DOI: 10.3745/KIPSTC.2008.15-C.6.469

동기화 문제를 해결한 새로운 동적 아이디기반 RFID 상호 인증 프로토콜

임 지 환[†] · 오 희 국[††] · 김 상 진[†††]

요 약

기 제안된 해쉬 기반 RFID(Radio Frequency Identification) 인증 프로토콜들은 리더와 태그간의 인증을 위해 이용하는 정보가 태그에 고정되어 저장되어 있는 값인지, 동적으로 변경되며 저장되는 값인지에 따라 두 가지 유형으로 분류할 수 있다. 본 논문에서는 이를 각각 정적 아이디기반과 동적 아이디기반 인증 프로토콜로 분류하고 이들 각각의 장단점에 대해서 살펴본다. 또한 본 논문에서는 전방향/후방향 위치추적, 동기화, 위장 공격의 개념을 포함하는 새로운 보안 모델을 제시하며 이에 근거해 기 제안된 프로토콜들과 제안하는 프로토콜의 안전성을 분석한다. 제안하는 프로토콜은 기 제안된 프로토콜들에 비해 더욱 강화된 사용자 프라이버시를 제공하면서 태그 및 데이터베이스의 연산량 측면에서도 더 효율적으로 태그를 인식할 수 있다.

키워드 : RFID 프라이버시, 해쉬 기반 RFID 인증 프로토콜, 동기화

A New Dynamic-ID based RFID Mutual Authentication Protocol Eliminated Synchronization Problem

Jihwan Lim[†] · Heekuck Oh[††] · Sangjin Kim[†††]

ABSTRACT

The recently proposed RFID(Radio Frequency Identification) authentication protocol based on a hash function can be divided into two types according to the type of information used for authentication between a reader and a tag: either a value fixed or one updated dynamically in a tag memory. In this paper, we classify the protocols into a static ID-based and a dynamic-ID based protocol and then analyze their respective strengths and weaknesses. Also, we define a new security model including forward/backward traceability, synchronization, forgery attacks. Based on the model, we analyze the previous protocols and propose a new dynamic-ID based RFID mutual authentication protocol. Our protocol provide enhanced RFID user privacy compared to previous protocols and identify a tag efficiently in terms of the operation quantity of a tag and database.

Keywords : RFID Privacy, Hash-Based RFID Authentication Protocol, Synchronization

1. 서 론

RFID 시스템은 RF통신을 이용하여 원거리에서 개체의 정보를 읽을 수 있는 자동인식 기술로서 태그 또는 태그가 부착된 개체를 인식하는데 그 기능적 목적이 있다. 일반적인 RFID 시스템은 RFID 태그, RFID 리더, 호스트 시스템의 3가지 구성요소를 가지고 있으며 리더와 백엔드 시스템은 안전한 채널이 형성되어 있음을 가정하여 단일 개체로 간주되기도 한다[1,4-7]. RFID 태그는 리더의 질의에 무조건적으로 반응하는 작은 무선 디바이스이다. 리더는 태그에게 질의(query)를 보내 태그의 고유 아이디를 응답받고 데이터베이스로부터 고유 아이디와 맵핑되는 EPC(Electronic Product Code)를 획득하게 된다[1].

RFID 시스템에서는 그 잠재적 응용 가능성만큼이나 프라이버시 보호에 대한 필요성도 강조되고 있다. 공개된 채널(insecure channel)로 리더와 통신하는 태그는 리더의 신호에 반응하여 정당한 리더인지에 대한 확인 없이 자신의 고유 정보를 전송하기 때문에 악의적인 공격자에 의한 프라이버시 침해 문제를 야기 시킬 수 있다. 프라이버시 측면에서

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성·지원사업의 연구결과로 수행되었음.
※ 이 논문은 2008년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2006-000-10957-0).
† 준 회 원 : 한양대학교 컴퓨터공학과 박사과정
†† 종신회원 : 한양대학교 컴퓨터공학과 교수
††† 종신회원 : 한국기술교육대학교 인터넷미디어공학부 조교수
논문접수 : 2008년 9월 24일
수 정 일 : 1차 2008년 11월 5일
심사완료 : 2008년 1월 7일

RFID 시스템은 정당한 리더 이외의 누구도 특정 태그에 관련된 정보를 획득할 수 없게 하는 것에 목적이 있으며 보안적 측면에서는 정당한 리더와 태그간의 상호인증을 보장하여 RFID 시스템의 기능적인 완전성을 제공하는 것이 RFID 시스템의 목적이라 할 수 있다.

본 논문에서는 RFID 시스템에서 고려되어야하는 보안이슈들을 반영하여 RFID 보안 모델을 제시하고 강화된 사용자 프라이버시 및 효율성을 보장하는 동적 아이디 기반 RFID 상호인증 프로토콜을 제안한다. 또한 제안한 보안 모델을 이용하여 기 제안된 관련 연구 및 제안하는 프로토콜의 안전성을 분석한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 RFID 시스템의 프라이버시와 보안에 관한 모델링 관련 연구들과 해쉬 기반 인증 프로토콜의 분류에 대해서 소개한다. 3장에서는 공격의 목적, 공격자의 능력, 공격 게임을 포함하는 RFID 보안 모델 정의하며, 4장에서는 제안한 보안 모델을 이용하여 기 제안된 인증프로토콜의 안전성을 분석한다. 5장에서는 새로운 동적 아이디 기반의 RFID 상호인증 프로토콜을 제안하며 6장에서 제안한 프로토콜의 안전성 및 효율성을 분석하고 7장에서 결론을 짓는다.

2. RFID 보안과 프라이버시

2.1 RFID 보안 모델

지금까지 RFID 인증 프로토콜에 대한 많은 연구 결과들이 발표되고 있지만 안전한 RFID 시스템에 관한 정형적인 모델에 관한 연구는 상대적으로 많은 비중을 차지하진 못했다. 최근 들어 RFID 시스템의 프라이버시와 보안에 관한 보안 모델을 설계한 몇 몇 연구 결과들이 발표되고 있다[2-7]. 이들 연구는 RFID 시스템에 대한 정형적인 보안 모델을 제안하여 이론적인 안전성의 등급을 제시하고 있으며 공격자의 능력과 공격의 목적(aim)으로 정리될 수 있는 공격자 모델에 따라 주장하는 스킴의 안전성을 분석하고 있다.

Avoine[2]은 RFID의 보안 이슈를 서비스 거부(Denial of Service)와 프라이버시 2가지 측면으로 구분하고 있으며 태그 정보의 노출 뿐 아니라 비밀성이 보장된 정보의 추적 가능성에 대한 개념을 소개하였다. Avoine의 모델에서 공격자는 태그를 물리적으로 포획할 수 있는 능력이 있으며 포획된 태그 메모리 정보를 획득하여 공격에 이용할 수 있다. Avoine은 공격자가 이용할 수 있는 오라클의 종류(Query, Send, Execute, Reveal)에 따라 공격자의 등급을 결정하였으며 위치 추적의 등급을 *Existential-UNT*(untraceability), *Forward-UNT*, *Universal-UNT*의 3가지로 구분하여 프로토콜을 분석하였다.

Juels[4] 등은 Avoine의 모델을 보다 현실적이면서 간단한 모델로 다시 정의하였다. Juels 등은 오라클의 결정적 함수가 아닌 태그 내부의 상태에 따라 가변적인 출력을 만들어내는 모델을 정의하기 위해서 각 참여 객체의 기능성(functionality)을 정의해 보안 모델을 정의한다. Juels 등의 모델에서 공격자는 부-채널 공격(side-channel) 수 있는 기능성의 질의 횟수를 변수화하여 RFID 스킴의 프라이버시의 등급을 *(r, s, t)-Privacy*로 정의하였다.

Vaudenay[6]는 Damg˚ard-Østergaard[5] 등의 모델을 기반으로 모든 통신 메시지를 모니터할 수 있고 제한된 시간 동안 태그를 추적할 수 있으며 태그를 포획하고 부-채널 공격을 수행 할 수 있는 강한 공격자의 개념을 모델링하였다. 공격자를 부-채널 공격을 할 수 있는지의 여부에 따라 *narrow/wider* 공격자로 분류하고, 다시 태그 포획 능력의 정도에 따라 *Strong, Destructive, Forward, Weak*의 공격자 등급을 나눈다. Vaudenay는 제안한 모델의 *narrow-strong privacy*가 대칭키 기반 스킴에서 만족될 수 없다고 주장하고 공개키 기반의 RFID 인증 프로토콜을 제안한다.

