RFID 보안을 위한 인증 시스템의 설계 및 구현

이지용* · 주홍일** · 한종욱 · 류대현*

*한세대학교, **ETRI

Design and Implementation of Authentication System for RFID Security

J. Y. Lee* · H. I. Joo** · J. W. Han** · D. H. Ryu*

*Hansei University, **ETRI

E-mail : sharp026@daum.net

요 약

본 논문에서는 먼저 RFID 시스템에서 발생될 수 있는 보안과 프라이버시 문제와 관련된 각종 위협을 살펴보고, 이를 해결하기위해 진행되고 있는 연구 주제들에 대해 간단히 기술하였다. 또한 패시브로 동작하는 저전력 8비트 마이크로프로세스를 적용한 태그와 리더 그리고 PC로 구성된 시스템에서 태그의 인증을 위한 인증 시스템을 설계하고 구현하였다.

ABSTRACT

In this paper we review the security and privacy problems in the RFID system and briefly describe the research topics to solve these problem. And, we design and implement the tag authentication system to authenticate tags in the RFID system which is composed of PC, reader and passive type tag with low power 8 bit microprocessor.

키워드

RFID, Security, Privacy, Authentication, Tag

Ⅰ. 서 론

최근 주목을 받고 있는 유비쿼터스 환경은 기술, 비즈니스, 산업의 접목과 융합에 의한 새로운 (공간) 가치와 재화의 창출을 그 특성으로 할 것이다. 즉, 유비쿼터스 컴퓨팅을 기반으로 일상생활의 사물들, 어플라이언스, 상품들, 기업의 생산, 물류, 판매 · 고객관리 등의 비즈니스 프로세스를 구성하는 기기나 시스템들이 모두 지능화되고 네트워크로 연결됨으로써 매우 다양한 새로운 비즈니스를 출현시킬 것이다. 이러한 유비쿼터스 환경을 구현할 수 있는 기술로서 RFID(Radio Frequency Identification) 시스템이 주목을 받고 있다.

RFID 시스템은 RF를 이용하여 전기적 연결 없이 상품에 대한 정보를 읽거나 기록하는 자동인식기술의 일종이다. 유사한 기술인 바코드에 비해서 저장능력이 크고 빠른 속도로 대량으로 손쉽게 상품정보를 읽을 수 있으므로 물류 등에서 바코드를 대체할 시스템으로 부각되고 있다. 최근 교통요금 지불시스템, 가축관리, 산업 자동차, 의료분야 등에서도 일부 활용되고 있다.

그러나 RFID 시스템은 사용자 정보에 대한 추적과 접근이 용이하여 사업자의 오남용 또는 RFID 태그의 오작동으로 인한 프라이버시 침해의 위협이 상존하고 있어 많은 사람들로부터 개인정보 침해의 위험성이 증가할 것이라는 우려를 낳고 있다.

본 논문에서는 먼저 RFID 시스템에서 발생될 수 있는 보안과 프라이버시 문제와 관련된 각종 위협을 살펴보고, 이를 해결하기위해 진행되고 있는 연구 주제들에 대해 간단히 기술하였다. 또한 패시브로 동작하는 저전력 마이크로프로세스를 적용한 태그와 리더 그리고 PC로 구성된 시스템에서 태그의 인증을 위한 인증 시스템을 설계하고 구현하였다.

논문의 구성은 다음과 같다. 2장에서는 RFID 시스템에서 발생될 수 있는 보안과 프라이버시 문제와 관련된 각종 위협을 살펴보고, 이를 해결하기위해 진행되고 있는 연구 주제들에 대해 간단히 기술한다. 3장에서는 태그와 리더기, 인증프로그램에 대한 설계내용을 설명한다. 4장에서는 시험결과를 기술하고, 5장에서는 결론 및 향후 연

구 내용을 정리한다.

