RFID 인증 및 제어 알고리즘 연구

최 성, 임준환
남서울대학교 컴퓨터학과
E-mail : sstar@nsu.ac.kr

Study on the Authentication and Control Algorithm in RFID System

Sung Choi, Joon hwan Lim
Dept. of Computer Science, Namseoul University

요 약

인터넷이 보편화 되면서 정부기관의 주민 관리업무나 은행의 계좌 거래도 인터넷으로 해결하고 있다. 그러나 피싱 등의 인터넷 사기 수법이 발각되고 이슈화 되면서 많은 사람들이 인터넷에 대하여 편리함을 뒤로 하고 개인정보 유출에 대해서 두려워하고 있다. 이것은 앞으로 RFID기술이 사용자들에게 익숙하게 다가가기 위해 선행되어야 할 과제이다. 실제로 보안에 관한 문제가 해외 시범사업 사례에서 드러났으며 해당 사업체도 RFID기술 도입을 정책적으로 끌고 가기 보다는 그에 앞서 서서히 시간을 두고 조심스럽게 리스크를 최소화 시키는 방법을 연구하였다.

1. RFID 개인정보 보호 문제점

1.1 기술 도입에 따른 보안 문제

보안 문제가 RFID기술이 빠르게 확산되지 못하는 이유 중 하나이다. 인터넷이 보편화 되면서 정부기관의 주민 관리업무나 은행의 계좌 거래도 인터넷으로 해결하고 있다. 그러나 피싱 등의 인터넷 사기 수법이 발각되고 이슈화 되면서 많은 사람들이 인터넷에 대하여 편리함을 뒤로 하고 개인정보 유출에 대해서 두려워하고 있다. 이것은 앞으로 RFID기술이 사용자들에게 익숙하게 다가가기 위해 선행되어야 할 과제이다. 실제로 보안에 관한 문제가 해외 시범사업 사례에서 드러났으며 해당 사업체도 RFID기술 도입을 정책적으로 끌고 가기 보다는 그에 앞서 서서히 시간을 두고 조심스럽게 리스크를 최소화 시키고 있다.

1.2 기존의 시스템과 RFID 시스템의 차이

RFID 시스템에서 활용되는 정보는 기존의 인터넷 환경의 정보와는 많은 차이를 보인다. 기존의 시스템에서는 회원관리, 재고관리 등에서 처음에 생성된 정보가 거의 변하지 않는 형태를 지니지만 RFID 시스템에서는 제조업체부터 시작된 상품의 생성부터 진열에 이르기까지의 유통정보가 누적될 뿐만아니라 그 상품을 구입한 소비자의 개인 정보와 결합되어 소비자의 구매패턴 이라던지 이동경로까지 정보로서 저장될 수 있다.

이렇게 기존의 시스템과 데이터의 성질이 정적인 차원에서 동적인 수준으로 달라졌기 때문에 보다 정보가 중요해질 뿐더러 RFID는 정보획득과정에서 무선주파수를 이용하기 때문에 데이터가 대기공간에서 전달됨으로써 정보노출위험이 더욱 급격히 높아진다.

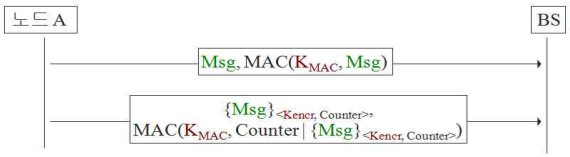
이 문제를 해결함에 있어서도 기존의 시스템은 더욱더 폐쇄적인 체계로 인증방식을 강화한다던지 암호화를 반복하는 방식으로 해결이 가능했지만 RFID 시스템은 태그와 리더 간의 정보 전달 방식에서 메모리의 한계 때문에 연산과 기억능력이 제한적임을 고려해야 하고 RFID는 효율성을 위한 새 기술이기 때문에 기존의 시스템과 비용적인 측면도 고려해야 한다.

