

신뢰받는 제3자 기반의 RFID 태그 소유권 이전 프로토콜

김 영 식*

RFID Tag Ownership Relocation Protocol Based on Trusted Third Party

Young-Sik Kim*

요 약

최근 RFID는 수년 동안 재고관리, 물류 등 다양한 분야에 널리 활용되고 있을 뿐만 아니라 사물인터넷의 중요 구성 요소로 진화하고 있다. RFID의 활용분야가 증가함에 따라 RFID를 위한 보안 및 프라이버시 기술들에 대한 연구가 다양하게 이루어져 왔고, 그 중에서 RFID가 내장된 제품의 구매시 필요한 RFID의 소유권 이전을 위한 보안 프로토콜에 대한 연구도 활발하게 제안되어 왔다. 최근에 Kapoor와 PIRAMUTHU는 기존에 제안된 소유권 이전 프로토콜들이 갖고 있던 보안상의 문제점을 해결한 단일 RFID 태그의 소유권을 이전하는 새로운 프로토콜을 제안하였다. 이 논문에서는 Kapoor-PIRAMUTHU의 프로토콜 역시 보안상의 문제를 갖고 있음을 보이며, 이 문제를 해결한 새로운 프로토콜을 제안한다. 보안 분석을 통해 새로 제안한 프로토콜은 기존 프로토콜의 문제를 해결하였음을 보였다.

Key Words : ownership transfer protocol (OTP), trusted third party, authentication, RFID, lightweight cryptography

ABSTRACT

Recently RFID not only is widely utilized in various fields such as inventory management, merchandize logistics, etc., but also, has evolved as an important component of the Internet of Things (IoT). According to increasing the utilization field of RFID, studies for security and privacy for RFID system have been made diverse. Among them, the ownership transfer protocols for RFID tags have also been proposed in connection with the purchase of products embedded with RFID tag. Recently, Kapoor and PIRAMUTHU proposed a RFID ownership transfer protocol to solve the problems of security weakness of the previous RFID ownership transfer protocols. In this paper, we show that Kapoor-PIRAMUTHU's protocol also has security problems and provide a new protocol to resolve them. Security analysis of newly proposed protocol shows the security concerns are resolved.

1. 서 론

오늘날 RFID 시스템은 재고관리, 소매, 물류 등에 널리 활용되고 있으며, 향후 사물인터넷을 구성하게 될 중요 장치 중 하나가 될 것으로 전망된다^[1-4]. 그러

나 RFID 시스템은 오래 전부터 다양한 실제 응용 환경에서의 보안 및 프라이버시 문제에 대한 우려로 인해 이를 해결하기 위한 많은 연구들이 제안되어 왔다.

보안 및 프라이버시 문제와 별도로 RFID를 내장한 제품의 판매와 유통이 증가하면서 RFID의 소유권을

* 이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2014R1A2A2A01006870).

• First Author : Chosun University, Department of Information and Communication Engineering, iamyskim@chosun.ac.kr, 정회원
논문번호 : KICS2014-12-477, Received December 3, 2014; Revised February 28, 2015; Accepted March 16, 2015

이전하기 위한 소유권 이전 프로토콜(ownership transfer protocol; OTP)에 대한 연구도 함께 진행되어 왔다⁵⁻¹¹⁾. 소유권 이전 프로토콜에 참여하는 주체로는 권리를 이전하게 될 RFID 태그(tag) T , 태그를 소유 하던 원 소유자 혹은 판매자(seller), 태그를 소유하게 될 새로운 소유자 혹은 구매자(buyer)로 구성된다.

이 때 소유권이 이전된 후에는 이전 소유자가 태그에 접근하는 것이 차단되어야 한다. 이를 위해서는 크게 두 가지 다른 방법이 사용된다. 먼저 신뢰받는 제3의 기관(the trusted third party; 이후 TTP로 표기)를 통해 전체 소유권 이전을 관리하도록 하는 방법과 이전 소유자와 새로운 소유자 사이에 안전한 보안 통신 환경을 생성하는 방법이다. 이 때 새로운 소유자는 이전 소유자에게 노출되지 않고서 RFID 태그의 비밀키를 업데이트할 수 있어야 한다.

RFID 소유권 이전 프로토콜에 대한 연구는 2005년에 Molnar 등⁵⁾과 Saito 등⁶⁾이 처음으로 시작하였다. 최근에는 Kapoor와 Piramuthu가 새로운 소유권 이전 프로토콜을 제안하였다⁷⁻¹¹⁾. 그러나 많은 프로토콜들이 취약성이 있음이 알려져 있고¹²⁾ 이 문제들을 해결한 프로토콜이 2012년에 Kapoor와 Piramuthu에 의해서 제안되었다¹⁰⁾.

