유비쿼터스 환경에서의 개인정보 보호 기술

Personal Information Security Technology in the Ubiquitous Environment

남택용(T.Y. Nam) 개인정보보호연구팀 책임연구원, 팀장
장종수(J.S. Jang) 네트워크보안그룹 책임연구원, 그룹장
손승원(S.W. Sohn) 정보보호연구단 책임연구원, 팀장

본 논문에서는 최근 IT 신성장 동력 기술 중의 하나인 유비쿼터스 환경에서의 개인정보 보호 기술에 대해 살펴 보고자 한다. 유비쿼터스 환경에서는 사람이나 물건의 상황과 주변 환경 등을 센싱하여 다양한 대량의 데이터를 수집하게 되며, 또한 서비스 제공에 의해 개인 프라이버시에 관한 정보를 센싱 노드나 네트워크 상에서 주고 받게 된다. 본 논문은 이와 같은 유비쿼터스 환경을 실현하기 위한 기술 중의 하나인 RFID 태그 시스템에서의 프라이버시 보호 방법에 관한 것으로, RFID의 특성을 기술하고, RFID 프라이버시의 위협에 대응하기 위한 기술들을 알아본다. 그리고 유비쿼터스 환경에서 개인정보를 보호하기 위해 블로커 태그를 이용한 프라이버시 보호 기법을 제안하고, 결론과 함께 향후 연구 개발이 필요한 사항들을 제시하고자 한다.

I. 서 론

개인정보는 인터넷에서 이루어지는 시장 경제의 활성화를 위해 반드시 필요한 것으로, 기업의 입장에서 보면 이러한 개인정보를 통해 온라인의 특성을 활용한 마케팅과 판매활동을 적극적으로 수행할 수 있다. 그러나 개별적인 인터넷 사용자들의 입장에서 볼 때 이들은 자신의 개인정보를 제공함으로써 발생할 수 있는 위험에 대해 매우 우려하는 것 또한 사실이다. 그런 면에서 개인정보 보호기술은 개별적인 사용자 혹은 기술 관리자가 어떠한 경우에 정보를 공개할 것인지에 대한 통제 능력을 부여한다는 점에서 매우 효율적인 프라이버시 보호 솔루션을 제공한다고 할 수 있다.

따라서 개별적 기업들은 먼저 프라이버시 보호 기술을 자사의 네트워크에 결합함으로써 사용자들의 프라이버시를 보호할 수 있는지에 대해 평가하는 것이 필요하다. 기업은 어떻게 프라이버시 보호기술이 브라우저나, 다른 하드웨어 혹은 휴대용 제품들과 호환되어 표준화될 수 있는지를 고려하여야 할 것으로 보인다. 마찬가지로 인터넷 서비스 제공자는 프라이버시 보호기술을 제공함으로써 가입자들이 우려하고 있는 프라이버시 보호 문제가 경감될 수 있는지를 고려하는 노력이 필요할 것으로 보인다 [1],[2].

본 논문에서는 최근 IT 신성장 동력 기술 중의 하나인 유비쿼터스 환경에서의 개인정보 보호 기술에 대해 살펴 보고자 한다. 유비쿼터스 환경에서는 사람이나 물건의 상황, 그의 주변 환경 등을 센싱하여 다양하고 대량의 데이터를 수집하게 된다. 이와 같은 데이터 중에는 영상이나 바이오 메트릭스처럼 직접 개인의 프라이버시에 관계되는 정보가 있으면, 체온이나 혈압 등의 미세한 정보를 조합하여 건강상태를 알 수 있듯이 통합 또는 분석에 의해 의미 있는 정보로 되는 것도 있다. 따라서 서비스 제공에 의해 개인 프라이버시에 관한 정보를 센싱 노드나 네트워크상에서 주고 받게 된다. 또한 센싱하거나 센싱된 정보의 소유자가 누구의 것인가? 그 정보의 처리, 가공, 유통, 삭제의 권리는 누구인가 등에 관해 방법을 정리할 필요가 있다. 유비쿼터스 센서 네트

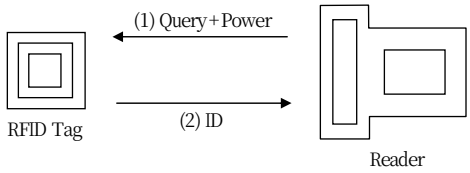
워크의 실현, 보급에 있어서 현장 실험 등을 통해 어떠한 정보를 누가 어떻게 취급하는가에 관한 기본적인 생각을 이용자를 포함한 관련자간에 충분히 검토하여 기술적인 대책을 연구할 필요가 있다. 또한 이용자로부터의 문의나 불만에 대해 명확한 책임 주체를 확립하여야 한다[3],[4].

