RFID 시스템에서 OTP를 활용한 개인프라이버시 보호

이주형*, 장태무**
동국대학교 컴퓨터공학과
e-mail : {jhpower7, jtm}@dgu.edu

Personal privacy protection using OTP in RFID System

Joo-Hyoung Lee*, Tae-Mu Chang**
Dept of Computer Engineering, Dongguk University

요 약

최근 물류, 교통, 환경 등 우리가 살아가는 생활 중 다양하게 많이 사용되어지는 RFID 시스템은 우리에게 많은 편의를 제공하고 있다. 이러한 시스템은 무선네트워크를 이용하기 때문에 이것이 가지고 있는 보안적 취약점이 크게 문제가 되고 있다. 개인정보를 도용하여 악의적인 목적으로 사용하고 사생활까지 침해하여 사회에서 큰 불신을 갖게 되는 이러한 취약점을 안전하게 이용할 수 있도록 여러 가지 보안방식들을 사용한다. 본 연구에서는 이러한 보안방식 중 OTP(One Time Password)라는 보안방식을 RFID 시스템에 응용하여 이러한 시스템에서 지금까지 사용되고 있는 여러 보안방식들 보다도 더욱 안전하게 개인 프라이버시를 보호하고자 한다.

1. 서 론

최근 건축, 의료, 교통 분야 등 실생활에서 널리 사용되고 있는 전자태그인 RFID(Radio Frequency Identification)는 물품에 부착하여 사물의 정보와 주변 환경정보를 확인한다. 이를 사용하여 주변 상황을 감지하는 시스템들이 앞으로의 IT시장을 선도할 핵심기술로 자리 잡을 것이다.

RFID 환경에서 안전하지 않은 태그를 사용하는 경우 물리적 공격, 위조, 스푸핑, 도청, 트래픽 분석, DoS 공격 등에 의한 보안적 취약점에 노출되어진다. 이러한 취약점은 개인 및 조직의 보안이나 프라이버시에 매우 중요한 영향력을 갖는다.[1]

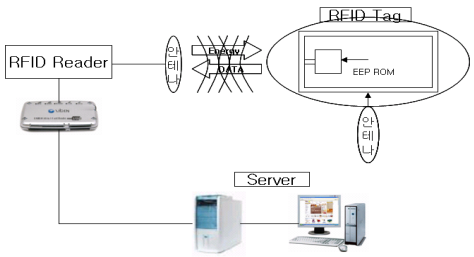
이러한 시스템은 무선 네트워크를 이용하기 때문에 유선 네트워크를 이용했을 때보다 보안적으로 취약하다. 따라서 적절한 암호·인증의 적용이 필수적이라 할 수 있다.

본 연구에서는 RFID 시스템에서 OTP를 활용하여 보다 안전한 개인 프라이버시 보호를 위한 인증방식을 제시하고자 한다. 2장에서는 RFID 시스템, OTP에 대한 관련연구, 그리고 기존의 RFID 시스템 보안방식을 알아보고 3장에서는 본 연구에서 제시하는 RFID 시스템에서 OTP를 활용하여 기존의 방식보다 안전한 개인프라이버시 보안방식을 소개하고 평가하며, 4장에서 결론을 맺고자 한다.

2. 관련연구

2.1 RFID 시스템

RFID 시스템은 말 그대로 무선 자기장 등을 이용하여 물리적인 무선 주파수로 전송하고 처리하는 인식 시스템이다. 이러한 RFID 시스템의 구성요소는 <그림 1>과 같다.



<그림 1> RFID 시스템의 구성요소

2.1.1 RF 태그

태그는 송·수신기의 합성어인 트랜스폰더라 불리어지고, IC칩(메모리 등)과 안테나회로로 구성된다. 이러한 RF 태그에 대한 각각의 분류는 아래의 <표 1>로 정리해 볼 수 있다.[2]

태그의 종류	내 용
능동형 태그	· 자체전력을 이용 · 읽기/쓰기 형으로 데이터 전송시간 제한적 · 건축분야, 의료분야 등에 사용
수동형 태그	· 리더에서 수신한 전자기파에 의해 전력 공급 · 읽기 전용 형으로 동작 수명이 길며 데이터 전송시간이 비제한적 · 물류관리, 교통 분야 등에 사용
칩태그	· 기존의 RFID는 하나이상의 마이크로칩과 트랜지스터 회로로 구성
무칩태그	· 아주 작은 센서들을 도로, 건물, 의류 그리고 인체 등에 먼지처럼 뿌려서 주변 환경(온도, 습도, 압력, 가속도 등)의 정보를 무선망으로 감지하고 관리

<표 1> 각종 태그의 분류

지난 1월 한국전자통신연구원(ETRI)에서는 세계최초로 스티로폼이나 합성수지 등을 사용하여 가격을 예전보다 훨씬 낮출 수 있는 태그를 개발하여 향후 RFID에 대해 큰 기대를 가져오게 되었다.