이 논문에서는 Kapoor와 Piramuthu가 제안한 프로토콜이 갖고 있는 문제점을 개선한 새로운 소유권 이전 프로토콜을 제안한다. 특히 RFID의 제한적인 연산 능력을 고려하여 공개키 암호 기반이 아닌 비밀키 암호 기반으로 프로토콜을 설계한다. 또한 RFID 태그 간 보안 채널을 형성하는 제한적인 응용 보다는 서버를 통해 태그를 인증하고 관련 정보를 참조하는 환경이 일반적이므로 TTP를 가정한 소유권 이전 프로토콜을 제안한다.

본 논문은 다음과 같이 구성되어 있다. 먼저 제2장에서는 기존의 Kapoor-Piramuthu 프로토콜을 설명하고 이 프로토콜이 갖고 있는 보안상의 문제점을 분석한다. 제3장에서는 기존 프로토콜이 가진 문제를 해결한 새로운 프로토콜을 제안한다. 제4장에서는 새로운 프로토콜의 보안 특성을 분석하고 제5장에서는 결론을 맺는다.

II. 기존의 소유권 이전 프로토콜

이 장에서는 Kapoor와 Piramuthu가 제안한 프로토콜¹⁰⁾ 설명하고 보안 취약성을 분석한다. 기본적인 프로토콜 동작은 그림 1에 제시되어 있다.

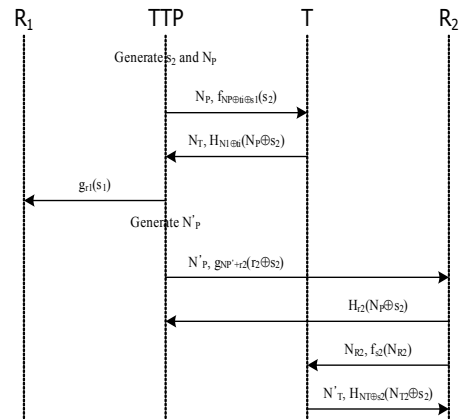


그림 1. Kapoor와 Piramuthu의 TTP를 통한 소유권 이전 프로토콜¹⁰⁾

Fig. 1. RFID Ownership Transfer Protocol (OTP) with Trusted Third Party by Kapoor and Piramuthu¹⁰⁾

2.1 사전 설정 및 가정들

프로토콜이 시작되기 전에 기본적으로 사용되는 파라미터들을 다음과 같다. 먼저 TTP는 이전 소유자 R_1 과 새로운 소유자 R_2 와 각각 비밀키 r_1 과 r_2 를 사전에 공유하고 있다고 가정한다. 또한 이전 소유자 R_1 은 태그 T 와 비밀키 s_1 을 공유하고 있으며 소유권 이전 과정이 끝나면 새로운 소유자 R_2 는 태그와 비밀키 s_2 를 공유하게 될 것이다. 이 s_2 는 이전 소유자 R_1 이 알지 못하는 정보이며, 소유권 이전 후에는 s_1 은 폐기된다. 또한 TTP는 각각의 태그들과 비밀키 t_i 를 공유하고 있으며 s_1 과 s_2 를 모두 알고 있다고 가정한다.

또한 두 개의 암호 알고리즘 $f_k(x)$ 와 $g_k(x)$ 가 사용된다. 이 때 비밀키는 k 이고 메시지 x 를 암호화하는 함수들이다. $f_k(x)$ 는 태그와 이전 소유자 혹은 다른 소유자, 또는 TTP 사이에서 사용되고, $g_k(x)$ 는 TTP와 이전 또는 새로운 소유자 사이에서 사용된다. $f_k(x)$ 와 $g_k(x)$ 는 같은 암호화 알고리즘을 사용할 수 있지만, 일반적으로 태그의 제한적인 연산능력을 고려하여 태그와 함께 사용하는 $f_k(x)$ 는 경량 암호를 사용하고 일반 사용자와 TTP 사이에 사용하는 $g_k(x)$ 는 보안 수준이 더 높은 알고리즘을 사용할 수 있다. 또한 $H_k(x)$ 는 메시지 x 의 메시지 인증 코드(message authentication code; 이후 MAC으로 표기)를 사전에 공유된 비밀키 k 를 이용해서 생성하는 함수이다. 본 논문에서 사용되는 파라미터를 표 1에 정리하였다.

