주 제

RFID 환경에서의 프라이버시 보호기술

한국전자통신연구원 오경희, 김호원

차례

I. 서 론

국내외에서 많은 관심의 대상이 되는 RFID 기술은 USN 기술과 더불어 유비쿼터스 환경을 현실화하는 기술로서, 유통 및 물류, 자동차, 의료 등 산업체 전 분야에 걸쳐 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, 읽고 쓰기가 가능한 EPC Class 1 Gen 2 태그가 시장에 나오게 됨에 따라 RFID 태그에 대한 활용도가 매우 넓어지게 되었다[1].

일반적으로 RFID 시스템은 크게 RFID 태그와 리더, 그리고 백엔드 데이터베이스로 구성되며, 수 미터의 거리에서도 초당 수백 개 이상의 태그를 한꺼번에 읽을 수 있다[2]. RFID 기술은 기존의 바코드 시스템을 대체할 수 있는 기술로 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.

900MHz 대역의 수동형 RFID인 경우, 일반적으로 유효복사전력값이 4W이고 태그와 리더간의 인식거리가 5m인 경우, 태그가 수신 가능한 소비 전력은 약 50uW다. 이에 비해, 13.56MHz의 비접촉식 스마트카드인 경우에는 10MHz로 동작할 때, 소비전력이 약 30mW 정도이다[3]. 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 하드웨

어 로직으로 구현하는 경우, 능동형 RFID 태그는 자체 전원이 있기 때문에 응용 목적에 따라 수 십만 게이트 급의 회로도 구현 가능하지만, 수동형 RFID 태그인 경우에는 가급적 수 천 게이트급 이하로 정보보호 기능을 구현하는 것이 바람직하다[4]. 또한, RFID 태그에 구현된 프로세서를 사용하여 해당 RFID 프로토콜을 처리하는 경우도 있는데, 이 경우, 이전에서 언급한 것처럼 저전력 특성을 가지는 프로세서를 사용해야 한다.

적절한 정보보호 기술을 사용하지 않은 RFID 태그는 기존의 보안 공격 기법인 도청, 트래픽 분석, 스푸핑, DoS 등의 공격에 취약하며 이러한 공격으로 사용자의 개인 정보와 관련 있는 민감한 정보들이 누출 될 수 있다. 또한, 위치 프라이버시 및 운송 데이터에 대한 위협도 가능하기 때문에, 적절한 접근 제어와 인증 과정을 통해 허용된 자만 태그 데이터를 읽을 수 있도록 해야 한다. 그리고, 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[4].

II. RFID 태그 정보보호 기술

2.1. 태그 사용의 차단

태그에 대한 접근을 모든 리더부터 차단하는 방법으로, 태그를 영구적으로 사용할 수 없도록 손상시키거나, 일시적으로 차단하기 위한 별도의 장비를 사용하여야 한다.

● **영구적인 태그 무효화(Kill)**

Kill Tag 방법은 Auto-ID 센터에서 제안되어 EPCglobal 규격에 적용된 방법으로, 태그의 설계에 32-bit의 패스워드를 포함하고 태그가 이 패스워드와 'Kill' 명령을 받을 경우 태그가 비활성화 되는 방식이다. 태그는 내부에 단락회로가 있기 때문에 이를 끊음으로써 Kill 명령을 실행하게 되는데 한 번 죽은 태그는 다시 살릴 수 있는 방법이 없다. 이런 경우 태그를 재사용할 필요가 있는 분야에서는 사용이 불가능하다. 아주 간단한 예로 반품이 가능한 물건에 붙어 있는 태그의 경우 이런 Kill Tag 명령 방식을 사용할 수 없다.

물론, 읽고 쓰는 것이 가능하게 설계된 태그의 경우 플래그(Flag) 비트를 이용하여 태그를 죽였다 다시 살릴 수도 있을 것이다. 하지만, 이 경우 또한 여전히 태그에 사용하는 패스워드의 크기에 대한 문제가 남는다. 수많은 제품에 사용될 태그라는 것을 감안하고 보안을 생각한다면 128-bit 이상을 패스워드로 사용해야 안전 하겠지만 이는 태그에 상당한 부담이 된다. 태그마다 다른 암호를 사용한다면 이를 데이터베이스에 저장하는 것도 문제가 될 수 있다.