2.2 해쉬 기반 RFID 인증 프로토콜

지금 까지 제안된 RFID 프라이버시 문제 해결 기법은 크게 해쉬 기반의 접근[3,4,6-12], 재-암호화 기반의 접근[13-15], XOR 기반의 접근[16-20]의 3가지로 분류할 수 있으며, 다시 해쉬 기반의 RFID 상호 인증 프로토콜들은 리더와 태그간 인증을 위해 이용하는 정보가 태그에 고정되어 저장되어 변하지 않는 값인지, 동적으로 갱신되며 저장되는 값인지에 따라 동적 아이디 기반[3,6-10]과 정적 아이디 기반[4,11,12]의 상호 인증 프로토콜로 분류할 수 있다[22,23].

먼저 정적 아이디 기반 상호인증 프로토콜에서 태그는 리더의 질의에 고정된 아이디(인증/식별 정보) 값을 사용하여 응답한다. 즉 매 세션마다 랜덤수를 사용하는 방법으로 응답하는 값을 변형하긴 하지만 태그에 저장되어 있는 고유 아이디 자체는 변경되지 않는다. 즉 정적 아이디 기반 상호인증 프로토콜은 태그가 고정된 아이디 값을 유지하기 때문에 태그-데이터베이스간 공유하고 있는 비밀정보에 대한 동기화가 필요 없다. 하지만 태그는 고정된 아이디 값을 매 응답마다 변형하여 응답하기 위해 자신의 랜덤 수와 아이디를 해쉬하여 전송하게 되는데 데이터베이스가 이 메시지로부터 태그를 구분하고 인증하기위해서는 매번 수신한 난수 값과 태그 ID를 저장하고 있는 태그의 수만큼 해쉬하여 비교해 보아야하는 단점이 있다. 또한 태그가 변형 억제(tamper resistant) 기능을 가지도록 만드는 것이 태그의 생산가격 측면에서 현실적이지 못 하다는 점을 감안할 때 태그 포획 능력이 있는 공격자는 태그를 포획하여 저장되어 있는 고유 아이디 정보를 획득할 수 있고 이를 이용하여 태그 사용자의 과거 행적을 추적할 수 있어 전방향 안전성(forward secrecy)을 만족시킬 수 없다는 단점이 있다.

반면 동적 아이디 기반 상호인증 프로토콜에서 태그는 매 세션마다 새로운 아이디로 이전 세션의 아이디를 갱신하여 리더의 질의에 응답하는 값을 변형한다. 동적 아이디 기반 상호인증 프로토콜은 정상적인 경우 동기화된 아이디 및 인증 정보를 이용하여 데이터베이스에서 저장하고 있는 아이디를 별도의 계산과정 없이 검색을 통해 태그를 인식할 수 있으며 아이디 갱신에 일방향 함수(one-way function)를 활

용하여 전방향 안전성을 보장해 줄 수 있는 장점이 있다. 하지만 이를 위해서 데이터베이스와 태그는 갱신되는 아이디 및 인증 정보를 동기화하여 유지하여야 하고 동기화가 깨진 경우 재 동기화를 위한 알고리즘이 필요하다는 단점이 있다.

3. 보안 모델

본 장에서는 기 제안된 보안 모델들에서 중점적으로 다루어지고 있는 위치추적 프라이버시 이외에 서비스 거부와 위장 공격의 개념을 포함하는 새로운 RFID 보안 모델을 정의하고 이를 이용해 기 제안된 프로토콜 및 제안하는 프로토콜을 분석한다. 제안하는 보안 모델에서는 리더와 백엔드 시스템간의 통신 채널을 안전한 채널로 가정하며, 공격자는 Juels[4] 등의 모델에서처럼 전방(forward) 채널과 후방(backward) 채널[2]을 모두 도청할 수 있다고 가정한다. 즉 리더와 백엔드 시스템을 하나의 개체로 간주하며, 공격자는 리더-태그 구간의 통신 채널을 도청할 수 있고 제약적으로 태그를 포획하여 태그의 메모리 채널[2]을 도청할 수 있다고 가정한다.

3.1 표기법

본 논문에서는 다음과 같은 표기법을 사용한다.

- T: RFID 시스템의 태그 집합 $T=\{t_1, t_2, \ldots, t_n\}$
- R: RFID 리더 객체
- I_m: 프로토콜 세션 구간, 세션구간 $I_m=[I_{m_1}, I_{m_s}]$은 총 s 개의 프로토콜 세션으로 구성
- *Challenger*: 공격자와 객관적 공격 게임을 수행할 제 3의 개체
- $\Omega_{I_m}(T)$: 태그 집합 T에 대해 구간 I_m에서 공격자가 획득할 수 있는 실험 결과 집합
- O: 공격자가 이용할 수 있는 오라클의 집합 $O \subset \{L, S, F, D, C\}$

$O^+(X)$는 'X' 오라클을 포함하는 모든 오라클의 부분 집합을 의미하고 $O^-(X)$는 'X' 오라클을 제외한 모든 오라클의 부분 집합을 의미한다.

3.2 공격의 목적

본 모델에서 공격자는 태그-리더 구간의 기밀성이 보장된 전송 메시지에 대해 위치추적, 서비스 거부, 위조 공격시도하며 공격자가 무시할 수 없는 확률[6]로 다음과 같은 성과를 거두었을 때 공격자의 해당 공격이 성공하였다고 말한다.

- 위치추적(Traceability): 공격자는 임의 태그 또는 태그 집합을 다른 태그들로부터 구분해 이전 있었던(forward) 또는 다음에 벌어질(backward) 행적을 추적할 수 있다.
- 서비스 거부(Denial of Service): 공격자는 RFID 시스템이 임의 태그 또는 태그 집합을 인식/인증 할 수 없게 할 수 있다.
- 위조(Forgery): 공격자는 특정 태그를 위장하여 해당 태그인 것처럼 인증 받을 수 있다.

본 모델에서 태그-리더 구간의 전송메시지는 랜덤 오라클[21]을 기반으로 기밀성이 확보되어 있다고 간주하며, 서비스 거부 공격의 경우 RFID 시스템을 대상으로 하는 자원 고갈(resource exhaustion)류의 공격이 아닌 프로토콜의 취약성을 이용하여 특정 태그 또는 태그 집합을 불능으로 만드는 공격만을 고려한다.

공격자가 변형 억제(tamper-resistance) 기능을 구현할 수 없는 태그를 물리적으로 포획하였다면 이는 태그의 모든 기능을 획득하였다고 할 수 있으므로 위에 제시한 공격자의 목적 중 서비스 거부와 위조 공격의 경우에는 태그 포획이 가능한 공격자는 고려하지 않는다.[1] 다만 공격자의 태그 포획은 포획시점 이후의 태그 제어권을 의미하므로 위치추적의 경우 포획 시점 이전 행적에 대한 추적 불가능성을 제공할 수 있어야하며 이를 보장할 때 전방향 안전성을 만족한다고 한다.

본 보안 모델에서는 공격자가 어떤 프로토콜에 대해 위 3가지 공격 목적을 달성할 수 없을 때 해당 프로토콜이 *TDF-O-Secure*하다고 정의한다.

3.3 공격자의 능력

본 모델에서의 공격자는 정당한 리더-태그 구간의 모든 메시지를 도청할 수 있으며, 통신에 끼어들어 전송되는 메시지를 선택적으로 전달할 수 있고 태그를 포획하여 내부 정보를 읽어 들일 수 있다.

공격자는 공격을 위한 수단으로 다음과 같은 오라클을 사용할 수 있다.