표 1. Kapoor-Piramuthu와^[10] 새로 제안하는 TTP를 통한 소유권 이전 프로토콜에서 사용되는 파라미터의 의미
Table. 1. Parameters for RFID Ownership Transfer Protocol (OTP) with Trusted Third Part of Kapoor and Piramuthu^[10] and new proposed one

Meaning of parameters	
r_1	Secret key between TTP and R_1
r_2	Secret key between TTP and R_2
s_1	Secret key between R_1 and T
s_2	Secret key between R_2 and T
t_i	Secret key between TTP and T
$f_k(x)$	Encryption of message x using secret key k between T and R_1 , R_2 , or TTP
$g_k(x)$	Encryption of message x using secret key k between R_1 or R_2 and TTP
$H_k(x)$	Message authentication code (MAC) for message x using secret key k

2.2 소유권 이전 프로토콜

소유권 이전 프로토콜은 다음과 같은 단계로 일어난다.

단계 1: 먼저 소유권 이전이 개시되면 TTP는 두 개의 난수 s_2 (비밀키)와 N_p 를 생성한다. 그리고 N_p 와 함께 새로운 비밀키 s_2 를 $N_p \oplus t_i \oplus s_1$ 로 암호화해서 태그 T 로 전달한다.

단계 2: 태그는 수신 메시지를 확인하여, 메시지에 문제가 없으면 s_1 을 s_2 로 대체한다. 그리고 난수 N_T 를 생성하고 단계 1에서 수신한 값들의 XOR인 $N_p \oplus s_2$ 의 MAC을 $N_T \oplus t_i$ 를 비밀키로 하여 생성한 후 TTP로 전달한다.

단계 3: TTP는 이전 소유자에게 키 업데이트가 완료되었음을 알리기 위해 이전 소유자와 태그 T 가 공유한 비밀키 s_1 를 TTP와 이전 소유자 R_1 사이에 공유된 비밀키 r_1 으로 암호화하여 보낸다.

단계 4: 이제 TTP는 다시 난수 N'_p 를 생성한 후 새로운 소유자 R_2 에게 새로운 태그의 비밀키 s_2 를 전달하기 위해 TTP와 R_2 가 공유하고 있는 비밀키 r_2 를 이용해 $s_2 \oplus r_2$ 를 생성한 후 이 값을 $r_2 \oplus N'_p$ 를 비밀키로 해서 암호화한 암호문 $g_{r_2 \oplus N'_p}(s_2 \oplus r_2)$ 를 새로운 소유자 R_2 에게 전송한다.

단계 5: 새로운 소유자 R_2 는 s_2 를 정확하게 수신한 것을 인증해 주기 위해서 $s_2 \oplus N'_p$ 의 MAC 값을 비밀키 r_2 를 사용해서 생성한 후에 TTP에게 전달한다.

단계 6: 새로운 소유자 R_2 는 새로 소유하게 된 태그에게, 새로운 태그 비밀키 s_2 를 확인하기 위해서 난수 N_{R2} 를 생성한 후 s_2 를 비밀키로 하여 N_{R2} 를 암호 알고리즘 f 로 암호화하여 암호문 $f_{s_2}(N_{R2})$ 를 태그로 전송한다.

단계 7: 태그는 단계 6에 대한 응답으로 새로운 난수 N'_T 를 생성한 후에 $N_{R2} \oplus s_2$ 에 대한 MAC을 비밀키 $N'_T \oplus s_2$ 를 사용하여 생성한 후에 새로운 소유자에게 전송한다.

2.3 Kapoor- Piramuthu 소유권 이전 프로토콜의 문제점

Kapoor와 Piramuthu가 제안한 RFID 소유권 이전 프로토콜은 기존의 프로토콜들이 갖고 있던 많은 보안 취약성을 해결하기는 하였지만, 여전히 몇 가지 문제점을 갖고 있는 프로토콜이다.

1) Kapoor-Piramuthu 프로토콜은 소유권 이전을 개시할 때 인증된 요청 명령을 전송하지 않는다. 따라서 제3자가 태그 T 에 대한 R_1 의 소유권을 R_2 로 이전하도록 임의로 이전 프로토콜을 개시시킬 수 있다. 이 경우 TTP는 R_1 의 실제 의사와 상관없이 태그 T 의 소유권을 R_2 로 이전해 버릴 수 있다.