● Faraday Cage

무선 주파수가 침투하지 못하도록 하는 방법으로 금속성의 그물이나 박막을 입히는 방법이다. 실제로 RSA 연구소는 2005년 유로화의 RFID 시스템의 도입에 대비하여 돈 봉투에 그물을 입힌 상품을 제시하였다. 그러나 이 경우도 사용 범위가 극히 제한적이 될 것이다.

● Active Jamming

리더가 제품을 읽지 못하도록 방해 신호를 보내는 물건을 소비자가 들고 다니자는 것인데, 악용될 소지가 크고, 방해 신호에 의해 다른 RFID 시스템이 손상될 수 있다.

● Blocker 태그

Blocker 태그는 모든 질문 메시지에 대해서 '그렇다' 또는 '아니다'라는 일관적인 응답만 하는 태그를 말한다. 모든 질문 메시지에 응답하기 때문에 바이너리 트리워킹을 사용하여 태그를 읽어 들이는 방식에서는 바이너리 트리의 모든 영역을 검색하게 만드는 결과를 가져온다. 태그의 고유번호가 길어지면 길어질수록 리더는 리더의 용량을 초과하는 개수의 태그를 찾기 위해 시도할 것이고 이는 리더에게 치명적인 결과를 가져올 것이다.

Blocker 태그를 조금 더 유용하게 사용하는 방법은 자신이 비밀을 지키고자 의도하는 태그들의 비트에 맞춰 처음 비트들을 제어함으로서 비밀 구역(Privacy Zone)을 만드는 것이다. Blocker 태그와 동일한 시작 비트를 갖는 태그들은 Blocker 태그가 만드는 비밀 구역 안에서 안전하게 보호될 수 있다. 그런데, 이러한 기법 자체가 서비스 거부 공격의 수단으로 악용될 우려가 있다.

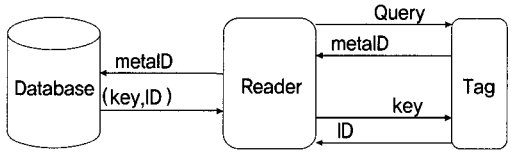
한편, 소프트웨어적으로 작동하는 Tag Privacy Agent를 사용하여 다양한 프라이버시 정책에 따라 태그에 대한 접근제어를 수행하는 Soft Blocking 기법도 제안되어 있다[5].

2.2. 인증 및 추적 방지

태그가 리더를 인증하는 방법이 제공되면, 도청자에 의하여 태그 정보가 유출되는 것을 방지할 수 있다. 그리고, RFID의 추적을 방지하기 위해선 태그에서 리더로 전송되는 데이터를 난수화하거나 익명성 기술의 사용, 혹은 리더를 인증함으로써 합법적인 리더만 읽을 수 있도록 제어하면 된다. 다음은 이를 구현한 기술들이다.

● Hash Lock 기법

RFID 태그가 리더를 인증하기 위하는 기법으로는 해쉬 함수의 단방향 특성을 사용한 Hash lock 기법이 있다[6]. 동작 과정을 보면, 잠겨진 태그는 리더의 쿼리에 대해 메타 ID로만 응답하고 이때 리더는 안전하다고 가정된 통신 채널을 통해 DB에서 메타 ID에 해당하는 태그 키와 ID 값을 가져 온 후, 리더는 태그에 키 값을 전송한다. 태그 내부에서 그 키 값에 대한 해쉬를 계산한 후, 자신의 메타 ID 값과 같을 경우에만 태그가 가지고 있는 ID 값을 리더로 출력한다. 이는 단방향 해쉬 함수의 역함수 계산의 어려움에 기반하며 불법적인 리더가 태그 내용을 읽는 것을 방지한다. 하지만, 메타 ID가 일종의 식별자로 사용될 수 있기 때문에 사용자 추적이 가능하다는 단점을 가진다. 이 기술은 능동형 공격(active attack)보다는 도청과 같은 수동형 공격(passive attack)에 초점을 맞춰 개발된 프로토콜이다.

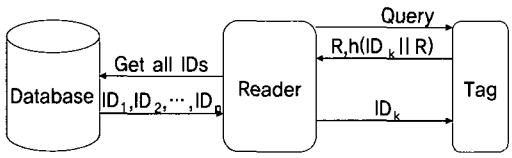


(그림 1) RFID 환경에서 리더 인증을 위한 Hash Lock 기법

● 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[7]. 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 power

로 설계해야 한다는 부담이 있다. 이 기법은 한정된 응용 범위를 가지는 경우에는 사용 가능하지만 많은 태그를 필요로 하는 경우에는 부적합하다.

