told}' 또는 S_{Tnew}'값을 계산하게 할 수 없다. 따라서 제안한 프로토콜은 4장에서 소개한 스푸핑 공격에 대해서도 안전하다.

(5) 트래픽 분석 공격(Traffic Analysis Attack): 제안한 프로토콜에서는 난수 N_R과 N_T에 의해 계산된 S_T와 S_{DB}는 매 세션마다 변경되기에 공격자는 현재 세션에서 태그의 응답 S_{Tnow}가 과거 세션에 도청한 응답 S_{Told}와 동일한지를 비교할 수 없다. 즉, 매 세션마다 서로 다른 난수들을 생성함으로, 매 세션마다 서로 다른 두 개의 응답 S_{Tnow}와 S_{Told}이 동일한 태그로부터 송신된 것인지 여부를 쉽게 구별할 수 없음으로, 태그의 이동경로를 쉽게 트래킹 할 수 없다. 따라서 제안한 프로토콜은 트래픽 분석 공격에 안전하다.

(6) 위치 트래킹 공격(Location Tracking Attack): 제안한 프로토콜에서는 위 트래픽 분석 공격과 마찬가지로 난수 N_R과 N_T에 의해 계산된 S_T와 S_{DB}는 매 세션마다 변경되기 때문에 공격자가 특정한 태그를 식별할 수 없어 위치 트래킹을 할 수 없기에 사용자의 프라이버시 보호할 수 있다. 따라서 제안한 프로토콜은 위치 트래킹 공격에 안전하다.

(7) 서비스 거부 공격(Denial of Service Attack): 제안한 프로토콜에서는 리더와 태그 간에 일방향 해쉬 함수 기반의 연산만을 이용하여 상호인증을 수행함으로, 태그 측에 서비스 거부 공격을 수행할 만큼의 많은 연산량을 요구하지 않는다. 또한 매 세션마다 리더의 DB와 태그 간에 안전한 검증을 통한 상호인증을 완료 후에 다음 세션에서 사용되어 지는 비밀키 값으로 갱신되어지기 때문에 공격자에 의한 서비스 거부 공격은 쉽게 발견되어 질수 있다. 따라서 제안한 프로토콜은 서비스 거부 공격에 안전하다.

(8) 전방향 안전성(Forward Secrecy): Kim-Ryoo가 제안한 프로토콜에서는 매 세션마다 동일한 비밀키 값인 하나의 ID만을 이용하여 상호인증을 수행한다. 이로 인해 공격자가 폐기되어진 RFID 태그로부터 부채널 공격(Side-Channel Attack)등을 통해 태그 내에 저장된 비밀키 값을 획득하였을 때 과거에 해당 태그와 리더 간에 통신된 모든 메시지들에 대한 무결성과 기밀성은 보장되어 질 수 없다. 하지만, 제안한 프로토콜에서는 리더와 태그 간에 상호인증을 수행한 후에 DB는 이전의 비밀 값인 ID를 다음 세션을 위해 새로운 비밀 값 쌍인 $ID_{old} = ID$와 $ID_{new} = h(2 \| ID \| N_T \| N_R)$로 갱신하여 사용하며 태그는 새로운 비밀 값인 $ID_{new} = h(2 \| ID \| N_T \| N_R)$로 갱신하여 사용함으로, 공격자가 임의의 태그 내에 저장된 비밀 값인 $ID_{new} = h(2 \| ID \| N_T \| N_R)$를 알더라도 안전한 일방향 해쉬함수의 성질에 의해 과거에 사용된 비밀키 값인 ID를 얻을 수 없다. 특히 Step5에서 공격자 및 네트워크의 오류로 인하여 세션이 종료되었다면 동기화 문제가 발생할 수 있는데, 제안한 프로토콜에서는 백-엔드 데이터베이스 내에 각 태그를 위한 기존 ID의 새로운 갱신된 값인 ID_{new}와 ID의 가장 최근 값인 ID_{old} 쌍을 가지고 있게 하여 안전한 상호인증 수행 및 ID_{new}와 ID_{old} 값을 각각 갱신하게 하여 동기화 문제를 해결할 수 있다. 따라서 제안한 프로토콜은 전방향 안전성을 제공할 뿐만 아니라 동기화 문제도 발생하지 않는다.

