저가형 RFID를 위한 효율적인 프라이버시 보호 기법†

이상신, 김진, 김광조

국제정보보호연구소 (IRIS)

한국정보통신대학교 (ICU)

An Efficient Privacy Protection Scheme for Low-cost RFID

Sangshin Lee, Zeen Kim, Kwangjo Kim

International Research center for Information Security (IRIS)

Information and Communications University (ICU)

요 약

RFID(Radio Frequency Identification)는 초소형 반도체에 식별정보를 넣고 무선주파수를 이용해 이 칩을 지닌 객체를 판독·추적·관리할 수 있는 기술을 말한다. RFID 시스템의 확산은 인해 산업에서의 자동화뿐만 아니라 개인의 실생활에서도 많은 편의를 제공할 것이다. 그러나 그 편의만큼이나 프라이버시 침해라는 중요한 문제를 내재하고 있다. 저가형 RFID를 생산하기 위해서 보안을 목적으로 사용될 수 있는 자원이 매우 한정적이기 때문에 적은 자원으로 구현 가능한 RFID 보호 프로토콜을 필요로 한다. 본 논문에서는 비교적 적은 자원으로도 구현 가능한 해쉬 체인을 이용하는 RFID 보호 프로토콜을 제안한다. 그리고 백-엔드 서버의 계산 복잡도를 낮추기 위해서 태그와 백-엔드 서버가 공유하는 2개의 비밀정보를 사용한다. 제안 프로토콜은 완벽한 불추적성(untraceability)을 가지고 있으며 위장(impersonation)을 검출하는 기능도 있다. 같은 보안성을 가지는 Ohkubo[6]의 프로토콜과 비교해 보았을 때 태그의 계산량은 비슷하지만 백-엔드 서버에 부가되는 계산량이 현저하게 줄어든다.

I. 서론

RFID는 초소형 반도체에 식별정보를 넣고 무선주파수를 이용해 이 칩을 지닌 객체를 판독·추적·관리할 수 있는 기술을 말한다. RFID 시스템의 확산으로 인해 산업에서의 자동화뿐만 아니라 개인의 실생활에서도 많은 편의를 제공할 것이다. 그러나 그 편의만큼이나 프라이버시 침해라는 중요한 문제를 내재하고 있다. RFID의 보안 문제가 RFID를 다양한 산업에 적용할 수 있는 가능성을 막고 있다.

저가형 RFID를 생산하기 위해서 보안을 목적으로 사용될 수 있는 자원이 매우 한정적이다. 따라서 기존의 암화학적 기법인 대칭키와 비대칭키 암호화 기법을 적용하지 못한다. 이에 따라서 태그에서의 계산량이 적은 여러 기법들이 제안되고 있다.

Golle 등은 메시지를 재암호화할 때 최초의 메시지의 암호화에 사용된 공개키 정보를 요구하지도 생성하지도 않는 기법인, 유니버설 재암호화(universal re-encryption)에 기반을 두는 프로토콜을 제안하였다[1]. Saito 등은 [1]의 개선된 프로토콜을 두 가지 제안하였다[2]. 하나는 태그에 의해 수행되는 연산이 변경되었고, 다른 하나는 리더에 의해서 수행되던 재암호화가 태그에 의해서 수행되는 것이다. Henrici 등은 태그와 백-엔드 서버(back-end server)에 ID와 두 개의 키를 저장하고, 동기화

† 본 연구는 산업자원부 지역협력연구사업 (R12-2003-004-00015-0) 지원으로 수행되었음

를 유지하며 갱신하는 프로토콜을 제안하였다[3]. Weis 등은 "임의의 제어 통제(randomized access control)"을 이용하는 프로토콜을 제안하였다[4]. Ohkubo 등은 해쉬 체인(hash chain)을 이용한 기법을 소개하였다[5]. Gildas는 RFID에 대한 공격 모델을 제시하고 위 모든 프로토콜에 관한 안전성 분석을 하였다[6].