II. RFID 보안

1. RFID 보안과 프라이버시에 대한 위협요소

프라이버시는 유비쿼터스 RFID 시스템의 주요한 이슈이다. 대부분의 소비자는 이웃에게 RFID 태그가 부착된 속옷의 상표나 처방 약을 노출시키기를 원치 않는다. 그러나 안전하지 않은 태그가 부착된 제품은 인근의 수상한 리더의 질의에 의해 민감한 정보를 노출 시킬 수 있다. 소매상들도 허가되지 않은 리더에 의해 위협을 받을 수 있다. 예를 들어 산업 스파이는 상점 선반의 재고를 주기적으로 모니터하여 제품 판매와 관련된 데이터를 얻을 수도 있다.

또 다른 위협은 추적 또는 "위치 프라이버시"에 대한 침해이다[1]. 위치 프라이버시에 대한 관심은 최근 메이저 타이어 제조사가 그 제품에 RFID 태그를 적용하겠다고 발표하면서 증가하고 있다. 태그의 내용이 안전할지라도 태그의 응답을 예측함으로서 통해 태그와 그 소유자의 신원을 연결할 수 있다. 태그들이 각각의 유니크한 신원 정보를 노출하지 않는다 할지라도, 테그 세트는 "집합체"로 추적될 수 있다. 즉 태그를 소지한 개인은 고정된 태그 리더를 지나갈 때 추적될 수 있다. 또한 기업의 스파이는 안전하지 않은 RFID 태그로부터 실제적인 패키지의 내용 자체를 모르더라도 중요한 물류정보를 빼낼 수 있다.

서비스 거부도 또 다른 위협이다. RF 신호채널에 재밍을 하거나 다른 방법으로 태그를 무력화하는 공격도 가능하다. 이러한 공격은 특별히 RFID로 자동 계산을 하는 소매상 같은데서 발생될 수 있다. 즉 태그가 가게의 리더기로부터 "은폐"될 수 있다면 이러한 결과가 발생될 수 있다. 물론 금속선으로 만들어진 백에 물건을 넣는다던지 하는 공격을 막기 위해 보안 감시원이나 카메라 같은 전통적인 방어가 필요할 수도 있다. 도둑들이 효과적으로 태그를 속이는 것이 쉽지만은 않다. 유효한 상품을 속이기 위해 그들 자신의 태그를 만들어야 한다. 즉 실제의 상품을 그들의 유인 태그로 바꿔치기함으로서 도둑은 상품이 그대로 있는 것처럼 속일 수 있다. 또한 계산 시 싼 값으로 표시되도록 태그의 내용을 다시 쓰려는 시도를 할 수도 있다.

이러한 위험은 널리 통용될 수 있는 매우 중요한 위험이 될 수 있다. 현재 널리 사용되고 있는 바코드 시스템은 누구나 읽을 수 있고 속이거나 무력화 할 수 있으므로 같은 위험성을 갖고 있다. 그러나 RFID 시스템에서는 이러한 공격이 무선으로 그리고 대량으로 이루어질 수 있는 가능성이 있다. 어떤 방법으로 큰 비용 부담 없이 RFID의 효과적인 무선 인터페이스에 의해 이루어지는 광범위하게 또는 자동적인 공격을 막을 것인가 하는 것이 중요한 이슈가 되고 있다.

2. 중요 연구 주제들

프라이버시와 접근제어 메카니즘을 제공하는데 있어서, 저가의 RFID에서 자원의 부족을 어떻게 해결할 것인가 하는 것이 중요한 도전이 된다. 일반적으로 RFID 태그는 스마트카드보다도 매우 적은 게이트만을 갖는다. 패시브 타입 태그의 보안 메카니즘은 태그가 안정하지 않은 상태 또는 전력 부족 또는 인터럽션 상태로 가지 않도록 신중하게 설계되어야 한다. 뿐만 아니라 보안 프로토콜은 순방향 또는 역방향 채널간의 비대칭적인 신호세기를 고려하여야한다. 예를 들어 태그 리더에 의해 수행되는 충돌방지 알고리즘은 다수의 태그를 어드레싱하여 신호의 크기가 큰 순방향 채널에서 데이터를 유출할 수 있어 위협이 된다[2].