<표 1>은 제안한 프로토콜과 해쉬 연산 기반의 프로토콜들인 해쉬락, 랜덤해쉬락, 해쉬체인 그리고 Kim-Ryoo의 프로토콜과의 안전성을 비교·분석한 표이다. <표 1>과 같이 해쉬락, 랜덤해쉬락, 해쉬체인, Kim-Ryoo 프로토콜들은 도청공격, 재전송 공격, 스푸핑 공격 등에 취약하여 안전한 상호인증을 수행할 수 없으며, 전방향 안전성도 제공하지 않는다. 특히 해쉬락과 랜덤해쉬락 프로토콜은 트래픽 분석 공격과 위치 트래킹 공격에도 취약하다. 하지만 제안한 프로토콜은 기존의 프로토콜과 비교하여 상호인증을 명시적으로 안전하게 제공하며, 도청공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전할 뿐만 아니라 전방향 안전성을 제공함을 알 수 있다.

6.2 효율성 분석

<표 2>는 제안한 프로토콜과 Kim-Ryoo의 프로토콜과의 효율성을 비교·분석한 표이다. <표 2>와 같이 Kim-Ryoo가 제안한 프로토콜과 비교하여 제안한 프로토콜은 태그 측의

〈표 1〉 관련 프로토콜들과의 안전성 비교·분석

프로토콜 / 공격유형	해쉬락 [2, 3]	랜덤 해쉬락 [7]	해쉬 체인 [8]	Kim-Ryoo [11]	제안 프로토콜
안전한 상호인증	×	×	×	×	○
도청공격	×	×	×	○	○
재전송 공격	×	×	×	×	○
스푸핑 공격	×	×	×	×	○
트래픽 분석 공격	×	×	○	○	○
위치 트래킹 공격	×	×	○	○	○
서비스 거부 공격	○	○	○	○	○
전방향 안전성	×	×	×	×	○

○ : 제공/안전, × : 제공안함/안전안함

<표 2> 관련 프로토콜들과의 효율성 비교 · 분석

프로토콜 / 연산종류	Kim-Ryoo 프로토콜[11]			제안 프로토콜		
	태그	리더	DB	태그	리더	DB
해쉬 연산량	4	0	n+3	3	0	2n+2
XOR 연산량	3	0	n+2	0	0	0
난수 생성수	1	1	0	1	1	0
태그의 쓰기연산	불필요			필요		
리더와 태그간 통신메시지수	$1Q+2h()+2Rn$			$1Q+2h()+2Rn$		
리더와 태그간 통신라운드수	3라운드			3라운드		

