전자태그 시스템을 위한 인증 프레임워크의 요구 사항

지 성 배, 이 현 록, 윤 성 준, 김 광 조
국제정보보호기술연구소, 한국정보통신대학교

The Requirements of RFID Authentication Framework

Sungbae Ji, Hyunrok Lee, Sungjune Yoon, Kwangjo Kim
International Research center for Information Security (IRIS),
Information and Communication University (ICU)

요 약

최근 다양한 분야에서 전자태그(RFID)가 활용되고 있지만 동시에 개인정보의 침해와 태그의 위조 등과 같은 보안 문제들이 제기되고 있다. 이미 많은 종류의 인증 프로토콜이 이러한 보안 문제를 해결하기 위해 제안되었으나, 전자태그 시스템을 사용하는 다양한 응용들에서 각기 다른 보안 요구 사항과 이를 만족하는 많은 인증 프로토콜이 존재하게 되어 해당 시스템의 확장성 및 관리의 측면에서 많은 문제점을 가지고 있다. 본 논문에서는, 서로 다른 전자태그 인증 시스템의 통합을 위한 인증 프레임워크의 필요성을 도출하고 기존에 무선 환경에서 많이 쓰이는 인증 프레임워크인 EAP의 적용 가능성을 검토한다. 또한 RFID 인증 프레임워크의 설계 시 고려해야 할 요구 사항들을 제시한다.

ABSTRACT

Recently, various applications of RFID have been developed and researched while security issues such as privacy infringement and the forgery of tags have being raised. Many types of authentication protocols were proposed in order to solve these security problems, but it is a another difficult problem to combine heterogeneous RFID systems which have different security requirements and authentication protocols. In this paper, we explain why we need an authentication framework for integrating different RFID authentication systems, and examine the applicability of EAP, which is an authentication framework widely used in wireless environments. We also present requirements and considerations for RFID authentication framework design.

Keywords: 전자태그 (RFID), 인증 프레임워크

Ⅰ. 서 론

전자태그 또는 RFID (Radio Frequency IDentification) 기술은 공급/유통망에서 상품의 유통 경로의 추적 또는 재고 관리 시스템, 도서관의 대출/반납 시스템, 전자 결제 시스템, 또는 전자 여권 등의 용도로 폭 넓게 사용되고 있다. 그러나 안전한 전자태그 시스템을 도입하기 위해서는 해결되어야 할 많은 보안 문제들이 남아있다.

* 본 연구는 MIC/IITA의 IT R&D 프로그램 연구과제 (2005-S-106-02, RFID/USN용 센서 태그 및 센서 노드 기술 개발) 지원으로 수행하였습니다.

Feldhofer 등은 전자태그 시스템에서의 세 가지 보안 문제점을 지적하였는데, 개인정보 또는 사생활의 자유에 대한 침해, 태그의 위조, 태그에 대한 인가되지 않은 접근을 문제점으로 도출하였다.[1] 이와 더불어 도청, 태그의 스푸핑, 태그의 복제, 재전송 공격 등과 같은 문제점들이 또 다른 논문들을 통해 지적되었다.[7,11,12] 이러한 보안 문제들은 적절한 인증 메커니즘에 의해 해결될 수 있으며, 최근 연구 결과들에서 해쉬[7,8,9], 개인 식별 번호 (PIN)[3], 블록 암호화[1] 기반의 많은 인증 프로토콜이 제안되고 있지만, 많은 종류의 시스템에 동일하게 적용할 수 있는 인증 프로토콜은 없다. 오히려 실제로는 각각의 응용 시스템마다 서로 다른 보안 요구 사항을 가지고 있기 때문에 다양한 인증 프로토콜이 필요하다. 더구나 전자태그의 종류마다 다른 특성을 보이므로 응용 시스템에서 필요로 하는 태그의 종류는 다양할 수밖에 없다. 이는 결국 이질적인 전자태그 시스템은 하나의 전자태그 인증 시스템으로 통합될 수 없는 문제를 가지며, 이를 해결하기 위해 통합 인증 프레임워크의 필요성이 대두된다.

Dantu 등은 주로 무선 랜 환경에서 사용되는 인증 프레임워크인 EAP (Extensible Authentication Protocol)[4]를 전자태그 시스템과 WiMAX 환경에도 적용할 수 있다는 전제하에 기존 EAP 인증 방식의 적용 가능성을 검토하였다.[15] 그러나 전자태그 시스템에 EAP를 직접 적용하기에는 한 번에 많은 수의 태그를 읽을 수 있는 벌크-리딩 (bulk-reading) 능력, 추적 가능성 (traceability), 사생활 침해, 태그의 낮은 가용 자원과 같이 추가적으로 고려해야할 문제점들이 존재하며, 이러한 점들은 EAP를 수정 없이 전자태그 시스템에 적용하는 것을 어렵게 한다.

