유비쿼터스 환경에서의 정보보호 기술

손 승 원(한국전자통신연구원 정보보호 연구단)

차 례

Ⅰ. 서 론

1988년 미국 제록스의 PARC (제록스 팰로앨토연구소 : Xerox Palo Alto Research Center)의 마크 와이저(Mark Weiser) 소장에 의해 제안된 유비쿼터스 컴퓨팅(ubiquitous computing)이란 용어는 항상 네트워크에 접속되어있고, 컴퓨터는 사용자의 눈에 보이지 않으며, 현실 세계 어디서나 컴퓨터를 사용할 수 있고, 인간화된 인터페이스 기술인 calm technology를 사용함으로서 사용자의 상황에 따라 서비스가 변하는 등의 특성을 가진다[1]. 1999년에 이르러 유비쿼터스 컴퓨팅 용어는 유비쿼터스 네트워크로 그 개념이 확장되었다. 즉, 유비쿼터스 컴퓨팅이 모든 곳에 컴퓨터 칩을 넣은 환경이라고 보면, 유비쿼터스 네트워크는 언제 어디서나 컴퓨터에 연결이 되어 있는 IT 환경을 의미한다.

이는 컴퓨터를 가지고 다니면서 멀리 떨어져 있는 각종 사물과 연결하여 그 사물을 사용한다는 개념으로 확장된 것을 의미한다. 즉, 유비쿼터스 환경은 유비쿼터스 컴퓨팅과 유비쿼터스 네트워크를 기반으로 물리 공간을 지능화하고, 물리 공간의 각종 사물이 네트워크로 연결되는 상태를 말한다. 따라서, 유비쿼터스 환경을 구성하는 객체(object)는 기본적으로 연산 능력(computing power)을 제공하는 프로세서를 가지며, 이 프로세서는 외부 환경 정보를 감지하는 센서와 유무선의 네트워킹 능력을 가진다. 여기에는 휴대폰이나 가전제품뿐만 아니라 궁극적으로는 책이나 선반, 욕조, 거울 등, 일상 생활에서 사용되고 있는 거의 모든 생활 용품과 버스 정류장, 도로 표지판 등, 모든 주변 환경이 포함될 수 있다. 이러한 객체들은 기존의 인터넷에 연결된 모니터와 키보드를 갖춘 컴퓨터와는 전혀 다른 모습을 가질 것이며, 멀지않은 장래에 수 백, 수 천대 이상의 유비쿼터스 객체들이 우리 일상생활에서 현실화 되는 날도 멀지 않았다.

최근, 유비쿼터스 환경의 초기 모델로써, RFID 기술에 대한 관심이 고조되고 있는데, 이는 RFID 기술을 SCM(Supply Chain Management)에 적용할 경우, 기존의 물류 체계를 보다 효율적으로 만들 수 있기 때문이다. 현재까지의 RFID 기술은 단순히 이러한 SCM 환경을 구현하는 수단으로 인식 되고 있지만, RFID

에 자체 연산 기능을 강화 되고 센싱 기능과 배터리를 장착할 경우, 센서 노드(sensor node)로 진화할 것으로 보인다. 이러한 센서 노드는 바로 유비쿼터스 객체를 현실화하는 필수 요소로 볼 수 있다.

한편에서는 유비쿼터스 컴퓨팅을 편재형 컴퓨팅 (pervasive computing)이라는 개념으로 보기도 한다. 이는 IBM 등이 많이 사용하는 용어로서 네트워크상에 연결된 무수한 기기를 언제 어디서나 네트워크를 통한 접속으로 e-business까지 수행할 수 있는 컴퓨터 환경을 의미한다. 따라서, 유비쿼터스 컴퓨팅과 동일한 의미로 봐도 무리가 없다. 이러한 유비쿼터스 혹은 편재형 컴퓨팅의 등장을 정보통신 환경 측면에서 보면 새로운 패러다임 전이로 받아들여야 할 것이다.

유비쿼터스 환경에서 컴퓨터들은 사람에게 착용되거나 혹은 여러 환경에 내재되어야 하며 (embedded), 시스템간에는 ad-hoc 네트워크 등과 같은 새로운 통신 기능을 갖춰야 한다. 이를 위해서는 구성 요소관점에서 여러 가지 제약 사항이 존재하는데, 대표적인 것으로는 저전력 소비 및 소형이어야 한다. 또한, 유비쿼터스 환경은 anytime, anywhere, anynetwork, anydevice, anyservice를 지향하고 있기 때문에, 본질적으로 그 안전성에서 문제를 내포하고 있다. 그러나, 인터넷 환경에의 보안성을 높이기 위해 개발된 여러 가지 보안 기술은 유비쿼터스의 자원 제약성과 특별한 네트워킹 특성에 의해 바로 적용하기 쉽지 않다. 따라서 여러 가지 편리성에도 불구하고 유비쿼터스 환경이 오히려, 보안의 취약성 및 관리의 어려움으로 그 장점을 충분히 살리지 못하게 될 가능성이 크다.

따라서 본 고에서는 유비쿼터스 환경에서의 보안 취약성을 먼저 살펴본 후, 최근 유비쿼터스 환경을 현실화하는 수단으로 인식되고 있는 RFID을 중심으로 관련 정보보호 기술을 다루기로 한다.