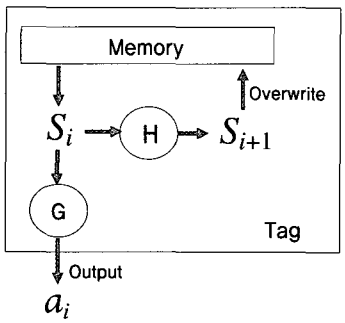


(그림 2) Randomized Hash Lock 기법

● Hash Chain 기법

Hash chain 기법은 태그에서 PRNG를 사용하지 않고도 태그 소유자의 프라이버시를 보호할 수 있다. 출력되는 값은 해쉬된 값이고 동작시 그 출력값이 계속 바뀌므로 역추적을 방지할 수 있게 된다.

동작 방식을 보면, 리더와 태그는 초기에 ID 값과 초기 비밀값 S를 가지고 리더에는 G 함수로 해쉬 처리된 값을 출력하며 비밀값은 H 해쉬로 갱신된다. 이 때 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 3) 해쉬 Chain 기법

2.3. 도청 방지

● 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 키의 발생 및 분배, 관리가 필요 없다. 동작 방식을 보면 각 태그는 비밀키 xt와 공개키 yt 값을 생성하고 DB에 각 태그의 (xt, IDt)를 저장한다.

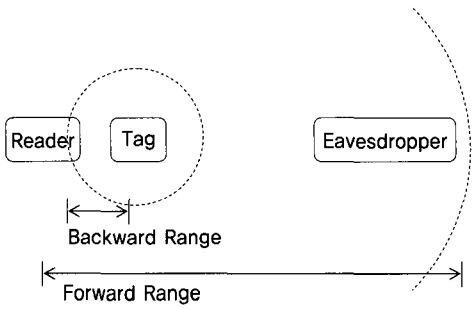
리더는 각 태그의 암호문 C와 난수 값을 사용해서 one-time pad를 생성하고 초기에 one-time pad 값과 암호문 값은 태그에 저장되고 그 다음부터 이 값을 갱신한다. 리더(서버)가 태그로부터 암호문을 받으면 서버는 해당 ID가 식별 될 때까지 DB에 저장된 모든 태그의 비밀키를 이용하여 복호화를 수행한다. 태그가 리더로 다시 신호를 보낼 때 one-time pad에서 2개의 값을 선택해서 암호화를 수행한다. 이 때 공개키 값을 사용하지 않는다[8].

● Silent Tree-Walking

기존의 tree-walking 프로토콜에서는 리더에서 broadcast되는 신호만으로 태그의 ID 추론이 가능하다. Silent tree-walking 방식은 그림 4 와 같은 상황을 가정하여 도청자가 리더와 태그 사이의 통신을 들을 수 있는 경우를 상정하게 된다. forward range는 리더가 태그에게 데이터를 전송하는 범위이며 backward range는 태그가 리더에게 데이터를 전송하는 범위이다. 이 경우에서 backward range 밖 그리고 forward range 안에 도청자가 있다고 가정할 때, 도청자는 리더가 태그에게 보내는 메시지를 엿들을 수 있으나 태그에서 리더로 전송되는 신호는 들을

수 없게 된다.

Silent tree-walking은 리더에서 태그로 가는 전방향 신호가 도청되더라도 태그에서 리더로 전송되는 신호만 도청되지 않는다면, 도청자가 태그의 ID를 추론하지 못하게 하며, 실행 시간에 있어서도 일반 binary tree-walinkg과 동일한 알고리즘을 갖는다.



(그림 4) Forward Range와 Backward Range

● Randomized Tree-Walking

랜덤 트리워킹은 태그가 랜덤한 수를 생성하여 이를 리더에 보내고 이를 기초(Portion)로 하여 트리워킹을 시도하는 방식이다. 태그는 반드시 자신이 생성했던 랜덤한 수를 기억하고 있어야 하며, RNG를 가지고 있고 전원이 끊어지지 않도록 해야 한다는 제약사항이 있다.

2.4. RFID 태그 보안 구현 기술

태그 위변조 방지하기 위한 방법으로, 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[4].

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 실행할 때마다, 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 강한 암호 알고리즘을 사용하지 않는 한, 안전성에 문제가 있다[4].

