키 변환을 이용한 랜덤 대칭키 기반의 RFID 인증 프로토콜

김경율*, 김영백*, 박용수*, 윤태진**, 안광선*
*경북대학교 전자전기컴퓨터학부
**경운대학교 모바일공학과
e-mail:kimm2001@ee.knu.ac.kr

An RFID Authentication Protocol Based a Random Symmetric Key using Key Change

Kyoung-Youl Kim*, Young-Back Kim*, Yong-Soo Park*
Tae-Jin Yun**, Kwang-Seon Ahn*
*School of Electrical Engineering and Computer Science, Kyung-Pook University
**Dept of Mobile Engineering, Kyung-Woon University

요 약

RFID(Radio-Frequency IDentification) 시스템은 무선주파수를 이용한 자동 인식 기술로 개인의 위치 추적이나 사용자 프라이버시와 같은 정보 유출의 위험성을 내포하고 있다. 이러한 문제점을 해결하기 위해 대칭키 기반의 AES 암호화 알고리즘은 해시함수나 공개키 암호화 기법에 비해 메모리를 적게 소모하고 구현이 쉬운 장점 때문에 수동형 RFID태그에 더 적합하다. 그러나 기존의 AES를 이용한 RFID 인증 프로토콜에서는 항상 고정된 키를 이용하여 암호화하였고 태그와 리더사이의 안전하지 않은 무선 채널에서 공격자에 의해 키 값이 노출될 수 있는 또 다른 문제점을 가지고 있다. 본 논문에서는 태그와 서버의 고정된 키와, 리더 태그 서버에서 생성된 난수를 차례로 이용하여 대칭키를 변환한다. 그리고 매 세션마다 변환된 키로 난수를 암호화 하면서 태그와 리더를 상호 인증한다. 이와 같이 변환된 키를 이용할 경우 키 값의 노출 문제가 해결되며, 이 키를 통해 암호화하여 인증할 경우 재전송, 도청, 위치추적 및 스푸핑과 같은 공격에도 안전하다.

1. 서론

RFID(Radio-Frequency IDentification) 시스템은 태그와 리더가 무선주파수를 이용하여 물리적 접촉 없이 대량의 사물을 동시에 인식하는 자동 인식 시스템이다. RFID 태그는 리더의 요청에 따라 자신의 식별 정보를 무선 주파수를 사용하여 아무런 제약이 없이 전송하기 때문에 도청을 통한 개인의 정보 노출이나 위치 추적 등의 사용자 프라이버시 측면에서 여러 가지 문제점이 발생한다. 이러한 문제점을 해결하기 위한 암호학적 접근 방안으로 대칭키 및 공개키 기반의 암호화 기법과 해시함수가 있다. 표준 SHA 계열의 해시함수는 충분한 저장 공간과 높은 연산 능력을 필요로 하기 때문에 제한적인 수동형 RFID 태그에 적용하기에는 문제가 있다. 또한 공개키 기반의 암호화 기법은 누구나 공개키를 가지고 있으므로 키 분배 문제를 해결하지만 암호화와 복호화의 연산 능력이 해시함수보다 더 높다.

대칭키 기반의 암호화 기법은 해시함수나 공개키 암호화 기법에 비해 메모리를 적게 소모하고 구현이 쉬운 장점이 있다. 특히 AES(Advanced Encryption Standard) 알고리즘[1]의 경우 RFID 태그에서 구현 가능한 형태의 저전력 AES 기법[2]이 제안되었고 이를 이용한 RFID 인증 프로토콜에 대한 연구도 진행되고 있다[3][4]. 하지만 기존의 AES를 이용한 RFID 인증 프로토콜에서는 항상 고정된 키를 이용하여 암호화하였고 태그와 리더사이의 안전하지 않은 무선 채널에서 공격자에 의해 키 값이 노출될 수 있는 또 다른 문제점을 가지고 있다.

본 논문에서는 태그와 서버의 고정된 키와 리더, 태그, 서버에서 생성된 난수를 차례로 이용하여 대칭키를 변환한다. 그리고 변환된 키로 매 세션마다 난수를 암호화하여 서버에서 태그를 인증하고 태그에서 리더를 인증한다. 이와 같이 변환된 키를 이용할 경우 키 값이 노출될 우려가 없다. 또한 변환된 키를 이용하여 난수를 암호화하였기 때문에 태그의 응답은 가변적이므로 재전송, 도청, 위치추적 및 스푸핑과 같은 공격에도 안전하다.