- LISTEN(t_i, R, I_m): 구간 I_m에서 공격자 A가 태그 t_i와 R간 통신 채널의 메시지를 도청한다.
- SEND(t_i, m, I_m): 구간 I_m에서 공격자 A가 태그 t_i에게 메시지 m을 전송하고 이에 대한 응답을 수신한다.
- FORWARD(t_i, R, I_m, m_1, m_3): 구간 I_m에서 공격자 A가 태그 t_i에게 메시지 m_1을 보내고 이에 대한 응답을 수신해 R에게 보낸다. 이후 공격자는 R의 응답 m_3를 태그 t_i에게 전달한다.
- DESYNCH(t_i, R, I_m, m_1): 구간 I_m에서 공격자 A가 태그 t_i에게 메시지 m_1을 보내고 이에 대한 응답을

1) Vaudenay는 자신의 *Destructive* 공격자 모델에 포획된 태그는 포획 이후 더 이상 정상적인 RFID 태그로서의 역할을 수행 할 수 없다는 제약을 포함시키고 있는데 이는 의미적으로 본 논문의 모델과 같은 공격자 가정이다. 반면 Vaudenay의 *Strong* 공격자 모델에서 공격자는 태그를 포획한 후 키 등의 태그 내부 정보를 획득한 후에도 태그를 정상적으로 시스템에서 동작시킬 수 있는 능력을 가지고 있다. Vaudenay 등은 *Strong* 공격자 모델에 대해 안전한 RFID 스킴은 대칭키 기반의 프로토콜로는 구현할 수 없고 공개키 기반의 키 동의 프로토콜이 필요하다고 분석하고 있다. 해쉬 기반의 RFID 인증 프로토콜을 제안하는 본 논문에서 서비스 거부와 위조 공격에 대해 포획이 가능한 공격자를 배제하는 이유도 Vaudenay의 분석과 같은 이유에 있다. 즉 본 모델에서는 Vaudenay의 *Strong* 공격자 모델은 고려하지 않는다.

수신해 R에게 보낸 후 세션을 종료 시킨다.

- CORRUPT(t_i, I_m): 구간 I_m에서 공격자 A가 태그 t_i를 포획해 내부 메모리 정보를 획득한다.

3.4 공격 게임

제안하는 모델의 위치추적, 서비스 거부, 위조 공격은 공격자와 *Challenger* 간의 공격 게임으로 정의할 수 있다. O를 공격자가 사용할 수 있는 오라클의 집합($O \subset \{L, S, F, D, C\}$)이라고 할 때 *Oracle*은 태그 t_i 또는 태그 집합 $T=\{t_1, t_2, \ldots, t_n\}$와 세션 구간 I_m을 입력으로 공격자 오라클 집합 O를 실험하여 그 결과 집합 $\Omega_{I_m}(T)$를 출력한다.

3.4.1 위치추적 게임

1) 구간 I_m에서 공격자 A는 *Oracle*(T, I_m, O)를 이용하여 모든 태그 T에 대한 실험 결과 집합 $\Omega_{I_m}(T)$를 획득한다.
2) *Challenger*는 공격 대상 태그 t_b를 랜덤하게 선택하여 ($b \in \{1,2,\ldots,n\}$) 공격자 A에게 넘긴다.
3) 구간 I_l에서 공격자 A는 *Oracle*(t_b, I_l, O)를 이용하여 태그 t_b에 대한 실험 결과 집합 $\Omega_{I_l}(t_b)$를 획득한다.
4) 공격자 A는 실험 결과 집합 $\Omega_{I_m}(T)$, $\Omega_{I_l}(t_b)$로부터 임의 알고리즘 Φ를 이용하여 $\Omega_{I_m}(t_i)=\Phi(\Omega_{I_l}(t_b))$를 만족하는 태그 t_i를 찾는다.
5) 공격자 A는 t_b가 t_i라고 추측한다.

3.2절에서 언급하였듯이 오라클 CORRUPT를 사용할 수 있는 공격자 A-O^*(C)는 $l \le m$인 구간에서 모든 태그에 대해 추적이 가능하므로 $l \le m$인 경우에는 공격자 A-O^c(C)만을 고려하며 해당공격자에 대해 위치 추적에 안전한 프로토콜을 *T-O^c(C)-Secure* 하다고 정의한다. 다만 공격자 A-O^*(C)에 대해 $l > m$인 경우에도 위치추적에 안전한 프로토콜을 전방향 안전성을 보장하는 프로토콜이라고 정의하며 *T-O*(C)-Secure* 하다고 한다. 전방향, 후방향 안전성을 모두 보장하는 프로토콜을 *T-O-Secure* 하다고 정의한다.

3.4.2 비동기 게임

1) *Challenger*는 공격 대상 태그 t_b를 랜덤하게 선택하여 ($b \in \{1,2,\ldots,n\}$) 공격자 A에게 넘긴다.
2) 공격자 A는 구간 $I_m=[I_{m_1}, I_{m_s}]$에서 아래의 오라클을 필요한 만큼 전략적인 순서로 호출한다.
   2-1) SEND(t_b, m, I_m)를 호출해 태그 t_b에게 메시지 m을 전송하고 m'을 수신한다.
   2-2) FORWARD(t_b, R, I_m, m_1, m_3)를 호출해 t_b에게 메시지 m_1을 전송하고 이의 응답을 리더 R에게 전송한 후 리더의 응답 값 m_3를 돌려준다.
   2-3) DESYNCH(t_b, R, I_m, m_1)를 호출해 t_b에게 메시지 m_1을 전송하고 이의 응답을 리더 R에게 전송한 후 리더의 응답을 수신한 후 세션을 종료 시킨다.
3) 공격자 A는 $m_1 < m_s < l$인 구간 I_l에서 공격의 성공 여부를 추측한다.

위 비동기 공격에 대해 안전한 프로토콜을 *D-O-Secure* 하다고 정의한다.

3.4.3 위장 게임

1) 구간 I_m에서 공격자 A는 *Oracle*(T, I_m, O)를 이용하여 모든 태그 T에 대한 실험 결과 집합 $\Omega_{I_m}(T)$를 획득한다.
2) *Challenger*는 공격 대상 태그 t_b를 랜덤하게 선택하여 ($b \in \{1,2,\ldots,n\}$) 공격자 A에게 넘긴다.
3) $l \neq m$인 구간 I_l에서 공격자 A는 $\Omega_{I_m}(T)$를 이용하여 메시지 m_1'를 만들고 FORWARD(t_b', R, I_l, m_1', m_3)를 호출하여 t_b'를 t_b인척 위장하여 인증을 시도한다.

위 위장 공격에 대해 안전한 프로토콜을 *F-O-Secure* 하다고 정의한다.

3.2 절에서 언급하였듯이 서비스 거부와 위장 공격의 경우 공격자는 A-O^c(C)만을 고려한다. 즉 *DF-O-Secure*의 경우 기본적으로 *DF-O^c(C)-Secure*를 의미한다. 따라서 어떤 프로토콜이 *TDF-O-Secure*하다는 것은 *T-O-Secure*하고 동시에 *DF-O^c(C)-Secure*하다는 것을 의미한다. 반면 어떤 프로토콜이 *TDF-O^c(C)-Secure*하다는 것은 *T-O^c(C)-Secure* 하고 동시에 *DF-O^c(C)-Secure*하다는 것을 의미한다.

4. 관련연구

4.1 정적 아이디 기반 프로토콜

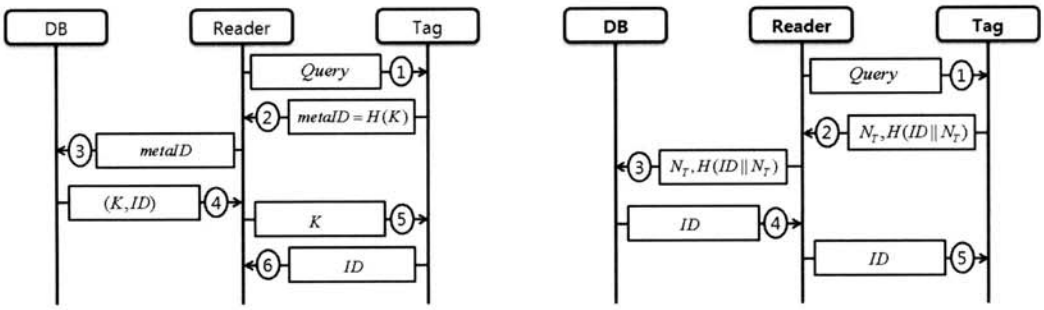
4.1.1 Weis 등의 Randomize Hash-Lock

Weis 등의 Hash-Lock과 Randomize Hash-Lock[12]은 대표적인 정적 아이디 기반 프로토콜이라 할 수 있다. Hash-Lock에서 태그는 리더의 질의에 자신의 $metaID=h(key)$를 리더에게 전송하고 데이터베이스는 *metaID*에 대응되는 태그의 ID와 *key*를 찾아서 리더에게 전송한다. 이후 리더는 *key*를 태그에게 전송하고 이를 확인한 태그는 리더에게 ID를 전송한다. Randomize Hash-Lock에서는 *metaID*로 고정된 응답에 변형을 주기위해 태그의 난수를 ID와 함께 해쉬하여 전송한다.