본 논문에서는 RFID 태그의 프라이버시 보호를 위한 새로운 기법을 제안한다. 이 기법은 발표된 다수의 프로토콜이 그러하듯이 해쉬 체인을 사용한다. 한 가지 기존의 프로토콜과 다른 점은 제안 프로토콜은 태그의 ID를 검색하는 과정에서 백-엔드 서버의 계산량을 줄이기 위해서 태그와 백-엔드 서버에 2개의 비밀정보를 공유한다는 점이다. 이에 따라 현저하게 서버의 계산 복잡도가 떨어진다. 이 기법을 [6]에서 제시한 공격 모델로 분석하여 기존의 기법과 안전성을 비교하고 안전성이 동일하게 좋은 [5]와 효율성을 비교한다.

본 논문의 구성은 우선 Ⅱ에서 일반적인 RFID 시스템, 관련 보안 문제, 공격 모델 및 해쉬 체인에 대하여 소개한다. Ⅲ에서 제안 프로토콜을 소개하고 Ⅳ에서 제안 프로토콜의 안전성 분석을 한 후 다른 프로토콜과 안전성과 효율성을 비교한다. Ⅴ장에서 결론을 제시한다.

II. 기반 지식

1. RFID 시스템

일반적인 RFID 시스템은 태그(Tag), 리더(Reader), 그리고 백-엔드 서버(back-end server)로 구성 된다. 태그는 IC 칩과 안테나로 구성되어 있으며, 무선 신호에 대한 응답으로 자신의 정보를 리더에 보낸다. 리더는 태그에게 무선 주파수 신호를 보내고, 태그에 의하여 전송된 정보를 받으며, 백-엔드 서버에게 그 정보를 보낸다. 백-엔드 서버는 각각의 태그에 대한 다양한 형태의 정보를 저장·관리하는 안전한 서버이다.

2. 보안 요구 사항

태그가 공격자로부터 보호되어야 할 가장 중요한 요소는 기밀성(Confidentiality)과 불추적성(untraceability)이다. 기밀성은 태그의 ID에 적용 되어야 할 보안 요소로 허가된 개체를 제외한 다른 개체는 태그와 리더로부터 전파되는 정보를 이용해서 태그의 ID를 알아내지 못해야 한다는 점이다.

태그와 리더가 방출하는 정보를 이용해서 태그를 추적하지 못하게 하는 불추적성 또한 사용자의 프라이버시 보호를 위해서 중요한 점이다. 태그를 추적하기 위해서는 태그 ID를 알 필요는 없다. 단지 태그와 리더가 방출하는 정보에서 공격자가 일정한 패턴을 찾아낼 수 있다면 공격자는 태그의 ID를 알지 못하더라도 연속적인 질의(query)를 통해서 태그의 위치를 추적할 수 있다.

추가적인 보안 요구 사항으로 위장(impersonation)에 대한 방지 또는 검출이 가능해야 한다. 공격자가 리더에게 자신이 원하는 태그 ID로 인식되게 할 수 있다면 RFID 시스템의 큰 불안 요소가 될 것이다.

3. RFID의 공격 모델

[6]에서 공격모델을 제안하였다. 공격자의 수단은 Query(), Send(), Execute(), Reveal()이다. Query()는 태그에게 Send()는 리더에게 능동적으로 메시지를 보내고 응답을 받는 것이며, Execute()는 태그와 리더간의 메시지를 수동적으로 읽을 수 있는 것이고, Reveal() 메모리를 읽는 공격방법을 나타낸다.

공격에 대한 안전성의 정도는 3가지로 나누었다. 공격자에게 특정 공격 수단이 주어졌을 때, 어떠한 조합으로도 태그를 추적할 수 없을 때 Existential-UNT가 만족하고, 과거의 태그의 정보를 알 수 없으면 Forward-UNT가 만족하며, 일부 조합으로 추적이 가능하다면 Universal-UNT를 만족한다고 한다. 공격 수단과 안전성의 정도의 함축관계는 다음과 같다.