2) 단계 1에서 전송된 암호문 $f_{N_p \oplus t_i \oplus s_1}(s_2)$ 를 태그 T 가 인증할 수가 없다. 왜냐하면 평문 s_2 는 그 자체로는 난수이기 때문에 태그 T 가 암호문 $f_{N_p \oplus t_i \oplus s_1}(s_2)$ 를 정확하게 복구한 경우에도 TTP가 새롭게 생성한 난수 s_2 를 얻게 되므로 s_2 가 정확한지 여부를 태그는 판단할 수가 없다.

3) 또한 단계 1에서 TTP에 대한 인증과정이 없기 때문에 공격자는 TTP를 위장하여, 임의의 업데이트 요청을 보내면 태그는 다른 본래의 소유자의 비밀키가 아닌 다른 비밀키로 인증 없이 업데이트하게 되어 원래의 소유자 R_1 이 태그에 대한 소유권을 행사하지 못하게 된다. 즉, 공격자가 임의의 난수 N 과 임의의 난수 C 를 암호문으로 전송하게 되면, 태그는 인증과정이 없으므로 $N \oplus t_i \oplus s_1$ 을 암호문으로 해서 $f_{N \oplus t_i \oplus s_1}^{-1}(C) = s'_2$ 를 소유자의 새로운 비밀키로 업데이트할 수 있다.

이러한 문제들을 해결하기 위해서 본 논문에서는 새로운 RFID 소유권 이전 프로토콜을 제안한다.

III. 새로운 RFID 소유권 이전 프로토콜

이 장에서는 새로 제안하는 RFID 소유권 이전 프로토콜에 대해서 설명한다.

3.1 사전 설정 및 가정들

기존의 Kapoor-Piramuthu 프로토콜에서처럼 이 논문에서 제안하는 새로운 프로토콜도 R_1 은 원래의 태그 소유자, R_2 는 소유권을 이전받는 새로운 소유자, 그리고 TTP는 태그의 소유권 및 그 이전과 관련된 정보를 관리하는 신뢰받는 제3자, T 는 소유권이 R_1 에서 R_2 로 이전될 태그를 의미한다.

이전 프로토콜과 마찬가지로 TTP는 원 소유자 R_1 과 새로운 소유자 R_2 사이에 비밀키 r_1 과 r_2 를 각각 공유하고 있다. 또한 소유권을 가진 R_1 은 T 와 비밀키 s_1 을 공유하며, R_2 는 소유권이 이전된 후에 태그와 비밀키 s_2 를 공유하고 R_1 은 s_1 에 대해서는 알지 못한다. TTP는 모든 태그들과 비밀키를 공유하고 있으며 이 키를 t_i 라 한다.

3.2 새로운 소유권 이전 프로토콜

기존 Kapoor-Piramuthu 프로토콜이 갖고 있는 세 가지 문제를 해결한 새로운 프로토콜은 그림 2에 도시하였다. 새로운 프로토콜은 다음과 같은 단계로 동작한다.

단계 1: 이전 소유자 R_1 은 소유권 이전을 위해서 난수 N_{R1} 을 생성한 후에 원 소유권자의 아이디 ID_{R1} , 이전받을 소유자의 아이디 ID_{R2} , 소유권을 이전할 태

그의 아이디 ID_T 와 난수 N_{R1} 을 연결한 후에 이 값들의 MAC을 $N_{R1} \oplus r_1$ 을 비밀키로 하여 생성한 후 TTP로 함께 전송한다.

단계 2: R_1 에서 R_2 로의 소유권 이전 요청에 따라 TTP는 난수 N_{P1} 와 새로운 비밀키 s_2 를 생성한 후 $ID_{R1} \| ID_{R2} \| s_2$ 를 $N_{P1} \oplus t_i$ 를 비밀키로 하여 암호화 함수 f 를 사용해 암호화한 후 태그 T 에게 N_{P1} 와 암호문 $f_{N_{P1} \oplus t_i}(ID_{R1} \| ID_{R2} \| s_2)$ 를 전송한다.

단계 3: 태그 T 는 난수 N_{T1} 을 생성한 후 $ID_{R1} \| ID_{R2} \| s_2$ 에 대한 MAC을 $N_{T1} \oplus t_i$ 를 비밀키로 하여 생성한 후에 N_{T1} 과 함께 TTP로 전송한다.

단계 4: TTP는 난수 N_{P2} 를 생성한 후 $ID_T \| s_1$ 의 MAC을 $N_{P2} \oplus r_1$ 을 비밀키로 하여 생성한 후 N_{P2} 와 함께 전송한다.

