다항식 해쉬함수를 이용한 RFID 인증 프로토콜+

연용호*,이선영**, 이종연**, 신문선**
*목원대학교 정보통신공학부
**충북대학교 컴퓨터교육학과
e-mail:msshin9@nate.com

RFID Authentication Protocol using Polynomial Hash Function

YongHo Yon*, SunYong Lee**, JongYun Lee**, MoonSun Shin**
*MokWon University.
**Chungbuk National University.

요 약

RFID 시스템은 RFID 태그, RFID 리더 , Back-end 서버로 이루어져서 짧은 거리의 무선통신을 통해 정보를 인식하는 시스템이다. 최근 RFID기술은 다양한 응용 분야에서 활용되고 있으며 보안과 프라이버시 침해에 대한 우려와 문제점을 해결해야한다는 논의가 높아지고 있다. 본 논문에서는 중간자 공격 및 재생공격에 대응할 수 있는다항식 해쉬함수를 이용한 강력한 상호인증 프로토콜을 제안한다. 본 논문에서는 대량의 RFID 태그와 리더간 상호인증을 위해 다항식을 이용한 해쉬함수를 적용한다. 제안된 다항식 해쉬함수를 적용한 RFID 인증 프로토콜은 전체 시스템에 부담을 주지 않으면서 보안강화를 할 수 있는 인증 프로토콜이며 특히 태그 쪽에 컴퓨팅 오버헤드가 추가되지 않는다. 또한 공격자에게 공격이 어렵거나 불가능한 복잡도를 가지는 프로토콜이다.

1. 서론

RFID 시스템은 RFID 태그, RFID 리더, Back-end 서버로 이루어져서 짧은 거리의 무선통신을 통해 정보를 인식하는 시스템이다. 최근 RFID기술은 다양한 응용 분야에서 활용되고 있으며 보안과 프라이버시 침해에 대한 우려와 문제점을 해결해야 한다는 논의가 높아지고 있다. 태그의 인증과정에서 RFID 시스템은 다음과 같은 제한사항으로 인한 취약점을 가지고 있다. 첫째, 태그는 값싼 칩으로 한정된 기계적 성능을 가지고 있어 컴퓨팅 능력이 제약적이다. 둘째, RFID 시스템은 무선 주파수를 사용함으로써 쉽게 도청될 수 있어 중간자 공격및 위조 공격들에 쉽게 노출된다. 셋째, 수동형 태그의 경우 상호인증을 제공하는데 어려움이 따른다. 따라서 태그와 리더 간 상호 인증을 위한 다양한 프로토콜이 연구되고 있다.

+ 본 논문은 2008년도 지식경제부 성장동력기술개발 사업의 일환으로 (주)코리아컴퓨터의 위탁과제로 수행되었음

본 논문에서는 대량의 RFID 태그와 리더간 상호인증을 위해 다항식을 이용한 해쉬함수를 적용한다. 제안된 다항식 해쉬함수를 적용한 RFID 인증 프로토콜은 전체 시스템에 부담을 주지 않으면서 보안강화를 할 수 있는 인증 프로토콜이며 특히 태그 쪽에 컴퓨팅 오버헤드가 추가되지 않는다. 또한 공격자에게 공격이 어렵거나 불가능한 복잡도를 가지는 인증 프로토콜이다.

2. 관련 연구

RFID 시스템 환경은 무선통신이라는 환경적 제약사항으로 인해 다양한 보안 위협이 존재한다. RFID 시스템에서의 가능한 공격 모델들을 살펴보면 다음과 같다.

- MITM공격(Man In The Middle Attack) :공격자는 정당한 리더로 흉내 내어서 태그의 정보를 얻거나, 공격자는 정당한 태그로 흉내내서 리더에게 응답 후 다음 세션에 정당한 리더에 의해서 공격자는 쉽게 인증을 받음.

- Replay attack : 공격자는 T로 부터의 공격 메시지를 도청하거나 정당한 리더에게 메시지를 계속해서 전송하는 공격
- Forgery :도청에 의한 태그의 정보를 위한 단순한 복사는 적에 의해 가능
- Data loss: Dos, Power interruption, hijacking은 스니핑이나 무작위 추측 공격을 도용하여 데이터 손실을 가져오는 공격

따라서 이러한 공격 모델에 안전한 RFID 태그 리더간 상호 인증 프로토콜이 요구되어 이와 관련된 많은 연구가 이루어지고 있다.