2.1.2 RF 리더

태그에서 전송된 정보를 식별하는 장치로서 리더기는 마이크로 컨트롤러, 발전기, 전력 증폭기, 피크 검출기, 그리고 필터링, 증폭기, 세이핑 등으로 구성된다.

2.1.3 호스트컴퓨터

태그의 정보를 저장하고 리더의 요청이 있을 때 태그의 데이터를 리더로 전송해주는 역할을 한다. 이때 SSL(Secure Sockets Layer)과 같은 보안적으로 안전한 통신채널을 사용한다.

2.2 RFID 통신방식

리더와 태그(active)에 있는 안테나 코일 사이에 발생된 자기장은 태그에 있는 메모리에 저장된 데이터를 안테나를 통하여 리더에게 전송한다. 그 후 리더는 태그로부터 받은 데이터를 수신한 후 데이터가 처리되면 리더 내에 있는 마이크로 컨트롤러에서 수신된 신호가 타당한가를 검사하고 타당하다고 판단된 신호는 데이터 신호로 변환하여 호스트컴퓨터에 전송하고 호스트컴퓨터는 미리 저장된 데이터베이스와 비교하여 필요한 서비스를 제공한다.

2.3 일회용 패스워드

일회용 패스워드란 패스워드의 이중 보안을 위해 매번 시스템에 접근할 때마다 새로운 패스워드를 부여하고 다음번 접속 시에는 또 다른 패스워드를 부여하여 보안성이 높고 사용하기 편리한 보안방식 중 하나이다. 이러한 OTP 방식은 MD4, MD5 해싱 알고리즘을 이용하여 만들어 낼 수 있다. 일부 게임업체에서는 최근 개인의 정보유출 방지를 위해 매 접속 시마다 ID와 패스워드를 입력한 후 모바일 장치를 이용하여 인증번호를 부여받고 다시 부여된 인증번호를 입력하여 게임에 접속하는데 이러한 방식은 OTP 방식의 좋은 예라 할 수 있다.

2.4 기존의 RFID 보안 방식

기존의 RFID 시스템의 개인정보 보호 기술로써 아래의 <표 2>와 같이 나타낼 수 있다.[3][4][5][6][7]

정보보호 기법	내 용
Kill Tag	· 태그에 kill 명령어를 전송. 태그가 영구적으로 비활성화 되는 방식 · 재활용할 수 없음
Faraday Cage	· 내부에 있는 태그를 허가되지 않는 리더에서 읽는 것을 막아주는 방식 · 사용범위가 제한적
Active Jamming	· 방해할 수 있는 전파를 보내어 불법적 태그의 허용을 방지 · 가까이에 있는 태그까지 접근을 막을 수 있는 단점
Hash Lock	· 저장된 ID를 보호하기 위하여 해쉬함수 H로 metaID=H(ID)를 만들어 전송 · ID는 보호할 수 있으나 위치 추적 문제는 해결하지 못함

<표 2> RFID시스템의 정보보호 기법

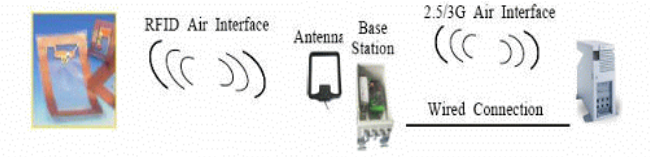
본 연구에서는 OTP를 이용한 정보보호 기법으로 <표 2>의 MIT에서 제안하는 방법 중 하나인 Hash Lock 기법을 개선하였다.

이러한 기법들 외에 Re-Encryption기술, Blocker Tag 기술, 순방향 안전성이 보장되는 기술 등이 있다.