본 논문은 이러한 전자태그 시스템의 통합 인증 프레임워크를 설계할 때 기존의 EAP로는 부족한 부분들을 살펴보고 추가적으로 전자태그 시스템에서 고려해야할 요구 사항들을 제시한다.

II. 관련 연구

1. 전자태그 응용 시스템 보안 요구사항

Phillips 등은 전자태그 시스템을 세 가지의 응용 시스템으로 분류하였다.[2] "Logistical 응용 시스템"은 공급/유통망에서 재고 관리, 상품의 유통 경로를 추적하기 위해 사용되는 전자태그 응용 시스템을 말한다. 상품들은 물리적 안전이 보장되어야 하고 추적할 필요가 있기 때문에, 강한 인증 메커니즘이 필수적으로 요구되지는 않는다. 낮은 지연, 높은 인식률, 벌크-리딩 훨씬 중요하다.

반면에, "Consumer 응용 시스템"은 소비자 사생활의 보호가 중요하다. 인가되지 않은 사람이나 장치가 스마트카드나 전자 여권 또는 소비자의 소지품을 접근하려고 할 때, 개인정보와 사생활의 보호를 위해서 어느 정도 높은 수준의 인증이 필요하다.

"Vertical 응용 시스템"은 위의 두 가지 시스템의 중간적인 특성을 가지는데 응용 시스템의 목적에 따라 특정한 보안 기능을 요구한다. 예를 들면, 전자태그가 부착된 지폐[5]는 사용자의 사생활 보호를 위해 제한된 접근 제어가 필요하고 동시에 불법적인 거래를 모니터링하기 위해 경로 추적 능력 또한 필요로 한다.

2. 전자태그의 특성과 보안 기능

다양한 응용 시스템에 따라 다양한 종류의 전자태그가 필요하다. 라디오 주파수의 대역에 따라 전자태그를 분류하면 저주파 (LF: low-frequency), 고주파 (HF: high-frequency), 초고주파 (UHF: ultra-high-frequency) 태그로 구분할 수 있다. 일반적으로 수동형 태그는 값이 싸고 작기 때문에 물류의 용도로 많이 사용된다. 수동형 태그와 달리, 능동형 태그는 전력을 필요로 하면서 더 높은 계산 능력을 위한 시스템 자원을 가진다.

EPC Gen 2 Class 1 UHF 태그는[6] 공급/유통망에 사용하도록 설계된 수동형 태그이다. 따라서 태그의 기능이 단순하고 값이 싸다. 의사난수생성기 (PRNG: pseudo random number generator)와 에러 검출을 위한 CRC (cyclic redundancy check), 32 비트의 kill PIN을 이용한 태그를 죽이는 기능, 32 비트의 access PIN을 이용한 접근 제어 기능을 가지고 있다.

반면 스마트카드와 전자태그가 부착된 전자 여권은 ISO/IEC 14443[13]와 15693[14] 인터페이스를 사용하는 전형적인 예이다. ISO/IEC 표준에는 보안 기능이 정의되어 있지 않기 때문에, 스마트카드를 제작하는 업체들은 DES, 3DES, AES, RSA, SHA-1 등의 암호학적 프리미티브들을 사용

하여 각 회사 소유의 인증 접근 프로토콜을 구현하고 있다.

3. 전자태그 인증 방식

해쉬 기반의 인증은 방식의 단순함 덕분에 저가의 태그를 위해 많이 제안되었다. Hash-lock 방식은 키를 평문의 형태로 노출시키고 고정 메타 ID를 사용해 인증하기 때문에 위치 정보를 보호하지 못한다. [7] Randomized hash-lock 방식은 태그가 랜덤화된 ID로 응답을 하지만 여전히 추적 가능하고, 확장성이 떨어진다. [7] Hash chain 방식은 백-엔드 데이터베이스에 일련의 해시 연산의 부담이 있고 태그는 두 가지 다른 해시함수를 가지고 있어야 한다. [8] 해시 기반의 ID variation 방식은 추적불가능 하고 재전송 공격에 안전하지만 스푸핑 공격이 가능하다. [9]

BasicTagAuth+ 프로토콜은 EPC 태그를 위해 설계되었다. [3] 이 프로토콜은 EPC Gen 2 태그의 kill PIN을 사용하여 이루어진다. 신뢰할 수 없는 리더를 가정하기 때문에, 인증은 태그와 검증을 담당하는 백-엔드의 서버 사이에서 이루어진다.