2. 관련연구

본 절에서는 수동형 RFID 태그에 적합한 대칭키 기반의 암호화 기법과 인증 프로토콜에 대해서 서술한다. 또한 기존의 대칭키 기반의 RFID 인증과정에서 키를 이용한 암호화 과정에서의 문제점에 대해서 서술하고자 한다[5].

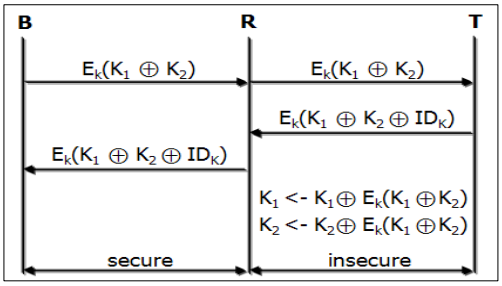
2.1 대칭키 기반의 암호학적 접근 방법

최근 임베디드 기술과 시장이 발전함에 따라 RFID 태그에서도 적용 가능한 암호학적 접근 방식이 다양하게 연

구되고 있다. 대표적으로 대칭키 기반의 암호학적 접근 방식 중 AES(Advanced Encryption Standard)는 벨기에의 수학자 존 대이먼과 빈센트 라이먼에 의해서 만들어진 Rijndael 알고리즘을 바탕으로 하여 미국 정부 표준으로 지정된 블록 암호 형식이다. AES는 기존의 AES를 개선하여 수동형 RFID 태그에 적합한 형태로 구현 가능한 연구가 진행 중이다. Martin Feldhofer는 기존의 32bit AES를 효율적이고 저 전력 설계를 위해 8bit만으로 진행되는 소형의 AES를 제안하였고[2], 다양한 논문을 통해 해시함수나 공개키 암호화보다 AES 대칭키 암호화 기법이 저 전력 설계에 더 적합함을 입증했다[6][7][8].

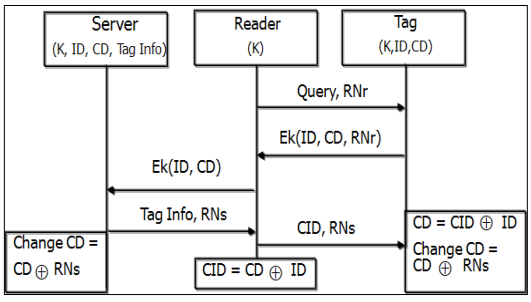
2.2 AES를 이용한 인증 프로토콜

Martin Feldhofer는 저 전력 AES를 이용해 인증 프로토콜을 제안하였지만 난수를 이용한 단방향 인증이었고 다양한 공격에 취약하다[2]. (그림 1)은 서버와 태그사이에서 사전에 저장된 두 개의 비밀 키를 이용해서 상호 인증하는 방법을 나타낸 것이다[3].



(그림 1) An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems

이 프로토콜은 위치추적을 막기 위해 두 키를 일정한 방식으로 업데이트를 시키고 업데이트된 키는 서버와 태그에 동일하게 저장한다. 업데이트된 비밀 키는 다음에 인증하는데 사용되지만 각각 태그마다 다른 키를 사용할 경우 태그를 식별하는데 문제가 있다. 또한 각각의 태그마다 같은 키 값으로 암호화하는 잠재적인 문제점도 있다. (그림 2)는 서버와 태그사이의 사전에 공유된 CD값을 이용하여 서버와 태그의 인증에 사용하고 서버에서 생성한 난수를 이용하여 동일하게 CD값을 업데이트 한다[4].



(그림 2) AES 암호화 프로세서를 이용한 강인한 RFID 인증 프로토콜 설계

이 프로토콜은 첫 단계에서 리더난수가 노출되어 다음 단계의 도청을 통해 키 값을 유추해 낼 수 있으며 키가 노출 시에 태그의 식별정보도 노출 된다.

이와 같이 기존의 AES를 이용한 RFID 인증 프로토콜에서는 항상 고정된 키를 이용하여 암호화하였고 태그와 리더사이의 안전하지 않은 무선채널에서 공격자에 의해 키 값이 노출될 수 있는 또 다른 문제점을 가지고 있다[5].

3. 제안하는 RFID 인증 프로토콜

본 논문에서 제안한 프로토콜은 태그와 서버의 고정된 키와 리더, 태그, 서버에서 생성된 난수를 차례로 이용하여 대칭키를 변환하고 매 세션마다 변환된 키로 난수를 암호화 하면서 태그와 리더를 상호 인증한다.