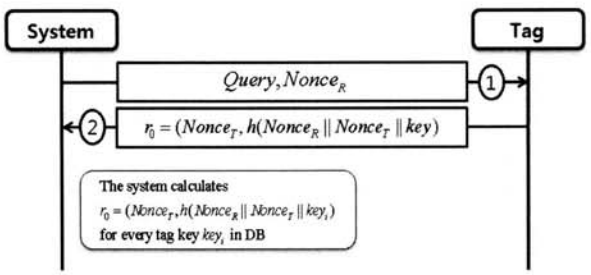
하지만 Hash-Lock 및 Randomize Hash-Lock 프로토콜은 리더의 질의에 응답하는 태그의 메시지를 확보한 공격자가 메시지 재전송을 통해 위장 공격을 할 수 있다. 또한 태그에게 전달되는 마지막 리더의 응답에 태그의 아이디 또는 키가 포함되어 있기 때문에 전방향, 후방향 위치추적이 가능하다. Weis 등의 프로토콜은 본 보안 모델에서 *D-O-Secure*[2] 프로토콜로 분류된다.

---

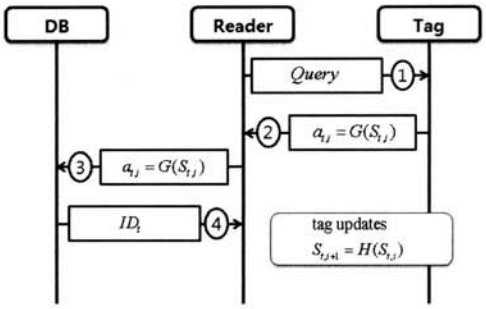
2) 논문 길이의 제약으로 사례 연구에 대한 증명은 6장의 제안하는 프로토콜에 대한 증명으로 대신한다.



(그림 1) Weis 등의 Hash-Lock 과 Randomize Hash-Lock



(그림 2) Juels 등의 Improved Randomize Hash-Lock



(그림 3) Ohkubo 등의 해쉬 체인 기법

4.1.2 Juels 등의 Improved Randomize Hash-Lock

Juels[4] 등은 Weis 등의 Randomize Hash-Lock 프로토콜을 계선하여 Improved Randomize Hash-Lock 프로토콜을 제안하였다. Improved randomize hash-lock 프로토콜은 첫 리더의 질의에 $Nonce_R$을 추가하여 재전송 공격에 강건하게 수정하였으며 리더의 질의에 태그는 자신의 $Nonce_T$와 $Nonce_R$를 추가하여 해쉬함으로서 위치추적에 대한 안전성을 확보한다. Ree 등은 Jules 등 보다 먼저 CRAP(Challenge-Response based Authentication Protocol)[11] 프로토콜을 제안한 바 있으며 두 프로토콜은 프로토콜의 메시지 흐름이 같아 동일한 프로토콜로 볼 수 있다.

하지만 이 프로토콜은 태그 내부에 저장된 고정된 ID 값을 확보한 공격자 A-O^*(C)에 의해 전방향 안전성을 보장할 수 없으며 시스템은 해쉬된 태그의 응답으로부터 매칭되는 태그 ID를 찾아내기 위해 데이터베이스에 저장된 태그의 수만큼 해쉬 연산을 수행해 보아야하는 단점이 있다. 이 프로토콜을 본 제안하는 보안모델에서 TDF-$O^c(C)$-$Secure$ 프로토콜로 분류된다.

4.2 동적 아이디 기반 프로토콜

4.2.1 Ohkubo 등의 해쉬 체인 기법

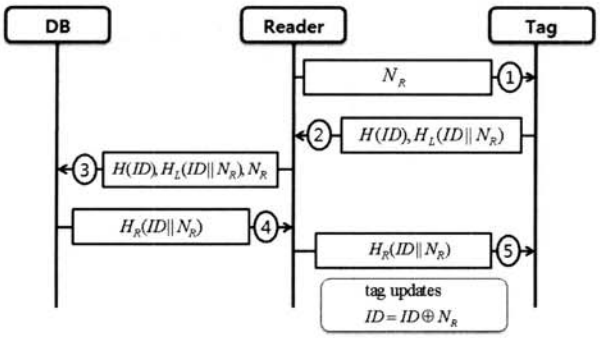
Ohkubo 등이 제안한 해쉬 체인 기법[10]은 두 개의 일방향 해쉬 함수를 이용하여 태그의 아이디를 변경하고 인증 정보를 생성하는 동적 아이디 기반의 인증 기법이다. 태그는 다음과 같은 두 개의 해쉬 함수 G, H: $0,1^* \rightarrow 0,1^l$를 사용한다. 태그는 리더의 질의에 비밀 값 $S_{t,i}$값을 사용하여 $S_{t,i+1} = H(S_{t,i})$ 값을 생성하고 G 해쉬 함수를 사용하여 $a_{t,i} = G(S_{t,i})$을 생성한다. 태그는 리더가 질의를 할 때마다, $S_{t,i+1} = H(S_{t,i})$, $a_{t,i} = G(S_{t,i})$을 생성하여 전송한다.

이 스킴은 일방향 함수를 이용하여 전방향 안전성을 보장하고 동적인 키 갱신을 통해 후방향 프라이버시를 보장하고자 하였다. 하지만 상호인증이 이루어지지 않아 공격자 A-$O^*(L,S)$에 의해 위조공격이 가능하다. 또한 데이터베이스는 모든 태그에 대한 시드 값 $S_{t,i}$ $(1 \le t \le n)$과 모든 해쉬 체인에 대해 $a'_{t,i} = G(H^{i-1}(S_{t,i}))$ $(1 \le i \le m)$를 계산하여 리더로부터 수신한 $a_{t,i}$와 일치하는 계산 결과 $a'_{t,i}$를 내는 시드 값 $S_{t,i}$를 찾아야한다. 즉 n을 데이터베이스에 저장되어 있는 태그들의 개수라고 하고 m을 해쉬 체인의 최대 길이라고 할 때 최악의 경우 데이터베이스는 태그의 인증에 O $(n \times m)$번의 해쉬 연산을 수행해야 한다.

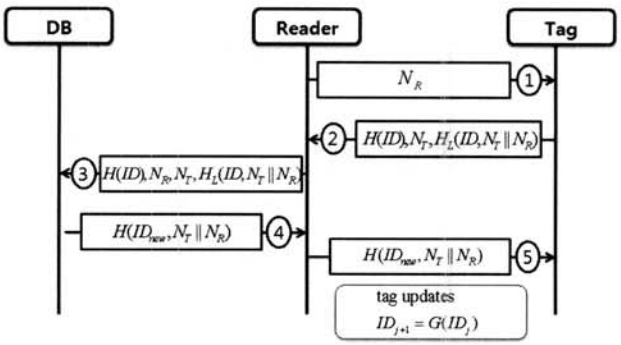
Juels 등은 Okubo 등의 스킴이 해쉬 체인의 최대 길이 이상의 질의에 대해 응답 불능이 되는 특징을 이용하여 공격 대상 태그를 "*mark*"하여 다른 태그들로부터 구분해내는 공격 알고리즘을 제시한 바 있다[4]. 이 경우 공격자는 "*mark*"된 태그를 구분해 냄으로서 태그의 위치를 추적할 수 있게 되지만 본 논문에서는 이 공격을 비동기 공격으로 간주한다. 즉 Ohkubo 등의 해쉬 체인 기법은 본 모델의 T-O-$Secure$ 프로토콜로 분류된다.

4.2.2 Lee 등의 LCAP 스킴

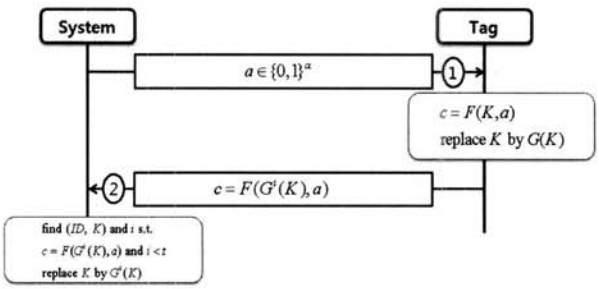
Lee 등이 제안한 LCAP(Low-Cost Authentication Protocol)[9]은 동적 아이디 기반 상호인증 프로토콜에서 발생할 수 있는 태그와 데이터베이스간의 비동기 문제를 해결하면서 재동기화를 위한 데이터베이스의 연산량을 효율적으로 개선한 상호



(그림 4) Lee 등의 LCAP



(그림 5) Dimitriou의 LTC



(그림 6) Vaudenay의 NDP

인증 프로토콜이다. 데이터베이스는 태그의 현재 아이디와 아이디의 해쉬 값 그리고 이전 세션의 아이디와 그 아이디의 해쉬 값을 비동기 상황의 제어를 위해 유지하고 있다. 태그의 아이디는 리더로부터 수신한 랜덤 수와 XOR하는 방법으로 갱신되며 데이터베이스는 별다른 연산 없이 태그의 리스트를 검색하는 것만으로 태그를 식별해 낼 수 있다.