본 논문은 이와 같은 유비쿼터스 환경을 실현하기 위한 기술중의 하나인 RFID 태그 시스템에서의 프라이버시 보호 방법을 살펴본다. Ⅱ장에서는 RFID의 특성을 기술하고, Ⅲ장에서 RFID 프라이버시의 위협에 대응하기 위한 기술들을 알아본다. Ⅳ장에서는 유비쿼터스 환경에서의 개인정보를 보호하기 위해 블로커(blocker) 태그를 이용한 프라이버시 보호 기법을 제안하고, 마지막으로 Ⅴ장에서 결론과 함께 향후 연구 개발이 필요한 사항들을 제시하고자 한다.

Ⅱ. RFID 시스템의 특성

RFID 태그는 무선 통신용 안테나와 IC 칩을 조합한 저가의 소형 장치이다. 태그에 질의를 발생시켜, RFID 태그 메모리에 쓰여져 있는 ID를 읽어내는 무선 장치를 reader라 부른다. Reader에 의해 질의를 할 때, 전원도 함께 보내며, 이 경우 RFID 태그 자신에는 전원이 필요 없다. 이 때문에, RFID 태그는 장차 바코드를 대신하는 식별 기능으로 활용될 것이다. 바코드와 같이 폭 넓은 이용을 위해서는 RFID 태그 하나 당 가격은 50원정도, 크기는 0.4mm×0.4mm 이하로 종이에 심을 수 있을 정도로 얇은 것이 바람직하다. 따라서, RFID 태그의 계산 능력은 제한되어, RFID 태그가 복잡한 능력을 처리하는 것은 곤란하다. 또한 전파를 이용하는 특성상, RFID 태그와 reader 사이에 주고 받는 내용을 쉽게 도청할 수 있다.

RFID 태그에는 몇 종류가 있으며, 통신 거리, 메모리 종류, 전원의 유무에 의해 분류된다. 우선, 통신 거리에는 밀접형(0~수mm), 근접형(수mm~수10cm), 원격형(수10cm~수m)이 있다. 메모리에는 읽기 전용형, 한번만 쓰기 및 읽기형, 읽기 및 쓰기



(그림 1) 일반적인 RFID 시스템

가능형이 있다. 쓰기 가능한 메모리를 탑재한 경우, RFID 태그의 ID 정보를 reader/writer라 부르는 무선통신 장치에 의해 써넣기가 가능하다. 또 RFID 태그의 전원에는 능동형과 수동형이 있다. 능동형은 RFID 태그에 전원을 내장하고 있고, 수동형은 reader로부터 전원을 얻는다. 이 태그와 reader를 이용한 개인정보 식별 시스템을 RFID 시스템이라 부른다. 일반적으로 RFID 태그와 reader 사이에 주고 받는 절차를 (그림 1)에 보인다.

RFID 시스템을 이용하면, 상품의 포장을 개방하지 않아도, 상자 속에 태그가 부착된 상품 인식이 가능하기 때문에, 상품의 재고 관리나 물류 관리에 이용된다. 태그는 상품에 붙여져 있으며, 바코드 같은 기능이 부여되어 있으므로 도난 방지 역할을 기대할 수 있다. 또한 상품 구입 후에도 RFID 시스템은 소비자에 편리한 기능을 준다. 예를 들면, 리더가 부착된 냉장고가 태그에 부착된 식료품의 유통 기한을 감시한다든지, 양복장에 보관되고 있는 옷에서 양호한 조합을 제공하는 것이 가능하게 될 것이다. 또한 유럽중앙은행은 유로 지폐에 RFID 태그를 심는 것을 제안하고 있다. RFID 태그의 ID와 지폐에 인쇄된 일련번호를 조합한 식별을 이용하면, 위조 방지 능력 및 가짜 금융차용의 억제를 기대할 수 있다.

Ⅲ. RFID의 프라이버시 보호에 대한 위협

RFID 태그 정보는 reader를 사용하면 간단히 그 정보를 인출하는 것이 가능하므로, 태그 소유자의 프라이버시 침해와 연결되어 있다. RFID 태그에는 고유 ID가 설정되어 있기 때문에, 그 ID를 입수하면 태그가 붙여진 대상의 정보를 얻는 것이 가능하다.