Existential-UNT
⇒ Forward-UNT
⇒ Universal-UNT

UNT-QSER
⇒ UNT-QSE
⇒ UNT-E, UNT-Q

4. 해쉬 체인 (Hash Chain)

해쉬 체인은 계산하기는 쉽지만 역을 구하는 것은 어려운 공개 함수 h에 기반하고 있다. 이런 함수를 일방향 함수(one-way functions)라 하고 일방향 함수의 출력의 길이가 고정되었다면 일방향 해쉬 함수라고 한다. 길이 N의 해쉬 체인은 시드(seed) 값에 대하여 일방향 해쉬 함수 h()를 재귀적으로 적용함으로써 얻을 수 있다.

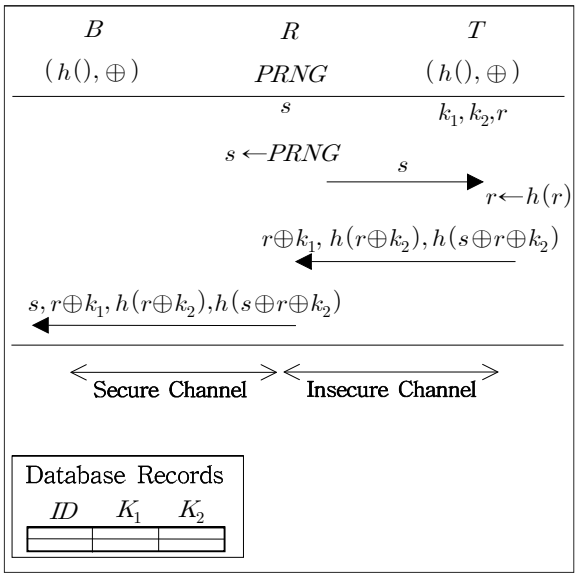
$$h^N(s) = h(h(h(...h(s)...))) \quad (N\text{번})$$

마지막 값인 $h^N(s)$를 알더라도 s값을 모르는 이는 $h^{N-1}(s)$를 생성하지 못하지만 주어진 $h^{N-1}(s)$ 값의 정확함(correctness)은 $h^N(s)$를 이용해서 증명할 수 있다.

III. 제안 프로토콜

본 논문에서 리더와 백-엔드 서버는 안전한 채널 상에서 통신이 이루어지며, 리더와 태그 간의 채널은 안전하지 않다고 가정한다. 공격자는 질의를 통한 응답뿐만 아니라 물리적인 접촉으로 태그 메모리를 읽는 공격법인 메모리 채널(memory channel)[6]을 이용 가능하다고 가정한다.

제안 프로토콜에서 백-엔드 서버 B와 태그 T는 각각 공통의 해쉬함수 $h()$와 XOR 연산을 수행할 수 있다. 리더 R은 PRNG (PseudoRandom Number Generator) 연산을 수행할 수 있다. T는 두 개의 비밀정보 k_1, k_2를 저장하고 있고 $k_1 \oplus k_2$ 값이 T마다 다르게 설정된다. T는 가변적인 해쉬 값 r도 가지고 있다. R는 위장(impersonation)을 검출하기 위해 사용되는 s값을 저장한다. B의 데이터베이스에는 각각의 T의 ID를 저장하는 레코드 ID와 두 비밀정보 k_1, k_2를 저장하는 레코드 K_1, K_2가 있다.



<그림1> 제안 프로토콜

R이 T의 ID를 알아내기 위한 절차는 다음과 같다 <그림1>.

1. R이 $PRNG$를 이용해 새로운 의사 난수 s를 생성해서 저장하고 T에게도 보낸다.

2. T는 해쉬 체인의 다음 값으로 r을 갱신한 후 $r \oplus k_1, h(r \oplus k_2), h(s \oplus r \oplus k_2)$값을 계산하여 R에게 전송한다.

3. R는 전송받은 값에 s값을 추가하여 B에게 전달한다.

4. ID를 알아내기 위해서 B는 데이터베이스 내의 다음 식을 만족하는 (k_1', k_2')쌍을 모두 찾는다.

$$h((r \oplus k_1) \oplus k_1' \oplus k_2') \equiv h(r \oplus k_2) \quad (*)$$

여기서 k_1', k_2'는 각각 K_1, K_2에서 읽어 들인 값이다. (*)를 만족하는 두 개 이상의 쌍을 찾았다면 충돌(collision)을 찾은 것으로 리더에게 처음부터 다시 질의(query)할 것을 명한다. (*)를 만족하는 유일한 (k_1', k_2')쌍을 찾았다면 **정리1**에 의해 이 쌍에 대응하는 ID가 태그의 ID임을 확인할 수 있다.