하지만 이 프로토콜은 아이디의 갱신에 XOR 연산만을 사용하여 전방향 안전성을 보장하지 못하고 프로토콜의 마지막 메시지를 공격자가 의도적으로 차단하게 되면 태그는 항상 같은 값으로 리더의 질의에 응답하게 되어 구별불가능성을 만족하지 못하고 결과적으로 위치추적이 가능하게 된다. LCAP 스킴은 제안하는 모델의 *DF-O-Secure* 프로토콜로 분류된다.

4.2.3 Dimitriou의 LTC 스킴

Dimitriou는 일방향 해쉬함수를 사용하여 태그의 아이디를 갱신하는 방법으로 전방향 안전성을 보장해 줄 수 있는 LTC(Lightweight RFID protocol to protect against Traceability and Cloning attacks)[8] 프로토콜을 제안하였다. LTC는 동적 아이디 기반 상호 인증 프로토콜로 이전 세션 아이디를 일방향 함수로 해쉬하여 태그의 아이디를 갱신한다. 하지만 이 프로토콜은 동적 아이디에 기반을 두고 프로토콜을 설계하였음에도 불구하고 비동기에 대한 제어와 재동기화를 고려하지 않아 세션의 마지막 메시지가 공격자에 의해 또는 채널 오류로 인해 전달되지 않게 되면 ID의 비동기가 발생하여 데이터베이스가 태그를 식별할 수 없게 된다. LTC 스킴은 제안하는 모델의 *TF-O-Secure* 프로토콜로 분류된다.

4.2.4 Vaudenay의 NDP 스킴

Vaudenay는 Ohkubo 등의 해쉬 체인 기법을 변형하여 NDP(Narrow-Destructive-Private RFID scheme based on a random oracle)[6] 프로토콜을 제안하였다. 시스템 리더는 α 비트 난수 a를 생성하여 태그에게 전송하고 태그는 수신한 난수 a를 현재 키 K와 함께 해쉬하여 응답 값 $c=F(K,a)$를 만들어낸다. 이후 태그는 현재키 $K=G(K)$로 갱신한다. 리더는 자신이 유지하고 있는 모든 태그에 대해 $c=F(G^i(K),a)$ 값을 계산하고 일치하는 (ID, K)를 찾는다. 리더가 ID를 획득하게 되면 (ID, K)는 $(ID, G^i(K))$로 갱신된다.

본 스킴에서 시스템은 태그의 응답 값 $c=F(K,a)$와 매칭되는 $c=F(G^i(K),a)$를 계산하기 위해, 즉 $G^i(K) \equiv K$인 태그를 찾기 위해 데이터베이스에 저장되어 있는 모든 태그에 대해 $G(K)$를 최대 t번 해쉬하여 그 결과를 비교해본다. 따라서 태그를 인식하기 위한 데이터베이스의 연산량은 $O(n \times t)$가 되고 저자가 논문에 언급한 것처럼 시스템은 공격자에 의해 t번 이상 키가 갱신된 태그를 인식할 수 없게 된다. 따라서 이 스킴은 본 모델의 *TF-O-Secure* 프로토콜로 분류된다.

5. 제안하는 프로토콜

제안하는 RFID 시스템에서 태그 t_i는 각각 EPC_i에 의해 유일하게 식별될 수 있으며 시스템과 각 태그는 다음의 정보를 유지하고 있다.

- EPC_i: 태그 t_i의 EPC 코드.
- K_i^m: 태그 t_i와 데이터베이스간의 대칭키로 $K_i^{m+1} = H(K_i^m, N_R)$와 같이 계산된다.
- ID_i^j: 데이터베이스와 동기화되어 있는 태그 t_i의 j번째 동적 아이디로 다음과 같이 계산 된다. $ID_i^{j+1} = H(K_i^m, ID_i^j)$
- N_T, N_R: 각각 태그와 리더의 *Nonce* 값.
- C_Key_i: 데이터베이스가 다음 세션에서 태그를 인증할 때 사용하게 될 태그 t_i의 현재 키 값. 프로토콜이 정상

적으로 실행되고 있을 경우 태그와 데이터베이스의 키 값은 이 *C_Key* 값으로 동기화가 이루어져 있다.

- *P_Key* $_i$: 데이터베이스가 이전 세션에서 태그를 인증할 때 사용한 태그 t_i의 이전 키 값. 프로토콜이 비정상적으로 실행되고 있을 경우, 즉 태그와 데이터베이스간의 동기화가 깨졌을 경우 데이터베이스는 *P_Key*값을 이용하여 태그를 식별해낼 수 있다.

5.1 실행 단계

제안하는 프로토콜의 실행 단계에서 태그, 리더, 데이터베이스는 (그림 7)과 같은 메시지를 주고받으며 다음과 같이 동작한다.

- 단계 1: 리더는 태그의 응답에 메시지 최신성(freshness)을 보장하여 재전송 공격 및 스푸핑 공격을 방지하기 위해 *Nonce* N_R을 생성하여 전송한다.
- 단계 2: 태그는 리더로부터 수신한 N_R과 자신의 키 값 K_i^m, 랜덤 수 N_T를 이용하여 $H_L(K_i^m, N_R \| N_T)$을 계산하고 이를 리더에게 전송한다. 이후 태그는 자신의 현재 아이디 ID_i^j를 $ID_i^{j+1} = H(K_i^m, ID_i^j)$로 갱신한다. 태그의 아이디는 세션의 정상 종료 여부와 무관하게 갱신되는 것으로 태그는 리더의 질의에 응답한 직후 자신의 현재 아이디를 갱신한다.
- 단계 3: 단계 2의 메시지를 수신한 데이터베이스는 수신한 ID_i^j값으로 저장하고 있는 태그 리스트를 검색하여 같은 *ID* 값을 찾는다. 수신한 *ID* 값과 저장하고 있는 아이디 값이 같으면 데이터베이스는 해당 태그를 정당한 태그로 간주하게 되고 동기 상태의 확인과 키 갱신을 위해 해당 태그의 C_Key값으로 $H_L(K_i^m, N_R \| N_T)$을 계산한다. 만약 이 값이 수신한 값과 일치한다면 태그의 현재 아이디와 현재 킷값 그리고 이전 세션의 킷

	System 〔ID, C_Key, P_Key, EPC〕		Tag t_i 〔ID_i^j, K_i^m, N_T〕
1	Query, N_R	⇒	
2		⇐	$ID_i^j, N_T, H_L(K_i^k, N_R \| N_T)$

3	if(*stored ID* = *received* ID_i^j){
	if(received $H_L = H_L(\text{C\_Key}_i, N_R \| N_T)$){
	update C_Key: $K_i^{m+1} = H(K_i^m \| N_R)$
	P_Key: K_i^m
	}
	update $ID_i^{j+1} = H(K_i^m, ID_i^j)$
	}else{
	for all tag $x = [1, n]$
	if(received $H_L = H_L(\text{C\_Key}_x, N_R \| N_T)$){
	update C_Key: $K_i^{m+1} = H(K_i^m \| N_R)$
	P_Key: K_i^m
	ID_i^{j+1} = H(K_i^m, received ID_i)
	break
	}else if(received $H_L = H_L(\text{P\_Key}_x, N_R \| N_T)$){
	ID_i^{j+1} = H(K_i^m, received ID_i)
	break
	}
	}
			update
			$ID_i^{j+1} = H(K_i^m, ID_i^j)$

4	EPC, $H_R(K_i^m, N_R \| N_T)$	⇒	

5			if(H_R = received H_R){
			$K_i^{m+1} = H(K_i^m \| N_R)$
			}

(그림 7) 제안하는 프로토콜

값을 갱신한다. 만약 $H_L(K_i^m, N_R \| N_T)$ 값이 C_Key로 계산한 값과 일치하지 않으면 현재 태그의 키 K_i^m는 P_Key와 동기화 되어있는 것이므로 데이터베이스는 킷값은 갱신하지 않고 아이디 값만 갱신한다. 단계 2의 메시지를 수신한 데이터베이스가 수신한 아이디로 태그를 검색하지 못했다면 데이터베이스는 저장하고 있는 모든 태그의 C_Key값으로 $H_L(K_i^m, N_R \| N_T)$를 계산하여 수신한 값과 일치하는 값을 찾는다. 일치하는 값이 찾아 진 경우 데이터베이스는 현재 킷값과 이전 세션의 킷값을 갱신하고 수신한 메시지의 아이디 값을 이용해 현재 아이디 값을 갱신한다.