단계 5: TTP는 난수 N_{P3} 를 생성한 후 $ID_{R2} \| ID_T \| s_2$ 를 $N_{P3} \oplus r_2$ 를 비밀키로 하여 암호화 함수 g 를 사용해 암호화한 후에 난수 N_{P3} 와 함께 암호문 $g_{N_{P3} \oplus r_2}(ID_{R2} \| ID_T \| s_2)$ 를 R_2 로 전송한다.

단계 6: R_2 는 난수 N_{R2} 를 생성한 후 $ID_T \| s_2$ 의 MAC을 $N_{R2} \oplus r_2$ 를 비밀키로 하여 생성한 후 N_{R2} 와 함께 TTP로 전송한다.

단계 7: R_2 는 난수 N'_{R2} 를 생성한 후 $ID_{R2} \| s_2$ 를 $N'_{R2} \oplus s_2$ 를 비밀키로 하여 암호화 함수 f 로 암호화한 후에 암호문 $f_{N'_{R2} \oplus s_2}(ID_{R2} \| s_2)$ 를 태그 T 로 전송한다.

단계 8: 태그 T 는 난수 N_{T2} 를 생성한 후 N_{T2} 의 MAC을 $N_{T2} \oplus s_2$ 를 비밀키로 하여 생성한 후 N_{T2} 와 함께 R_2 로 전송한다.

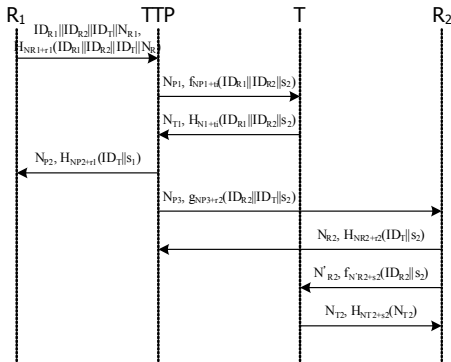


그림 2. 새로운 TTP를 통한 소유권 이전 프로토콜
Fig. 2. Proposed RFID Ownership Transfer Protocol (OTP) with Trusted Third Part

3.3 새로운 소유권 이전 프로토콜 유효성 분석

이 장에서는 새로 제안한 소유권 이전 프로토콜의 유효성을 분석한다. 제안하는 프로토콜은 사용되는 암호 알고리즘 관점에서 MAC을 사용하는 인증과 암호화 알고리즘을 이용한 인증 두 가지로 나눌 수 있다. 이 두 가지 방식의 유효성을 증명함으로써 전체 인증 프로세스의 유효성을 증명할 수 있다.

보조정리 1: 송신자와 수신자를 각각 S_1 과 S_2 라 하자. 그리고 S_1 과 S_2 사이에 유효한 비밀키 K 가 공유되어 있다고 하자. 만일 S_1 이 S_2 에게, $M \| R \| H_{K \oplus R}(M \| R)$ 을 전송했을 때, 수신된 MAC이

일치하면, 수신자 S_2 는 송신자가 S_1 임을 인증할 수 있다.

증명) S_2 는 ‘ S_1 으로 주장’하는 송신자로부터 $M \| H_{K \oplus R}(M \| R)$ 을 수신한다. 이 때 $K \oplus R$ 은 전송되지 않고 R 만 전송되었다. S_2 는 S_1 과 사전에 공유된 유효한 비밀키 K 를 알고 있으므로 전송된 R 로부터 $K \oplus R$ 을 생성할 수 있다. 반면에 K 를 모르는 공격자는 $K \oplus R$ 를 생성할 수 없다. S_2 는 수신된 메시지 $M \| R$ 에 대해 MAC을 다시 생성할 수 있다. 이 때 수신된 $H_{K \oplus R}(M \| R)$ 과 새로 생성한 MAC이 일치하면 S_2 는 다음 사실을 확인할 수 있다. 1) 송신자는 $K \oplus R$ 을 동일하게 알고 있다. 2) 송신자는 K 를 알고 있다. 3) K 를 알고 있는 것은 S_2 외에 S_1 뿐이다. 4) 따라서 송신자는 S_1 이다. □

마찬가지로 다음과 같은 보조정리도 증명할 수 있다.