Feldhofer 등은 8 비트 구조의 하드웨어로 복호화를 제외한 AES를 구현하였다. [1] 그들은 수동형 태그의 제한을 만족할 정도의 적은 전력 소비와, 작은 회로 사이즈의 구현에 성공하였다. 이 결과는 AES 암호화 알고리즘이 전자태그 인증 프로토콜의 암호학적 프리미티브로서 사용될 수 있음을 보여준다.

Ⅲ. 전자태그 인증 프레임워크의 필요성

전자태그 시스템의 구조는 그림 1과 같이 전자태그와 리더, 그리고 미들웨어 (또는 백-엔드 서버)로 이루어진다. 최근에 제안되는 인증 프로토콜에서는 보통 미들웨어와 태그 사이에서 전자태그의 인증이 이루어진다. 리더는 태그와 미들웨어 사이의 메시지를 중계하는 역할을 할 뿐, 인증 방식에 사용되는 중요한 정보나 인증 여부를 결정에는 관여하지 않는다.

그림 1. 전자태그 시스템의 구성 요소

대부분의 전자태그 시스템의 구성이 그림 1과 같이 이루어져있지만 전자태그 응용 시스템에 따라 태그의 종류와 사용하는 인증 방식이 달라진다. 각각의 전자태그 응용 시스템은 저마다의 목표와 보안 요구사항을 가지고 설계된다. 따라서 라디오 주파수와 연산 능력, 데이터 입출력 속도 등의 기술적인 특징에서 뿐만 아니라 해시 함수, PIN, 암호화 알고리즘 등 보안 기능 측면에서도 다양한 특성을 가진 다양한 형태의 전자태그가 사용되게 된다. 인증을 위해서 각각의 시스템은 태그의 능력과 응용 시스템의 보안 목표에 따라서 적합한 인증 프로토콜을 사용한다.

그러므로 다양한 응용에 사용되는 서로 다른 전자태그와 인증방식을 사용하는 시스템을 하나의 인증 시스템으로 통합하기 위해서는 전자태그 시스템에 적합한 인증 프레임워크가 필요하다. 인증 프레임워크를 사용하면 태그의 종류와 인증 방식에 따라 분리된 인증 시스템을 하나의 시스템으로 통합하여 관리적인 측면에서 보다 용이하며 소유권 변경 후에 소유자가 원하는 인증 방식으로 쉽게 변경할 수 있다는 장점을 가진다.

Ⅳ. EAP의 적용 가능성

EAP는 무선 랜에서 주로 사용되지만 무선 랜뿐만 아니라 어떠한 네트워크 환경에도 쓰일 수 있는 보편적인 인증 프레임워크이다. [4] EAP는 RFC로 정의된 40여 개의 인증 방식을 포함하여 다수의 인증 방식을 지원한다. 인증 방식은 EAP peer의 인증 혹은 EAP peer와 authenticator 사이의 상호 인증 프로토콜을 구현한다. EAP-MD5, LEAP, EAP-TLS, EAP-TTLS, PEAP 등의 인증 방식이 무선 랜에서 주로 쓰이는데 다양한 암호학적 프리미티브를 사용해서 다양한 보안 기능과 성능을 제공한다. Peer와 authenticator는 다양한 인증 방식 중에서 각자가 원하는 인증 방식을 협상 (negotiation) 과정을 통해 선택할 수 있다.

1. 무선 랜과 전자태그 시스템의 유사점

전자태그 시스템은 무선 랜 사이와 구조적 유사하기 때문에 EAP가 전자태그 인증 프레임워크로서 잘 맞는 것처럼 보인다. 전자태그와 리더 사이의 통신은 Access Point (AP)와 모바일 노드 (supplicants) 사이의 통신과 같이 RF 시그널을 이용한다. 또한 AP가 인터넷 서비스를 제공하는 인터페이스인 것과 마찬가지로 리더 전자태그 시스템의 인터페이스이다. 무선 랜에서 상호 인증은 허위 AP (Rogue AP) 문제 때문에 AP와 모바일 노드가 사이가 아닌 인증 서버(예, RADIUS)와 모바일 노드 사이에서 이루어진다. 같은 이유로, 최근의 전자태그 인증 방식들은 미들웨어와 태그 사이에서 인증이 이루어지고, 리더는 중계기로 동작한다.