Ari Jules는 두 개의 태그가 동시에 인식되었다는 것을 검증자에게 증명하는 프로토콜을 제안하였으며, Saiko와 Sakurai 는 Ari Jules가 제안한 프로토콜의 취약점을 보완하기 위해 타임스탬프를 사용하는 프로토콜을 제안하였다. 그러나 이 방법은 유효범위의 노출과 재생공격에 취약하다는 문제점이 있다. Selwyn Piramuthu는 검증자로부터 전달받은 임의의 수를 바탕으로 하는 프로토콜을 제안하였다. [3]에서는 YA-TRAP이라고 하는 간단하면서 추론이 불가능한 인증 프로토콜을 제안하였으며 이 프로토콜은 태그와 리더간 계산 비용과 부하가 없는 single keyed hash를 이용한다. 백엔드 서버에도 로드가 없다는 장점을 지닌다. YA-TRAP은 태그에서 one light-weight cryptographic operation 만 필요하며 하나의 키값을 저장하면 되므로 태그와 백엔드 서버에 부하가 없는 프로토콜이다. 그러나 공격에 필요한 복잡도가 높지 않아 재생 공격에 노출될 가능성이 높다.

따라서 본 논문에서는 중간자 공격및 재생공격에 강력히 대응할 수 있는 강력한 다항식 해쉬함수를 이용한 상호인증 프로토콜을 제안한다.

3. 다항식 해쉬함수를 이용한 RFID 인증 프로토콜

3.1 보안 요구 사항

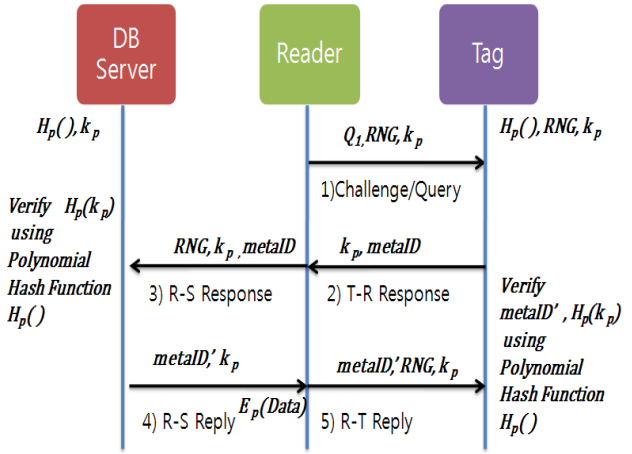
앞 장에서 제시된 공격 모델에 대응하기 위해서 RFID 리더 태그간 상호 인증 프로토콜에서 필요로 하는 보안 요구사항은 다음과 같다.

- 데이터 기밀성(Data Confidentiality) : 태그의 응답이 공격자에겐 무의미해야 함.
- 태그 익명성(Tag Anonymity) : 그의 ID를 공격자가 알 수 없어야 함. 사용자의 소지품 정보 노출 방지
- 데이터 무결성(Data Integrity) :수신된 데이터가 정확히 권한 있는 실체가 송신한 것임을 확신.수정, 삽입, 삭제, 재전송이 없음
- 태그 비추적성(Tag Untracebility) : 태그를 추적할 수 없어야 함.

따라서 위의 보안 요구사항을 만족하면서 공격자에게 공격이 쉽지 않은 강력한 복잡도를 가지는 해쉬함수 기반의 RFID 인증 프로토콜을 설계하였다.

3.2 제안된 RFID 인증 프로토콜

본 논문에서 제안하는 다항식 해쉬함수를 이용한 RFID 인증 프로토콜은 다음 [그림 1]과 같다.



[그림 1] 다항식 해쉬함수를 이용한 RFID 인증 프로토콜

먼저 초기화 단계에서는 다항식 해쉬함수를 이용한 키 값을 생성한다. 백엔드 디비 서버는 생성된 키값을 저장한다.

리더가 쿼리를 보내면 상호 인증을 위한 과정은 5단계로 수행된다.

1) Challenge

리더 태그구간의 안전성을 확보하기 위해 리더는 *RNG*(Random Number Generator) 값과 키 값 k_p 를 쿼리와 함께 태그에 보낸다.

2) T-R Response

쿼리를 받은 태그는 익명성 보장을 위해 metaID와 키값 k_p 를 보내 리더에 응답한다.

3) R-S Response

리더는 태그로부터 받은 metaID와 키값 k_p 를 백엔드 디비 서버에 보낸다.

4) R-S Reply

백엔드 디비 서버는 키 테이블에서 리더로부터 받은 metaID와 키값 k_p 를 확인한 후 인증된 태

그이면 metaID'과 키값 k_p 를 리더에 보낸다.

5) R-T Reply

리더는 디비서버로부터 받은 metaID'과 키값 k_p 를 태그에 보내 인증된 리더임을 태그에 알린다.