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. 이를 위하여 몇 가지 대표적인 암호 알고리즘에 대한 소비 전력 특성을 통하여 RFID 암호 모듈의 경량 특성을 살펴본다.

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-bit 기반 구조를 가지도록 하거나 혹은 gated clock 기법이 적용된 레지스터를 활용한 메모리를 사용함으로써 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[9].

스트림 암호를 포함해서 현재 LFSR(Linear Feedback Shift Register)을 기반으로 하는 암호 알고리즘이 많이 존재한다[10]. 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[4].

Hash lock이나 Hash chain 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[4,11]. 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.

III. RFID 프라이버시 보호

개인 정보를 의미하는 프라이버시는 식별된 혹은 식별 가능한 개인과 관련된 모든 정보를 말한다. 예를 들어 민족과 인종을 나타내는 개인데이터, 정치적인 의견이나 종교 및 철학적인 믿음, 노동조합원 정보, 건강관련 데이터 등은 프라이버시와 관련된 민감한 데이터들이라 할 수 있다.

RFID의 경우, RFID 태그에서 방출하는 정보는 사람과 관련된 정보가 아니라 사물에 대한 정보이며, 이러한 정보를 기반으로 사람을 식별하지는 않지만, 상점에서의 사물정보에 대한 적극적인 수집으로 개인 취향에 대한 프로파일링이나 위치추적을 하는 문제 등은 프라이버시의 문제가 될 수 있다.

프라이버시 보호를 위한 많은 국내외 정부 혹은 비정부 기구들이 존재하고 있으며, 프라이버시 보호 법률이나 가이드라인을 통하여 소비자의 프라이버시 보호를 위해 데이터를 수집하는 기업이나 정부에 대해 규제하는 것이 일반적이다.

국내의 경우, 직접 RFID에 관련되어 프라이버시를 보호하는 입법은 아직 없다. 그러나, 공공기관개인정보보호법 (1994), 정보통신망촉진 및 개인정보보호법 (2001), 위치정보의 보호 및 이용 등에 관한 법률 (2005)이 제정되어 있으며, 공공 및 민간에 모두 적용되는 개인정보보호법(안)이 입법 발의 중에 있다. 또한, SKT 등 이동통신사 3사를 대상으로 개인정보영향평가제를 시범 적용하고 있다.

정보통신부와 한국정보보호진흥원에서 마련한 'RFID 프라이버시보호 가이드라인(안)' (2005)에서는 RFID를 통한 개인정보 수집 및 연계를 제한하고, RFID태그의 부착사실 표시하며, RFID 리더기 설치에 대한 규제 강화하고, 가이드라인의 법제화 방향을 제시하고 있다. 한편, 함께하는 시민행동에서 'RFID에서의 프라이버시 보호를 위한 10가지 최소

가이드라인' (2004)을 제안한 바 있다.

그리고, 모바일 RFID 포럼에서 이루어지고 있는 표준화 활동의 일환으로 '모바일 RFID 프라이버시 보호 가이드라인'이 마련 중이며, 모바일 RFID 서비스를 제공하는 자가 준수하여야 할 기본적인 사항과, 모바일 RFID 서비스 이용과 관련된 정보 주체의 프라이버시를 보호하고 안전한 모바일 RFID 이용환경을 조성하기 위한 표준 가이드라인을 제공하는 것이 목적이다. 여기에서 모바일 RFID 서비스와 서비스 네트워크에서의 보안 요구사항들을 정의하고, 성인물 서비스에 관련된 사용자 성인인증, 모바일 RFID 단말 플랫폼의 안정성을 보장하기 위한 WIPI 기반의 보안 API 등을 표준화하고 있다.

국내외의 여러 법제 및 가이드라인의 공통된 요구사항 및 이슈를 정리하면 다음과 같다.

● **수집제한**(Collection limitation)

데이터 수집가는 꼭 필요한 정보만을 수집해야 하며, 데이터 주체에게 고지하거나 동의를 얻는 것과 같이 합법적인 방법에 의해야 한다. 불필요한 데이터의 수집으로 인해 향후 수집된 데이터에 대한 책임질 필요가 있으며, 필요한 정보만을 수집할 수 있도록 하는 필터링 등의 기술적 메커니즘 필요하며, 수집된 정보 중에서 관련 없는 데이터를 즉시 제거하기 위한 방법이 필요하다.

● **정확성** (Data quality, Accuracy)

수집된 데이터는 최신의 것이어야 하며, 필요한 정보만을 저장해야 한다.

