중계 공격을 예방하는 효율적인 RFID Distance-Bounding 프로토콜

정회원 부 창 희*, 전 문 석*

An Efficient RFID Distance-Bounding Protocol to Prevent Relay Attacks

Chang-hee Boo*, Moon-seog Jun* *Regular Members*

요 약

최근 다양한 분야에서 사용되고 있는 RFID 시스템은 악의적인 공격자로부터의 중계공격에서 취약함을 갖고있다. 따라서 Brands등은 Distance-Bounding 이라는 개념을 이용하여 증명자와 검증자 간의 인증 프로토콜을 제안하였고, 여기에 Hancke등은 RFID의 개념을 도입하였다. 그러나 RFID의 주요 기능 중 하나인 태그 아이디의 전달이 없다는 점과, Kim이 제안한 태그 아이디 전달에서의 익명성 및 리더 태그 간에 데이터 교환 단계에서 발생 가능한 에러 체크 방법에서 태그 아이디 검색의 비효율성의 단점이 있다. 따라서 본고에서는 태그의 익명성 및 위치 추적 불가능성을 만족하고, 태그의 정보 교환 단계에서 발생 가능 에러에 대한 저항성과, 태그 아이디의 검색에서 보다 효율적인 검색이 가능한 프로토콜을 제안한다.

Key Word : RFID, Distance-Bounding, Relay Attack, Mafia Fraud, Terrorist Fraud

Abstract

RFID (radio frequency identification) systems, recently being used in a wide range of areas, are vulnerable to relay attack from malicious attackers. For that reason, Brands, et al. proposed a certification protocol between a certifier and a verifier based on the concept of distance-bounding, and in addition Hancke et al. introduced the concept of RFID. However, the delivery of tag IDs, one of the main RFID features, is not still available, and there are two important demerits: anonymity in the delivery of tag IDs suggested by Kim et al. and inefficiency in finding a tag ID with regard to how to check errors which may occur in the process of data exchange between readers and tags. Therefore, this study proposes a protocol that meets the requirements of tag anonymity and location untraceability, has resistance to errors which may take place in the phase of tag data exchange, and is very efficient in finding tag IDs.

Ⅰ. 서 론

최근, RFID(Radio Frequency IDentification) 시스템을 이용한 다양한 서비스들이 제공되고 있다. RFID는 태그와 리더, 그리고 태그의 정보를 가져오는 데이터베이스로 구성되어진다[1]. RFID 시스템의 예로 교통카드 시스템 등이 있으며, 이는 이용 요금의 결제와 관련되는 중요한 부분이므로 보안적인 측면에서 많은 부분을 신경써야 한다. 기존의 RFID 연구는 주로 태그와 리더 사이의 인증 및 안전한 태그의 아이디 전달에 초점이 맞추어져 있었다. 즉, 태그의 안전한 인증 및 태그에 익명성을 제공하여 위치 추적을 불가능하

* 숭실대학교 컴퓨터학과(chboo0598@bible.ac.kr, mjun@ssu.ac.kr)
논문번호 : KICS2010-02-063, 접수일자 : 2010년 2월 6일, 최종논문접수일자 : 2010년 4월 5일

게 하는 방법 등 다양한 보안성을 제공하는 방법들이 제안되었다. 하지만, 이러한 형태의 인증 방법은 중계 공격(Relay Attack)에 매우 취약한 단점이 있다. 중계 공격은 태그와 리더 사이에 제 3자가 끼어들어 태그와 리더사이를 이어주는 공격으로, 물리적으로 다른 위치에 존재하는 태그를 이용하여 리더에게 인증을 요구할 수 있다. 실제로 이러한 공격은 비접촉식 스마트카드 등의 시스템에 적용하였을 경우 매우 심각한 문제를 일으킬 수 있다. ISO-14443 표준 스마트 카드의 경우 비접촉식으로 그 인증 거리를 10cm 로 규정하고 있으며, 인증에 걸리는 시간은 4ms ~ 4949ms 로 규정하고 있다. Ziv Kfir등은 leech와 ghost로 구성되는 악의적인 리더와 태그 쌍을 이용하여 10cm 인 통신 거리를 최대 55cm까지 늘리는 실험에 성공하였다[2]. 또한 이러한 시스템이 100달러 이하에 구현 가능함을 참고문헌에서 보이고 있다[3]. 이는 실제로 대중교통 시스템에 13.56Mhz 방식의 교통카드를 이용하는 결제 시스템에 적용하여 다른 사람의 교통카드를 이용하여 나의 승차요금을 지불하는 등과 같은 공격이 가능할 수 있다는 것을 보여주며, Thomas S.등은 이와 관련된 취약성 분석[4]을 하였다. 이와 유사한 실험으로 블루투스 디바이스의 경우 10미터 정도의 통신거리를 약 100미터 까지 높이는 실험도 성공하였다[5].

이러한 중계공격을 예방하기 위해서는 다음의 3가지 방법들이 고려될 수 있다[6]. 첫 번째로 태그가 보내는 신호의 세기를 측정하여 실제로, 태그가 물리적으로 가까이 있는지 거리를 측정하는 방법으로, 이는 신호의 세기를 증폭시키는 디바이스를 활용한 공격에 약한 단점이 있다. 두 번째로 GPS등과 같은 지리정보 시스템의 도움으로 실제 디바이스의 물리적인 위치를 측정하는 것으로 이는 경량화된 RFID 시스템에 적용하기에는 비용적인 부담이 크다고 할 수 있다. 세 번째 방법으로 Distance-Bounding 프로토콜을 이용하여 리더와 태그 사이의 응답시간 차이를 측정하는 방법으로 이는 어떠한 매체도 빛의 속도보다 빠르게 전송될 수 없다는 이론에 근거하고 있다[7]. 빛의 속도는 1ns에 약 30cm의 거리를 이동할 수 있으며, 이를 RFID시스템에 적용하여 물리적으로 가까운 곳에 위치하지 않으면, 특정 신호를 보내고 받는데 시간차가 발생하기 때문에 이러한 시간차이 측정을 통하여 물리적으로 태그가 근처에 있음을 측정하는 방법이다.