본 논문에서 제안한 RFID 인증 프로토콜의 장점은 해쉬함수 기반의 키 생성에 초점을 맞추어 복잡도가 높은 다항식 해쉬함수을 적용한다는 것이다. 이는 공격에 쉽게 노출되지 않는 강력한 인증 프로토콜임을 수학적으로 검증가능하다는 것을 의미한다. 다음 4장에서 RFID 인증 프로토콜을 위해 설계된 다항식 해쉬함수에 관하여 기술하였다.

4. 다항식 해쉬함수의 설계

[6]에서 설계한 해쉬함수는 결합법칙, 교환법칙이 성립하지 않으며 항등원과 역원이 없는 해쉬함수를 다항식을 이용하여 설계하였다. 그러나 역원이 존재하여 복원이 가능하므로 교환법칙은 성립하지 않고 역원은 존재하는 해쉬함수를 설계하여 한다. 또한 행렬을 이용한 해쉬함수는 충돌 발생이 빈번하다는 단점이 존재하므로 본 논문에서 설계한 해쉬함수는 곱집합의 연산을 이용하였다.

곱집합(Cartesian Product)을 이용한 binary operation을 기반으로 한 해쉬함수를 설계하기 위해서 다음과 같이 binary operation 을 정의하였다.

[정의] binary operation

* 체(field) K와 F의 곱집합 $K\times F$에서 F로의 주어진 두 함수 α 와 β에 대하여 $K\times F$에서의 이항연산(binary operation) $\circ$ 을 다음과 같이 정의하면 $(K\times F,\ \circ)$ 는 groupoid를 형성한다.

$$(a,u)\circ(b,v)=(ab,\ \alpha(a,v)+\beta(b,u)),$$

$a, b\in K,\ u, v\in F$

* 다음의 성질을 만족하는 함수 $\alpha : F\times F\to F$를 오른쪽 가법함수(right additive map)라 한다.

$$\alpha(a,\ u+v)=\alpha(a,\ u)+\alpha(a,\ v)$$

[정의] grouppoid

* 함수 $\alpha,\beta : K\times F\to F$의 형태에 따라 groupoid $(K\times F,\ \circ)$ 의 연산 구조가 달라진다.

[정리 1] 함수 $\alpha,\beta : K\times F\to F$가 오른쪽 가법함수라 할 때, $\circ$ 가 결합법칙이 성립하기위한 필요충분조건은 α 와 β가 다음의 세 가지 성질을 만족하는 것이다.

(A1) $\alpha(a,\ \alpha(b,u))=\alpha(ab,\ u)$,

(A2) $\beta(a,\ \beta(b,u))=\beta(ba,\ u)$,

(A3) $\alpha(a,\ \beta(b,u))=\beta(b,\ \alpha(a,u))$

따라서 α 와 β가 위의 성질을 만족하면 $(K\times F,\ \circ)$ 는 semigroup이 된다.

[정리 2] $\circ$ 는 교환법칙이 성립하기 위한 필요충분조건은 $\alpha=\beta$ 이다. 따라서 $\alpha=\beta$ 이면 $(K\times F,\ \circ)$ 는 commutative groupoid가 된다.

[정리 3] α 와 β가 (1)의 세 가지 성질을 만족할 때, $(K\times F,\ \circ)$가 항등원 $(1,0)$를 갖기 위한 필요충분조건은 α 와 β가 모두 전사함수인 것이다.

[정리 4] α 와 β가 (1)의 세 가지 성질을 만족하고 모두 전사함수이면 $a\neq 0$ 인 모든 원소 $(a,u)\in K\times F$는 역원 $(a,u)^{-1}$ 을 갖는다.

설계한 해쉬함수를 이용한 인증과정은 다음과 같다.

<인증을 위한 해쉬 함수 : 비트스트링 $b_1b_2\cdots b_n$ 의 해쉬 코드 생성>

① 위에서 다룬 연산에 사용된 두 체를 $K=\boldsymbol{F}_{2^k}$, $F=\boldsymbol{F}_{2^l}$ $(k\geq l)$라 하고, 적당한 $a, b\in\boldsymbol{F}_{2^k}$와 $u, v\in\boldsymbol{F}_{2^l}$에 대하여 함수 $\pi:\{0,1\}\to\boldsymbol{F}_{2^k}\times\boldsymbol{F}_{2^l}$를 다음과 같이 정의한다.