- 단계 4: 태그를 식별한 시스템은 태그의 EPC와 인증값 $H_R(K_i^m, N_R \| N_T)$을 태그 t_i에게 전송한다.
- 단계 5: 단계 4의 메시지를 수신한 태그는 $H_R(K_i^m, N_R \| N_T)$ 값을 검증하고 올바르게 검증되었다면 현재 키를 $K_i^{m+1} = H(K_i^m \| N_R)$로 갱신하여 저장한다. 단계 4의 메시지를 수신하지 못한 경우나 검증 값이 올바르지 않은 경우에 태그는 킷값을 갱신하지 않는다.

6. 분 석

본 장에서는 제안하는 프로토콜이 ***TDF-O-Secure*** 프로토콜임을 보인다.

Lemma 1. 제안하는 프로토콜은 공격자 $(A\text{-}O^{f}O\subset)\{L, S, F, D, C\}$에 대해 ***T-O-Secure***하다.

증명. 1) ***A-O^{f}(C)***에 대한 후방향 위치추적 불가능성

T-O-Secure를 증명하기 위해 3.3절에서 정의한 공격 게임을 생각해보자. 공격자 ***A-O^{f}(C)***는 다음과 같은 위치 추적 게임을 수행한다.

1) 공격자 A는 구간길이가 $s(=|I_m|)$인 $I_m=[I_{m_1}, I_{m_s}]$에서 $Oracle(T, I_m, O)$를 이용하여 모든 태그 $T=\{t_1, t_2, \ldots, t_n\}$에 대한 실험 결과 집합 $\Omega_{I_m}(T)$를 획득한다.
2) *Challenger*는 공격 대상 태그 t_b를 랜덤하게 선택하여 $(b\in\{1,2,\ldots,n\})$ 공격자 A에게 넘긴다.
3) 구간길이가 $u(=|I_l|)$인 $I_l=[I_{l_1}, I_{l_u}]$에서 공격자 A는 $Oracle(t_b, I_l, O)$를 이용하여 태그 t_b에 대한 실험 결과 집합 $\Omega_{I_l}(t_b)$를 획득한다.
4) 공격자 A는 실험 결과 집합 $\Omega_{I_m}(T)$, $\Omega_{I_l}(t_b)$로부터 임의 알고리즘 Φ를 이용하여 $\Omega_{I_m}(t_i)=\Phi(\Omega_{I_l}(t_b))$를 만족하는 태그 t_i를 찾는다.
5) 공격자 A는 t_b가 t_i라고 추측한다.

실험 결과 집합 $\Omega_{I_l}(t_b)$에 포함된 t_b의 응답 메시지 집합을 다음과 같이 분류해보자. 먼저 응답 ID 집합을 리스트 Γ에, 인증 정보 $H(Key, Nonce)$ $(H: 0,1^{\alpha}\rightarrow 0,1^{\beta})$ 집합을 리스트 Δ에 담아 분류한다. 같은 방법으로 구간 I_m에서 수집된 태그 응답 집합을 Γ'', Δ'이라 할 때 공격자는 $\gamma=\Phi(\gamma')$ $(\gamma\in\Gamma, \gamma'\in\Gamma')$ 또는 $\delta=\Phi(\delta')(\delta\in\Delta, \delta'\in\Delta')$을 만족하는 γ, γ', Φ과 δ, δ', Φ'을 찾을 수 있어야한다.

여기서 공격 게임을 공격자에게 더 유리하도록 수정한다. 수정된 게임은 구간 I_m에서 수집한 태그 응답 중 공격대상 태그 t_b의 응답을 공격자에게 직접 제시하고 I_m구간의 응답 집합 $\Gamma=\{ID_b^{m_1}, ID_b^{m_2}, \ldots, ID_b^{m_s}\}$, $\Delta=\{H(K_b^{m_1}, Nonce), H(K_b^{m_2}, Nonce), \ldots, H(K_b^{m_{s'}}, Nonce)\}(s'\le s)$과 I_l 구간의 응답 집합 $\Gamma'=\{ID_b^{l_1}, ID_b^{l_2}, \ldots, ID_b^{l_u}\}$, $\Delta'=\{H(K_b^{l_1}, Nonce), H(K_b^{l_2}, Nonce), \ldots, H(K_b^{l_{u'}}, Nonce)\}$ $(u'\le u)$에서부터 $\gamma=\Phi(\gamma')(\gamma\in\Gamma, \gamma'\in\Gamma')$ 또는 $\delta=\Phi(\delta')(\delta\in\Delta, \delta'\in\Delta')$을 만족하는 γ, γ', Φ과 δ, δ', Φ'을 찾는 게임이다.

공격자가 게임에서 이기기 위해서는 ① $\gamma=\Phi(\gamma')$ $(\gamma\in\Gamma, \gamma'\in\Gamma')$를 만족하는 γ, γ', Φ를 찾거나 ② $\delta=\Phi(\delta')$ $(\delta\in\Delta, \delta'\in\Delta')$ 을 만족하는 δ, δ', Φ'을 찾을 수 있어야한다.

① 제안하는 프로토콜에서 태그의 ID는 이전 ID와 다음 ID의 해쉬체인의 관계가 있으며 $ID_i^{j+1}=H(ID_i^j, Key)$의 형태로 계산된다. 따라서 일방향 해쉬 함수 $H^{(*)}$를 Φ로 하는 γ, γ' 쌍을 찾기 위해선 $ID_i^{m_j}$로부터 $ID_i^{m_{j+1}}$을 계산해 낼 수 있어야한다. 공격자 ***A-O^{f}(C)***는 α-bit의 Key에 대해 $1/2^{\alpha}$의 확률로 $ID_i^{m_j}$로부터 $ID_i^{m_{j+1}}$을 계산해 낼 수 있다. 따라서 $ID_i^{m_s}$로부터 $ID_i^{l_u}$을 계산할 확률, 즉 γ, γ' 쌍을 찾을 확률은 $1/2^{\alpha}$보다 작다.

② 같은 방법으로 $K_b^{m_{s'}}$와 $K_b^{l_{u'}}$는 해쉬체인 관계에 있으므로 일방향 해쉬 함수 $H^{(*)}$를 Φ'으로 하는 δ, δ' 쌍을 찾기 위해선 $K_b^{m_j}$로부터 $K_b^{m_{j+1}}$를 계산해 낼 수 있어야 한다. 따라서 α-bit의 Key 및 $Nonce$에 대해 $H(K_b^{m_s}, Nonce)$를 만족하는 $K_b^{m_s}$를 찾고 이로부터 $K_b^{m_{s+1}}$을 계산 해낼 확률, 즉 δ, δ' 쌍을 찾을 확률은 $1/2^{\alpha}$보다 작다.

①과 ②로부터 공격자가 $\Gamma, \Gamma', \Delta, \Delta'$로부터 t_b를 추적할 수 있는 확률은 $1/2^{\alpha-1}$보다 작으며 이는 무시할 수 있는 확률이다[6]. 따라서 본 프로토콜은 ***T-O^{f}(C)-Secure***하다.

증명. 2) A-O*(C)에 대한 전방향 프라이버시

위 위치 추적 게임을 $m>l$인 상황에서 진행한다. 단 공격자 ***A-O*(C)***는 구간 I_l에서 태그를 포획하여 태그의 현재 (I_l) 키를 포획한 상태이며 이전 구간의 결과 집합 $\Omega_{I_m}(T)$으로부터 공격 대상 태그의 응답을 구분하여야 한다. 1)과 마찬가지로 공격 대상 태그 t_b의 응답집합을 $\Gamma, \Gamma', \Delta, \Delta'$에 구분하여 담는다고 할 때 공격자는 $\gamma'=\overline{\Phi}(\gamma)(\gamma\in\Gamma, \gamma\in\Gamma')$ 또는 $\delta'=\overline{\Phi}'(\delta)(\delta\in\Delta, \delta'\in\Delta')$ 을 만족하는 $\gamma, \gamma', \overline{\Phi}$과 $\delta, \delta', \overline{\Phi'}$을 찾을 수 있어야 한다. 1)과 같은 방법으로 $\gamma, \gamma', \overline{\Phi}$과 $\delta, \delta', \overline{\Phi'}$ 쌍을

찾기 위해선 결국 $K_b^{m_{j+1}}$로부터 $K_b^{m_j}$를 계산해 낼 수 있어야 한다. 하지만 *Key* 갱신 사용하는 일방향 함수 Φ의 역함수 $\overline{\Phi}$는 일방향 함수의 가정에 따라 존재하지 않으며 *Key*를 계산할 수 없는 사용자가 γ, δ로부터 γ', δ'을 구할 수 있는 확률은 $1/2^{n-1}$보다 작다. 따라서 본 프로토콜은 *T-O*(C) -Secure*하다.