저가의 태그 보안 메카니즘은 보통 일반적인 공격에 대해 강하지 않다. 공격은 쉽게 삼품을 검출하기 위해 태그의 적은 동작 영역(보통 2m)내에서 시작할 필요가 있다. 소매품에 사용되는 저가의 태그는 약 10분 동안 프로토콜 공격(예를 들면 물리적 또는 전자기적 특성에 의존하지 않는)에 강할 필요성이 요구된다. 태그가 초당 1000개의 명령어를 지원한다고 가정한다면 약 600,000개의 부루트포스 시도가 가능하다는 것을 의미한다. 이러한 제약 조건에서 해쉬함수에 기반하는 간단한 접근제어 "lock" 메카니즘이 제안되었다[2, 3].

저가의 태그가 갖는 제약조건 내에서 하드웨어적으로 효율적인 해쉬 함수를 제공하는 것이 중요한 연구 주제이다. 뿐만 아니라 저가의 대칭키 암호 방식도 매우 중요한 요소이다. DES나 AES에 비해 구현에 있어서 작은 크기의 "Tiny Encryption Algorithm"에 대한 연구가 진행되고 있다[4, 5].

위치정보에 대한 보안과 관련해서 태그는 질의에 대해 예측 가능한 방식으로 응답할 수 없다. 이 때문에 태그 응답을 무작위로 하기 위해 해쉬록 설계에서와 같이 온 보드 난수 발생기가 필요할 수도 있다[2]. RFID의 설계와 많은 응용분야에서는 실제적인 저가의 슈도 난수 발생기 또는 물리적인 무작위성 발생장치에 대한 연구가 필요하다. 하드웨어적으로 효율적인 완벽한 해쉬 함수가 태그의 추적을 피할 수 있는 또 다른 유용한 요소가 된다[5].

프라이버시와 접근제어를 제공하는 기본 메카니즘과 무관하게 태그 키의 관리도 중요한 이슈이다. 키의 초기화, 저장 과 전달이 경제적으로 이루어 질 필요가 있다. 태그가 제조사, 중간 상인 또는 소비자를 거치면서 태그의 소유권을 전달하는 효율적인 수단이 존재해야한다. 어떤 환경에서는, 태그의 물리적 소유가 태그의 광학적 정보나 접촉 채널을 통해 태그의 소유권을 의미한다. 임대와 같은 시나리오에서는 외부의 키 데이터가 태그의 소유권을 의미한다.

태그, 리더 그리고 백엔드 데이터베이스의 설계를 위해서 적절한 비용의 유연한 접근제어나

키 관리 툴에 대한 연구가 필요하다. 설계의 유연성과 개방성이 성공적인 RFID 시스템을 위해서 가장 중요한 요소이다. 향후 저가이면서도 많은 저장 공간을 가지며 속도가 빠르고 새로운 기능을 갖는 태그의 개발이 이루어 질 것이다.

RFID 시스템에 대한 현재의 보안 메카니즘이 미래의 기술을 사용하는 것을 지연시키지 말아야 하며 사용자의 경험에 좋지 않은 영향을 미쳐서도 안 된다. 소매상인은 RFID 시스템이 소비자들의 결재 과정을 방해한다면 사용하지 않을 것이다. 또한 고객들은 우유를 하나 살 때마다 복잡한 보안 과정을 수행하려하지는 않을 것이다.

한편 RFID 태그는 현존하는 응용과 아직 구현되지 않은 응용을 지원하기 위해 가능한 오픈 플랫폼이어야 한다. 보안관련 특징들이 서드파티에 새로운 응용 시스템을 개발하는데 방해가 되어서는 안 된다. 많은 유용한 응용이 풀뿌리 개발자들에 의해 등장할 수 있는데 독점적이거나 제한된 보안 메카니즘으로 인해 제대로 기능을 하지 못해서는 안 된다.

III. RFID 인증 시스템의 설계 및 구현

태그와 리더 및 PC에서 태그를 인증하는 인증 프로토콜을 설계하고 구현하였다. PC의 인증프로그램은 리더를 통하여 태그와 리더의 통신과정을 제어한다. 태그는 저전력 8bit 마이크로프로세서인 PIC 16F636을 사용하여 구성하였다. 인증 프로토콜은 챌린지-리스펀스 방식을 적용하였으며 해쉬함수 대신 계산량이 적은 RC4 알고리즘을 일부 변형하여 적용하였다.