$\pi(0)=(a,u),\ \pi(1)=(b,v)$

② 비트스트링 $b_1b_2\cdots b_n$ 을 일정한 길이 t 의 블록으로 다음과 같이 나눈다. (마지막 블록에 비트가 부족한 경우 0으로 채움)

$$B_1=b_{11}\cdots b_{1t},\ \cdots,\ B_m=b_{m1}\cdots b_{mt}$$

③ 두 함수 $\alpha,\beta : \boldsymbol{F}_{2^k}\times\boldsymbol{F}_{2^l}\to\boldsymbol{F}_{2^l}$ 를 각각 다음과 같이 정의하자.

$$\alpha(f,g)=fg\ ,\ \beta(f,g)=g=f\ (\mathrm{mod}\ q(x))$$

α , β 를 이용하여 만든 연산 $\circ$ 을 이용하여 다음과 같이 블록의 해쉬코드를 생성한다.

$H(B_i)=(\cdots(((\pi(b_{i1})\circ\pi(b_{i2}))\circ\pi(b_{i3}))\cdots)\circ\pi(b_{it})$
$\in\boldsymbol{F}_{2^k}\times\boldsymbol{F}_{2^l}$

④ 각각의 블록 해쉬 코드를 같은 연산을 사용하여 다음과 같이 해쉬코드를 생성한다.

$H(b_1b_2\cdots b_n)=(\cdots((H(B_1)\circ H(B_2))\circ\cdots)\circ H(B_m)$

예) 위의 연산을 이용한 비트 스트링 10111의 해쉬코드

체 $\boldsymbol{F}_2=\{0,1\}$ 에서의 다항식 환 $\boldsymbol{F}_2[x]$ 에서의 기약다항식

$$p(x) = x^2 + x + 1, \quad q(x) = x^3 + x + 1$$

에 대한 유한체

$K = \boldsymbol{F}_{2^2} = \boldsymbol{F}_2[x]/(p(x))$, $F = \boldsymbol{F}_{2^3} = \boldsymbol{F}_2[x]/(q(x))$ 의 곱집합에서

$$\pi(0) = (10, 011),\ \pi(1) = (11, 010)$$

라 하자. 주어진 비트 스트링을 길이 3인 두 개의 블록 $B_1 = 101$, $B_2 = 110$으로 나누고 이들을 해쉬화하면 다음과 같다.

$$H(B_1) = (\pi(1) \circ \pi(0)) \circ \pi(1)$$
$$= ((11, 010) \circ (10, 011)) \circ (11, 010)$$
$$= (01, 111) \circ (11, 010)$$
$$= (11,001) = 11001$$

$$H(B_2) = (\pi(1) \circ \pi(1)) \circ \pi(0)$$
$$= ((11, 010) \circ (11, 010)) \circ (10, 011)$$
$$= (10, 101) \circ (10, 011)$$
$$= (11,100) = 11100$$

$$H(10111) = H(B_1) \circ H(B_2)$$
$$= (11 ,001) \circ (11, 100)$$
$$= (10, 100)$$
$$= 10100$$

위의 예에서 설계한 해쉬함수의 안전성을 높이기 위해서는 비트스트링의 길이을 가변화하는 방법도 고려해볼 수 있다.

5. 결론

RFID 시스템은 환경적 제약으로 인해 다양한 공격 모델에 취약하다. 특히 중간자 공격이나 재생 공격과 같은 공격에 강력하게 대응하여 데이터 기밀성과 데이터 무결성, 태그 익명성 등의 보안 요구사항을 충족하여야 한다.

본 논문에서는 위의 보안 요구사항을 만족하는 강력한 RFID 인증 프로토콜을 제안하였다. 제안된 RFID 인증 프로토콜은 해쉬함수 기반의 인증 프로토콜로써 다항식 해쉬함수의 특성에 기반해 그 안전성을 보장하는 강력한 RFID 인증 프로토콜이다.
향후 수학적 모델의 검증과 실험평가에 대한 연구가 수행될 계획이다.

참고문헌

[1] Istv Vajda and Levente Butty. Lightweight authentication protocols for low-cost rd tags. Workshop on Security in Ubiquitous Computing, October 2003.

[2] S. Weis and S. Sarma and Ronald Rivest and D. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Indentication Systems. Proc. of the 1st Security in Pervasive Computing, LNCS, October 2004.

[3] Gene Tsudik. Ya-trap: Yet another trivial rd authentication protocol. International Conference on Pervasive Computing and Communications, PerCom, 2006.

[4] Jeongkyu Yang and Kui Ren and Kwangio Kim. Security and Privacy on Authentication Protocol for Low-cost RFID. Symposium on Cryptography and Information Security,January 2005.

[5] D. Henrici and P. Muller. Hashed-based Enhancement of Location Privacy for Radio-Frequency Identication Devices using Varying Identiers. . PerSec '04, March 2004.

[6] V. Shpilrain, Hashing with Polynomials, The City College of NewYork, 2006