2. RFID 보안 요구 사항

2.1 기밀성

먼저, 통신 당사자 간의 비밀정보를 공격자로부

터 보호해야 한다. 둘째로 도청(Eavesdropping), 트래픽 분석(Traffic Analysis) 등의 공격으로부터 보호해야한다. 셋째, 암호알고리즘을 사용하여 구현해야한다. 알고리즘으로는 대칭키 암호화와 공개키 암호화 등을 적용할 수 있다. 대칭키 암호화는 빠르고 효율적이나 키 분배가 문제이다. 공개키 암호화는 키 분배 문제를 해결할 수 있으나 계산량이 복잡하고 속도가 느리다. 암호화를 하여 보안을 강화할 수는 있지만 충분한 보호는 단언할 수 없다. 예를 들어 동일 메시지가 동일한 암호문으로 암호화되는 경우 재생공격(Replay Attack)이 가능하다.



(그림 1 : 인증 및 기밀성)

2.2 인증 및 부인봉쇄

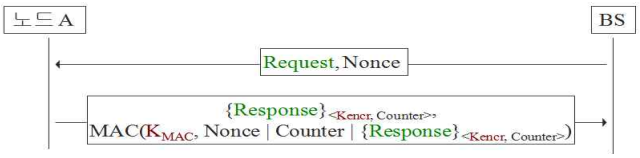
첫째, 메시지 수신자가 메시지의 소스에 대한 신뢰성(Authenticity)을 검증할 수 있게 한다. 참여자가 자신의 신원을 증명할 수 있고, 위조 혹은 위장 공격에 대한 보호를 해야 한다. 둘째, 참여자들(Peer)의 사전 공유 정보(Shared secret)가 있다면 대칭키 기반 기술로도 충분히 하다. 셋째, 사전 공유 정보가 없는 경우에는 대칭키 기반 기술이 아닌 계산량이 복잡하고 속도가 비교적 느린 전자서명 기술을 이용할 수 있다.

2.3 무결성

첫째, 메시지가 불안전한 통신채널로 손상되지 않았다는 것을 보장해 주어야한다. 둘째, 메시지가 전송 중에 공격자로 인해 의도적으로 훼손되지 않았다는 것을 보장되어야 한다. 셋째, MD5, SHA 등 해쉬 함수를 통해 구현해야 한다.

2.4 적시성(Freshness)

첫째, 메시지가 현재 세션에 해당되는 내용인 것을 보장해야한다. 둘째, 메시지에 순서가 부여됨으로써 이전 전송된 메시지의 복사본이 아니라는 것을 보장해야한다. 약한 적시성(Weak Freshness)은 메시지의 일부 순서(Partial Ordering)를 제공한다. 메시지를 수신자가 올바르게 검증하면 검증된 메시지는 이전에 올바르게 검증된 메시지 이후에 전송되었다는 것을 보장한다. 예를 들어 MAC에서 사용되는 Counter 정보를 이용하여 이전 메시지가 재전송되는 것을 방지한다. 강한 적시성(Strong Freshness)은 메시지의 전체 순서(Total Ordering)을 제공한다. 노드 A에게 자신의 메시지에 대한 응답 메시지를 B가 생성하였다는 것을 보장한다. 예를 들어 Counter 정보 및 난수 값을 이용하여 양방향 통신으로 설계한다. 셋째, 타임스탬프(Timestamp),시퀀스넘버(Sequence Number), 난수를 이용하여 구현이 가능하다.



(그림 2: Strong Freshness)

3. RFID 보안의 기술적 해결방안

기존의 컴퓨터 네트워크 보안 기술이 강화되어야 함은 물론이고 RFID 시스템에 적합한 영역별 정보보호 인프라가 구축되어야 할 것이다. 본 논문에서는 태그와 리더기 사이의 통신 취약성을 보완하기 위해서 나온 아이디어와 기술들을 연구하였다.