1) 인증절차

인증 프로그램은 리더를 제어하여 태그의 정보를 가져와 사용자를 인증하는 역할을 한다. 다음 [그림1]는 인증 프로그램과 리더 및 태그간의 동작을 도식화한 것이다.

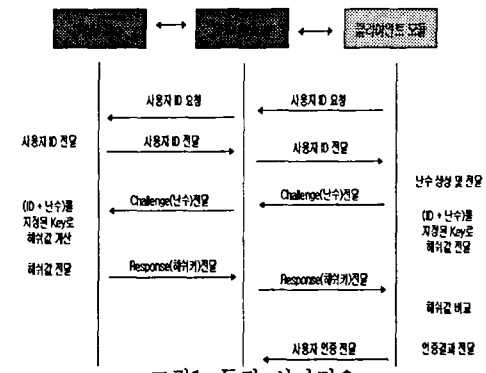

그림1. 동작 시나리오

인증 프로그램은 VC++를 사용하여 제작하였으며, 리더간의 통신에서는 RS232 표준을 사용한다.

2) 태그부

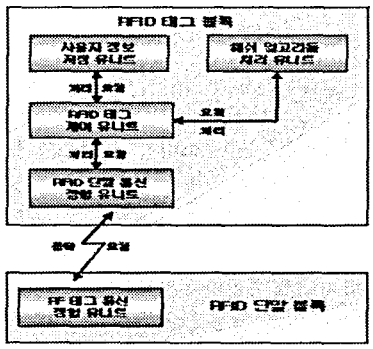

그림2. 태그부 블록도

태그는 사용자 정보를 저장하거나 리더의 요청에의해 사용자의 정보를 리더에게 전달해주는 역할을 하며 정보의 보호를 위해 변형된 RC4 알고리즘을 사용한다. 다음 [그림2] 은 태그에 대한 구현내용을 블록도로 표시한 것이다.

사용자 정보유니트는 사용자의 아이디정보와 패스워드 정보를 가지고 있으며, RFID 태그 제어 유티트의 요청시 사용자의 ID 또는 패스워드를 전달한다. 해쉬 알고리듬 처리 유니트는 RFID 태그 제어 유니트의 요청시 변형된 RC4 알고리즘으로 패스워드를 처리하여 결과를 전달한다. RFID 단말 통신 정합 유니트는 태그와 리더간의 송수신 역할을 한다.

3) 리더부

리더는 태그에 대한 별도의 인증과정을 하지 않으며 단순히 PC의 인증프로그램에 대한 명령을 수행하여, 태그와의 통신 역할을 한다. 다음 [그림3]은 리더의 구현내용을 블록도로 표시한 것이다.

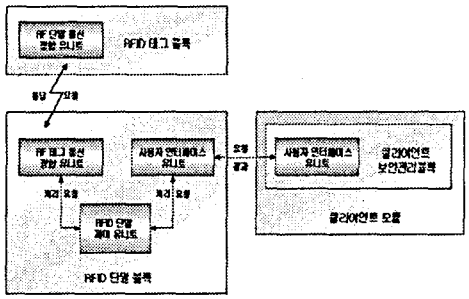

그림3. 리더부 블록도

RFID 단말 제어 유니트는 사용자 인터페이스 유니트를 상호 연결하여 데이터 전송을 제어하는 기능을 수행한다. RFID 태그 통신 정합유니트는 태그와의 송수신 기능을 수행하며, 사용자 인터페이스 유니트는 어플리케이션의 명령이나 데이터를 RFID 제어유니트에 전송하는 역할을 한다.

IV. 실험 및 고찰

[그림 5]에 리더와 태그를 나타내었다.