본 논문의 2장에서는 Distance-Bounding 프로토콜을 자세히 살펴보고, 이를 RFID에 적용한 다양한 방법들을 알아본다[7][8][9][10]. 그리고 중계공격의 자세한 공격형태를 분석하고, 기존의 연구들에서 언급되지 않고 있는 태그의 아이디 전송과 관련하여 살펴본다. 3장의 제안하는 프로토콜에서는 기존의 제안된 논문들의 단점을 해결한 중계공격을 예방하는 효율적인 Distance-Bounding 프로토콜을 제안하며, 4장의 공격 가능성 및 보안성 분석에서는 기존 연구 대비 제안하는 논문의 공격 성공률 및 태그의 위치 추적 가능성과 태그의 익명성 그리고 전방향 안전성 만족여부를 살펴보고, 태그의 아이디 검색 및 에러 검증여부와 관련하여 제안하는 논문의 효율성을 분석하고 있다. 그리고 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 관련연구

2.1 Distance-Bounding Protocols

Distanec-Bounding Protocols(이하 DBP)은 Brands와 Chaum에 의해 제안된 프로토콜로 일반적인 DBP는 저속 → 고속 → 저속의 단계로 진행되며, 처음 저속단계에서는 태그 리더 간의 필요한 공유값을 사전에 주고 받으며, 중간의 고속 단계는 거리 체크를 위한 빠른 속도의 정보 교환이 이루어진다. 마지막 저속단계에서는 고속단계에서 주고받은 정보들에 대한 검증을 수행한다. 처음과 마지막의 저속단계는 생략되기도 하지만, 중간의 고속단계가 DBP의 핵심 단계로 반드시 포함되어야한다. 고속단계에서는 어떠한 암호학적 연산도 없으며, XOR 연산과 같이 수 나노초 정도의 매우 빠른 연산만을 수행하는데 이것은 연산속도로 인한 지연을 막기위함이다[1]. 고속단계에서 검증을 원하는 검증자(이하 V)는 증명자(이하 P)에게 한 비트씩 시도(challenge) 비트를 보내고 그에대한 응답(response)으로 한 비트씩 빠른속도의 응답비트를 V에게 보낸다. 이러한 응답은 일정한 상한값(upper-bound)이내에 이루어져야 하며, V는 단계의 시작과 끝 시간의 시간차를 체크하여 상한값 이내에 메시지가 송수신 되었는지를 판단하여, P가 물리적으로 주변에 있음을 인증할 수 있다.[7]

2.1.1 프로토콜의 기본 구조

prover (P) : 인증을 원하는 증명자
verifier(V) : 증명자를 검증하는 검증자
$\|$: 연접연산
α_i : V가 생성하는 랜덤한 비표값 $(i=1, 2, ..., n)$
β_i : P가 생성하는 랜덤한 비표값 $(i=1, 2, ..., n)$
$\oplus$: XOR 연산
m_i : $m_1\|.....\|m_n$
γ_i : $\alpha_i \oplus m_i$ 하여 나온 결과값 $(i=1, 2, ..., n)$

Distance-Bounding 프로토콜의 기본 구조는 [그림 1]과 같으며, 이 구조는 저속(slow)단계 없이 고속(Fast)단계와 저속단계의 2가지 단계로 이루어져 있다.

1) 고속단계에서 V는 랜덤한 0과 1의 비트를 P에게 한 비트씩 전송하고 이를 전송받은 P는 전송받은 비트에 랜덤한 비트로 한 비트씩 응답을 한다. 총 n번의 비트 교환이 끝나면, P는 서로 주고 받은 비트의 모든 값을 연접한 결과로 a를 얻는다.

$$a \Leftarrow \alpha_1 \| \beta_1 \| \ldots\ldots \| \alpha_n \| \beta_n \qquad (i)$$

2) 저속단계에서 V는 위의 고속 단계에서의 비트 교환이 상한값(upper-bound)이내에 이루어 졌는지를 검증하고, 상한값 이내에 비트 교환이 이루어진 경우, P는 a값을 서명하여 V에게 전송하여 자신이 실제 P가 맞음을 검증받는다.

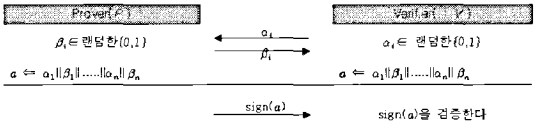

그림 1. Distance-Bounding 프로토콜의 기본 구조

2.1.2 프로토콜의 확장 구조

프로토콜의 확장 구조는 [그림 2]와 같이 저속→고속→저속의 3단계로 이루어져 있다.

1) 처음 저속단계에서 P는 랜덤한 0과 1의 n개를 연접하여 안전한 채널을 통하여 V에게 보낸다

$$\text{commit}(m_1 \| \ldots\ldots \| m_n) \qquad (i)$$

2) 고속단계에서 V는 랜덤한 0과 1의 값인 α_i를 P에게 전송하고, α_i를 전송받은 P는 V가 보낸 α_i와 m_i를 XOR 연산하여 그 결과값인 γ_i를 V에게 전송한다.

$$\gamma_i \leftarrow \alpha_i \oplus m_i \qquad (ii)$$

3) 마지막 저속단계에서 P는 V가 보내온 α_i와 (ii)의 γ_i를 모두 연접한 결과 값인 a를 서명하여 V에게 보내고, V는 이를 검증한다.

$$a \leftarrow \alpha_1 \| \gamma_1 \| \| \ldots\ldots \| \alpha_n \| \gamma_n \qquad (iii)$$

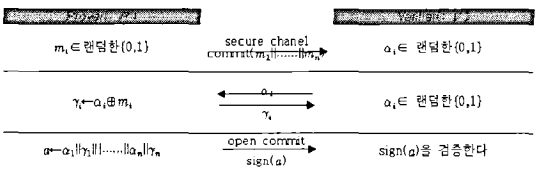

그림 2. Distance-Bounding 프로토콜의 확장 구조

2.1.3 프로토콜의 특징

DBP의 기본 구조와 확장 구조의 Mafia Fraud 공격 성공 확률은 $(1/2)^n$이며[7], 두 구조의 차이점은 기본 구조의 경우 고속 교환단계에서 송/수신되는 값들은 서로 비의존적 구조이지만, 확장 구조의 경우는 γ_i 값은 α_i에 의존적이이다. 또한 확장 구조에서는 XOR 연산을 사용함으로써 V가 받은 γ_i가 P가 보낸 것인지 아닌지를 분별할 수 있다는 것이 차이점이다. 확장 구조의 문제점은 서명하여 보낸 값이 정당한 인증을 원하는 원래의 P인지의 여부를 판단할 수 없으며, 아이디 값의 전달이 없다는 점이다.