3.1 가정 사항 및 용어 정의

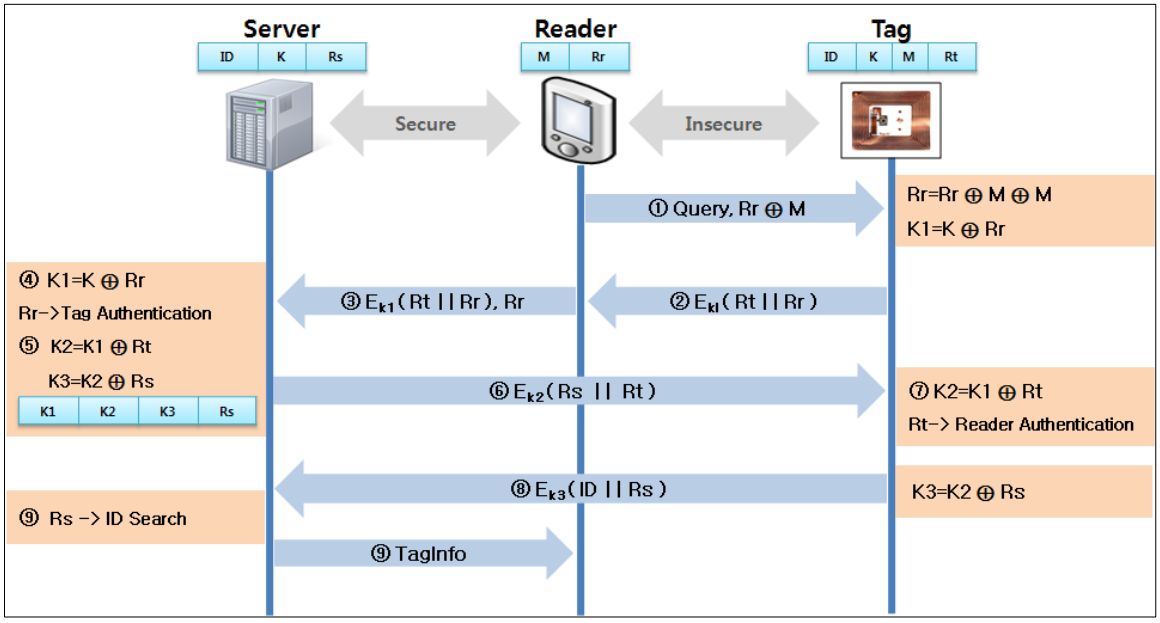
본 논문에서는 다음과 같이 가정 사항을 제시한다. 첫째, 리더와 서버 사이는 기존의 통신 채널을 이용함으로써 공격자의 공격에 안전하지만 리더와 태그의 통신 채널은 무선 주파수를 사용하기 때문에 공격자의 공격에 취약하다. 둘째, 태그와 서버는 대칭키 기반의 암호화 및 복호화 연산을 수행할 수 있다. 셋째, 리더와 서버, 태그는 각각 난수를 생성할 수 있다. 넷째, 서버와 태그는 사전에 동일한 대칭키를 가지고 있으며 리더와 태그는 사전에 동일한 공유키를 가지고 있다. 마지막으로 태그는 리더로부터 전원을 공급받는 수동형 태그로 가정한다. 본 논문에서는 제안한 RFID 인증 프로토콜에 사용된 용어는 다음과 같다.

<표1> 용어 정의

용 어	설 명
Rr	리더가 생성한 난수
Rt	태그가 생성한 난수
Rs	서버가 생성한 난수
K	서버와 태그에 사전에 저장된 대칭키
K1, K2, K3	서버와 태그에서 랜덤하게 생성된 대칭키
ID	태그의 고유 식별 값
||	연접
⊕	Exclusive-OR (XOR)
M	리더와 태그에 사전에 저장된 공유키

3.2 상세 프로토콜

기존 인증 프로토콜의 경우 프로토콜을 설계하는데 있어서 키 변환을 고려하지 않고 데이터를 일정하게 변경하여 암호화하였다. 따라서 키 값이 노출되면 태그의 식별정보도 그대로 노출된다. 본 논문에서는 기존의 연구에서 키 변환을 고려하지 않은 문제를 보안하고 다양한 공격에 안전하도록 설계하였다. (그림 3)은 본 논문에서 제안한 RFID 인증 프로토콜의 암호화 및 인증과정이다.