예를 들면, 소비자의 양복 사이즈나 가격, 상점의 상품 재고 정보 등을 아는 것이 가능하여, 소비자의 프라이버시가 침해된다. 또 태그의 ID 내용은 알 수 없어도 특정 태그의 정보를 추적함으로써, 태그 소유자의 거주 장소를 규명한다든지 추적하는 것이 가능하다. 이 위치 정보에 관한 프라이버시를 location 프라이버시라 부른다. 이 때문에 소매점이 소비자를 추적한다든지, 상품의 유통 정보가 누설되어 버리는 문제가 일어난다. 이것에 의해 소유자가 다른 피해를 입는 것이라고 생각된다. 지폐에 RFID 태그가 심어져 있는 경우, 은행에서 예금을 인출 후에 RFID 정보가 읽혀져, 정확하게 추적되어 범죄에 말려 들 수 있을 가능성이 있다.

최근 RFID 태그에 의해 발생되는 프라이버시는 신문에 많은 관심을 가지며, 부정적인 면이 부각되어 상품에 RFID 태그를 이용할 계획이 취소되는 경우도 있다. 따라서 RFID 태그에서 프라이버시 보호 대책이 아주 중요하다. 이를 개선하기 위한 연구가 계속 진행되고 있으나, 프라이버시 조건을 완벽하게 만족시킬 수 있는 한 가지 방법은 없다. 그러므로 여러 가지 방법을 조합하여 사용하는 것이 가장 좋은 방법이다. 따라서 RFID 태그에 관계 있는 프라이버시 보호 기술을 소개한다[5]-[7].

1. RFID 태그의 무효화(kill) 방법

고객의 프라이버시 보호를 위한 가장 단순한 방법은 상품이 고객에게 인도되기 전에 RFID 태그를 무효화(kill)하는 것이다. 무효화된 태그는 다시는 re-activated 되어 사용될 수 없다. AutoID 센터에 의해 제안된 동작의 표준 모드를 살펴보면 태그는 태그 부착 상품을 구매함으로써 무효화(killed)되는 것을 의미한다. AutoID 센터가 제안한 태그 설계에서는 특별한 “kill” 명령을 보내므로 태그가 무효화된다. 이때 명령에는 8비트 패스워드가 포함된다. 예를 들면, 어떤 슈퍼마켓에서는 선반에 있는 제품 감시 및 재고품 관리를 쉽게 하기 위해 RFID 태그를 사용한다. 고객의 프라이버시를 보호하기 위해, 카운터 점원은 구매된 상품의 태그를 무효화(kill) 할 것이다. 구매되지 않는 상품은 능동 RFID 태그를 가지고 있다.

그러면, 무엇 때문에 무효화(kill)하는 방법은 부적합한 것인가? 그 답은 여러 환경이 있을 수 있으며, 이러한 환경에서 “kill”과 같은 단순한 방법은 개인 프라이버시 시행을 위해 동작하지 않을 수 있고, 바람직하지 않다. 예를 들면, 고객은 자기가 물건을 소유하고 있는 동안에 동작하는 RFID 태그를 원할 수도 있다. 가정에서 사용하는 예로, 식료품 패키지로부터 요리 방법을 읽어 들일 수 있는 레인지는 능동적으로 동작 태그에 의존한다. 유사한 방법으로 RFID 태그를 위해 새롭고 고기능의 고객 의존형 응용이 나타날 것이다. 일반 고객을 위한 RFID 태그 응용의 다른 예로는 힘들이지 않고서 물리적 접근제어, 소유물의 도난 방지, 무선 현금 카드 등을 생각할 수 있다. RFID 태그와 같은 저가격의 강력한 기술은 오늘날 우리가 상상할 수 없을 정도로 수많은 분야의 응용에 필연적으로 사용될 것이다. 대부분의 응용에서는 고객이 소유하는 동안에 태그가 능동 상태로 있기를 요구한다. 따라서 구매자는 태그의 무효화를 원하지 않을 수도 있다. 여기에 가능한 몇 가지 응용을 나타낸다.