2.2 중계 공격(Relay Attack)

중계 공격은 실제 인증과정에서 어떠한 메시지의 암호학적 위/변조 과정이 없이 단순히 전송되는 메시지를 전달하는 형태의 공격이며, 형태에 따라서는 사전에 메시지의 위/변조를 통하여 특정 정보를 얻을 수는 있어도 이는 실제 인증 과정에서 전송되는 메시지를 위/변조 하는 과정은 아니다. Avoine등은 다음의 4가지의 중계 공격 시나리오를 정의하고 있다[6].

1) Cheat Fraud - 증명자(이하 P)와 검증자(이하 V) 사이에 공격자(이하 A)가 없는 형태의 공격 시나리오 이다. 이때 P는 악의적인 공격자로 볼 수 있다.

2) Man-In-The-Middle(이하 MITM) - MITM은 P와 V사이에 A라는 악의적인 공격자가 개입하는 것으로 A는 P와 V사이의 메시지 전송을 보류하고, P의 메시지를 가로채서 V에게 대신 전달할 수 있으며, 이때 메시지의 위/변조가 가능하다(이때 위/변조 되는 메시지는 실제 인증과정에서 사용되는 메시지가 아닌 사전 정보를 얻기 위한 메시지의 위/변조 과정이다). MITM은 P가 악의적인지 아닌지 구별하지 않는 형태의 공격 시나리오이다.

3) Mafia Fraud - MITM 공격 시나리오에서 P가 악의적이지 않은 경우에 해당한다.

4) Terrorist Fraud - MITM 공격 시나리오에서 P가 악의적인 경우에 해당한다. 여기서 P와 A가 하나의 요소로 취급되면 이는 위에서 살펴본 Cheat Fraud와 같은 공격 시나리오가 될 수 있다.

2.3 용어

이하 관련연구 및 제안 프로토콜에서 다음의 용어로 표현하고 기술하였다

N_P, r_P : 태그가 생성하는 랜덤한 비표값(n bits)
N_V, r_V : 리더가 생성하는 랜덤한 비표값(n bits)
k : 태그 리더 간에 공유하는 비밀값 (n bits)
f : 의사 난수 함수
c_i: 리더가 생성하는 랜덤한 비표값 $(i=1,2,...,n)$
C_P : 미리 정해놓은 공개된 상수값
ID_P, ID : 태그의 아이디 (평문의 n bits)
ID_V : 리더의 아이디 (평문의 n bits)
$\oplus$: Execlusive-OR 연산

$$R_i^{c_i} : \begin{cases} R_i^0 : & if \quad c_i = 0 \text{ 또는 } c_i' = 0 \\ R_i^1 : & if \quad c_i = 1 \text{ 또는 } c_i' = 1 \end{cases} \quad (i=1,2,...,n)$$

R_i^0 : $f(k,\ ID_P \| ID_V \| r_P \| r_V)$
R_i^1 : $R_i^0 \oplus k \quad (i=1,2,...,n)$
$R^0 = ID \oplus f_k(N_P \| N_V),\ f_k(C_P, N_P)$
$R^1 = ID \oplus f_k(N_V \| N_P),\ R_i^0 \oplus k \quad (i=1,2,...,n)$
err_c : 시도((challenge)비트의 에러
err_r: 응답(response) 비트의 에러
err_t : 시간의 상한값에 대한 에러
err_c : $c_i \neq c_i'$ 인 경우 err_c +1 $\quad (i=1,2,...,n)$
err_r : $c_i = c_i'$이고 $R_i^{c_i} \neq (R_i^{c_i})'$ 인 경우 err_r+1 $\quad (i=1,2,...,n)$
err_t : $c_i = c_i'$이고 $R_i^{c_i} = (R_i^{c_i})'$이고 $\Delta t_i > t_{max}$ 인 경우 err_t+1 $\quad (i=1,2,...,n)$
T : 실패율에 대한 허용 임계치
t_P : 태그가 생성하는 값으로, 리더에게 태그 자신을 인증하기 위한 것이다.
t_V : 리더가 생성하는 값으로, 태그에게 리더 자신을 인증하기 위한 것이다.
$f_k(Value)$: k 를 키 값으로 갖는 의사랜덤함수로 n비트 이상의 비트값을 입력값으로 받아서, 출력값으로 n bits를 출력하는 함수이다.
ΔT_s : 빠른 교환 단계에서 교환을 시작하는 시간
ΔT_e : 빠른 교환 단계에서 교환을 종료하는 시간
ΔT_{time} : 빠른 교환 단계의 상한값으로 ΔT_e - ΔT_s 의 값이 ΔT_{time} 보다 큰 경우 리더는 태그의 인증을 거절한다.
tc : 시간차이 보정 상수로, 빠른 교환 단계에서 ΔT_{time}를 초과한 경우, 그 값을 보정해 주기 위한 값이다.
ΔT : $err_c + err_r + err_t$ 값과 비교되는 임계치 값
err_i : err_c나 err_r의 에러가 발생한 경우 표 1의 검증테이블의 err_i 필드를 err로 표기함.

표 1. 검증 테이블

i	1	2	..	n
c_i	c_1	c_2	..	c_n
$R_i^{0'}$	if(c_1=0) $R_1^{0'}$ else 'Null(-)'	if(c_2=0) $R_2^{0'}$ else 'Null(-)'	..	if(c_n=0) $R_n^{0'}$ else 'Null(-)'
$R_i^{1'}$	if(c_1=1) $R_1^{1'}$ else 'Null(-)'	if(c_2=1) $R_2^{1'}$ else 'Null(-)'	..	if(c_n=1) $R_n^{1'}$ else 'Null(-)'
ID_i	$R_1^{c_1'} \oplus v_1^{c_1}$	$R_2^{c_2'} \oplus v_2^{c_2}$	..	$R_n^{c_n'} \oplus v_n^{c_n}$
err_i	-	-	..	-

2.4 An RFID Distance Bounding Protocol

Hancke와 Kuhn은 Distance Bounding 프로토콜의 개념을 RFID 시스템 환경에 적용한 An RFID Distance Bounding Protocol(이하 RDBP)를 제안하였다[8]. RDBP를 설명하기 위하여 2.1절의 설명과 같이, 인증을 원하는 객체(*prover*)는 태그(또는 *P*)로 검증자(*verifier*)는 리더(또는 *V*)로 표기하여 설명한다.

2.4.1 프로토콜의 가정

RDBP는 다음과 같은 3가지의 가정을 하고있다.