1)과 2)로부터 본 프로토콜은 *T-O-Secure*하다.

□

Lemma 2. 제안하는 프로토콜은 공격자 *A-O* ($O \subset \{L, S, F, D\}$)에 대해 *D-O-Secure*하다.

증명. 3.3절의 비동기 게임을 수행하는 공격자 A를 생각해보자. *Challenger*에게 공격 대상 t_b를 넘겨받은 공격자 A는 구간 $I_{m_1} \sim I_{m_*}$에서 SEND, FORWARD, DESYNCH 오라클을 전략적으로 호출한다. 공격자가 오라클을 호출할 때마다 태그와 데이터베이스의 내부 상태는 변경되게 되며 이에 따라 동기화 상태도 변하게 된다.

<표 1, 2>와 (그림 8)은 데이터베이스와 태그의 동기화 상태 및 재동기가 되는 과정을 게임에서 공격자가 어떤 오라클을 호출하는가에 따라 보여주고 있다. 데이터베이스와 태그의 동기화 상태는 <표 2>와 같이 5가지 상태로 분류할 수 있고 공격자의 *O(F,S,D)* 호출은 프로토콜에서 <표 2>와 같은 결과를 가져오게 된다.

〈표 1〉 태그와 데이터베이스의 동기화 상태

State	ID Synch.	Key Synch.
Normal-C	match	Synch. with C_Key
Normal-P	match	Synch. with P_Key
Abnormal-C	X	Synch. with C_Key
Abnormal-P	X	Synch. with P_Key
Broken	X	X

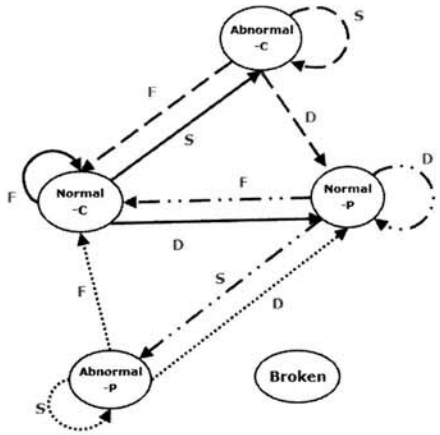
〈표 2〉 공격자의 활동(Oracle)에 따른 세션의 진행 상태

Oracle	프로토콜에서의 효과
FORWARD	정상세션
SEND	단계 2의 메시지차단
DESYNCH	단계 4의 메시지차단

공격자는 태그와 데이터베이스의 동기화 상태가 *State-Broken*로 전이되는 것을 목표로 오라클 *O(F,S,D)*를 전략적으로 호출하지만 (그림 8)의 동기화 상태 전이도에서 보이는 것처럼 어떠한 경우에도 *State-Broken*로 전이되지 않는다. 따라서 본 프로토콜은 *D-O-Secure* 프로토콜이다.

□

<표 3, 4, 5, 6>은 (그림 8)의 상태 변화를 세션의 진행 상태에 따라 데이터베이스와 태그의 아이디 및 키의 동기



(그림 8) 태그와 DB의 동기화 상태 전이도

〈표 3〉 정상상태에서 단계 2 메시지가 차단

Oracle	데이터베이스			태그		State
	ID	C_Key	P_Key	ID	Key	
Initial	ID_i^j	K_i^m	K_i^{m-1}	ID_i^j	K_i^m	N-C
S	ID_i^j	K_i^m	K_i^{m-1}	ID_i^{j+1}	K_i^m	A-C
F	ID_i^{j+2}	K_i^{m+1}	K_i^m	ID_i^{j+2}	K_i^{m+1}	N-C

〈표 4〉 정상상태에서 단계 4 메시지가 차단

Oracle	데이터베이스			태그		State
	ID	C_Key	P_Key	ID	Key	
Initial	ID_i^{j+2}	K_i^{m+1}	K_i^m	ID_i^{j+2}	K_i^{m+1}	N-C
D	ID_i^{j+3}	K_i^{m+2}	K_i^{m+1}	ID_i^{j+3}	K_i^{m+1}	N-P
F	ID_i^{j+4}	K_i^{m+3}	K_i^{m+2}	ID_i^{j+4}	K_i^{m+3}	N-C

〈표 5〉 단계 4, 단계 2의 메시지가 순차적으로 차단

Oracle	데이터베이스			태그		State
	ID	C_Key	P_Key	ID	Key	
Initial	ID_i^{j+4}	K_i^{m+3}	K_i^{m+2}	ID_i^{j+4}	K_i^{m+3}	N-C
D	ID_i^{j+5}	K_i^{m+4}	K_i^{m+3}	ID_i^{j+5}	K_i^{m+3}	N-P
S	ID_i^{j+5}	K_i^{m+4}	K_i^{m+3}	ID_i^{j+6}	K_i^{m+3}	A-P
F	ID_i^{j+7}	K_i^{m+4}	K_i^{m+3}	ID_i^{j+7}	K_i^{m+4}	N-C

〈표 6〉 단계 2, 단계 4의 메시지가 순차적으로 차단

Oracle	데이터베이스			태그		State
	ID	C_Key	P_Key	ID	Key	
Initial	ID_i^{j+7}	K_i^{m+4}	K_i^{m+3}	ID_i^{j+7}	K_i^{m+4}	N-C
S	ID_i^{j+7}	K_i^{m+4}	K_i^{m+3}	ID_i^{j+8}	K_i^{m+4}	A-C
D	ID_i^{j+9}	K_i^{m+5}	K_i^{m+4}	ID_i^{j+9}	K_i^{m+4}	N-P
F	ID_i^{j+10}	K_i^{m+5}	K_i^{m+4}	ID_i^{j+10}	K_i^{m+5}	N-C

〈표 7〉 관련 연구 및 제안하는 프로토콜의 안전성 및 효율성 비교.

	프로토콜 구분	위치추적		비동기	위장	비고	데이터베이스 연산량		태그의 연산량
		후방	전방				Normal	Worst	
Weis	정적	X	X	O	X	*D-O-Secure*	O(n)	O(n)	H+R*
Juels	정적	O	X	O	O	*TDF-O^c(C)-Secure*	O(n)	O(n)	2H+R
Ohkubo	동적	O	O	X	X	*T-O-Secure*	O(n × m)**	O(n × m)	2H
Lee	동적	X	X	O	O	*DF-O-Secure*	O(log n)***	O(log n)	2H+R
Dimitriou	동적	O	O	X	O	*TF-O-Secure*	O(log n)	O(n)	4H+R
Vaudenay	동적	O	O	X	O	*TF-O-Secure*	O(n × t)	O(n × t)	2H
Ours	동적	O	O	O	O	*TDF-O-Secure*	O(log n)	O(2n)	3H+R

H는 해쉬 연산, n은 저장하고 있는 태그의 수일 때, O(n)은 해쉬 연산을 최대 n번만큼 수행한다는 의미
*: R은 랜덤 수의 생성하기위한 연산.
**: m 은 태그가 가진 해쉬체인의 길이로 태그가 읽혀질 수 있는 최대 횟수를 나타냄.
***: 데이터베이스가 저장하고 있는 n개의 태그에 대해 해당 값을 비교 검색하는 검색비용을 의미

상태가 어떻게 변화되는지 예를 통해 보여주고 있다. <표 3>은 데이터베이스와 태그가 동기화 되어있는 상태(*State N-C*)에서 세션이 시작되어 공격자가 오라클 SEND를 호출한 후 세션을 종료 시킨 상황이다. 즉 공격자에 의해 프로토콜 단계 2의 메시지가 차단되어 세션이 종료된 것으로 데이터베이스와 태그의 동기화 상태가 <표 1>의 *State A-C*, 즉 아이디의 동기화는 깨어지고 데이터베이스에 저장된 태그의 이전 킷값과 태그의 현재 킷값이 동기화 되어있는 상태로 변하게 된 것을 보여준다.