Ⅱ. 유비쿼터스 환경에서의 정보보호 기술

2.1 유비쿼터스 환경에서의 security challenge

유비쿼터스 환경의 고유한 특성(anytime, anywhere, anynetwork, anydevice, anyservice 특성)과 구성 요소의 자원 제약성에 의해 다음과 같은 보안을 위한 당면 문제들을 생각할 수 있다.

- 보안 설계자들은 기존의 인터넷 환경에서 사용하던 다양한 정보보호 기술(암호 기술, 보안 프로토콜 기술, 운영체제 보안 기술, 네트워크 정보보호 기술 등)을 유비쿼터스 환경의 특성 및 연산 능력 및 메모리 용량, 통신 대역폭과 같은 제한된 자원을 가지는 유비쿼터스 환경에는 적용할 수 없게 된다.
- 보안 설계자들은 이러한 유비쿼터스의 자원 제약성을 극복하기 위해 경량 암호 기술 및 정보보호 기술을 개발하여 이를 사용하고자 할 것인데, 이는 다양한 기술적 문제를 유발할 수 있다.
- 유비쿼터스 환경은 수 천대의 컴퓨터가 서로 연결된 인터넷 환경의 단순한 무선 네트워킹 버전이 아니므로 기존의 분산 시스템을 위한 전통적인 정보보호 기술을 적용할 수 없다. 특히, 인증 및 권한부여, 심지어 소유(ownership)에 관한 기본적인 개념까지 재고할 필요가 있으며, 유비쿼터스 환경에서는 보안 문제 및 프라이버시(privacy) 문제뿐만 아

니라 신뢰(trust)와 제어(control)에 관한 새로운 문제가 발생할 수 있다.

이러한 상황에서 유비쿼터스 환경에 적합한 정보보호 기술을 개발하기 위해선 기존의 인터넷 환경에서 사용하던 정보보호 기술의 특성을 살펴본 후, 유비쿼터스 환경에 적합한 정보보호 기술을 논할 필요성이 있다.

보안 위협에 대한 전통적인 분류법은 위협 대상 시스템의 특성에 의존하지만, 크게 기밀성(confidentiality), 무결성(Integrity), 가용성(availability)과 같은 세 가지 범주로 분류할 수 있다. 이 중, 기밀성은 인가되지 않은 개체가 보호하고자 하는 정보를 알게 될 때 침해 되며, 무결성은 인가되지 않은 개체가 정보를 임의로 변조할 때 침해 된다. 가용성은 예로서 누군가가 웹 사이트를 다운시키는 것처럼 시스템의 기능을 수행하는 것을 방해할 때 침해 된다고 볼 수 있다[2]. 이 경우 모두 인가된 개체와 인가되지 않은 개체는 구별이 필요한데, 두 개체를 구별하기 위해선 다음과 같은 식별과 인증, 권한 부여라는 세 단계의 처리 과정이 필요하다[3].

- 식별(identification): 사용자가 자신이 누구인지를 말함
- 인증(authentication): 시스템이 그 주장의 당위성을 검증
- 권한부여(authorization): 사용자가 특정 접근 권한을 부여 받음

인증의 실패는 쉽게 기밀성과 무결성, 가용성 침해를 유발한다. 예를 들어, 수신자의 진짜 신원이 송신자가 기대한 개체가 아니라면, 암호화를 통해 비밀을 보호하는 것이 무의미한 일이 될 것이다.

2.2 유비쿼터스 환경에서의 인증

유비쿼터스 환경에서는 기존의 인터넷 환경과는 달리 개체가 항상 네트워크상에 존재하지 않을 수 있다. 즉, 오프라인 상태에서 존재하다가 필요할 경우 온라인 상태로 될 수 있음을 의미한다. 이 경우, 기존의 Kerberos나 공개키 인증 기법과 같은 전통적인 인증 기법들은 개체의 상시 온라인 연결을 가정하기 때문에 이 기법들은 유비쿼터스와 같이 단속적으로 온라인 연결되는 상황에는 적용하기 힘들다. 단속적으로 연결되는 네트워크에서의 인증 문제를 일시적으로 안전한 합의(secure transient association)라고하며, 이를 구체화하기 위해 다음과 같은 상황을 예를 들어 생각해 볼 수 있다[4].

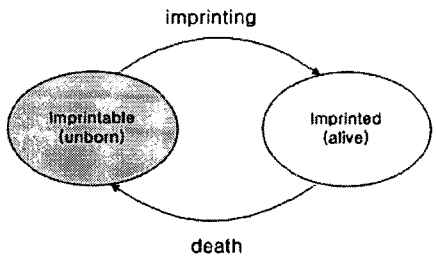
예를 들어, 유비쿼터스 환경에서는 TV와 스테레오, DVD, VCR, 커튼, 히터, 에어컨 등을 위한 각각의 리모컨을 사용하지 않고 이들 구성 시스템에 동일하게 적용할 있는 PDA와 같은 형태의 공통 리모컨을 사용하게 될 것이다. 이때 우리는 응용 기기를 제어하기 위한 리모컨을 더 이상 새로 구입하지 않기 때문에, 기기를 새로 구입한 경우 이를 사용하기 위해선 공통의 리모컨과 새로운 기기 사이의 어떤 연관성(association)을 설정할 필요가 있다. 또한 우리는 외부인이 자신의 기기를 불법적으로 조작하는 것을 원하지 않기 때문에 이러한 합의는 안전하게 이뤄지길 바라며, 공통 리모컨을 그대로 유지하면서 스테레오 장비를 팔거나, 자신의 모든 기기들에 대한 제어권을 잃지 않고 고장 난 리모컨을 교체해야 하는 상황도 있을 수 있으므로, 그 합의가 일시적이고,

취소할 수 있기를 바란다.