1) 보안 목표의 가정 : RDBP 는 태그 리더 간에는 인증만을 수행하며, 이와 관련된 부인방지 기능을 제공하지 않는다.

2) 암호학적 가정 : 태그 리더간에는 암호화 키를 이용한 의사난수함수를 가지고 있으며, 공격자는 태그와 리더간에 공유하는 의사난수함수와 이 함수에 사용된 암호화키를 알 수 없다.

3) 시간적 가정 : 의사난수함수의 계산 시간은 수밀리초가 소요되며, Distance-Bounding 의 핵심 과정인 고속 교환단계에서의 최대 지연시간은 10 나노초 정도가 소요된다.

2.4.2 프로토콜 구조

RDBP의 구조는 DBP와 다르게 서명과정을 포함하지않으며 [그림 3]과 같이 저속 → 고속의 단계로 이루어진다.

1) 처음 저속단계에서 리더와 태그는 서로의 랜덤한 비표값인 N_V와 N_P를 주고 받는다. 그리고 교환된 비표값을 이용하여 다음과 같이 총 2n 비트의 값을 생성한다.

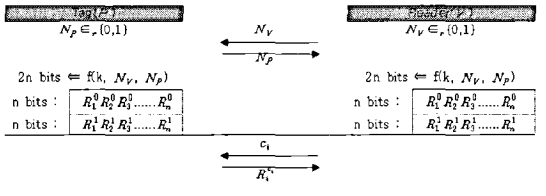

그림 3. An RFID Distance Bounding Protocol

$$2n \text{ bits} \Leftarrow f(k,\ N_V,\ N_P)$$

생성된 2n 비트는 다음과 같이 처음의 n 비트는 R^0 값으로 할당되고, 나머지 n 비트는 R^1값으로 할당된다.

$$R_1^0 R_2^0 R_3^0 \ldots\ldots R_n^0, \quad R_1^1 R_2^1 R_3^1 \ldots\ldots R_n^1$$

2) 고속단계에서 리더는 태그에게 랜덤한 비표값인 c_i를 한 비트씩 보내고, 태그는 리더에게 c_i가 0이면 R_i^0를, c_i가 1이면 R_i^1를 한 비트씩 전송한다. 즉, $R_i^{c_i}$를 리더에게 응답값으로 전송하며 이는 총 n번 주고받으며, 송/수신에 걸리는 시간은 사전에 정의된 시간 내에 이루어져야 한다. $(i = 1, 2, ..., n)$

2.4.3 프로토콜의 특징

RDBP는 DBP에 비하여 인증 시간이 빠르다. 이는 DBP의 경우는 DBP의 경우 마지막 저속 단계에서 태그의 서명에 걸리는 시간과 서명 값을 전송하는 시간이 소요되지만, RDBP는 고속단계에서 인증과정을 함께 수행하기 때문에 DBP는 RDBP 보다 전체적인에 인증시간이 더 많이 걸린다[8]. RDBP의 공격 성공률은 공격 시나리오가 Mafia Fraud인 경우는 $(1/2)^n$이고, Terrorist Fraud인 경우의 공격 성공률은 $(3/4)^n$로 이후 제안된 프로토콜들과 동일한 공격 성공률을 가지고 있다[8]. Terrorist Fraud 공격의 경우 공격 성공률이 $(3/4)^n$인 이유는, 악의적인 공격자가 사전에 고속 교환 단계에서 V가 전송할 비트를 미리 예상하여 P에게 전송하기 때문이다. 따라서 공격자는 나머지 절반의 비트만 예상하면 되기 때문에 Terrorist Fraud의 경우 공격 성공률이 더 높다고 할 수 있다. 일반적인 RFID 프로토콜은 태그 아이디 정보를 전송하는 것이 매우 중요한 요소임에도 불구하고 RDBP에서는 태그 아이디 전송을 수행하지 않는 것이 단점이라할 수 있다.

2.5 Detecting Relay Attacks with Timing-Based Protocols

Reid 등이 제안한 Detecting Replay Attacks with Timing-Based Protocols(이하 TBP)은 2.4절에서 살펴본 RDBP[8]에서 언급되지 않은 태그의 아이디 전송 과정을 추가한 형태의 프로토콜이다[9].

2.5.1 프로토콜 구조

TBP는 [그림 4]와 같이 저속 단계와 고속 단계의 2가지 단계로 이루어져 있다.

1) 처음 저속단계에서 리더와 태그는 서로 자신의 아이디 값(ID_P, ID_V)과 자신이 생성한 랜덤한 비표값(r_P, r_V)을 주고 받는다. 그리고 교환된 값(ID_P, ID_V, r_P, r_V)과 공유하는 비밀키(k)를 이용하여 R_i^0를 생성하고 이를 비밀키(k)와 XOR 연산하여 R_i^1를 생성한다.

$$R_i^0 \leftarrow f(k,\ ID_P \| ID_V \| r_P \| r_V), \quad R_i^1 \leftarrow R_i^0 \oplus k \quad (i)$$

2) 고속단계에서 리더는 랜덤한 비표값 c_i를 태그에게 한비트씩 전송하고, 이를 전송받은 태그는 $R_i^{c_i}$를 리더에게 한 비트씩 전송한다. 이 과정은 총 n번 이루어지며, 송/수신에 걸리는 시간은 사전에 정의된 시간 내에 이루어져야 한다.

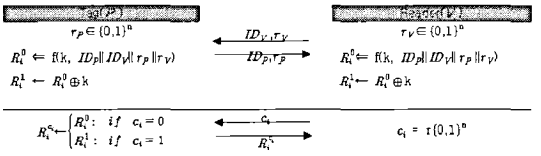

그림 4. Detecting Relay Attacks with Timing-Based Protocols

2.5.2 프로토콜의 특징

TBP[9]의 공격 성공률은 공격 시나리오가 Mafia Fraud인 경우는 $(1/2)^n$이고, Terrorist Fraud인 경우의 공격 성공률은 $(3/4)^n$로 기존에 제안된 프로토콜들과 동일한 공격 성공률을 가지고 있다[9]. TBP는 RDBP에서 제시하지 않은 태그 아이디의 전송을 하고 있으나, 태그 아이디를 평문형태로 전송하기 때문에 태그의 익명성이 보장되지 않는다. 또한 매번 같은 아이디 값을 전송하기 때문에 태그의 위치추적이 가능한 단점이 있다.