5. 위장을 검출하기 위해서 다음 식이 만족하는지 검사한다.

$$h(s \oplus (r \oplus k_1) \oplus k_1' \oplus k_2') \equiv h(s' \oplus r \oplus k_2) \quad (**)$$

여기서 좌항의 s는 리더로부터 전송받은 값이고 우항의 s'는 T가 생성한 해쉬 값이 기원이다. (**)식이 만족하려면 충돌 또는 $s = s'$이여야 한다. 여기서 충돌 회피 해쉬(collision-resistant hash)를 사용한다고 가정하고 충돌은 무시한다. R는 $PRNG$를 이용해 계속해서 새로운 값을 생성하여 T에게 그에 대응하는 계산을 요구하기 때문에 R이 보낸 의사 난수를 이용해 정당하게 프로토콜의 절차를 T가 따를 때만 (**)식이 만족한다. 위식이 만족하지 않으면 $s \neq s'$임으로 정당한 프로토콜을 따르지 않은 재전송(replay)과 같은 위장이다.

정리1. *충돌이 없는 조건하에서 태그의 ID 확인식 (*)이 성립하면 (k_1', k_2')는 올바른 쌍이다.*

증명. 충돌이 없다면 (*)식을 만족하는 두 $h()$의 입력 값인 $(r \oplus k_1) \oplus k_1' \oplus k_2'$와 $r \oplus k_2$가 같다. 두 값을 등식으로 둔 $(r \oplus k_1) \oplus k_1' \oplus k_2' = r \oplus k_2$의 양변에 $r \oplus k_1$을 XOR하면 $k_1' \oplus k_2' = k_1 \oplus k_2$가 성립한다. 초기 설정에 의해 $k_1 \oplus k_2$가 태그마다 유일한 값이므로 (k_1', k_2')는 올바른 쌍이다.

<표1> 프로토콜의 안전성 분석

프로토콜	O	X
Golle 등[1]	-	Existential-UNT-Q Existential-UNT-E
Saito 등[2]	-	Existential-UNT-Q
Saito 등[2] 개선	-	Universal-UNT-QS
Henrici 등[3]	-	Existential-UNT-Q Universal-UNT-QE
Weis 등[4]	Existential-UNT-QSE	Forward-UNT-QSER
Ohkubo 등[5]	Existential-UNT-QSE Forward-UNT-QSER	
제안 프로토콜	Existential-UNT-QSE Forward-UNT-QSER	

IV. 안전성 분석 및 비교

안전성 분석을 위해 [6]에 제시되어 있는 공격 모델을 적용한다. 리더로부터 태그에게 제공되는 정보는 의사 난수로 아무런 유효한 정보를 공격자에게 주지 않고, 태그로부터 리더에게 제공되는 정보는 모두 응답마다 내부적으로 변화하는 해쉬 값에 의존하는 값으로, 추적 가능한 정보를 제공하지 않음으로 Existential-UNT-QSE이다. 그리고 메모리 채널을 이용한 공격을 하더라도 태그에 저장되어 있는 값은 일방향 함수에 의해서 생성되었기 때문에 이전의 결과를 추적하지 못함으로 Forward-UNT-QSER이다.

안전성에 대한 분석을 다른 프로토콜과 비교하면 <표1>과 같다. 완벽한 불추적성을 가지는 프로토콜은 [5] 프로토콜과 제안 프로토콜이다. 이 둘 프로토콜의 효율성을 비교하면 <표2>와 같다.