Lemma 3. 제안하는 프로토콜은 공격자 A-$O(O \subset \{L, S, F, D\})$에 대해 *F-O-Secure*하다.

증명. 3.3절의 위장 공격 게임을 수행하는 공격자 A를 생각해보자. 공격자 A는 구간 I_m에서의 실험 집합 $\Omega_{I_m}(T)$을 획득한다. 이후 $l \neq m$인 구간 I_l에서 공격자는 $\Omega_{I_m}(T)$을 이용하여 t_b인척 위장하여 시스템으로부터 인증을 시도한다. 공격자는 공격에 성공하기 위해 다음이 가능해야 한다.

- 이전 구간에서 수집된 메시지로부터 적법한 메시지를 새롭게 생성하여 인증을 통과한다.
- 이전 구간에서 전송된 태그의 메시지를 재전송하여 인증을 통과한다.

하지만 공격자가 공격 대상 태그 t_b의 이전 메시지 m으로부터 인증 가능한 메시지 m'을 생성해 내기 위해선 위치추적게임에서처럼 태그 t_b의 키 K_b^m을 계산할 수 있어야한다. 공격자가 키를 계산할 수 있는 확률은 α-bit 키에 대해 $1/2^\alpha$이므로 이는 무시할 수 있다. 또한 제안하는 프로토콜은 태그 ID를 지속적으로 갱신하고 있으며 인증 값 H_L은 리더의 *Nonce*가 포함되는 형태로 메시지 최신성을 보장하고 있기 때문에 최신성이 확보되지 못한 재전송된 메시지는 (그림 7)에서 제시한 시스템의 태그 인증 알고리즘을 통과할 수 없다. 따라서 공격자는 이전 메시지의 재전송을 통해서는 인증을 통과할 수 없다.

따라서 본 프로토콜은 *F-O-Secure*하다.

□

Lemma 1, 2, 3로부터 제안한 프로토콜은 *T-O-Secure*하고 *D-O-Secure*하며 *F-O-Secure*하므로 *TDF-O-Secure*하다.

7. 결 론

본 논문에서는 기 제안된 해쉬 기반 RFID 인증 프로토콜들을 정적 아이디 기반 프로토콜과 동적 아이디 기반 프로토콜로 분류하고 이들 각각의 장단점에 대해서 살펴보았다. 또한 본 논문에서는 전방향/후방향 위치추적, 동기화, 위장공격의 개념을 포함하는 새로운 보안 모델을 제시하였으며 이에 근거해 기 제안된 프로토콜들과 제안하는 프로토콜의 안전성을 분석하였다. 제안된 동적 아이디기반 상호인증 프로토콜은 제안하는 보안 모델의 *TDF-O-Secure* 프로토콜로 분류되며 강화된 사용자 프라이버시를 제공하면서 태그 및 데이터베이스의 연산량 측면에서도 효율적으로 태그를 인식할 수 있다.

참 고 문 헌

[1] A. Juels, "RFID Security and Privacy: A Research Survey," IEEE Journal on Selected Areas in Communication, Vol.24(2), pp.381-394. 2006.

[2] G. Avoine, "Adversarial Model for Radio Frequency Identification," Cryptology ePrint Archive, Report 2005/049,

2005.

[3] C. Lim and T. Kwon, "Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer," *Proc. of the ICICS 2006*, Vol.4307 of LNCS, pp.1-20, Springer-Verlag, 2006.

[4] A. Juels and S. Weis, "Defining Strong Privacy for RFID," *Cryptology ePrint Archive*, Report 2006/137, 2006.

[5] I. Damgård and M.Ø. Pedersen, "RFID Security: Tradeoffs between Security and Efficiency," *Proc. of the CT-RSA 2008*, Vol.4964 of LNCS, pp.318-332, Springer-Verlag, 2008.

[6] S. Vaudenay, "On Privacy Models for RFID," *Proc. of the Asiacrypt 2007*, Vol.4833 of LNCS, pp.68-87, Springer-Verlag, 2007.

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

[8] T. Dimitriou, "A Lightweight RFID protocol to protect against traceability and cloning attack," *Proc. of the SecureComm 2005*, pp.59-66, 2005.

[9] S. Lee, Y. Hwang, "Efficient authentication for low-cost RFID systems," Proc. of the ICCSA 2005, Vol.3480 of LNCS, pp.619-629. Springer-Verlag, 2005.

[10] M. Ohkubo, K. Suzuki and S. Kinoshita, "Efficient hash-chain based RFID privacy protection scheme," *Proc. of the Workshop on Privacy: Current Status and Future Direction*, 2004.

[11] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," *Proc. of the SPC 2005*, Vol.3450 of LNCS, pp.70-84, Springer-Verlag, 2005.

[12] S.A. Weis, S. Sarma, R. Rivest and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," *Proc. of the SPC 2003*, Vol.2802 of LNCS, pp.201-212, Springer-Verlag, 2004.

[13] P. Golle, M. Jakobsson, A. Juels and P. Syverson, "Universal re-encryption for mixnets," *Proc. of the CT-RSA 2004*, Vol.2964 of LNCS, pp.163-178, Springer-Verlag, 2004.

[14] J. Saito, J. Ryou and K. Sakurai, "Enhancing privacy of universal re-encryption scheme for RFID tags," *Proc. of the EUC 2004*, Vol.3207 of LNCS, pp.879-890, Springer-Verlag, 2004.

[15] A. Juels and R. Pappu, "Squealing euros: Privacy protection in RFID-enabled Banknotes," *Proc. of the FC 2003*, Vol.2742 of LNCS, pp.103-121, Springer-Verlag, 2003.

[16] A. Juels, "Minimalist cryptography for Low-Cost RFID Tags," *Proc. of the SCN 2004*, Vol.3352 of LNCS, pp.149-164, Springer-Verlag, 2004.

[17] E. Choi, S. Lee and D. Lee, "Efficient RFID Authentication protocol for Ubiquitous Computing Environment," *Proc. of the SecUbiq 2005*, Vol.3823 of LNCS, pp.945-95, Springer-Verlag, 2005.

[18] A. Juels and S.A. Weis, "Authenticating Pervasive Devices with Human Protocols," *Proc. of the Crypto 2005*, Vol.3621 of LNCS, pp.293-308, Springer-Verlag, 2005.

[19] H. Gilbert, M. Robshaw and H. Sibert. "An Active Attack Against HB+ - A Provably Secure Lightweight Authentication Protocol," *IEE Electronics Letters*, Vol.41(21), pp.1169-1170, IET, 2005.

[20] K. Jonathan and J. Shin. "Parallel and Concurrent Security of the HB and HB+ Protocols," *Proc. of the Eurocrypt 2006*, Vol.4004 of LNCS, pp.73-87, Springer-Verlag, 2006.

[21] M. Bellare, P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," *Proc. of the CCS 1993*, pp.62-73, ACM, 1993.

[22] J. Lim, S. Kim and H. Oh, "A New Hash-base RFID Mutual Authentication Protocol Providing Enhanced User Privacy Protection," *Proc. of the ISPEC 2008*, Vol.4991 of LNCS, pp.278-289, Springer-Verlag, 2008.

[23] S. Kim, J. Lim, J. Han and H. Oh, "Efficient RFID Search Protocols Using Counters," *IEICE Trans. Commun.*, volume. E91-B(11), 2008.

임 지 환

e-mail : jhlim@cse.hanyang.ac.kr

2005년 한양대학교 전자컴퓨터공학부 (학사)

2007년 한양대학교 컴퓨터공학과(석사)

2007년~현 재 한양대학교 컴퓨터공학과 박사과정

관심분야 : 네트워크 보안

오 희 국

e-mail : hkoh@hanyang.ac.kr

1983년 한양대학교 전자공학과(학사)

1989년 아이오와주립대학 전자계산학과 (석사)

1992년 아이오와주립대학 전자계산학과 (박사)

1993년~1994년 한국전자통신연구원 선임연구원

1995년~현 재 한양대학교 컴퓨터공학과 교수

관심분야 : 암호프로토콜, 네트워크 보안

김 상 진

e-mail : sangjin@kut.ac.kr

1995년 2월 한양대학교 전자계산학과 (학사)

1997년 2월 한양대학교 전자계산학과 (석사)

2002년 8월 한양대학교 전자계산학과 (박사)

2003년 3월~현 재 한국기술교육대학교 인터넷미디어공학부 조교수

관심분야 : 암호기술 응용