2.6 The Swiss-Knife RFID Distane Bounding Protocol

Kim등이 제안한 The Swiss-Knife RFID Distance Bounding 프로토콜(이하 SKP)은 상호인증 프로토콜(Mutual Authentication Protocol, 이하 MAP)의 구조

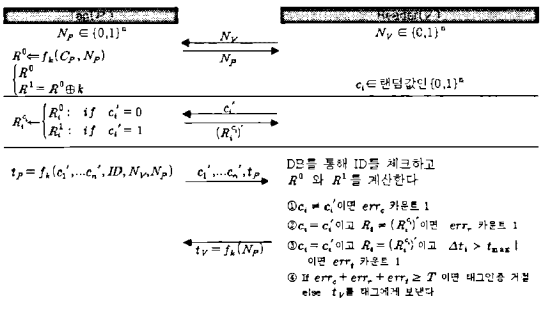

그림 5. The Swiss-Knife RFID Distance Bounding 프로토콜 구조

를 가지고 있다[10]. MAP에 대한 자세한 내용은 참고문헌를 참조하기 바란다[11,12].

2.6.1 프로토콜 구조

SKP는 [그림 5]와 같이 저속→고속→저속 단계의 인증과정이 진행된다.

1) 처음 저속단계에서 태그와 리더는 서로의 랜덤 비표값인 N_V와 N_P를 교환하고, 태그는 미리 정의된 상수값 C_P와 자신이 생성한 랜덤 비표값인 N_P를 이용하여 R^0를 생성하고, 비밀키 k와 XOR 연산을 하여 R^1을 생성한다.

$$R^1 = R^0 \oplus k \qquad (i)$$

2) 고속단계에서 리더는 미리 생성된 랜덤값인 c_i를 태그에게 빠른 속도로 한 비트씩 보내며, 이를 전송받은 태그는 c_i'(c_i는 전송도중에 에러가 발생할 수 있으므로 여기서는 c_i'로 표현함)가 0이면 R_i^0를 , c_i'가 1이면 R_i^1 를 리더에게 응답한다. 이때 리더는 처음 c_i를 전송한 시간과 마지막으로 c_i를 전송하여 $R_i^{c_i}$를 전송받은 시간의 차이를 Δt_i로 저장한다.

3) 마지막 저속단계에서 태그는 고속단계에서 전송받은 n비트의 c_i'와 ID, N_V, N_P를 입력값으로 f_k 를 이용하여 t_P를 생성하고 고속단계에서 전송받은 n비트의 c_i'와 t_P를 리더에게 전송한다. 리더는 t_P를 생성하는데 필요한 태그의 아이디 값인 ID를 제외한 모든 값을 알고 있으므로 데이터베이스에 저장된 태그들의 아이디 값을 이용하여 태그의 아이디 ID를 찾아낼 수 있다. 그리고 처음의 저속단계에서 태그가 생성한 것과 같이 R^0와 R^1를 생성할 수 있으며, 이를 이용하여 [그림5]에서 설명한 리더의 태그 인증과정이 ①~④로 진행된다.

2.6.2 프로토콜의 특징

SKP[10]의 공격 성공률은 앞에서 기술한 프로토콜과 동일한 공격 성공율을 가진다.

태그 아이디의 익명성 보장 : 평문이 아닌 암호화 형태로 태그 아이디를 전송한다.

태그 위치추적 공격을 피할 수 있다 : 매 세션마다 새로운 랜덤비표 값과 이를 이용한 값들을 전송한다.

에러 체크 기능 : 고속 교환단계에서 발생할 수 있는 비트에러의 검출을 위한 에러 체크 기능을 수행함으로써, 에러에 대한 저항성을 갖는다.

태그 아이디 검색이 비효율적 : 태그 아이디 값이 f함수를 이용하여 암호화된 형태로 전송되기 때문에, 이를 복호화하기 위해서 리더는 데이터베이스에 저장된 태그 아이디를 이용하여 암호화된 값을 생성해서 이를 비교해야 하는데, 이러한 경우에 데이타베이스 전체를 검색해야한다.

Ⅲ. 제안하는 프로토콜

RFID 태그와 리더 간에 태그 아이디의 안전한 전달이 매우 중요한 요소이며, 앞에서 살펴본 프로토콜 중에서는 TBP[9], SKP[10]에서만 태그의 아이디 전달 방법을 제시하고 있다. TBP[9]의 경우는 태그의 아이디를 평문 형태로 전송하여 태그의 익명성 및 위치추적 공격에 취약한 단점이 있으며, SKP[10]의 경우는 아이디의 정보를 찾기 위해서 최악의 경우 데이터베이스에 존재하는 RFID 태그의 아이디와 비밀키 k쌍의 모든 정보를 전수조사 해야 하는 구조이기 때문에, 데이타베이스의 검색면에서 효율성이 떨어진다. 따라서 제안하는 프로토콜에서는 태그 아이디를 평문이 아닌 형태로 전송하므로써 태그 아이디의 익명성 및 위치추적 공격으로부터 안전성 및 전방향 안전성의 제공과 거리 범위의 인증도 가능한 프로토콜을 제안한다. 더불어서 전송단계에서 발생할 수 있는 에러에 대하여 데이터베이스의 태그 아이디 정보와 매칭하여 검색하므로써 SKP의 단점인 데이타베이스 전수 조사로 인한 시간 낭비를 줄일 수 있을뿐만아니라 에러의 검색및 정정까지도 가능한 프로토콜을 제안한다.

3.1 프로토콜의 가정

제안하는 프로토콜은 다음과같은 가정을 한다.

1) 태그 리더간에 비밀정보인 k를 사전에 공유한다.
2) 공격자는 비밀정보인 k를 알 수 없다.
3) 공격자는 태그 아이디를 알 수 없다.
4) 프로토콜은 저속 → 고속 → 저속 의 3단계로 이

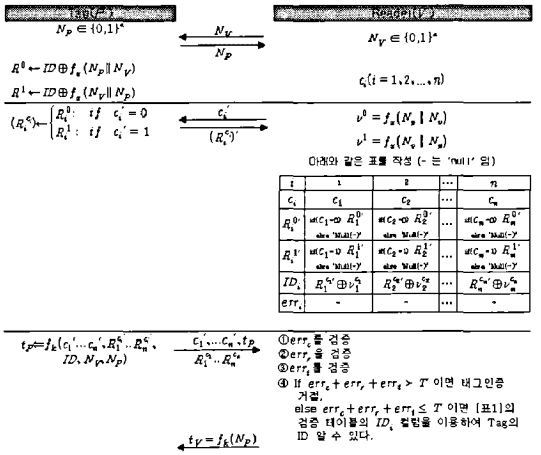

그림 6. 제안하는 프로토콜의 구조

루어지며, 저속단계에서는 에러 방지를 위한 에러 정정메커니즘이 하드웨어적으로 구현되어 에러가 발생하지 않는다고 가정한다. 따라서 에러는 고속단계에서만 발생할 수 있다.