① 상점은 만약에 제품이 하자로 인하여 반품될 때, 스캐닝이 가능한 태그를 갖는 제품을 원한다.
② 제품을 재활용 목적으로 분류하기 위해, 제품이 스캔될 필요가 있다.
③ 상점은 부착된 RFID 태그를 이용하여 영수증을 발행하며, 그 제품이 반품될 때, 자세히 구매를 확인할 수 있다.
④ 개인은 수취인에게 쉽게 스캐닝되도록 명함에 끼워진 RFID 태그를 갖길 원한다. 여기서 태그 ID는 실제 카드 데이터를 나타내는 URL을 만드는 데 사용될 수 있다.
⑤ 상점은 상점이 발행한 쿠폰에 RFID 태그를 삽입시켜, 카운터 점원이 쉽게 스캐닝하기를 원한다.
⑥ 사용자는 특별한 제품을 recall 할 때, 자기가 소유한 제품을 스캔하기를 원한다.
⑦ CD나 기호품 같은 수집품은 RFID 태그를 가지

길 원한다. 그러므로 소유자가 자신의 재산 목록을 잘 취급할 수 있다.

⑧ 상인은 마케팅 목적으로 고객의 스캐닝을 원할 수도 있다. 예를 들면, 이 고객은 오늘 사전에 무슨 상점을 방문하였는가? 이미 어떤 물건을 샀는가? 등이다.

⑨ 냉장고나 식료품 선반은 어떤 식료품이나 약품이 유통기간이 지났을 때, 알려줄 수 있다.

⑩ 항공권에 공항 내에서 승객의 추적을 간단하게 수행하기 위하여 RFID 태그를 끼워 넣을 수 있다.

⑪ 사업상 회신할 때, 분류를 쉽게 하기 위해 in-voices, 쿠폰, 회신용 봉투에 RFID 태그가 포함되길 원한다.

이처럼 RFID 태그가 수많은 분야에서 응용될 수 있으며, 능동태그는 고객 및 사업자에게 부가 가치를 부여할 것이다. 따라서 고객은 상인, 사설 탐정, 배우자, 부모 혹은 관련자에 의해 몰래 추적되고, 신원이 확인될 가능성이 있다. 그러므로 개인의 프라이버시에 관심이 있는 대부분의 응용에서는 구매와 동시에 태그를 무효화 하는 방법을 사용하지만, 만족스러운 방법은 아니다. 따라서 다른 대안을 개발하여야 하는 것은 피할 수 없는 방법으로 생각된다. 이러한 문제를 해결하기 위하여, 기능정지 명령과 재개 명령을 이용하는 방법이 있다. 이 방법을 이용하면, RFID 태그의 기능이 불필요할 때에는 기능을 정지시키고, 필요하면 기능을 재개시키는 것이 가능하다. 이러한 명령은 기능 무효화 명령과 똑같이 실행 명령 시 패스워드를 이용하는 방법을 생각할 수 있지만, 전파에 의한 통신 특성상 RFID 태그와 reader의 정보 교환은 간단히 도청되므로, 패스워드를 도난 당해 공격자에 그 기능이 악용될 소지가 있다. 또 RFID 태그가 부착된 대상이 증가함에 따라, 이러한 명령을 관리하는 것도 복잡하게 된다. 이러한 문제를 해결하기 위하여, RFID 태그와 reader 사이의 통신에 암호화나 인증을 이용하는 방법이 있다.

2. The Faraday Cage 방법

RFID 태그는 faraday cage(어떤 범위의 무선주파수를 차단할 수 있는 포일이나 금속 그물망으로 만들어진 용기)를 사용하여 정밀 조사로부터 차폐할 수 있다. 이러한 사실은 애완 도둑이 도난 방지 시스템을 속이기 위하여 foil-lined 가방을 이용하는 것으로 알려져 있다.

만약에 고액권 지폐에 RFID 태그를 공급한다면, 그때 foiled-lined 지갑은 대박을 터뜨릴 것임에 틀림 없을 것이다. 아마 어떤 회사는 개인 프라이버시 목적으로 faraday-cage-based product를 제공하고 있을 것이다. RFID 태그는 사물의 광범위 영역에 이용될 것이다. 그러므로 faraday cage는 적어도 고객의 프라이버시를 위한 부분적인 해법을 제시할 것이다.

3. The Active Jamming Approach

RF 신호의 액티브 jamming은 태그 통신을 차폐시키는 다른 형태의 물리적인 방법이다. 고객은 부근에 있는 RFID reader의 동작을 방해하거나 차단시키기 위해 능동적으로 무선 신호를 방송하는 장치를 가지고 다닐 수도 있다. 그러나 고출력으로 방송한다면, 이 방법은 불법이 되며, 조잡한 방법에 지나지 않는다. 또 주위의 모든 RFID 시스템을 교란시킬 것이며, 프라이버시에 관심이 없는 합법적인 시스템도 방해할 것이다.