위와 같은 상황에서 시스템이 만족할 만한 일시적이며 안전한 합의를 수행할 수 있는 성질을 "부활하는 새끼오리 정책(Resurrecting Duckling policy)"이라는 보안 정책 모델로 볼 수 있으며, 이에 대해 자세히 살펴보기로 한다[4].

먼저, 두 개의 장치 즉, 마스터와 슬레이브 사이에 일시적으로 안전한 합의를 설정하기 위한 방법으로는 DVD 플레이어와 같은 슬레이브 장치에게 각인 키(imprinting key) 또는 정신(soul)을 옮겨 PDA와 같은 주인(master)에게 각인시키는 것이다. 이때, 각인된 새끼오리, 즉 노예 기기는 soul이 유지되는 한 그의 엄마 오리, 즉 주인에게 충실하게 된다. 만일 새끼오리가 죽으면, 정신은 사라지고, 새끼오리의 몸은 새로운 다른 엄마오리에게 각인될 수 있다. 위와 같은 4가지 원리가 Resurrecting Duckling security policy 의 기본 모델이 된다.

이 모델은 [그림 1]과 같이 새끼오리가 각인될 수 있는 상태 (imprintable state)와 각인된 상태(imprinted state)와 같은 두 가지 상태를 가진다. 각인될 수 있는 상태에서는 누구라도 새끼오리를 인수할 수 있고, 각인된 상태에서는 엄마 오리에게만 복종한다. 다음으로, 각인 동작(imprinting)이라는 것은 엄마 오리가 새끼오리에 각인 키를 전송하여 각인될 수 있는 상태에서 각인된 상태로 변환시키는 과정을 의미하는 것으로 이 과정은 기밀성과 무결성이 적절히 보호되는 채널을 통해 수행되어야 한다.



▶▶ 그림 1. State diagram for the Resurrecting Duckling[2]

다음으로 죽음(death)은 각인된 상태에서 각인될 수 있는 상태로 다시 전환하는 것을 의미하는 것으로 엄마 오리의 명령에 의해서만 수행될 수 있다. 또한 Death가 아닌 상황에서 새끼 오리가 죽게 되는 암살(assassination) 상황은 비경제적인 방법으로만 가능해야 한다.

2.3 유비쿼터스 환경에서의 기밀성

자원 제약성이 높은 유비쿼터스 환경에서는 기존의 공개키 암호를 그대로 사용하기 어렵다. 즉, 많은 유비쿼터스 컴퓨팅 기기들은 공개키 암호를 처리하기에는 매우 느린 피넛(peanut) 프로세서를 가진다. 이러한 피넛 프로세서는 낮은 컴퓨팅 능력 때문에 이를 극복하기 위해 대부분의 작업을 background나 precomputation과 같은 기법을 통해 낮은 성능을 극복해왔다. 하지만, 유비쿼터스 환경에서는 성능 측면 외에도 사용할 수 있는 에너지의 양이 제한적이므로 피넛 프로세서에서 암호 알고리즘의 수행 특성을 평가하기 위해선 성능과 에너지를 함께 고려해야 하며, 이를 위해 기존의 bits per second 개념보다는 bits per joule 개념을 사용한다[2].

유비쿼터스 환경에서는 전송되는 메시지의 기밀성 보호뿐만 아니라 기기 자체에 존재하는 비

밀 정보에 대한 기밀성을 보호하는 것도 중요하다. 유비쿼터스 환경은 사용자의 존재를 탐지하고 이미 기억된 해당 사용자의 기호 및 행동을 토대로 지능적인 응용 환경을 구축할 수 있다는 장점이 있는데, 이를 위해선 유비쿼터스를 구성하는 기기가 사용자가 비밀로 간직하고자 하는 정보를 가져야 하는 상황이 있을 수 있고, 이 때문에 저장된 정보를 보호해야 할 필요성도 있다. 현실적으로 유비쿼터스 환경에 저장된 모든 정보를 보호할 수 없다면, 최소한 주인(master) 기기에 저장된 데이터의 기밀성은 보호할 수 있어야 한다. 이 경우, 특정 유비쿼터스 시스템을 설계하는 설계자는 개인의 중요한 정보를 주인 기기에만 저장하고 이에 대한 기밀성을 보장해야 한다.