5) err_c, err_r, err_t는 모두 0으로 초기화 된다.

3.2 프로토콜의 구조

[그림 6]과 같은 구조를 가지며 태그 리더 간에 세 단계로 통신을 한다.

1) 시작되는 저속 교환 단계 : 태그 리더 간의 랜덤한 비표값인 N_P 와 N_V를 교환하고, 태그는 다음과 같이 $R_i^0(i=1,2,\cdots n)$ 과 $R_i^1(i=1,2,\cdots n)$를 계산 한다.

$$R^0 = ID \oplus f_k(N_P \| N_V),\ R^1 = ID \oplus f_k(N_V \| N_P) \quad (\text{i})$$

그리고 리더는 랜덤한 시도(challenge) 값인 $c_i(i=1,2,...,n)$를 생성한다.

2) 다음 단계인 고속의 교환 단계가 시작되면 리더는 교환의 시작 시간인 ΔT_s를 기록하고, 랜덤하게 생성된 c_i를 태그에 전송한다. c_i를 전송받은 태그는 $c_i=0$ 인 경우 R_i^0 를 $c_i=1$ 인 경우 R_i^1 를 리더에 전송한다. 이러한 교환은 총 n번 반복되어 이루어지며 모든 교환이 완료되면 리더는 ΔT_e 를 체크한다. 리더는 중간 검증값인 $v_i^0(i=1,2,\cdots n)$와 $v_i^1(i=1,2,\cdots n)$를 다음과 같이 계산하고, 태그로부터 전송받은 $R_i^{c_i'}$ 값과 리더가 생성한 c_i 값을 이용하여 다음의 표를 만든다.

$$v^0 = f_x(N_P \| N_V),\quad v^1 = f_x(N_V \| N_P) \quad (\text{ii})$$

여기서 $R_i^{0'}$ 와 $R_i^{1'}$ 값은 c_i의 값에 따라서 하나의 값만 테이블에 채워지고 나머지는 null('-') 값으로 채워진다. 여기서 $R_i^{0''}$ 와 $R_i^{1''}$ 값은 c_i의 값에 따라서 하나의 값만 테이블에 채워지고 나머지는 null('-') 값으로 채워진다.

3) 마지막 단계인 저속단계로, 태그는 에러 체크와 자신의 검증을 위하여 다음과 같이 생성되는 t_P값과 고속단계에서 자신이 주고 받았던 $c_i'(i=1,2,...,n)$ 와 $R_i^{c_i'}(i=1,2,...,n)$ 를 함께, 리더에게 전송한다.

$$t_P = f_k\left(c_1', c_2', ..., c_n', R_1^{c_1'}, R_2^{c_2'}, ...R_n^{c_n'}, ID, N_P, N_V\right) \quad (\text{ii})$$

t_P를 전송받은 리더는 다음과 같이 3가지 에러변수를 계산하고, 최종적으로 ΔT와 비교하여 임계치를 넘지 않은 경우 리더는 태그를 인증한다.

3.2.1 err_c

리더 자신이 전송한 $c_i(i=1,2,...,n)$ 와 태그로부터 전송받은 $c_i'(i=1,2,...,n)$ 를 비교하여 만약 $c_i \neq c_i'$인 경우, 리더는 고속단계에서 오류가 있었음을 인식하고, 해당 비트에 대하여 'err' 라고 표기를 하고, err_c 값을 1 증가시킨다.

3.2.2 err_r

err_c 단계에서 에러가 발생하지 않은 경우, 리더는 자신이 전송받은 $R_i^{c_i'}(i=1,2,...,n)$ 값과 태그가 전송한 $R_i^{c_i}(i=1,2,...,n)$를 비교하여, $(c_i = c_i') \wedge \left(R_i^{c_i} \neq R_i^{c_i'}\right)$ 인 경우, 리더는 고속단계의 수신 과정에서 오류가 있었음을 인식하고, 해당 비트에 대하여 'err' 라고 표기를 하고, err_r 값을 1 증가시킨다. 이 경우, 실제로 수신 과정 중에 오류가 발생하였을 수도 있고, 공격자에 의하여 의도된 오류가 발생하였을 수도 있다.

3.2.3 err_t

Distance Bounding 프로토콜의 중요한 부분인 시간차이를 계산하는 과정으로 $(\Delta T_{time} > \Delta T_e - \Delta T_s)$ 인 경우, 고속 단계에서 시간차이의 임계치인 ΔT_{time}을 초과하여 교환이 일어났기 때문에 다음과 같이 err_t를 계산한다.

$$err_t = tc \times \left(\Delta T_e - \Delta T_s\right) \quad (\text{iii})$$

위의 3가지 에러 변수인 err_c, err_r, err_t의 계산이 완

료 되었으면 리더는 3가지 에러 변수의 합인 $err_c + err_r + err_t$를 계산하여 모든 에러의 임계치 값인 ΔT와 다음과 같이 비교하여 $err_c + err_r + err_t > \Delta T$인 경우 인증은 거절된다.

$err_c + err_r + err_t \leq \Delta T$인 경우 리더는 [표 1]의 검증 테이블의 ID_i 컬럼을 이용하여 태그의 아이디를 알 수 있다. 만약 에러가 발생하여 err_i 항목이 있는 경우 이 항목의 값들은 모든 경우의 수를 구하여 태그의 아이디 후보를 계산할 수 있다. (예를 들어 ΔT가 3 이고 err_t 에러가 발생하지 않은 경우, $err_c + err_r + err_t = 3$이라고 가정할 때, $2^3 = 8$인 총 8개의 ID_i 를 유추할 수 있다.) 리더는 태그의 아이디 값 후보를 생성하고, 생성된 아이디 후보값을 이용하여 다음과 같이 t_P'를 생성하여, $t_P' = t_P$ 인 경우 해당 아이디가 태그의 아이디임을 알 수 있다.

$$t_P = f_k(c_1', c_2', ..., c_n', R_1^{c_1}, R_2^{c_2}, ...R_n^{c_n}, ID, N_P, N_V) \quad \text{(iv)}$$

리더의 태그 인증이 완료되었으면, 리더도 태그에게 자신을 인증하기 위하여 t_V값을 다음과 같이 생성하여, 정당한 리더임을 인증 받을 수 있다.

$$t_V = f_k(N_V) \quad \text{(v)}$$

Ⅳ. 공격 가능성 및 보안성 분석

제안하는 프로토콜의 Mafia Fraud 및 Terrorist Fraud 공격에 대한 안정성을 살펴보면 다음과 같다.