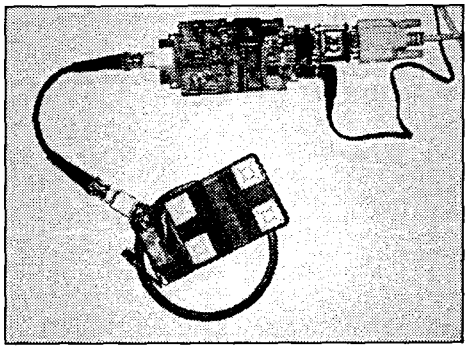

그림5. 태그와 리더

태그에는 사용자의 정보(아이디, 패스워드)가 저장되어있고, 리더와 태그 간에는 무선통신을 한다. PC에서 구현된 인증프로그램은 [그림1]와 같은 동작과정을 따르며 [그림6]은 태그의 인증 결과를 보여주는 것으로, 인증 프로그램 결과 화면을 캡쳐한 것이다.

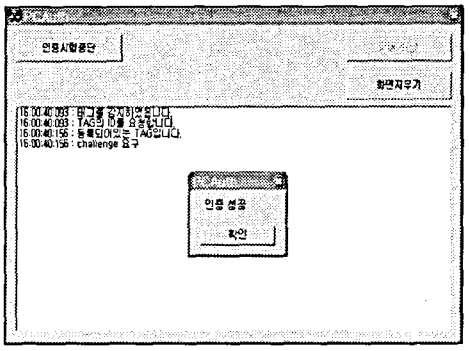

그림6. 인증 프로그램 실행결과 화면

V. 결 론

RFID 시스템의 성공은 보안과 프라이버시를 제공하기 위한 적절한 툴을 개발하는데 달려있다. 하드웨어적으로 효율적인 해쉬함수, 대칭키 암호 그리고 난수 발생기가 대규모의 공격을 무력화하는 RFID 보안 메카니즘을 개발하는데 결정적인 연할을 한다. 성능과 비용을 유지하면서 도청, 오류 유도 또는 전력 분석에 강한 새로운 프로토콜의 개발이 중요한 연구 분야이다. RFID 시스템을 키 관리 인프라와 결합하는 것도 향후 개발이 필요한 또 다른 이슈이다.

여러 가지 방법으로 범용 저가의 RFID 시스템 시스템이 유비쿼터스 컴퓨팅의 중요한 요소가 된다. 기술의 발달과 여러 가지 특성의 결합은 RFID 태그와 스마트카드 그리고 범용 컴퓨터간의 차이를 모호하게 한다. RFID 시스템으로부터 얻을 수 있는 보안관련 교훈은 미래의 안전한 유비쿼터스 컴퓨팅을 개발하는데 매우 유용할 것이다.

본 논문에서는 먼저 RFID 시스템에서 발생될 수 있는 보안과 프라이버시 문제와 관련된 각종 위협을 살펴보고, 이를 해결하기위해 진행되고 있는 연구 주제들에 대해 간단히 기술하였다. RFID 보안을 위한 인증 시스템을 설계하고 구현하였다. 개발된 시스템은 RFID Tag와 리더 그리고 응용 프로그램으로 구성된다. RF 사용 주파수는 13.56MHz 이며 Tag는 저전력 마이크로프로세서 PIC 16F636 를 사용하여 구성하였으며 패시브로 동작한다.

논문에서 사용된 시스템은 13.56MHz 주파수 대역을 사용하였지만, 향후 900MHz을 사용하기 위하여 연구, 개발 중이다. 또한 다중태그에 대한 인식문제 해결과 인증 프로시저의 보안 성능을 향상시키기 위한 방법에 대한 연구가 진행 중이다.

참고문헌

[1] RFID Journal. Michelin Embeds RFID Tags in Tires. http://www.rfidjournal.com, January 2003.

[2] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, 2003.

[3] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. RFID Systems and Security and Privacy Implications. In CHES, pages 454 - 470. LNCS, 2002.

[3] David J. Wheeler and Robert M. Needham. TEA, a Tiny Encryption Algorithm. Technical report, Computer Laboratory, University of Cambridge, 1995.

[4] David J. Wheeler and Robert M. Needham. TEA Extensions. Technical report, Computer Laboratory, University of Cambridge, 1997.)

[5] Ran Canetti, Daniele Micciancio, and Omer Reingold. Perfectly One-Way Probabilistic Hash Functions. In ACM Symposium on Theory of Computing, pages 131 - 140, 1998.