3. 제안구조

MIT에서는 임의의 난수 값을 이용함으로써 임의의 객체에게 태그의 출력을 랜덤하고 의미 없는 정보를 사용하여 사용자의 추적문제를 해결해 줄 수 있는 방식을 제안하였다.[5] 그러나 이러한 방식은 한번이라도 아이디가 노출되면 개인의 정보가 유출되며 그것을 다시 막기란 어려울 수뿐이 없다. 이러한 단점을 보완하여 본 연구에서 사용되고 있는 효과적인 방식은 RFID 시스템에서 OTP를 활용하여 태그 안에 있는 개인의 정보에 접근하는 것을 불가능하게 해준다. 여기에서는 OTP에서 사용하고 있는 암호학적 알고리즘을 통하여 사용자의 패스워드를 매번 바꿔준다. 그러면 처음의 패스워드 값이 노출되었다 하더라도 해시 알고리즘을 통하여 계속 패스워드 값은 변하기 때문에 개인의 정보 유출을 차단할 수 있다. 따라서 본 연구는 RFID 시스템에서 OTP라는 방식을 사용하여 개인의 프라이버시를 보호하고자 하는데 목적을 가지고 있다.

본 연구에서 제시하는 방식은 아래의 <표 3>과 같다.



태그		리더	호스트컴퓨터	
	⇐ ①			
	② ⇒		② ⇒ ⇐ ②	
③		③		
	⇐ ④		④ ⇒	
⑤				
⑥				
	⑦ ⇒			
			⑧ ⇒	
	⇐ ⑨		⇐ ⑨	⑨
⑩	⑩ ⇒			
			⑪ ⇒	
	⇐ ⑫		⇐ ⑫	⑫
⑬				

<표 3> OTP를 활용한 RFID 시스템 전송 방식

능동형태그는 수동형태그보다 비싼 단점이 있지만, RFID 기술이 발전하여 태그의 값은 점점 내려가고 있다. 따라서 암호화알고리즘을 적용해야하므로 계산용량을 가질 수 있는 메모리를 필요로 하기 때문에 능동형 태그를 사용하고 초기의 패스워드(P1)는 태그와 호스트컴퓨터 모두 동일하다는 가정을 둔다.

① 먼저 리더에서 태그에게 데이터를 전송받기 위해 쿼리를 보낸다.

② 태그는 자신의 고유아이디를 리더에게 전송하고 리더는 호스트컴퓨터에 태그의 정보를 보내어 보관되어 있는 데이터를 통해 허가된 태그인지 판단하여 리더에 정보를 보내준다. 만약 허가되지 않은 태그라면 접속을 차단하여 접근을 통제한다.

③ 허가된 태그라고 판단되었을 시 리더는 임의의 난수 RND1을, 태그는 임의의 난수 RND2를 생성한다.

④ 리더에서 새로 생성된 난수 RND1을 태그와 호스트컴퓨터에 전송한다.

⑤ 태그는 자신이 가지고 있는 초기의 패스워드 P1과 리더로부터 받은 난수 RND1을 암호화 알고리즘에 적용하여 새로운 OTP P2라는 패스워드를 생성한다.

⑥ 태그는 또한 새로 생성된 난수 RND2와 초기의 패스워드 P1을 암호화알고리즘에 적용하여 OTP P3라는 패스워드를 생성한다.

⑦ 태그는 새로 생성된 패스워드 OTP P2, OTP P3를 리더에 전송한다.

⑧ 리더는 OTP P2와 OTP P3를 태그로부터 받아 호스트컴퓨터로 전송한다.

⑨ 호스트컴퓨터는 처음의 패스워드인 P1과 태그에서 받은 OTP P2를 복호화 알고리즘을 적용하여 복호화 된 난수 RND3를 생성한다. 그리고 리더기로부터 받은 난수 RND1과 새로 생성된 RND3가 일치하는지 비교한다. 두 값이 일치한다면 OTP P3를 복호화 하여 RND4를 생성한다. RND4와 success메시지를 함께 리더를 통해 태그에 전송한다.

⑩ 태그는 호스트컴퓨터로부터 받은 RND4와 자신이 생성한 RND2가 일치하는지 비교하고 일치하면 자신이 가지고 있는 정보를 리더에게 전송한다. 동시에 RND2와 P1을 해싱 알고리즘에 적용하여 H1을 생성한다.

⑪ 리더는 태그로부터 받은 정보를 호스트컴퓨터에 전송한다.

⑫ 호스트컴퓨터는 RND4와 P1을 해싱 알고리즘에 적용하여 H2를 생성하고 H2의 일부분(N)을 다음에 사용할 패스워드로 등록하고, N을 리더를 통하여 태

그에 전송한다.