(그림 3) 제안 프로토콜

다음은 제안한 RFID 인증 프로토콜의 암호화 및 인증의 아홉 가지 과정을 기술한다.

① 리더는 리더난수와 공유키(M)를 XOR 연산하여 Query와 함께 태그에게 보낸다. 공유키(M)는 리더난수를 안전하게 보내기 위한 사용한다.

Reader -> Tag : Query, Rr⊕M

② 태그는 리더가 보낸 정보를 자신의 공유키(M)로 XOR 연산해서 리더난수(Rr)를 얻고, 대칭키(K)와 Rr를 XOR 연산하여 새로운 키 K1을 생성한다. 리더난수, 태그난수를 연접해서 K1키로 암호화해서 보낸다.

Tag : Rr = Rr⊕M⊕M

Tag : K1 = K⊕Rr

Tag -> Reader : E_{K1}(Rt||Rr)

③ 리더는 태그가 보낸 정보에 리더난수를 추가하여 안전한 채널을 통해서 서버에게 보낸다.

Reader -> Server : E_{K1}(Rt||Rr), Rr

④ 서버의 대칭키 K와 리더에서 보낸 리더난수를 XOR 연산하여 K1키를 생성하고 태그에서 보낸 정보를 복호화 한다. 복호화 후 리더난수와 안전한 채널을 통해 받은 리더난수를 비교해서 태그를 인증한다. 즉, 단계 ①, ②번 과정을 통해서 태그에서 암호화한 데이터가 유효하다는 것을 인증하는 것이다.

Server : K1 = K⊕Rr

Server : D_{K1}(E_{K1}(Rt||Rr))

⑤ 인증이 성공하면 복호화 한 태그난수를 K1키와 XOR 연산을 통해 K2키를 생성하고, 서버에서 생성된 서버난수를 K2키와 XOR 연산을 통해 K3키를 생성한다. 인증이 실패하면 종료한다. 생성된 키들은 임시 공간에 저장한다.

Server : K2 = K1⊕Rt

Server : K3 = K2⊕Rs

Server : (K1, K2, K3, Rs)

⑥ K2키로 서버난수와 태그난수를 암호화해서 보낸다.

Server -> Reader -> Tag : E_{K2}(Rs||Rt)

⑦ 태그는 자신의 난수 Rt와 K1키로 XOR 연산하여 K2키를 생성해서 서버가 보낸 정보를 복호화 한다. 그리고 태그의 난수와 복호화 된 태그의 난수를 비교를 통해 리더를 인증한다. 인증이 실패하면 종료한다. 인증에 성공하면 복호화 한 데이터 서버난수(Rs)를 K2키와 XOR 연산하여 K3키를 생성한다.

Tag : K2 = K1⊕Rt

Tag : D_{K2}(E_{K2}(Rs||Rt))

Tag : K3 = K2⊕Rs

⑧ K3키로 태그의 ID와 서버난수(Rs)를 암호화해서 서버에게 보낸다.

Tag -> Reader -> Server : E_{K3}(ID||Rs)

⑨ 서버는 K3키로 태그에서 보낸 데이터를 복호화 한 후에 서버난수(Rs)를 비교해서 값이 일치하면 태그 ID를 검색해서 태그 정보를 리더에게 보내고 그렇지 않으면 세션을 종료한다.

4. 보안 분석

(1) 도청

태그와 리더사이는 무선 통신을 하는 불안전한 채널로 ①, ②, ⑥, ⑧ 단계에서 공격자에 의해서 도청이 가능하다. 그러나 암호화하는 데이터와 키는 난수를 이용하기 때문에 응답 값은 가변적이다. 그러므로 도청된 가변 정보는 의미가 없다.

(2) 트래픽 분석

도청된 데이터를 매 세션 수집하여 중요값을 추측해 내는 공격 유형으로 리더와 태그사이에 사전에 저장된 공유키(M)를 이용해서 ①단계에서 리더난수를 안전하게 보낸다. 리더난수는 임의의 키 K1을 생성하는 중요 정보로서 안전하게 보내기 위해 공유키를 사용하고 또한 서버와 태그사이에 사전에 저장된 대칭키(K)를 숨김으로서 공격자는 트래픽 분석을 통해 중요정보인 K, M을 획득할 수 없고 그 비밀 정보도 노출될 수 없다.

(3) 위치 추적

태그의 출력 값이 일정한 경우에는 태그 값의 위치 변화를 감시하여 태그 소유자의 물품 위치를 추적할 수 있다. 본 논문에서는 매 세션마다 난수를 사용하기 때문에 응답 값이 매번 변경되어 추적이 불가능하다.