3.1 정보차단

3.1.1 영구적 차단

상품의 물류관리를 위해 유통과정에서만 필요했던 태그가 그 상품을 소비자가 구입하는 동시에 더 이상 정보로서 가치가 없어지도록 태그의 효력을 영구적으로 무력화 시키는 과정이 필요하다. 만약 계속 태그의 정보가 남아 있다면 소비자가 그 물건을 다 쓰고 난후 무심코 버렸을 때 악의를 가진 사람이 그 태그의 정보를 이용할 수 있는 문제점이 있기 때문이다. RFID태그가 부착된 상품을 무효화 하는 기능은 킬(Kill) 기능이라고도 불리며, 소비자가 상품을 구입한 후에 판매한 지점에서 리더기를 통해 Kill 명령어를 전송함으로서 더 이상 태그가 기능을 하지 못하도록 하는 것이다. 이 방법은 안전성이 높고 소비자의 입장에서 생각하기에 직감적으로 납득하기 쉬운 방법이다. 또한 낮은 비용으로 실현 가능하다. 그러나 누구나 Kill 명령어를 쓰지 못하도록 패스워드가 필요하며 무효화 처리 과정에서도 사람의

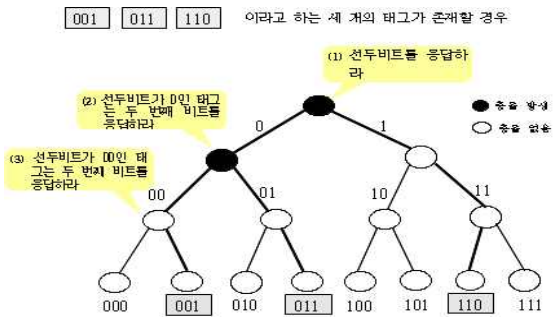
손으로 하는 행동이기에 누락되는 태그가 생겨난다는 단점이 있다. 또한 Kill 명령어가 적용된 뒤에는 재사용이 안 되기 때문에 이 방법은 넓은 응용환경을 지원하지는 못하는 단점도 가지고 있다. 이는 RFID태그 서비스가 유비쿼터스 사회에서 편리함으로서 부각되는 장점 중의 하나가 사라지는 것이다.

3.1.2 일시적 차단

정보를 영구히 차단하는 것보다 일시적으로 태그의 효력을 무력화 시키는 기술을 생각할 수 있다. 블로커 태그라고 불리는 전용 RFID태그를 소비자가 소지함으로써 가까이에 있는 태크의 ID를 읽을 수 없게 만드는 것이다. 블로커 태그는 이 세상에 존재할 수 있는 모든 태그가 그 장소에 있는 것처럼 보이게 하였다.

간단하게 ID가 3비트인 경우에 대해 생각해보자. 다음 그림과 같이 ID는 000부터 111까지 8가지가 있으며, 각각 바이너리 트리의 리프에 대응한다. 그중에서 하나의 ID가 아닌 001과 011, 110의 세 종류의 ID를 가진 태그를 리더가 인식할 경우 동작을 보자. 우선 리더는 태그에 대해 선두 비트의 값을 응답하도록 명령한다. 두 개의 태그로부터 0, 하나의 태그로부터 1이 응답되므로 리더는 그것을 충돌로 받아들인다. 이 충돌에 의해 리더는 선두 비트가 0과 1, 양방의 태그가 존재한다는 것을 인식한다.