⑬ 태그는 호스트컴퓨터로부터 받은 N을 H1에 적용하여 그 일부분(P2)을 다음에 사용할 패스워드로 등록한다.

⑩, ⑫에서 적용하는 해싱 알고리즘은 빠른 속도로 암・복호화가 가능하며 해시 함수는 원래의 값이나 키를 색인하는데 사용되고 항상 한 쪽 방향으로만 연산된다. 따라서 이러한 해시함수를 이용하여 새로운 해시 값 (⑩ H1, ⑫ H2)을 생성하는 것이다. ⑬에서는 그 해시 값을 적용하여 16bit 또는 32bit중의 일부분을 랜덤하게 선택하여 다음번 접속 시 사용될 패스워드(P2)를 만들어 태그에 저장된다.

이러한 방식으로 다음번 태그와 리더사이에 접속을 원할 땐 새로 만들어진 패스워드(P2)를 가지고 ①부터 ⑬까지 반복적으로 수행하여 한번 사용한 패스워드는 버리고 새로 생성된 패스워드를 가지고 다음 접속할 때 사용한다. 이러한 과정이 반복될 때 사용자의 아이디 또는 패스워드가 노출되어진다 하더라도 암호화알고리즘을 통하여 새로운 난수 값 그리고 새로운 패스워드 등이 생성된다. 따라서 사용자 ID를 매번 변화시켜 사용자의 위치를 추적해낼 수 없던 Hash Lock기술 방법은 한번 패스워드를 도용당할 시 더 이상 개인의 프라이버시 보호는 불가능하며 본 연구에서 제시하고자 하는 OTP를 이용한 방식은 기존의 방식을 보다 한 단계 발전시켜 패스워드를 계속 변화해줌으로써 개인의 ID를 도청했다 하더라도 패스워드는 매번 접속 시 변화가 되기 때문에 개인의 ID 또한 추적이 불가능하다. 이러한 방법으로 개인의 프라이버시는 항상 보호된다.

4. 결론

무선 네트워크에서는 QoS, 주파수 간섭 등 여러 가지 해결해야 할 과제가 있다. 이 중 주파수 간섭에 의한 개인의 정보는 크게 노출되어진다. 개인 정보를 도용하고 사생활 침해까지 하는 이러한 취약점은 사회에서 큰 이슈를 담고 있다. RFID 시스템 역시 무선 네트워크를 사용하고 있는데 이러한 문제점을 해결하기 위하여 본 연구에서는 RFID 시스템에서 OTP 보안방식을 적용하여 기존의 보안방식들보다 안전하게 개인의 정보를 보호할 수 있다. 리더와 태그의 안테나에서 자기장을 통하여 개인의 정보가 이동될 때 외부의 허가되지 않은 접근이 있다하더라도 모든 과정이 패스워드를 통하여 이루어지고 이 시스템에서는 패스워드가 아무도 모르게 매번 바뀌기 때문에 개인의 정보를 알아내기란 불가능하다. 그러므로 어디서든지 매번 도청을 하지 않는 한 개인의 프라이버시는 보호될 수 있다. RFID 시스템은 앞으로 많은 사용과 더불어 중요시되던 개인의 프라이버시 침해 문제를 더욱 안전하게 보호하며 미래사회에서의 큰 기대를 모을 것이다.

참고문헌

[1] “유비쿼터스 컴퓨팅 환경에서 보안 및 인증 서비스 방향 연구”, 한국 전산원, 2004. 9

[2] 장재득, 장문수, 최송인 “무선 주파수 인식 시스템 기술 분석”, 전자통신동향분석 제19권 제2호 2004년 4월

[3] 엄용진, “RFID시스템을 위한 암호 기술 동향″, http://www.dbguide.net/, 2005

[4] 최은영, 이동훈, “RFID 정보보호 기술 동향”, 정보처리학회지 제 12권 5호, 2005.

[5] 주학수, “RFID 시스템의 보안 및 프라이버시 보호를 위한 기술 분석”, http://www.eic.re.kr

[6] Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and privacy aspects of low-cost radio frequency identi cation systems. In Hutter, D., ed.: Proc. of the 1st International Conference on Security in Pervasive Computing, SPC 2003.

[7] Ari Juels, Ronald L.Rivest, Michael Szydlo, ″The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy, 10th ACM Conference on Computer and Communications Security, 2003

[8] Liu, Jingping, Zhao, Huichang, ″Active jamming simulation″, Nanjing Li Gong Daxue Xuebao/Journal of Nanjing University of Science and Technology, 24th, 2000