4.1 Mafia Fraud 및 Terrorist Fraud 공격

Mafia Fraud 공격에서 공격자는 태그와 주고받는 정보를 위/변조 할 수 없고 단순히 정보를 중계만 할 수 있다. 따라서 제안하는 프로토콜에서는 고속단계에서 c_i의 응답에 해당하는 $R_i^{c_i}$ 를 1/2의 확률로 응답할 수 있다. ($R_i^{c_i} = 0$ 인 경우 또는 $R_i^{c_i} = 1$ 인 경우의 2가지 경우가 있을 수 있음) 따라서 전체적으로 총 n번의 시도(Challenge)와 응답(Response)에 대하여 공격자는 $(1/2)^n$의 확률로 공격에 성공할 수 있다. 이는 일반적인 Distance-Bounding 프로토콜의 Mafia Fraud 공격에서 일어날 수 있는 공격 성공률과 같다고 할 수 있다. Terrorist Fraud 공격에서는 공격자는 태그와 주고받는 정보 중 일부를 위/변조 하여 태그에 전송할 수 있다. 즉, 공격자는 저속단계 이후 고속단계가 시작하기 전에 미리 태그에게 특정정보를 변조하여 전송할 수 있다. 예를 들어 악의적인 공격자는 태그에게 c_i를 모두 0으로 전송하여 $R_i^0 (i = 1,2,\cdots n)$를 얻을 수 있으며, 또는 c_i를 모두 1로 전송하여 를 얻을 수도 있다. 공격자는 이를 이용하여 리더의 c_i 에 대한 응답값중 절반에 해당하는 $n/2$개의 정확한 응답을 할 수 있고, 나머지 절반은 확률적으로 0 또는 1로 응답할 수 있을 것이다. 따라서 전체 공격 성공률은 $(1/2 \times 1 + 1/2 \times 1/2)^n = (3/4)^n$이 된다. 이는 앞에서 살펴본 다른 프로토콜에서 일어날 수 있는 Terrorist Fraud 공격 성공률과 동일하다.

4.2 태그의 위치 추적 가능성 및 태그의 익명성과 전방향 안전성 만족 여부

태그의 위치 추적 불가능성 : 리더 태그 간의 통신 시에 태그는 항상 다른 랜덤 비표값인 N_P로 응답을 하기 때문에 태그의 추적이 불가능하다. 즉, 리더의 요청에 매번 다른 값으로 응답하기 때문에 동일한 태그인지 구분할 수 없다.

태그의 아이디 익명성 : 태그의 아이디를 직접 전송하는 것이 아닌 c_i 값에 따라 R_i^0 나 R_i^1 의 응답정보에 XOR 연산을 통하여 결합된 형태로 전송하므로써 태그의 아이디를 노출시키지않고 리더로 전송할 수 있다.

전방향 안전성의 만족 : 리더 태그 간에 전송된 정보로 과거의 전송 정보를 알 수 없으며, 인증과정마다 새로운 랜덤값 N_V과 N_P를 사용하고, 고속 단계에서는 랜덤한 c_i 값을 전송하기 때문에 전방향 안전성을 만족한다.

4.3 태그 아이디 검색 및 에러 검증 여부

4.3.1 태그 아이디 검색 시간의 효율적인 단축

태그 아이디 검색 시간을 매우 효율적으로 단축시켰다. 그것은 데이터베이스의 리소스 절약을 위하여 리더에서 미리 태그 아이디의 후보를 생성하고 이를 t_P값과 비교하므로써 태그 아이디를 데이터베이스가 아닌 리더에서 검색 하는 방법을 사용하였다. SKP[10]의 경우, 태그 아이디와 비밀키(k)정보를 검색하기 위하여 데이터베이스의 $pair(ID, k)$ 정보를 검색하는데 최악의 경우인 데이타베이스 전체를 검색해야하는 문제점, 이것을 개선하기위하여 고속단계에서 태그 아이디 값을 $\oplus$연산하여 함께 전송하므로써, 태그 아이디의 검색에 있어서 데이터베이스의 도움 없이 태그 아

표 2. 프로토콜 비교

	Mafia Fraud 공격성공률	Terrorist Fraud 공격성공률	태그 아이디 전송여부	태그 아이디 익명성	에러 저항성	태그 아이디 검색시간	태그 아이디 검색위치
DBP[7]	$(1/2)^n$	$(3/4)^n$	No	No	No	-	-
RDBP[8]	$(1/2)^n$	$(3/4)^n$	No	No	No	-	-
TBP[9]	$(1/2)^n$	$(3/4)^n$	Yes	No	No	-	-
SKP[10]	$(1/2)^n$	$(3/4)^n$	Yes	Yes	Yes	최대 데이터베이스에 저장된 태그 아이디전체를 검색	데이터 베이스
제안하는 프로토콜	$(1/2)^n$	$(3/4)^n$	Yes	Yes	Yes	최대 $2^{(err_c+err_r)}$번 검색	리더

이디 값을 얻을 수 있다. 이는 검색에 소요되는 자원을 데이터베이스가 아닌 리더단에서 수행함으로써 검색시간의 단축을 물론, 동시에 다수의 요청이 데이터베이스에 요구되는 경우에는 더욱 효율적인 구조이다.

4.3.2 에러 검증 여부

RFID의 무선 환경인 제안하는 논문의 고속단계에서는 데이터의 송신 및 수신 단에서 에러 발생 가능성을 예측하기 때문에, 제안하는 프로토콜에서는 c_i'과 R_i'을 이용하여, 송신단에서 에러가 발생한 경우 err_c값을 증가시키고 [표 1]의 해당 err_i 필드를 체크 한다. 마찬가지로 수신단에서 에러가 발생한 경우 err_r값을 증가시키고 [표 1]의 해당 err_i 필드를 체크한다. 그리고 최종적으로 err_i 필드가 체크된 곳을 제외한 필드의 아이디 값을 알 수 있으며, 에러가 발생한 필드는 모든 경우의 수를 동원하여 태그 아이디의 후보값을 유추하여 t_p값과 비교하므로써 태그의 아이디를 찾아낸다.