유비쿼터스 환경에서는 익명성(anonymity)과 추적성(traceability), 그리고 트래픽 분석(traffic analysis) 등도 기밀성 관점에서 보호할 필요가 있다. 또한, 사용자의 프라이버시 보호를 위해 위치 프라이버시(location privacy)를 보호해야 하며 사용자의 거래를 다른 정보와 연결하는 것도 어렵도록 해야 한다.

2.4 유비쿼터스 환경에서의 무결성 및 가용성

유비쿼터스 환경에서는 인증 및 키 분배 문제가 해결된 상황에서 무결성에 대한 보호는 MAC과 같은 기존의 암호 메커니즘을 사용해서 구현할 수 있다. 하지만, ad-hoc 네트워크 특성을 가지는 유비쿼터스 환경에서는 브로드캐스트 데이터에 대한 인증을 수행하고자 하는 경우, 각 데이터에 대한 전자 서명을 위한 비용을 절감하기 위해 chaining 프로토콜과 같은 여러 가지 기법을 생각해 볼 수 있다. 또한, 유비쿼터스 환경을 구성하는 기기에 대한 물리적인 보호 기능도 필요하다. 일반적으로 스마트카드 칩에는 물리적인 보호 기술이 구현 되지만 유비쿼터스 기기에 이 기술을 적용한다는 것은 비용 문제 등으로 현실적으로 어렵다. 이 때문에 물리적인 공격에 대한 실시간 탐지에 대한 대안으로 사후에 공격 여부를 알 수 있도록 하는 tamper evidence 기술을 구현하는 것이 필요하다.

유비쿼터스 환경에서의 가용성 측면에서 서비스 거부 공격(DoS: Denial of Service attack)은 시스템의 가용성을 떨어뜨리는 대표적인 예가 될 수 있다. 기존의 유선/무선 환경에서도 큰 위협 요소가 되는 DoS 공격은 무선 통신을 기반으로 하고 제한된 전원을 가지는 유비쿼터스 환경에서는 약간의 DoS 공격으로도 시스템의 전원이 모두 고갈되어 시스템 기능이 정지될 수 있기 때문에 더욱 심각한 문제가 될 수 있다. 이에 전원 관리를 동시에 고려한 DoS 공격 탐지 및 대응 기술을 개발해야 한다.

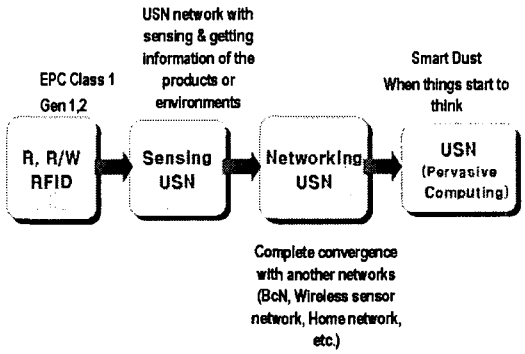
이상으로 유비쿼터스 환경에서의 주요 보안 위협 및 유비쿼터스 환경에서의 정보보호 기술을 인증과 기밀성, 무결성, 가용성 측면에서 살펴보았다. 유비쿼터스 환경이라는 것은 기존의 인터넷 망과 홈 네트워크, RFID 시스템, USN 시스템, WPAN 등을 모두 포함하는 광범위한 개념이므로 유비쿼터스 환경에서의 정보보호 기술을 논하는 것은 개념적으로 보안 위협을 확인하고 각각의 응용에 대한 정보보호 기술을 개발해야 할 것이다. 다음 절에서는 유비쿼터스 환경을 현실화하는 대표적인 예인 RFID 기술에 대한 특성과 해당 정보보호 기술을 살펴보고자 한다.

Ⅲ. RFID 정보보호 기술

최근 국내외에서 많은 관심의 대상이 되는 RFID 기술은 USN 기술과 더불어 유비쿼터스 환경을 현실화하는 기술로서 인식되고 있으며, 유통 및 물류, 자동차 등 산업체 전 분야에 다양하게 응용 될 수 있다. RFID 기술은 내부 전원의 유무에 따라 수동형 RFID와 능동형 RFID로 크게 나눌 수 있으며, 현재 시장에서 주로 많이 사용되고 있는 수동형 RFID 기술은 읽기만 가능한 EPC Class 1 Gen 1 버전이지만, 최근 읽고 쓰기가 가능한 EPC Class 1 Gen 2 태그가 시장에 나오게 됨에 따라 RFID 태그에 대한 활용도가 매우 넓어지게 되었다[5].

[그림 2]에서 보는 바와 같이 RFID 기술은 향후 자체 센싱 기능을 가지거나 물품 정보 및 주변 환경 정보를 센싱하는 "Sensing USN" 기술로 진화될 것이며, 차후에 이 기술은 기존의 BcN 네트워크나 무선 센서네트워크, 홈 네트워크 등과 같은 네트워킹 기술과 완벽히 통합되는 "Networking USN" 기술로 진화될 것으로 보인다. USN 기술의 최종 목적지는 스마트 더스트(smart dust) 수준의 센서 노드 혹은 마치 "물체가 스스로 생각하는 것처럼 착각을 불러일으키는 진정한 유비쿼터스 환경"이다.