● **목적명시**(Purpose specification)

데이터 수집 전에 수집의 목적이 명시되거나 알려져야 하며, 사용자가 정보수집의 목적이나 제한사항 등을 쉽게 파악할 수 있도록 하는 지원 메커니즘 필요하다.

● **이용제한**(Use limitation)

개인적인 데이터는 명시된 목적으로만 사용되어야 한다. 데이터 주체의 동의나 법적으로 필요한 경우는 예외가 될 수 있다. 이를 위하여 정보의 사용이나 공개, 보존 등이 사용자가 동의한 대로 이루어지고 있는지에 대한 확인 방법 필요하다.

● **보안조치**(Security safeguards)

수집된 데이터를 보호하기 위한 합리적인 보안조치가 취해져야 하며, 익명화, 도청방지, 해킹방지 등의 보안 요구사항 지켜져야 한다.

● **개방**(Openness)

데이터 주체가 데이터 제어자가 누구인지 알 수 있어야 하며 연락 가능한 방법을 알 수 있어야 하며, 데이터 수집을 하는 리더 자체를 식별/인증 할 수 있어야 한다.

● **개인 참여**(Individual participation)

데이터 주체는 자신의 데이터가 저장되었는지, 삭제되거나 수정되었는지 등에 관해 확인 및 질의할 수 있어야 하며, 쉽게 확인 및 질의할 수 있는 기술적인 방법을 제공하여 데이터를 확인하고 잘못된 부분에 대한 수정을 할 수 있어야 한다. 그리고, 잘못된 데이터를 고치는 것 뿐아니라 잘못된 데이터를 받은 제3자에게도 변경된 것을 알려야 한다. 데이터 전달 경로를 파악하고 잘못된 데이터에 대하여 고지하는 부분은 시스템 구현 시에 중요하게 다뤄져야 할 것이다.

● **책임**(Accountability)

데이터 제어자는 이 원칙들을 따라야 하고 이에 대

해 책임져야 한다. 이를 위하여 발생문제에 대한 책임 소재를 파악하기 위한 Audit을 위한 Tracking & Tracing 시스템 등과 같은 기술적인 접근 방법이 필요하다.

● **동의 (Consent)**

사용자 부담을 줄이기 위해서 자동화된 협상과정을 통한 동의 방법 필요하며, 사용자의 인지 없이 통신이 일어나는 RFID환경 상에서 적용될 수 있는 적절한 메커니즘 필요하다.

● **준수여부 확인 (Challenging compliance) / 강제시행 (Enforcement)**

규정을 준수하기 위한 메커니즘 제공되어야 하며, 이 compliance를 준수하는지를 확인 할 수 있는 기술적인 평가(Assessment) 필요하다.

〈표 1〉 프라이버시 보호를 위한 기술적 해결 방안

원 칙	기술적 해결방안 (FIP에 대한)	적용시점
수집제한	- Blocker/softblocker tag - Paraday cages - Recoding scheme - Inventory process에서 selection mask 이용 - RFID Guardian (접근제어)	판매전/중/후
정확성	- Privacy-aware DB	판매후
목적명시 (고지)	- Inventory command 확장을 통한 purpose declaration	판매전/중
이용제한	- Privacy-aware DB	판매후
보안	- Encryption, Signature 등 암호학적 접근법 - RFID 리더/태그 인증 - RFID Guardian (접근제어/인증/키관리) - DB 보안	판매후
개방성	- Inventory command 확장을 통한 reader ID, policy ID 제공 - RFID 리더 인증	판매전/중/후
개인 참여	- Privacy-aware DB	판매후
책임	- Inventory command 확장을 통한 reader ID, policy ID 확인 - RFID 리더/태그 인증 - RFID Guardian (Audit)	판매후
동의	- Watchdog 태그 이용 (reader와 policy ID 제공 시)	판매전/중

● **선택 (Choice)**

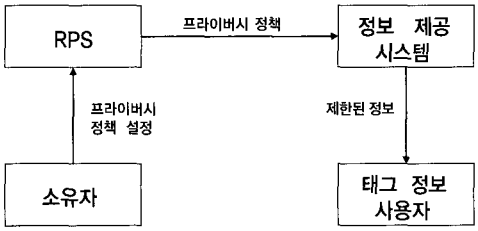
구입한 제품에서 EPC태그를 떼어내거나 비활성화 시킬 수 있음에 대한 설명을 들을 수 있어야 한다. 그리고, 태그를 비활성화 시키고자 하는 경우 비활성화 및 이에 대한 확인을 할 수 있는 기술적 장치가 필요하다.