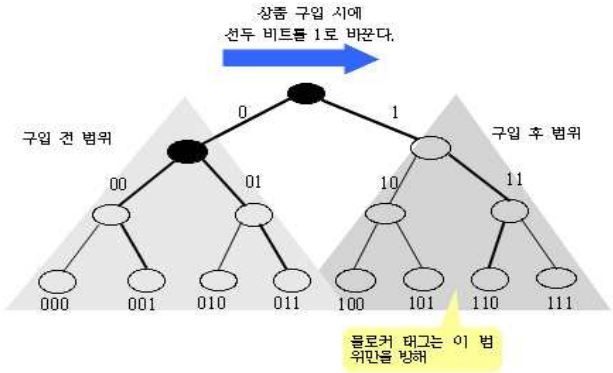
다음으로 리더는 선두 비트가 0인 태그의 한정하여 두 번째 비트의 값을 조회한다. 이 경우도 0과 1이 하나씩 응답되므로 여기서도 충돌이 발생한다. 또한 리더는 선두 비트가 0, 두 번째 비트도 0인 태그에 한정하여 세 번째 비트를 조회한다. 이 결과, 1만 응답되므로 001의 ID가 존재한다고 인식할 수 있다.



(그림 3 : 블로커 태그)

위에 과정에서 보았듯이, 블로커 태그는 바이너리 트리의 모든 노드에 있어서의 비트조회에 0과 1의 양방을 응답한다. 그 결과 모든 ID가 존재하고 있는 것처럼 보이게 해서 진짜 ID를 인식할 수 없도록 만들어 준다. 이것은 네트워크 보안에서 서비스 거부공격과 같은 것이다.

일종의 서비스 거부 공격으로 다른 리더기에 읽히지 못하도록 막았지만 반대로 블로커 태그를 악용하여 악의를 갖은 사람이 서비스 거부 공격을 할 수도 있고 악의가 없어도 블로커 태그가 점점 많아지면 리더기로 읽어야 할 시점에 인식하지 못할 수도 있다. 그에 대한 대책으로는 상품 구입 후 매장 밖으로 나갈 때 태그의 ID의 선두 비트를 바꿔서 일정 범위만 블로킹이 되도록 하는 것이다. 예를 들어 위의 그림에서 원래 상품의 ID가 010이었다면 구입후에는 110이 되도록 하여 선두 비트가 1로 시작하는 4개의 ID를 블로킹 되도록 하는 것이다. 그리 하면 매장 내에 설치한 리더는 블로커 태그가 주위에 있더라도 구입 전의 태그를 인식할 수 있다.



(그림 4 : 블로커 태그의 범위)

3.2 인증 및 접근 제어

좀 더 폐쇄적인 체계를 이루게 하는 기술들은 암호화 방법을 응용하였으며 해쉬 함수를 사용하여 가능하게 되었다.

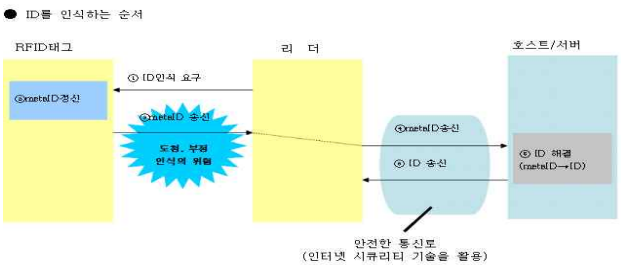
해쉬 함수란 단방향 함수라고도 불리며 역함수가 없는 함수를 의미한다. 예를 들어 3412를 100으로 나눈다고 생각하면 결과는 34이고 나머지는 12가 된다. 여기서 몫은 버려지는 알고리즘을 가정하면 나머지 12라는 숫자만 가지고는 원래 숫자를 역산할 수 없게 된다.

암호학에서는 이것을 이용하여 12라는 유용하지 않은 정보를 서로 주고받으면서 송신자와 수신자

가 원래는 같은 정보를 알고 있다는 것을 확인하는데 쓰일 수 있다. 송신자와 수신자가 주고받는 단방향 함수를 적용시켜 나온 결과 값을 해쉬라고 한다. 지금은 12라는 숫자가 나머지로 나올 수 있는 확률은 비교적 크기 때문에 송신자와 수신자가 잘못 판단할 경우가 있지만 숫자가 커지고 함수가 복잡해지면 해쉬가 일치할 확률은 거의 없어진다.