보조정리 2: 송신자와 수신자를 각각 S_1 과 S_2 라 하자. 그리고 S_1 과 S_2 사이엔 유효한 비밀키 K 가 공유되어 있다고 하자. 만일 S_1 이 S_2 에게, $E_{K \oplus R}(ID \| M)$ 을 전송했다고 하자. 단 $E_{K \oplus R}(ID \| M)$ 은 메시지 $ID \| M$ 을 비밀키 $K \oplus R$ 로 암호화한 것을 의미하고, ID 는 송수신자의 아이디정보, M 은 임의의 메시지이다. 만일 S_2 가 $E_{K \oplus R}(ID \| M)$ 를 복구했을 때 송수신자 ID 가 정확하게 확인되면, S_1 이 송신자임을 인증할 수 있고, M 은 S_1 과 S_2 사이의 새로운 비밀 정보가 된다.

증명) S_2 는 S_1 으로 주장하는 송신자로부터 $E_{K \oplus R}(ID \| M)$ 을 수신한다. 이 때 $K \oplus R$ 은 전송되지 않고 R 만 전송되었다. S_2 는 S_1 과 사전에 공유된 유효한 비밀키 K 를 알고 있으므로 전송된 R 로부터 $K \oplus R$ 을 생성할 수 있다. 반면에 K 를 모르는 공격자는 $K \oplus R$ 를 생성할 수 없다. 만일 $K \oplus R$ 이 암호문 생성시 사용된 값과 일치하지 않는다면, 암호 알고리즘의 특성에 의해 복구된 값은 $ID \| M$ 이 아닌 랜덤한 값이 되어 복구된 값에서 ID 를 추출할 수 없다. 정상 수신자 S_2 는 $K \oplus R$ 을 이용해서 암호문 $E_{K \oplus R}(ID \| M)$ 를 복호할 수 있다. 이 때 S_2 는 다음과 같이 판단할 수 있다. 1) 복호된 메시지서 송수신자의 ID 를 얻었다. 2) 암호 알고리즘의 특성에 의해 송신자는 $K \oplus R$ 을 동일하게 알고 있다. 2) 송신자는 K 를 알고 있다. 3) K 를 알고 있는 것은 S_2 외에 S_1 뿐이다. 4) 따라서 송신자는 S_1 이다. 따라서 임의의 메시지 M 은

S_1 이 생성한 값과 S_2 도 알게 된 값이며 K 를 모르는 제3자는 알 수 없는 값이 된다. □

두 가지 보조 정리에 의해 다음을 확인할 수 있다. 보조정리 1에 의해 제안하는 프로토콜의 단계 1, 3, 4, 6, 8이 정당한 인증과정이 증명된다. 그리고 보조정리 2에 의해 단계 2, 5, 7이 정확하게 동작함이 증명된다.

IV. 새로운 RFID 소유권 이전 프로토콜의 보안 특성

제안하는 프로토콜은 기본적으로 전송되는 데이터의 기밀성은 암호화에 의해서, 수신된 데이터의 무결성은 MAC에 의해서 보장된다. 이 장에서는 이를 기반으로 새로운 RFID 소유권 이전 프로토콜의 보안 분석을 분석한다.

4.1 전방향/후방향 안전성

전방향 안전성(forward secrecy)이란 현재 태그의 비밀키가 공격자에게 알려진 경우에도 이 키를 이용해서 이후의 비밀 정보를 알아낼 수 없는 것을 의미한다. 반대로 후방향 안전성(backward secrecy)이란 현재 태그의 비밀키가 공격자에게 알려진 경우에도 이 키를 이용해 이전 비밀 정보를 알아낼 수 없는 것을 의미한다.

먼저 공격자가 태그에 저장된 소유자의 비밀키 s_2 를 알았다고 가정하자. 제안하는 프로토콜에서는 s_2 를 생성하고 전송하는 과정에서 s_1 이 사용되지 않기 때문에, 이전에 s_1 을 이용한 메시지들은 s_2 로 해독이 불가능하다.

반대로 공격자가 이전 비밀키 s_1 을 알았다고 가정하자. 이 경우에도 소유권을 이전하는 새로운 비밀키를 전달하는 과정에서 TTP는 태그 T 와 공유한 별도의 키 t_i 를 이용해서 새로운 키를 설정하게 된다. 이 키는 TTP와 R_2 가 공유한 또 다른 비밀키 r_2 를 통해서 전달이 되고, 따라서 태그에 저장된 비밀키 s_1 이 유출되더라도 s_2 에 대한 정보는 알아낼 수 없다.

4.2 재전송 공격

제안하는 프로토콜에서는 기본적으로 암호화나 인증을 위해서 사용하는 세션키를 난수와 사전에 공유된 비밀키의 XOR 값을 이용해 생성한다. 난수는 일회용 난수로 매 번 변하기 때문에, 이전에 전송된 암호문이나 인증코드에 재활용되지 않는다.