4.4 제안하는 프로토콜의 효율성

[표 2]는 제안하는 프로토콜의 효율성을 기존에 제안된 프로토콜과 비교정리한 것이며, 공격자 입장에서의 공격 성공률은 다른 프로토콜과 동일하다.

태그 아이디의 전송 : DBP[7]와 RDBP[8]의 경우는 태그 아이디의 전송방법을 명시하지 않고 있는데 반하여, 본 논문에서는 고속단계에서 태그 아이디의 전송을 포함하고있다.

태그 아이디의 익명성을 보장 : 태그 아이디의 전송에서 TBP[9]의 경우는 평문의 형태로 전송하는 것에 반해, 본 논문은 암호화된 형태로 전송한다.

에러 저항성 및 검색시간의 효율적 단축 : 에러체크와 에러에 대한 저항성이 있으며, SKP[10]보다 태그 아이디의 검색 시간이 훨씬 단축된다. 즉 SKP는 데이터베이스의 모든 태그 아이디를 검색해야하지만, 본 논문에서 제안한 방법은 태그 아이디의 정보 중 에러가 발생 후보 비트만 대상으로 검색한다.

임계치($\triangle T$) 이상의 에러는 인증 거절 : 본 논문의 제안방법에서 검색 단계에서 비트수와 관련해서 지수적으로 검색시간이 증가하여 에러가 발생한 비트가 많은 경우에 시간이 매우 오래 걸릴 수 있기때문에 이는 $\triangle T$ 의 임계치를 정해두고 $\triangle T$ 이상의 에러가 발생한 경우는 리더는 태그의 인증을 거절한다.

데이타 베이스의 효율적 관리 : 다수의 리더가 태그의 아이디 정보를 얻고자 데이터베이스에 쿼리를 전송하는 경우에 SKP는 데이터베이스에 부하가 가중되는데 반해, 본 논문의 제안방법은 태그 아이디의 검색을 리더 측에서 하기때문에 데이터베이스에 더해지는 부하는 없다.

V. 결 론

본 논문에서는 RFID 시스템이 중계공격에 취약한[1-4]단점에대하여 태그 아이디의 안전한 전송및 태그-리더 간 정보교환시의 에러 저항성과 태그의 거리 인증 가능성, 그리고 태그 아이디 검색의 시간의 효율적인 단축이라는 점에서 기존 프로토콜과의 차별화된 장점으로써 중계공격을 방어하기위한 보다 효율적인 Distance-Bounding 프로토콜을 제안하였다.

일반적인 Distance-Bounding 프로토콜에 적용될 수 있는 Mafia Fraud 및 Terrorist Fraud 에서의 일반적인 공격 성공률인 $(1/2)^n$과 $(3/4)^n$의 공격 성공률은 본 논문에서 제안한 방법에서도 동일한 공격 성공률을 갖고있다는 점에서, 향후 공격 성공율을 더욱 낮출수 있는 방법에 대한 연구를 지속하여 진행해 나갈것이다.

참 고 문 헌

[1] Selwyn Piramuthu,"Protocols for RFID

tag/reader authentication", Decision Support Systems 43, pp.897-914, 2007

[2] Ziv. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smart-card systems", IEEE, In Conference on Security and Privacy for Emerging Areas in Communication Networks - SecureComm 2005, pp.47-58, September 2005

[3] Ilan Kirschenbaum1 Avishai Wool, "How to build a low-cost, extendedrange RFID skimmer", 15th USENIX Security Symposium, pp.43-57, 8 May 2006

[4] Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, Tom O'Hare, "Vulnerabilities in First-Generation RFID-enabled Credit Cards", Springer Berlin , Financial Cryptography and Data Security , Vol.4886, pp.2-14, 2007

[5] J. Hering, "The BlueSniper 'rifle'", Presented at 12th DEFCON, Las Vegas, 2004.

[6] Gildas Avoine, Muhammed Ali Bingol, Suleyman Kardas, Cedric Lauradoux, Benjamin Martin, "A Formal Framework for Cryptanalyzing RFID Distance Bounding Protocols", This work is partially funded by FP7-Project ICE under the grant agreement No.206546, 5 November 2009

[7] Stfan Brands, David Chaum, "Distance-Bounding Protocols", Springer Berlin/Heidelberg, Advances in Cryptology—EUROCRYPT '93 , Vol.765 of Lecture Notes in Computer Science, pp.344-359, May 1993

[8] Gerhard P. Hancke, Markus G. Kuhn, "An RFID Distance Bounding Protocol", IEEE, SecureComm, [4] C.Meadows, pp.67-73, 2005

[9] Jason Reid, Juan M. Gonzalez Nieto, Tee Tang, Bouchra Senadji ,"Detecting Relay Attacks with Timing-Based Protocols", ACM, ASIACCS, pp.204 - 213, March 2007

[10] Chong Hee Kim, Gildas Avoine, Francois Koeune, Francois-Xavier, Stadaert, Olivier Pereira, "The Swiss-Knife RFID Distane Bounding Protocol", Springer Berlin, ICISC 2008, vol 5461, pp.98-115 , 2008

[11] M. Bellare, P. Rogaway,"Entity Authentication and Key Distribution", Springer Berlin, CRYPTO' 93, Vol.773, pp.232-249, 1993

[12] J. D. Guttman, F. J. Thayer, L. D. Zuck ,"The faithfulness of abstract protocol analysis: Message authentication", IOS Press, Journal of Computer Security, Vol.12, pp.865-891, Number 6/2004

부 창 희 (Chang-Hee Boo) 정회원

1991년 2월 숭실대학교 전자계산학과 학사

2001년 2월 서울 산업대학교 컴퓨터공학과 석사

2010년 3월 숭실대학교 컴퓨터학과 박사과정

<관심분야> RFID 보안, 멀티미디어 보안, PKI, 정보보호

전 문 석 (Moon-seog Jun) 정회원

1981년 2월 숭실대학교 전자계산학과

1986년 2월 University of Maryland Computer Science 석사

1989년 2월 University of Maryland Computer Science 박사

1986년 9월~1989 12월 University of Maryland 강사

1989년 3월~7월 Morgan State University 조교수

1989년 9월~1991년 2월 New Mexico State University Physical Science Lab. 책임연구원

1991년 3월~현재 숭실대학교 정교수

<관심분야> 정보보호, 네트워크 보안, 전자여권, 암호학