이것을 리더와 태그 구간, 리더와 호스트 구간 두 구간으로 나누어서 두 구간에서 해쉬를 주고받으면서 태그의 ID를 알아 낼 수 있다. 아래 그림에서 보면 리더가 태그에게 ID를 요청하고 태그는 자신의 원래 ID에 대한 해쉬 값인 meta ID를 계산한 뒤 리더의 요청에 대해 응답한다. meta ID를 받은 리더는 유선으로 연결된 호스트로 meta ID를 전송한다. meta ID를 받은 호스트는 이 해쉬 값이 나올 수 있는 원래의 ID를 보관하고 있다가 리더기로 적합한 ID를 전송한다.

이 기술은 태그와 리더기 사이에 정보를 전달함에 있어 비 유익한 정보를 주고 받음으로서 정보를 차단하지 않고도 도청에 대한 위험이나 ID에 관한 정보를 알아내려는 부정한 리더기의 요청에 대한 위험 부분을 없앨 수 있다.



(그림 5 : meta ID 인식)

그러나 여전히 공격자들은 meta ID가 항상 일정하다는 점을 이용해서 추적할 수 있는 단서로 쓰기도 하고 리더기를 감시하면 ID를 알아낼 수 있다는 단점이 있다. 이를 해결하기 위한 태그가 해쉬함수와 난수생성기 기술도 개발되고 있다.

4. 결 론

본 논문에서는 RFID 기술의 도입 과정에서의 문제점을 보면서, 보안에 관하여 기존시스템과 비교, 분석해 보았으며 앞으로 해결해 나갈 수 있는 기술을 연구하였다. 암호학에 관한 내용은 다소 난해하였지만 보안 기술의 기본적인 개념들을 이해하는데 도움이 되었다. 보안기술의 방향은 공격자가 추격이 불가능하도록 재암호화와 난수생성의 방법을 채택하고 있지만 태그의 특성상 칩에 들어갈 수 있는 경량화된 암호화 방법이 연구되고 있다.

RFID기술이 발전하고 표준화 될수록 보안기술도 그에 맞게 발전하고 표준화되고 있으며 네트워크 구간별로 보안 인프라가 갖춰짐으로서 빈틈이 없는 시스템이 되어 가고 있다. 또한 기술적인 문제뿐만이 아니라 사생활 보호에 대한 법률도 제정되고 있으며 정부에서 나서서 가이드라인을 제시하고 있다. 완벽한 보안 기술은 없다. 방패가 있으면 항상 창이 있다. 그러나 보안기술들을 상황에 맞게 적용하고 안전의식을 가지고 생활한다면 앞으로 펼쳐질 세상에서 다양하고 진보적인 기술들을 접하게 됨으로 보다 편리하고 다채로운 삶을 살게 된다.

참고문헌

[1] 안재명, 이종대, 오해석, “EPCglobal Network 기반의 RFID기술 및 활용”,Global, 2007

[2] 유승화, “유비쿼터스 사회의 RFID", 전자신문사, 2005

[3] 샤람 모라드푸, 매니시붑타니, “RFID실무가이드”, SUNmicrosystem, 2005

[4] 일경 BP RFID 기술편집부, “유비쿼터스 RFID", 성안당, 2005

[5] 매튜 스트리브, “네트워크 보안과 해킹 방어”, 크라운출판사, 2006

[6] 홍승필, 김영철, “정보보호의 이해”, 길벗, 2004

[7] 한명묵, 이철수, “정보보호개론”, 정익사, 2005

[8] 척 이스탐, “쉽게 설명한 컴퓨터 보안 개론”, ITC, 2006

[9] RFID 산업활성화 지원센터,www.rfidepc.or.kr

[10] 홈네트워크 시큐리티 포럼 HSNF