일반적으로 RFID 시스템은 크게 RFID 태그(트랜스폰더)와 리더(트랜시버), 그리고 백엔드 데이터베이스로 구성되며, 수 미터의 거리에서도 초당 수 백개 이상의 태그를 한꺼번에 읽을 수 있다[6]. RFID 기술은 기존의 바코드 시스템을 대체할 수 있는 기술로 전술한 봐와 같이 응용 범위가 매우 넓다. 하지만, 보호되지 않은 태그가 부착된 상품은 쉽게 모니터링 되고 사용자의 위치를 추적할 수 있기 때문에 RFID 기술에 대한 프라이버시 및 정보보호 문제가 발생하게 되며, 이에 적합한 새로운 정보보호 기술 개발도 필요하게 된다.



▶▶ 그림 2. RFID/USN 기술의 진화와 유비쿼터스 환경

3.1 RFID의 특성

일반적으로 900MHz 대역의 수동형 RFID인 경우, EIRP(Effective Isotopically Radiated Power: 유효복사전력)값이 4W이고 태그와 리더 간의 인식 거리가 5m인 경우, 태그가 수신 가능한 소비 전력은 약 50uW이다. 이에 비해, 13.56MHz의 비접촉식 스마트카드인 경우에는 10MHz로 동작할 때, 소비전력이 약 30mW 정도다[9]. 이처럼 수동형 RFID 태그인 경우, 비접촉식 스마트카드와 비교해 볼 때, 수 백 배 이상의 소비 전력 차이가 있으며 이는 기존의 암호 알고리즘을 기반으로 하는 정보보호 기술을 RFID에 쉽게 적용하기 어렵다는 것을 의미한다.

만일 RFID 태그에 정보보호 관련 기능을 hardwired logic으로 구현하는 경우, 능동형 RFID 태그는 자체 전원이 있기 때문에 응용 목적에 따라 수 십만 게이트 급의 회로도 구현 가

능하지만, 수동형 RFID 태그인 경우에는 가급적 수 천 게이트급 이하로 정보보호 기능을 구현하는 것이 바람직하다[8]. 또한, RFID 태그에 구현된 프로세서를 사용하여 해당 RFID 프로토콜을 처리하는 경우도 있는데, 이 경우, 이전에서 언급한 것처럼 저전력 특성을 가지는 피넛 프로세서를 사용해야 한다. 즉, 수동형 RFID 태그에는 소비 전력이 적은 8051 계열의 8비트급 프로세서를 사용하는 것이 좋다. 예로서, Microchip사의 PIC16F627A 프로세서의 소비 전력을 보면, 2.0V의 전원에서 1MHz로 동작 할 때 약 120uA의 전류를 소비한다. 이는 비록 위에서 언급한 50uW의 소비 전력을 초과하는 것이지만 태그/리더간 인식 거리를 줄인다면 이론적으로 피넛 프로세서를 수동형 RFID 태그에 적용하는 것이 가능해질 것으로 보인다. 반면에 능동형 RFID 태그에서는 자체 배터리로 인해 소비 전력 특성에 여유가 있으므로 ARM 7 혹은 Atmega 128 정도의 프로세서도 사용할 수 있을 것으로 보인다[8].

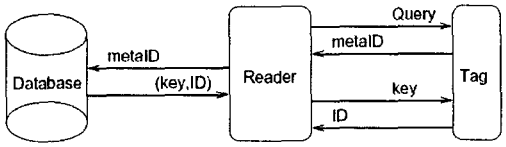
적절한 정보보호 기술을 사용하지 않은 RFID 태그는 기존의 보안 공격 기법인 eavesdropping과 traffic analysis, spoofing, DoS 공격에 취약하며 이러한 공격으로 사용자의 개인 정보와 관련있는 민감한 상품 정보 누출 될 수 있다. 또한, 위치 프라이버시 및 운송 데이터에 대한 위협이 되는 Traffic analysis attack도 가능하기 때문에, 적절한 접근 제어와 인증 과정을 통해 허용된 자만 태그 데이터를 읽을 수 있도록 해야 한다. 또한, 태그 내용이 보호되더라도 태그를 소유한 사람을 추적할 수 있고 여러 개의 리더로부터 정보를 가공하여 위치와 거래 정보를 추적할 수 있으므로 이에 대한 적절한 정보보호 기술도 함께 개발 되어야 한다[8].

3.2 RFID용 정보보호 기술

RFID용 정보보호 기술로는 태그의 리더 인증, 위치 추적 방지를 통한 프라이버시 보호 등, 다양한 기법들이 존재하는데, 다음에는 해쉬 락 기법을 중심으로 살펴보도록 한다.

가. Hash Lock 기법

RFID 태그가 리더를 인증하기 위하는 기법으로는 해쉬 함수의 one-way 특성을 사용한 Hash Lock 기법이 있다[13]. 동작 과정을 보면, locking된 태그는 리더의 쿼리에 대해 metaID로만 응답하고 이때 리더는 안전하다고 가정된 통신 채널을 통해 DB에서 metaID에 해당하는 태그 key와 ID 값을 가져 온 후, 리더는 태그에 key 값을 전송한다. 태그 내부에서 그 키 값에 대한 해쉬를 계산한 후, 자신의 meta ID 값과 같을 경우에만 태그가 가지고 있는 ID 값을 리더로 출력한다. 이는 일방향 해쉬 함수의 역함수 계산의 어려움에 기반하며 불법적인 리더가 태그 내용을 읽는 것을 방지한다. 하지만, metaID가 일종의 식별자로 사용될 수 있기 때문에 사용자 추적이 가능하다는 단점을 가진다. 이 기술은 능동형 공격(active attack)보다는 eavesdropping과 같은 수동형 공격(passive attack)에 초점을 맞춰 개발된 프로토콜이다.