효율에 있어서 가장 큰 차이는 백-엔드 서버의 계산량이다. [5]는 ID를 알기위해서 각각의 태그에 해당하는 해쉬 체인을 모두 검색해야 함으로 O(태그 수 * 해쉬 체인 길이)의 계산량이 필요하다. 그러나 제안 프로토콜은 태그 ID를 찾는데 필요한 계산은 데이터베이스 내의 각각의 태그 정보에 대하여 3번의 XOR 연산과 1번의 해쉬 연산 그리고 1번의 비교 연산만을 필요로 하여 O(태그 수)의 계산량만으로 전체 시스템을 검사한다. 그리고 위장 검출에 관한 연산은 1회만 수행하기 때문에 O(1)의 계산 복잡도를 가진다. 따라서 제안 프로토콜의 전체적인 계산 복잡도는 O(태그 수)이다.

<표2> [5]와 제안 프로토콜 효율성 비교

프로토콜	Ohkubo 등[5]	제안 프로토콜
백-엔드 서버 계산량	O(태그 수 * 해쉬 체인 길이)	O(태그 수)
필요한 해쉬 종류	2종류	1종류
태그 내 저장 값	1개	3개
태그 응답 시 방출 데이터 수	1개	3개
태그의 해쉬 계산 회수	2회	3회

그 외에 제안 프로토콜의 장점은 태그 내에 한 종류의 해쉬 함수만 필요로 한다는 점이다. 단점으로는 2개의 추가적인 고정 값을 저장해야 한다는 점과 태그의 응답 시에 전송하는 메시지의 길이가 [5]에 비해서 3배라는 점이다. 그리고 해쉬 계산 회수가 3회라는 점이다. 그러나 이런 단점은 백-엔드 서버의 계산량의 극적인 감소에 비하면 작은 차이라고 본다.

V. 결론

본 논문에서는 비교적 적은 자원으로도 구현 가능한 해쉬 체인을 이용하는 RFID 프라이버시 보호 프로토콜을 제안한다. 그리고 백-엔드 서버의 계산 복잡도를 낮추기 위해서 태그와 백-엔드 서버가 공유하는 2개의 비밀정보를 사용한다. 제안 프로토콜은 완벽한 불추적성을 가지고 있으며 위장을 검출하는 기능도 있다. 같은 보안성을 가지는 Ohkubo[6]의 프로토콜과 비교하면 태그의 계산량은 비슷하지만 백-엔드 서버에 부가되는 계산량이 현저하게 줄어든다.

앞으로의 과제는 더 치밀한 안전성 분석을 하는 것과, 해쉬의 사용과 데이터의 전송량을 줄이면서도 같은 기능을 하는 프로토콜을 연구하는 것이다.

[참고문헌]

[1] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson. "Universal re-encryption for mixnets." In Tatsuaki Okamoto, editor, The Cryptographers' Track at the RSA Conference - CT-RSA, volume 2964 of LNCS, pages 163-178, San Francisco, California, USA, February 2004. Springer-Verlag.

[2] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai. "Enhancing privacy of universal re-encryption scheme for RFID tags." In Laurence T. Jang, Minyi Guo, Guang R. Gao, and Niraj K. Jha, editors, Embedded and Ubiquitous Computing - EUC 2004, volume 3207 of LNCS, pages 879-890, Aizu-Wakamatsu City, Japan, August 2004. Springer-Verlag.

[3] Dirk Henrici and Paul M¨uller. "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers." In Ravi Sandhu and Roshan Thomas, editors, IEEE International Workshop on Pervasive Computing and Communication Security - PerSec 2004, pages 149 - 153, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society Press.

[4] StephenWeis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. "Security and privacy aspects of low-cost radio frequency identification systems." In Dieter Hutter, G¨unter M¨uller, Werner Stephan, and Markus Ullmann, editors, International Conference on Security in Pervasive Computing - SPC 2003, volume 2802 of LNCS, pages 454 - 469, Boppard, Germany, March 2003. Springer-Verlag.

[5] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. "Cryptographic approach to 'privacy-friendly' tags." In RFID Privacy Workshop, MIT, MA, USA, November 2003.

[6] Gildas Avoine "Adversarial Model for Radio Frequency Identification," available at http://eprint.iacr.org/2005/049