(4) 스푸핑 공격

스푸핑은 공격자가 도청한 정보를 이용하여 태그에게 자신이 정상적인 리더인 것처럼 위장하여 중요 정보를 획득하거나, 리더에게 자신이 정상적인 태그인 것처럼 위장하여 거짓 정보를 보내는 공격이다. 공격자가 위장 태그인 경우에는 ①, ②, ③ 단계를 통해 서버에서 리더난수의 비교를 통해 태그를 인증하기 때문에 거짓 정보인 경우 세션을 종료한다. 또한 공격자가 위장 리더인 경우에는 ⑦단계에서 태그난수의 비교를 통해 리더를 인증하기 때문에 공격자로부터 거짓 정보에 대해 사전에 방지하며 중요한 정보의 획득이 불가능하다.

(5) 재전송 공격

재전송 공격은 공격자가 태그와 리더간의 통신을 도청하여 그 메시지를 재전송 하는 것이다. 본 논문에서는 매 세션 마다 암호화하는 키 값이 변경되고 키를 가지고 암호화하는 데이터는 난수이므로 태그와 리더 사이의 고정된 값이 출력되지 않는다. 따라서 공격자가 도청을 통해 그 메시지를 그대로 전송하더라도 정상적인 리더와 태그 입장에서는 이전 값을 보낸다. 즉 서버에서는 난수에 의해 변경된 키 값과 태그의 키 값이 일치 하지 않기 때문에 인증과정에서 공격자로 판단하고 세션을 종료시킨다.

5. 결론

RFID 시스템은 무선을 이용한 자동인식 기술로 주목받고 있지만 개인의 위치추적이나 사용자 프라이버시와 같은 정보 유출의 위험성을 내포하고 있다. 이러한 문제를 해결하기 위해 다양한 암호학적 연구들이 진행되어 왔고 대칭키 기반의 AES 암호화 기법이 수동형 RFID 태그에 적합함이 입증 되었다. 그러나 기존의 AES를 이용한 RFID 인증 프로토콜은 항상 고정된 키를 이용하여 암호화하였고 태그와 리더사이의 무선 채널에서 공격자에 의해 키 값이 노출되는 문제점과 단순 인증 및 암호화하는 데이터를 일정하게 변경하는 것에 불과했다.

본 논문에서는 태그와 서버의 고정된 대칭키와 리더, 태그, 서버에서 생성된 난수를 차례로 이용하여 대칭키를 변환하고 매 세션마다 변환된 키로 난수를 암호화 하면서 태그와 리더를 상호 인증한다. 이와 같이 변환된 키를 이용할 경우 키 값의 노출이 해결되며 이 키를 통해 각각의 난수를 암호화하고 인증함으로써 재전송, 도청, 위치추적 및 스푸핑과 같은 공격에도 안전성을 보장한다.

참고문헌

[1] J. Daemen, V. Rijmen, “The Design of Rijndael,” AES-The Advanced Encryption Standard, Springer-Verlog, Berlin, Heidelberg, New York, 2002.

[2] M. Feldhofer, S. Dominikus, Rijmen, J. Wolkerstorfer, “Strong Authentication for RFID Systems Using The AES Algorithm,” ICCHES, pp. 357-370, 2004.

[3] B. Toiruul, K. Lee, “An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems,” IJCSNS, Sep. 2006.

[4] 이남기, 장태민, 전병찬, 전진오, 유수봉, 강민섭, “AES 암호 프로세서를 이용한 강인한 RFID 인증 프로토콜 설계”, 한국정보처리학회 논문집, 제15권, 제2호, pp. 1473-1476, 11월 2008.

[5] M. Feldhofer, M. Aigner, “Secure Symmetric Authentication for RFID Tags,” Telecommunication and Mobile Computing-CTCMC2005, March 2005.

[6] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, “AES implementation on a grain of sand.” IEE Proceedings Information Security, Vol. 152, Issue 1, pp. 13 - 20, October 2005.

[7] M. Feldhofer, J. Wolkerstorfer, “Strong Crypto for RFID Tags - A Comparison of Low-Power Hardware Implementations,” ISCAS, 27-30, pp. 1839-1842, May 2007.

[8] M. Jung, Horst Fiedler, and Renee Lerch, “8-bit Microcontroller System with Area Efficient AES Coprocessor for Transponder Application,” Workshop on RFID and Lightweight Crypto, pp. 32-43, July 2005.