4. RFID 태그와 Reader의 교신에 암호화 및 인증을 이용하는 방법

RFID 태그와 reader의 교신은 간단히 도청되기 때문에 그 통신에 암호화를 적용한다든지, RFID 태그가 소유자나 특정 reader만 통신이 가능하도록 인증을 이용하는 방법이다. Reader의 능력은 제한되어 있지 않기 때문에, RFID 태그에 써넣을 내용을 암호화하여 써넣은 것이 가능하다. 이것에 의해 RFID 태그의 정보가 인출되어도 그 내용을 이해하는 것은 어렵다. 가격은 RFID 태그 당 50원 정도가 바람직스럽기 때문에, RFID 태그에는 한정된 계산 능력밖에 탑재할 수 없다. 이 때문에, RFID 태그가 복잡한 암호화를 처리한다는 것은 현실적으로 어렵다. 이와

같은 이유에서, RFID 태그가 reader를 인증하는 방법을 적용해도, 인증에 필요한 정보를 암호화하여 전송하는 것이 불가능하기 때문에, 도청되어 가장 등의 공격을 받을 가능성이 있다. 따라서 RFID 태그가 특정 reader를 인증하는 것은 곤란하기 때문에, 공격자가 RFID 태그 정보를 인출하는 것을 방지하는 것은 곤란하다.

5. "Smart"한 RFID 태그로의 접근 방법

지금까지 설명한 방식과 다른 방법으로 RFID 태그를 조금 "smarter"하게 하는 것이다. 이 방법은 액티브 기능을 부여하여, 개인 프라이버시 보호를 좀더 잘하기 위한 방법을 상호 교환하는 것으로, 대부분 암호학적 방법을 사용하고 있다.

이 방법은 기본 RFID 태그에 코스트 제한이 엄격하게 적용되기 때문에, 설계하는 것이 대단한 도전이다(50원 예산 범위에서 추가적인 로직 코스트가 소요된다).

지금까지 증명된 "Smart RFID-Tag"의 3가지 예는 hash-lock 방법, 재암호화 방법, silent tree-walking 방법이다.

가. "Hash-Lock" 방법

이 방법에서, 태그는 "unlocked" 될 때까지 ID를 표시하는 것을 거절하기 위하여 "locked" 된다. 간단한 시나리오에서, 태그가 lock 될 때, 값 y(meta-ID)가 주어지며, 이는 다만 PIN 값 혹은 key의 값 x에 unlock 된다. 이때 관계는 y=h(x)이며, h는 단방향 해시 함수이다.

슈퍼마켓의 예에서, 태그는 계산 시 lock 된다. 고객은 태그를 위해 meta-ID y를 제공한다. 그때, 집에 돌아오자마자 태그를 unlock하기 위해 어떤 장치를 통해 PIN x를 보낸다. 이러한 방법이 가능하도록 하기 위해, reader가 meta-ID를 찾기 위해 태그에 질의할 필요가 있다. 즉 이는 reader가 태그를 unlock하기 위해 사용할 PIN을 알기 위함이다. 그러나 이것은 meta-ID를 통한 태그의 추적을 가능하게 만들 수도 있다.

이 문제를 풀기 위하여 해시 함수 계산에서 난수화하는 방법을 사용한다. 이것은 유효한 방법이지만, 이는 고객이 태그 수보다 많은 PIN 번호와 lock/unlock 패턴을 관리하여야 한다는 불편을 감수하여야 한다.