2. EAP의 적용의 한계

위와 같은 관점에서, Dantu 등은 전자태그 시스템에서 적합한 기존의 EAP 인증 방식을 검토하고 평가하였다.[15] 하지만 그들은 무선 랜과 전자태그 시스템의 주요 차이점을 간과하였다. 무선 랜에서 EAP 인증방식은 IEEE 802.1X 과정에서 인증의 목적뿐만 아니라 키 유도를 위한 요소의 생성을 목적을 가진다. IEEE 802.1i의 4단계 핸드쉐이크를 통해 유도된 키를 사용하여 데이터를 암호화하여 보호할 수 있다. 무선 랜에서는 데이터의 교환이 연속적인 반면에, 수동형 전자태그는 오직 리더가 인증 과정에서 요청을 한 경우에만 응답을 한다. 전자태그의 경우는 인증 과정 후에 추가로 연속적인 데이터의 교환을 할 필요가 없기 때문에 키를 생성할 필요가 없다. 또한, 전자태그 시스템의 특성을 고려하지 않아서 다음과 같은 EAP 적용의 한계점들에 대한 분석이 부족하였다.

- 벌크-리딩 능력: EAP에서 인증은 해당 EAP peer와 일대일로 수행되고, 각 개체는 다음 인증 단계를 동기적으로 진행하는 소위 'lock-step' 프로토콜이다. EAP와는 달리 전자태그 응용 시스템은 벌크-리딩 능력을 필요로 한다. 요청이 일어날 경우, 미들웨어는 0개 이상의 태그로부터 응답을 기대하고 각 태그별로 인증 상태를 타이머와 함께 유지해야 한다.
- 추적 가능성과 사생활 침해 문제: EAP에서 Identity (Type 1) 요청과 응답은 평문으로 보내진다. 선택적으로 사용되지만, RFC 문서에 의하면 우선적으로 사용되는 것이 권고된다.[4] 반면에 전자태그 시스템에서는, 태그의 식별자를 노출시키지 않기 위해 인증 방식 고유의 식별자 교환 방식의 설계가 필요하다. 대부분의 전자태그 응용 시스템에서 태그의 식별자를 알아내는 것이 유일한 목표이기 때문에, Identity 타입은 인증 방식에 있어서 주의해서 사용해야 한다.
- 시스템 자원의 한계: 수동형 전자태그는 리더가 보내는 RF 시그널로부터 전류를 유도하기 때문에 사용할 수 있는 전력이 극도로 낮다. 가용 전력의 많은 부분이 RF 통신의 메시지 전송을 할 때 소비되므로, 패킷의 길이가 더 짧을수록 전자태그 응용 시스템에 더 적합하다. EAP는 1020 옥텟의 최대 전송 유닛 (MTU: Maximum Transmission Unit)과 패킷의 단편화 (Fragmentation)를 지원하도록 설계되었다. 그러나 전자태그 시스템의 경우 MTU 크기는 상대적으로 작아야 하며, 패킷의 단편화를 고려할 수 없다.

Ⅳ. 전자태그 인증 프레임워크의 요구 사항

Dantu 등은 전자태그의 인증을 위한 다음 여섯 가지의 요구 사항을 설명하였다.[15]

- 상호 인증
- 재암호화
- 다양한 인증방식 지원
- 로깅
- 공격에 대한 안전성
- 적은 양의 메모리 사용

위의 요구 사항 중에서 재암호화와, 공격에 대한 안전성, 적은 양의 메모리 사용은 각 인증 방식이 고려해야할 요구 사항이다. 해당 논문에서는 전자태그의 인증은 반드시 상호 인증으로 이루어져야 하는 것처럼 기술되었는데 전자태그 응용에 따라 태그의 인증만으로도 충분한 경우도 있으므로 이는 인증 프레임워크 레벨에서 필요한 요구 사항이다.

따라서 Dantu 등이 제시한 것보다 전자 태그에 적합한 요구 사항을 정리하면 아래와 같다.

- 태그에 다수의 인스턴스 저장: 전자태그는 하

나 이상의 인증 프로토콜 인스턴스를 저장하고 이를 구별할 수 있어야 한다. 다수의 리더를 지원하기 위해서는 다수의 상태 정보 각각은 태그의 메모리에 인증 절차가 종료될 때까지 유지된다. 메모리가 부족하기 때문에, 인스턴스는 메모리에 라운드 로빈 방식과 같은 순환 방식으로 저장된다.