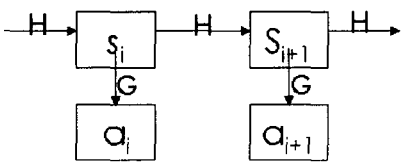


▶▶ 그림 3. RFID 환경에서 리더 인증을 위한 해쉬 락 기법

나. Hash Chain 기법

Hash Lock 기법의 변형된 형태로 쿼리에 대하여 태그가 임의 값을 발생하여 리더로 보내는 randomized hash lock 기법이 있는데, 이 방식은 태그에 PRNG(Pseudo Random Number Generator)를 가져야만 한다. 하지만, 여기서 소개하는 Hash Chain 기법은 태그에서 PRNG를 사용하지 않고도 태그 소유자의 프라이버시를 보호할 수 있다. 출력되는 값은 해쉬된 값이고 동작 시 그 출력값이 계속 바뀌므로 역추적을 방지할 수 있게 된다.

동작 방식을 보면, 리더와 태그는 초기에 ID 값과 초기 비밀값 S를 가지고 리더에는 G 해쉬 처리된 값을 출력하며 비밀값은 H 해쉬로 갱신된다. 이때 서버는 저장된 모든 태그의 S 값을 해쉬함으로서 해당 ID를 검출한다. 이는 서버에 해당 ID 값을 찾기 위해선 해쉬 함수를 반복적으로 수행해야 한다는 것을 의미한다. 또한, 태그 정보가 노출될 경우, 이전 위치는 추적할 수 없지만, 노출 이후에는 위치 추적이 가능하게 된다.

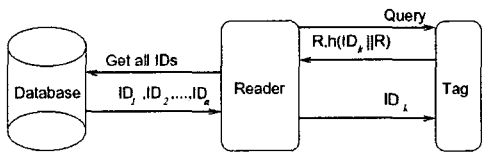


▶▶ 그림 4. 해쉬 Chain 기법

RFID의 추적을 방지하기 위해선 Hash Chain 기법처럼 태그에서 리더로 전송되는 데이터를 난수화하거나 익명성 기술의 사용, 혹은 태그가 리더를 인증함으로서 합법적인 리더만 읽을 수 있도록 제어하면 된다. 이를 구현한 기술로서 Randomized hash lock 기법과 Universal re-encryption 방법을 사용한 Variable ID 방식이 있으며 이를 다음에서 소개하도록 한다.

다. Randomized hash lock 기법

RFID 추적 방지 기술로 볼 수 있는 Randomized hash lock 기술은 리더가 태그를 읽을 때 마다 태그에서 발생한 난수값에 의해, 태그는 다른 값을 리턴하게 된다[14]. 이후, 리더는 DB로부터 모든 ID 값을 가지고 와서, 리더에서 해쉬를 수행하여 태그로부터 수신한 값과 비교하여 해당 ID 값을 찾는다. 이 기법은 리더에서 해쉬 함수를 반복적으로 수행할 필요가 있으며 ID에 대한 brute force look up의 필요성, 태그에는 해쉬 함수 외에 PRNG를 low cost, low power로 설계해야 한다는 부담이 있다. 이 기법은 한정된 응용 범위를 가지는 경우에는 사용 가능하지만 많은 태그를 필요로 하는 경우에는 부적합하다.



▶▶ 그림 5. Randomized 해쉬 Lock 법

라. Universal re-encryption 방식을 사용한 Variable ID

이 기법은 Universal re-encryption 방식과 one-time pad에 기반하는 것으로 태그값이 매 출력 때마다 달라지며, Elgamal에 기반한 universal re-encryption을 적용한 공개키 암호 시스템을 사용한다. Universal Re-encryption 기법은 공개키를 모르는 상황에서도 암호화가 가능하므로 이 때문에 key 발생 및 분배, 관리가

필요 없다. 동작 방식을 보면 각 태그는 비밀키 xt와 공개키 yt 값을 생성하고 DB에 각 태그의 (xt, IDt)를 저장한다.

리더는 각 태그의 암호문 C와 난수 값을 사용해서 one-time pad를 생성하고 초기에 one time pad 값과 암호문 값은 태그에 저장되고 그 다음부터 이 값을 갱신한다. 리더(서버)가 태그로부터 암호문을 받으면 서버는 해당 ID가 식별 될 때까지 DB에 저장된 모든 태그의 비밀키를 이용하여 복호화를 수행한다. 태그가 리더로 다시 신호를 보낼 때 one-time pad에서 2개의 값을 선택해서 암호화를 수행한다. 이 때 공개키 값을 사용하지 않는다[12].