n : DB에 저장된 태그의 개수
Q : 쿼리(Query) 개수
$h()$: 해쉬연산값 개수
Rn : 일회성 난수 개수

해쉬 연산량을 1번 줄여주며, DB측의 해쉬 연산량은 동기화 문제 해결 및 전방향 안전성을 제공하기 위한 비밀키 값 갱신에 대한 해쉬 연산량을 포함하여 최대 DB에 저장된 태그수(n)-1번을 더 수행한다. 또한, XOR 연산량을 전혀 요구되지 않기에 Kim-Ryoo가 제안한 프로토콜과 비교하여 제안한 프로토콜은 태그 측의 XOR 연산량은 3번, DB측의 XOR 연산량을 DB에 저장된 태그수(n)+2 만큼 줄여준다. Kim-Ryoo가 제안한 프로토콜과 마찬가지로 제안한 프로토콜 또한 리더와 태그 모두 난수를 각각 생성하여 안전한 상호 인증을 수행한다. Kim-Ryoo가 제안한 프로토콜은 전방향 안전성을 제공하지 않기에 태그의 쓰기 연산을 요구하지 않는다. 하지만 제안한 프로토콜은 전방향 안전성을 제공하기 위해 태그의 쓰기 연산을 필요로 한다. 물론 제안한 프로토콜이 전방향 안전성을 제공하지 않는 환경에 이용되어 진다며 DB와 태그의 비밀키 값 갱신 과정을 수행하지 않아도 됨으로 n+2번의 해쉬 연산량을 줄여 주어 더욱 효율적일 수 있다. 제안한 프로토콜과 Kim-Ryoo가 제안한 프로토콜 모두 $1Q+2h()+2Rn$ 만큼의 리더와 태그 간의 통신 트래픽이 요구되며 총 수행되는 통신라운드 수는 3라운드로 동일하다. 결론적으로 제안한 프로토콜은 <표 1>에서 보여주는 것처럼 명시적인 상호인증을 제공함으로 인해 다양한 공격에 안전하고 전방향 안전성을 제공할 뿐만 아니라 <표 2>와 같이 연산 오버헤드 측면에서도 태그 측에 많은 부담을 주지 않음으로 안전성과 효율성 모두를 보장해 줄 수 있다.

7. 결 론

본 논문은 Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜이 여전히 RFID 태그로 위장하여 공격자가 과거의 세션에서 사용된 인증 메시지들을 이용한 스푸핑 공격을 수행할 수 있음을 증명하였다. 또한 스푸핑 공격에 대한 보안 취약점을 해결할 뿐만 아니라 태그측 연산 오버헤드를 줄여주며 전방향 안전성을 제공하는 더욱 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안하였다. 결론적으로 제안한 RFID 상호 인증 프로토콜은 Kim-Ryoo의 프로토콜과 비교하여 더욱더 강한 보안성과 안전성을 제공하며, 태그 측에서 수행하여야 하는 해쉬함수 연산 및 XOR 연산 등의 연산 오버헤드 부담 또한 최대한 줄여 줌으로써 효율성 측면에서도 우수하다. 따라서 제안한 RFID 상호 인증 프로토콜은 유비쿼터스 컴퓨팅 환경에서 필요한 다양한 RFID 시스템 응용 환경에 안전성과 효율성 보장을 위한 인증 프로토콜로 사용이 가능할 것으로 기대된다.

향후 연구로는 제안한 전방향 안전성을 제공하는 RFID 상호 인증 프로토콜이 2장에서 정의된 공격들에 대해 안전하고 전방향 안전성을 보장함을 최근에 많은 보안 연구자들에 의해 사용되어 지는 정형적인 안전성 분석 방법들[16-19]을 기반으로 증명함을 목표로 둔다.

참 고 문 헌

[1] F. Klaus, "RFID handbook," Second Edition, Jone Willey & Sons, 2003.

[2] S. E. Sarma, S. A. Weis, D. W. Engels. "RFID systems, security & privacy implications," White Paper MIT-AUTOID-WH_014, MIT AUTO-ID CENTER, 2002.

[3] S. A. Weis, "Radio-frequency identification security and privacy," Master's Thesis, M.I.T. 2003.

[4] 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, Springer-Verlag, 2003.

[5] A. Juels, R. L. Rivest, M Szydlo "The blocker tag: selective blocking of RFID tags for consumer privacy," In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp.103-111, 2003.

[6] S. Junichiro, H. Jae-Cheol and S. Kouichi, "Enhancing privacy of universal re-encryption scheme for RFID tags," EUC 2004, Vol.3207 LNCS, pp.879-890, Springer-Verlag, 2004.

[7] S. A. Weis, S. Sarma, R. Rivest, D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, Springer-Verlag, 2004.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain based forward-secure privacy protection scheme for low-cost RFID," Proceedings of the SCIS 2004, pp.719-724, 2004.

[9] 양형규, 안영화, "유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구," 전자공학회논문지 42권 CI 1호, pp.45-50, 2005.