난수에는 시간 정보가 포함되어 있지 않기 때문에 단계 1에서 소유권 이전 요청을 하는 경우, 난수와 요청 메시지 전체를 재전송할 수 있다. 그러나 이 프로토콜이 사용되는 것은 특정 태그의 소유권을 이전하기 위한 것으로 이전 단계에서 R_1 에서 R_2 로 태그 T 의 소유권이 이미 이전되었다면, TTP에 동일한 요청이 재전송되더라도 이미 태그 T 의 소유권은 R_2 로 넘어가 있기 때문에, TTP는 이전 요청이 재전송된 것임을 쉽게 알 수 있다.

4.3 서비스 거부공격

RFID 소유권 이전에서는 공격자가 임의로 소유권 이전 요청을 변조함으로써 태그에 저장된 소유자의 비밀키를 임의로 업데이트하는 서비스 거부공격이 가능하다. 이 경우 실제 정상 데이터가 전송된 것이 아니기 때문에 태그의 데이터만 랜덤한 비밀키로 업데이트 되어, 향후에 RFID 소유 및 관리 권한에 문제를 일으킬 수가 있다.

대표적으로 제2장 3절의 세 번째 항목에서 Kapoor-Piramuthu의 프로토콜의 보안 문제가 서비스 거부공격과 관련되어 있다. 특히 Kapoor-Piramuthu 프로토콜에서는 새로운 소유자의 태그 비밀키 s_2 를 암호화한 메시지가 전송되고 이 값이 랜덤하기 때문에 태그는 암호를 복호화 후에 s_2 가 정상인지 아닌지 확인할 수가 없게 된다.

제안하는 프로토콜에서는 TTP가 태그로 s_2 와 함께 이전 소유자 정보 및 새로운 소유자 정보인 ID_{R1} 과 ID_{R2} 를 함께 암호화하여 전송한다. 따라서 태그에서 암호를 복호화하게 되면 s_2 와 함께 소유자 정보가 나오게 된다. 만일 현 소유자 정보인 ID_{R1} 이 정확하지 않은 경우 태그는 복호가 잘못된 것으로 판단할 수가 있고 랜덤한 요청에 대해 거부하는 것이 가능하다.

4.4 KP 프로토콜 취약성 제거

마지막으로 제2장 3절에서 Kapoor-Piramuthu 프로토콜의 문제로 지적한 취약성이 새로운 프로토콜에서 제거되었는지 여부를 분석하고자 한다.

1) 먼저 Kapoor-Piramuthu 프로토콜과 달리 새로운 프로토콜에서는 소유권 이전을 개시할 때 인증이 가능한 요청 명령을 전송한다. 이를 위해서 제1단계에서 소유자 R_1 은 TTP로 태그 T 의 소유권을 R_2 로 이전한다는 의사를 소유자 R_1 의 아이디, 새로운 소유자 R_2 의 아이디, 이전될 태그 T 의 아이디를 연결한 후

난수 N_{R1} 과 함께 MAC을 생성하여 TTP로 전달한다. MAC을 생성하기 위해서 R_1 과 TTP 사이에 사전에 공유된 비밀키 r_1 로부터 $N_{R1} \oplus r_1$ 이 생성되기 때문에 TTP는 이전 소유자, 새로운 소유자, 이전될 태그 T 의 정보를 MAC을 이용해서 검증이 가능하고, 따라서 Kapoor-Piramuthu의 프로토콜에서처럼 제3자가 태그 T 에 대한 R_1 의 소유권을 R_2 로 이전하도록 임의로 이전 프로토콜을 개시시킬 수가 없다.

2) 단계 2에서는 새로운 비밀키 s_2 와 함께 소유권 이전에 관련된 현 소유자와 새로운 소유자의 아이디가 함께 암호화되어 전송된다. 이 때 암호화에 사용되는 키는 태그 T 와 TTP 사이에 사전에 공유된 비밀키 t_i 와 난수 N_{R1} 을 이용해 생성한 세션키이다. 이 때 태그는 s_2 를 복구하면서 현 소유자 R_1 의 아이디 ID_{R1} 을 함께 복구하게 되고, 정확하게 복구되었는지 여부를 통해 복호화가 성공적인지 아닌지를 판단할 수 있고 성공적인 경우 s_2 를 정확하게 확보하는 것이 가능하다. 따라서 Kapoor-Piramuthu의 프로토콜과 달리 새로운 프로토콜은 s_2 가 실제 TTP에 의해 전송된 것을 인증할 수 있다.