3.3 RFID용 경량 암호 기술

가. RFID 태그 위변조 방지 기술

지금까지 RFID에 적용 가능한 정보보호 기술을 해쉬 락 기법을 중심으로 살펴봤다. 이 외의 태그 위변조 방지 기술로는 대칭키 기반 Challenge Response 방식이 있으며 비암호학적인 방식으로는 XOR나 Squaring 방식과 암호학적인 방식으로는 AES나 스트림 암호를 사용하는 방식이 있다. 또한, 비대칭키 방식으로는 Universal Re-encryption을 사용한 variable ID 방식과 External re-encryption 방식이 있다[8].

먼저 XOR를 사용하여 RFID의 태그 위변조를 방지하는 기법을 보면, 태그와 리더는 사전에 키를 공유했다고 가정하고 리더는 태그에 원하는 challenge 값과 키 값을 xor한 값을 전송하고 태그는 리더에 원하는 challenge 값과 키 값 을 xor 한 값을 전송한다. 이 때 각각의 키 값은 이미 태그와 리더가 공유하고 있기 때문에 해당하는 challenge 값을 복원할 수 있다. 하지만, 이는 프로토콜 실행 때마나, 다른 키를 사용해야 하므로 키 분배 문제가 발생한다. 이를 개선한 방식으로는 사전에 태그와 리더가 공유하는 키 값을 줄이는 여러 방법이 제안되고 있다. 하지만, 어느 경우든 strong cryptography를 사용하지 않는 한, 안전성에 문제가 있다[8].

비암호학적 방식을 사용한 RFID의 태그 위변조 방지 기술은 결국 공격 가능성이 있기 때문에 강한 정보보호를 위해선 대칭키 암호 혹은 비대칭키 암호, 해쉬 함수를 사용해야 한다. 하지만, RFID는 자원 제약성이 매우 크므로 암호 모듈에 대한 경량화 기술을 개발해야 실제 시스템에 적용할 수 있다. 다음은 몇 가지 대표적인 암호 알고리즘에 대한 소비 전력 특성을 살펴봄으로서 RFID 암호 모듈의 경량 특성을 알아보기로 한다.

나. RFID 암호 모듈의 소비 전력 특성

RFID 태그에 AES 대칭키 암호 알고리즘을 적용하면 리더가 태그를 인증하도록 만들 수 있다. 하지만, AES는 기본적으로 경량 암호 알고리즘이라 볼 수 없기 때문에 경량화를 위한 특별한 기술을 적용할 필요가 있다. 하드웨어 관점에서 적용할 수 있는 여러 가지 저전력화 기술이 있지만 AES인 경우, 암호 알고리즘 자체의 특성을 사용하여 8 비트 기반 구조를 가지도록 하거나 혹은 gated clock 기법이 적용된 레지스터를 활용한 메모리를 사용함으로서 저전력화를 이룰 수 있다. AES-128에 이와 같은 저전력화 기법이 적용된 결과를 보면, 실제 RFID 시스템에 응용 가능한 소비 전력 수준인 100KHz의 동작주파수에서 약 8.15uA의 소비전류를 가진다. 한편,

AES를 RFID 태그에 적용하는 경우에도 상호 인증을 위해 태그에서 난수값 발생이 필요하며, 저전력 AES-128은 초당 약 50개의 태그 인증 성능을 가지는데, 이는 소비 전력 특성을 좋도록 하기 위해 성능이 다소 떨어졌다는 사실을 알 수 있다[10].

스트림 암호를 포함해서 현재 LFSR(Linear Feedback Shift Register)을 기반으로 하는 암호 알고리즘이 많이 존재한다[3]. 일반적으로 LFSR은 레지스터의 출력단 상태 변화에서 많은 전력을 소비하는데, 이러한 레지스터간 데이터 shift에 의한 소비 전력은 조합 논리 회로(combinational logic)의 소비 전력보다 많다. 일반적으로 LFSR 계열은 하드웨어가 단순하기 때문에 소비 전력 특성이 좋다고 알려져 있지만, 하드웨어의 크기를 고려한 소비 전력 효율 측면에서는 그다지 효율적이지 않다. 또한, 성능도 다소 떨어진다는 단점을 가진다[8].

해쉬 락이나 해쉬 체인 등, RFID 환경에서는 해쉬를 응용한 프로토콜이 많이 개발 되어 있지만, 해쉬 함수는 그 기본 설계 사상이 하드웨어가 아닌 소프트웨어이므로 RFID 태그에 하드웨어로 구현한 결과가 효율적이라고 볼 수 없다. 이 때문에 저전력 해쉬 함수에 대한 연구가 많이 진행되고 있으며 기존에 많이 사용되고 있는 SHA-160의 소비 전력 특성을 보면 10MHz에서 약 1.32mW의 전력을 소비한다[8,15]. 타원곡선 암호 시스템(Elliptic Curve Cryptography)과 같은 공개키 암호 알고리즘의 소비 전력 특성을 살펴보면, 타원곡선 암호나 초타원곡선 암호 시스템이 대개 polynomial basis 혹은 Normal basis 기반 곱셈 회로(multiplication logic)를 그 primitive 연산자로 가지는데, 이를 저전력 구조로 알려진 Digit serial multiplier로 구현하는 경우, 저전력 digit 값에 대하여 10MHz에서 0.32mW 정도의 소비 전력을 가진다. 이는 공개키 암호 알고리즘을 저전력으로 만드는 것이 쉽지 않은 일이라는 것을 알려준다.