<표 1>은 OECD에서 프라이버시 보호 및 개인정보의 국제적 유통에 관한 가이드라인으로 공표된 FIPS(Fair Information Practice Principles)에 언급된 원칙들에 대한 기술적 해결방안들이다.

RPS(RFID user Privacy management System)를 사용하여 태그가 부착된 물품을 소유한 자의 프라이버시를 보호하는 방법이 제안된 바 있다 [13]. RPS는 개인의 프라이버시 정책을 관리하는 시스템으로 소유자는 RPS에 프라이버시 보호레벨에 따른 프라이버시 정책을 설정할 수 있다. 또한, 태그에는 프라이버시 보호레벨이 설정되어 있으며, RFID 태그에 연계된 정보 서비스를 제공하는 시스템은 RPS를 통하여 소유자가 설정한 프라이버시 정책에 따라 서비스를 제공함으로써 소유자가 원하지 않는 개인 정보의 유출을 방지할 수 있다. 이러한 과정에서 RPS는 다수의 소유자들과 정보 제공 시스템들 사이에 프라이버시 정책에 대하여 단일한 인터페이스를 제공하여 연결하는 역할을 한다.

IV. 결 론

RFID에 의한 인식기술은 기존의 바코드 등과 비교하여 편리함과 자동화 가능성 면에서 많은 이점이 있으나, 무선 구간을 통하



(그림 5) 모바일 RFID 프라이버시 보호 시스템 구성

여 정보가 전달되어 도청이 용이해진다는 점과, 프라이버시에 관련된 대량의 정보가 처리됨으로 인하여, 유출로 인한 피해가 매우 클 수 있다는 점에서 보안의 중요성은 매우 크다.

RFID 태그의 하드웨어 특성으로 인해 보안 기능 구현에 많은 제약이 있어, 현재 상용화되어 사용되고 있는 RFID 제품들에는 아직 취약점들이 많이 존재하고 있다. 그러한 제약들을 극복할 수 있는 경량화된 알고리즘과 프로토콜을 구현하여 태그와 리더 사이에서의 인증과 기밀성, 무결성, 그리고 추적 방지 기법과 같은 보안 기능을 적용하지 못한다면 RFID 응용 범위 역시 제한될 수 밖에 없을 것이다.

또한 RFID에 관련된 정보들은 개인의 프라이버시에 관련된 정보들이 많으며, 이러한 정보들이 제대로 관리되지 못한다면, 그 위험 역시 매우 크다. 따라서, 태그와 리더 사이에서의 보안만이 아니라, RFID 서비스를 제공함에 있어 관련 정보가 저장되고 처리되는 과정에서의 보안 역시 중요하다.

[참 고 문 헌]

[1] 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

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

[3] 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

[4] 김호원, Light weight crypto module for RFID and USN applications, 유비쿼터스 정보보호 workshop 2005

[5] A. Juels, and J. Brainard, "Soft Blocking: Flexible Blocker Tags on the Cheap," WPES 2004

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

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

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

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

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

[11] K. Yusel, J.P.Kaps, and B. Sunar, "Universal Hash Functions for Emerging Ultra-Low-Power Networks," CNDS,

Jan. 2004
[12] 임지형, 이병길, 김현곤, 정교일, 양대헌, 유비쿼터스 및 Ad-hoc 네트워크 망에서의 정보보호 분석, 주간 기술 동향, 2004년 11월
[13] TTA, 모바일 RFID 프라이버시 보호 프레임워크 표준(안), 2006

오경희

1999년 연세대학교 컴퓨터과학과 학사
2001년 연세대학교 컴퓨터과학과 공학석사
2000년 ~ 현재 한국전자통신연구원 정보보호연구단 선임연구원
관심분야 : 센서네트워크, RFID 보안, 정보보호

김호원

1993년 경북대학교 전자공학과 학사
1995년 포항공과대학교 전자전기공학과 공학석사
1999년 포항공과대학교 전자전기공학과 공학박사
2003년 ~ 2004년 Ruhr University Bochum, Germany, Post-Doctorial
1998년 ~ 현재 한국전자통신연구원 정보보호연구단 RFID/USN보안연구팀장
관심분야 : 타원곡선 암호모듈 설계, RFID 보안, USN 보안