3) 제4장 3절에서 설명한 바와 같이 단계 2에서 현 소유자의 R_1 의 아이디를 함께 암호화해서 전송하기 때문에 R_1 의 아이디가 복호화 과정에서 성공적으로 복구된 것을 확인함으로써 메시지를 암호화한 상대방이 TTP인 것을 태그가 인증할 수가 있다. 따라서 Kapoor-Piramuthu의 방식에서처럼 임의의 난수 N 과 암호문 C 쌍으로 임의의 세션키로 업데이트하는 공격자의 서비스 거부 공격 시도는 무력화된다.

V. 결 론

이 논문에서는 기존의 Kapoor-Piramuthu가 제안한 RFID 소유권 이전 프로토콜이 갖고 있는 보안 문제를 밝혀내고, 새로운 프로토콜을 통해서 기존의 RFID 소유권 이전 프로토콜이 갖고 있던 문제를 해결하였다. 제안하는 프로토콜은 비밀키 암호를 기반으로 설계가 되었기 때문에, 연산능력이 제한적인 다양한 RFID 환경에서 사용이 가능할 뿐만 아니라 현존하는 많은 공격에 저항성을 갖는 프로토콜임을 보였다.

References

[1] S. Dominikus and J.-M. Schmidt, "Connecting

passive RFID tags to the internet of things,” in *Proc. Interconnecting Smart Objects with the Internet Workshop*, Prague, 2011.

[2] W. S. Choi, S. S. Kim, Y. H. Kim, T. J. Yoon, K. W. Ahn, and K. J. Han, “Design of PUF-based encryption processor and mutual authentication protocol for low-cost RFID authentication,” *J. KICS*, vol. 39, no. 12, pp. 831-841, Dec. 2014.

[3] J. S. Kim, J. K. Park, and Y. T. Shin, “RFID-based automatic inspection system design and implementation for manufacturing and retail industry,” *J. KICS*, vol. 39, no. 1, pp. 97-105, Jan. 2014.

[4] S. J. Oh, C. H. Lee, T. J. Yoon, K. H. Chung, and K. S. Ahn, “Improved authentication protocol for privacy protection in RFID systems,” *J. KICS*, vol. 38, no. 1, pp. 12-18, Jan. 2013.

[5] D. Molnar, A. Soppera, and D. Wagner, “A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags,” in *Workshop on RFID Security and Light-Weight Crypto.*, Jul. 2005.

[6] J. Saito, K. Imamoto, and K. Sakurai, “Reassignment scheme of an RFID tag’s key for owner transfer,” in *Proc. EUC Workshops*, vol. 3823 LNCS, pp. 1303-1312, 2005.

[7] G. Kapoor and S. Piramuthu, “Single RFID tag ownership transfer protocols,” *IEEE Trans. Systems, Man, and Cybernetics, Part C*, vol. 42, no. 2, pp. 164-173, 2012.

[8] G. Kapoor, W. Zhou, and S. Piramuthu, “Multi-tag and multi-owner RFID ownership transfer in supply chains,” *Decision Support Syst.*, vol. 52, no. 1, pp. 258-270, 2011.

[9] H. Lei and T. Cao, “RFID protocol enabling ownership transfer to protect against traceability and dos attacks,” in *Proc. 1st Int. Symp. Data, Privacy E-Commerce*, pp. 508-510, 2007.

[10] G. Kapoor and S. Piramuthu, “Single RFID tag ownership transfer protocols,” *IEEE Trans. Syst., Man, and Cybernetics, Part C*, vol. 42, no. 2, pp. 164-173, 2012.

[11] G. Kapoor, W. Zhou, and S. Piramuthu, “Multi-tag and multi-owner RFID ownership transfer in supply chains,” *Decision Support Syst.*, vol. 52, no. 1, pp. 258-270, 2011.

[12] G. Kapoor and S. Piramuthu, “Vulnerabilities in some recently proposed RFID ownership transfer protocols,” in *Proc. NetCoM’09*, pp. 354-357, 2009.

김 영 식 (Young-Sik Kim)



2001년 2월 : 서울대학교 전기공학부 졸업
 2003년 2월 : 서울대학교 전기컴퓨터공학부 석사
 2007년 2월 : 서울대학교 전기컴퓨터공학부 박사
 2007년 3월~2010년 8월 : 삼성 전자 책임연구원

2010년 9월~현재 : 조선대학교 정보통신공학과 조교수
 <관심분야> 암호학, 정보보안, 정보이론, 오류정정 부호, 하드웨어 보안