지금까지 RFID 정보보호 기술과 소비 전력 특성에 대해 간략히 살펴봤다. RFID 정보보호 기술은 본고에서 언급한 암호학적인 방법 외에도 Faraday cage나 kill tag, Blocker tag 등[11], 다양한 여러 가지 기법이 존재한다. 이러한 기술은 단순하지만 실제 응용에서 사용하기 위해선 여러 문제를 해결해야 한다. 예를 들어, Blocker tag 기법을 사용하는 경우 Blocker tag 기법 자체가 서비스 거부 공격의 수단으로 악용될 우려가 있다.

Ⅳ. 결 론

본고에서는 유비쿼터스 환경이 당면한 보안 위협을 알아보았으며 이에 대한 적절한 정보보호 기술을 원론적인 차원에서 언급하였다. 유비쿼터스 환경이 기존의 인터넷 망과 홈 네트워크, RFID 시스템, USN 시스템, WPAN 등을 모두 포함하고 있는 광범위한 개념이기 때문에 본고에서는 유비쿼터스 환경에 대한 정보보호 기술을 인증과 기밀성, 무결성, 가용성 차원에서 살펴보았다. RFID 환경에 적합한 정보보호 기술을 개발하는 것은 안전한 유비쿼터스 환경을 위한 필수 요소이므로 본고에서는 RFID에 적용 가능한 리더 인증 기법, 위치 추적 방지 기법 등을 다뤘으며 또한, 저전력을 관점에서의 경량 RFID 암

호 구현 기술을 다뤘다.

향후 유비쿼터스 환경은 RFID 기술을 시작으로 사물의 지능화 및 네트워크화가 진행될 것으로 예상되며, 또한, RFID 기술은 센싱 USN 기술로 발전하여 궁극적으로는 진정한 유비쿼터스 환경으로까지 진화할 것으로 예상된다.

참 고 문 헌

[1] Mark Weiser, "The Computer for the Twenty-First Century". Scientific America, 265(3):94-104, Sep. 1991.

[2] Frank Stajano, "Security for Ubiquitous Computing", John Wiley & Sons, 2002

[3] Bruce Schneier, Applied Cryptography, John Wiley & Sons, 1996

[4] Frank Stajano, "The Resurrecting Duckling - What Next?", Security Protocols Workshop 2000

[5] EPC Global, "EPC Radio-Frequency Identity Protocols Class 1 Generation 2 UHF RFID Protocol for Communications at 860MHz-960MHz, version 1.0.9", Sep. 2004

[6] Klaus Finkenzeller, RFID Handbook 2nd Edition, John Wiley & Sons, 2003

[7] Steven Shepard, RFID : Radio Frequency Identification, McGraw-Hill, 2005

[8] 김호원, Light weight crypto module for RFID and USN applications, 유비쿼터스 정보보호 workshop 2005, 2005년 6월1일

[9] C.P.Yu, C.S.Choy, H. Min, C.F. Chan, and K.P. Pun, "A Low Power Asynchronous Java Processor for Contactless Smart Card," ASP-DAC 2004.

[10] Martin Feldhofer, Sandra Dominikus, Johannes Wolkerstorfer, "Strong Authentication for RFID Systems using the AES Algorithm," CHES 2004.

[11] 임지형, 이병길, 김현곤, 정교일, 양대헌, 유비쿼터스 및 Ad-hoc 네트워크 망에서의 정보보호 분석, 주간 기술 동향, 2004년 11월

[12] Philippe Goller a, Markus Jakobsson, Ari Juels, and Paul Syverson, "Universal Re-encryption for Mixnets," CT-RSA 2004.

[13] Weis S, "Security and Privacy Aspects of Low Cost Radio Frequency Identification System," First International Conference on Security in Pervasive Computing, 2003

[14] Dirk Henrici, Paul Muller, "Hash based Enhancement of Location Privacy for Radio Frequency Identification Device using Varying Identifiers," University of Kaiserslautern, Germany

[15] K. Yusel, J.P.Kaps, and B. Sunar, "Universal Hash Functions for Emerging Ultra-Low-Power Networks," CNDS, San Die해, CA< January, 2004

저 자 소 개

● 손승원(Sung-Won Shon)

- 1984년 2월 : 경북대학교 전자공학과(공학사)
- 1994년 2월 : 연세대학교 대학원 전자공학과 석사(공학석사)
- 1999년 2월 : 충북대학교 대학원 컴퓨터공학과 박사(공학박사)
- 1983년~1986년 : 삼성전자(주) 연구원
- 1986년~1991년 : LG전자(주)중앙연구소 HI8mm 캠코더팀장
- 1991년~현재 : 한국전자통신연구원 정보보호연구단 단장/책임연구원

<관심분야> : 네트워크 정보보호, RFID/USN 정보보호, 유비쿼터스 정보보호, Biometry, 정보보호 정책 등