[10] 최은영, 최동희, 임종인, 이동훈, "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜," 정보보호학회논문지 15권 5호, pp.59-71, 2005.

[11] 김배현, 유인태, "반사공격에 안전한 RFID 인증 프로토콜," 한국통신학회논문지 32권 3호, pp.348-354, 2007.

[12] M.S. Hwang, I.C. Lin, and L.H. Li. "A simple micro-payment scheme," The Journal of Systems and Software, Vol.55, pp.221-229, 2001.

[13] Auto-ID Center, "860Mhz-960MHz Class I Radio Frequency Identification Tag Radio Frequency and Logical communication Interface Specification Proposed Recommendation Version 1.0.0. Technical Report MIT-AUTOID-TR-007", AutoID Center, MIT, 2002.

[14] A. Juels, "Minimalist cryptography for lowcost RFID tags", In 4th Intel. Conf. on Security in Communication Networks-SCN 2004 Vol.3352 LNCS. pp.149-164.

[15] Choi, Eun Young and Lee, Su Mi and Lee, Dong Hoon, "Efficient RFID Authentication protocol for Ubiquitous Computing Environment" In International Workshop on Security in Ubiquitous Computing Systems - secubiq 2005, Volume 3823 LNCS, pp.945-95.

[16] Weis, S. et al, "Security and Privacy in Radio -Frequency Identification Devices", Massachusetts Institute of Technology, 2003.

[17] S. Vaudenay, "On privacy models for RFID," Proc. of the Asiacrypt 2007, Vol.4833, pp.68-87, Springer-Verlag, 2007.

[18] I. Damgard and M. Ø. Pedersen, "RFID security: tradeoffs between security and efficiency," Proc. of the CT-RSA 2008, Vol.LNCS4964, pp.318-332, Springer-Verlag, 2008.

[19] P. I. Paise and S. Vaudenay, "Mutual Authentication in RFID: Security and Privacy," Proc. of the CCS 2008, pp.292-299, ACM, 2008.

안 해 순

e-mail : ahs221@hanmail.net

1996년 경일대학교 컴퓨터공학과(공학사)

2001년 경일대학교 컴퓨터공학과(공학석사)

2009년 대구대학교 컴퓨터정보공학과 박사 수료

2004년~2008년 경일대학교 컴퓨터공학부 전임강사

2008년~현 재 대구대학교 교양교직부 컴퓨터과정 초빙교수

관심분야 : 정보보안, 정보검색, 데이터베이스 보안, RFID 보안

윤 은 준

e-mail : ejyoon@tpic.ac.kr

2003년 경일대학교 컴퓨터공학과(공학석사)

2007년 경북대학교 컴퓨터공학과(공학박사)

2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사

2008년~현 재 경북대학교 전자전기컴퓨터학부 연구교수

2007년~현 재 보안공학연구지원센터 보안공학논문지 편집위원

관심분야 : 암호학, 유비쿼터스보안, 네트워크보안, 데이터베이스 보안

부 기 동

e-mail : kdbu@kiu.ac.kr

1984년 경북대학교 전자공학과(공학사)

1988년 경북대학교 전자공학과(공학석사)

1996년 경북대학교 전자공학과(공학박사)

1983년~1985년 포항종합제철 시스템개발실

1988년~현 재 경일대학교 컴퓨터공학부 교수

관심분야 : 데이터베이스, GIS, 데이터베이스 보안, RFID 보안

남 인 길

e-mail : ignam@daegu.ac.kr

1978년 경북대학교 전자공학과(공학사)

1981년 영남대학교 전자공학과(공학석사)

1992년 경북대학교 전자공학과(공학박사)

1978년~1981년 대구은행 전산부

1980년~1990년 경북산업대학 부교수

1990년~현 재 대구대학교 컴퓨터·IT공학부 교수

관심분야 : 데이터베이스, 데이터베이스 보안, RFID 보안