● 미들웨어의 Timer-driven 인증: 하나의 요청 메시지에 다수의 태그가 응답할 수 있으므로 미들웨어는 각각의 유효한 응답으로부터 각 인스턴스를 타이머에 의한 방식으로 유지한다. 타이머가 종료된 인스턴스는 더 유지할 필요가 없으므로 버린다.

● 중계기 리더: 전자태그 리더는 인증 방식 계층의 기능과 상관없이 중계방식으로 동작하여 다양한 인증 방식과 호환되어야 한다.

● 상호 인증 방식의 지원: 인증 프레임워크는 비인가 리더로부터의 접근을 막기 위한 상호 인증 방식 또한 지원해야 한다.

● 인증 방식 협상: 다수의 인증 방식을 지원하기 위해서, 인증 방식 협상이 프레임워크에서 지원되어야 한다.

● 로깅의 지원: 미들웨어는 공격의 징후로 보이는 인증의 실패나 소유권 이전과 같은 이벤트 등의 로그를 기록하여 보다 안정적이고 관리가 용이하도록 할 수 있다.

V. 결 론

본 논문에서는 전자태그 인증 프레임워크의 필요성을 관련 연구를 통해 설명하고, 전자태그 시스템에 EAP의 적용 가능성을 검토하였다. 검토 결과 EAP를 전자태그 시스템에 그대로 적용하기에는 몇 가지 한계점이 있으며, 이를 해결하는 새로운 인증 프레임워크의 설계 시 고려해야 할 요구 사항들을 제시하였다.

향후 연구에서는 본 논문에서 제시된 요구 사항을 바탕으로 실제 전자태그를 위한 인증 프레임워크의 설계하고 프레임워크 상에서 동작하는 인증 방식의 예를 제시할 것이다. 또한 설계한 프레임워크를 구현하여 전자태그 인증 프레임워크의 타당성과 실현 가능성을 증명할 필요가 있다.

참 고 문 헌

[1] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm", CHES 2004, LNCS 3156, pp. 357-370, 2004.

[2] Ted Phillips, Tom Karygiannis, and Rick Kuhn, "Security Standards for the RFID Market, Security & Privacy Magazine", IEEE, vol. 3, no. 6, pp. 85-89, Nov-Dec. 2005.

[3] Ari Juels, "Strengthening EPC Tags Against Cloning", ACM Workshop on Wireless Security (WiSe), pp.67-76. 2005.

[4] Bernard Aboba, Larry J. Blunk, John R. Vollbrecht, James Carlson, and Henrik Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, IETF, 2004.

[5] Ari Juels and Ravikanth Pappu, "Squealing Euros: Privacy Protection in RFIDEnabled Banknotes", LNCS 2742, pp. 103-121, 2003.

[6] "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9", 2005.

[7] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing, LNCS 2802, pp. 201-212, 2004.

[8] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID", Proceedings of the SCIS 2004, pp.719-724, 2004.

[9] Dirk Henrici and Paul Müller,

"Hash-Based Enhancement of Location Privacy For Radio-Frequency Identification Devices Using Varying Identifiers", PerSec, 2004.

[10] Ken Traub, Greg Allgair, Henri Barthel, Leo Burstein, John Garrett, Bernie Hogan, Bryan Rodrigues, Sanjay Sarma, Johannes Schmidt, Chuck Schramek, Roger Stewart, and KK Suen, "The EPCglobal Architecture Framework", EPCglobal, 2005.

[11] Sanjay Sarma, Stephen Weis, and Daniel Engels, "Radio-Frequency Identification: Security Risks and Challenges", Cryptobytes, RSA Laboratories, 2003.

[12] István Vajda and Levente Buttyán, "Lightweight authentication protocols for lowcost RFID tags", Workshop on Security in Ubiquitous Computing, 2003.

[13] "ISO/IEC 14443-2, Identification cards - Contactless integrated circuit(s) cards - Proximity cards (PICCS) - Part 2: Radio frequency power and signal interface", 2001.

[14] "ISO/IEC 15693-2, Identification cards - Contactless integrated circuit(s) cards - Vicinity cards (VICCs) - Part 2: Air interface and initialisation", 2000.

[15] Ram Dantu, Gabriel Clothier, and Anuj Atri, "EAP methods for wireless networks", Computer Standards & Interfaces 29, pp. 289-301, 2007