나. 재암호화 방법

RFID 태그의 정보를 암호화하는 방법에 더하여, 암호화된 RFID 태그 정보를 다시 정기적으로 암호화하는 방법이다. 암호문을 다시 암호화하는 방법을 재암호화라 부른다. 이것은 공개키 암호화 방식을 이용하여 실행되며, 키 생성 알고리듬, 암호화 알고리듬, 복호화 알고리듬 외에, 재암호화 알고리듬이 필요하다. 재암호화 알고리듬은 공개키를 이용하여 실행된다. 암호화 알고리듬에는 평문에 관한 정보가 필요 없이 암호문을 재암호화하여, 몇 번 재암호화하여도 암호문은 한 번의 복호화로 비밀키를 이용하여 원래의 평문으로 복호화하는 것이 가능하다. 또 재암호화에 의해 강한 은닉 특성이 있지만, 공격자는 재암호화된 암호문에서 원래의 암호문을 추측하는 것은 곤란하다. 강 은닉 특성은 어떠한 부분 정보도 부분 해독은 곤란하다는 것을 의미하며, 암호문에서 평문에 관한 정보가 일체 누설되지 않음을 의미한다. 이 방법을 이용하면, RFID 태그의 정보는 재암호화에 의해 정기적으로 고쳐 써넣으므로, 특정의 RFID 태그 정보를 추적하는 것을 방지할 수 있다. 또 재암호화 처리의 쓰기가 가능한 reader/writer에 처리시키면, RFID 태그의 복잡한 처리 없이 RFID 태그의 코스트를 낮추는 것이 가능한 이점이 있다. 단 공개키 암호화 방식의 재암호화를 이용하여 reader/writer에 재암호화를 처리시키는 경우, 암호화 시 reader/writer에 공개키를 전달하지 않으면 안 된다. 그 때에, RFID 태그와 reader/writer의 교신이 도청되어, 공개키에 관한 정보가 누설되어 버릴 가능성이 있다. 공개키에 관한 정보에는 RFID 태그와 그 공개키에 관련된 정보가 있으며, 그 정보에 의해 RFID 태그를 특정화 시킬 가능성이 있다. RFID 태그 정보가 누설되지 않아도, 특정의 공개키에 관련된 RFID 태그를 추적하는 것이 가능하

여, location 프라이버시가 침해되어 버린다. 여기서 RFID 태그 자신에 재암호화 처리를 시키는 것을 생각할 수 있지만, RFID 태그의 계산 능력이 제한되어 있기 때문에 이것은 곤란하다.

다. Silent Tree - Walking 방법

Weis 등은 수동적인 도청자에 노출되는 위협은 가까이서 도청이 가능한 RFID 태그 신호를 듣는 것보다 수백 미터 떨어진 곳에서 도청이 가능한 태그 reader에 의해 방송되는 신호를 듣는 능력이라고 정확히 지적하였다. 이러한 사실은 표준 tree-walking singulation 프로토콜에 의해 읽혀지는 ID들은 단순히 reader에 의해 방송되는 신호를 듣고 추론이 가능하기 때문에 불행하다.

Weis 등은 수동적인 도청자가 읽은 ID를 추론하지 못하도록 하기 위해 reader의 전송을 암호화하는 방법을 나타냈다. 액티브 공격에 대해 방어할 수 없다는 사실은 다른 문제로 하고, 저자는 논문에서 사용한 가정이 태그들 사이에 공유할 수 있는 공통적이고 비밀 스트링의 어느 정도 비현실적인 가정에 의존한다고 하였다. 만약에 태그들이 singulation 전에 자신의 random pseudo ID를 발생할 수 있다면, 이러한 가정은 제거될 수 있다. 선택적인 블로킹 방법은 도청으로부터 reader의 전송을 보호하는 방법과 조화를 이룰 수 있다.

태그에 암호 동작을 포함하는 “smart” RFID 태그를 만들기 위해 “silent tree-walking”과 “hash-lock” 방법에 대해 설명하였다. 이러한 방법은 가격이 너무 비싸 가까운 미래에 경제적으로 실현 가능성이 없어 보인다.

Ⅳ. 블로커 태그를 이용한 프라이버시 보호 방법

1. 블로커 태그의 구성 및 역할

프라이버시 보호를 위한 간단한 blocker-tag 방식을 설명한다. 블로커 태그[8]가 tree-walking singulation 프로토콜과 어떻게 선택적으로 조화를 이루는가를 이해하는 것이 중요하다. 블로커 태그는 active jamming 형태는 아니다. 아주 정확한 방법으로 태그 reading 과정에 참여함으로써, passive jamming의 한 종류로 생각할 수 있다.

블로커 태그는 태그의 가능한 모든 일련번호의 전 스펙트럼을 방해하여, 다른 태그들의 일련번호를 감출 수 있다. 고객에 의해 수행될 때, 블로커 태그는 프라이버시 보호인 물리적 영역에 야기되어, reader가 태그를 구별하지 못하도록 한다. 여기에서 블로커 태그의 2가지 형태, 즉 프라이버시 보호 도구와 악의의 도구로 사용될 수 있음을 설명하기로 한다.

첫째, 블로커 태그는 프라이버시 protection tool로 제공할 수 있다. 블로커 태그는 자연스럽게 일련번호의 어떤 제한된 영역에 대해 singulation을 방지하도록 설계, 즉 특정 지역에 맞도록 설계된다. 다시 말해, 특정 지역의 프라이버시를 보호할 목적으로 ‘1’로 시작하는 모든 일련번호 영역 지역에 맞도록 설계하는 것을 의미한다. 선택적인 블로킹 특성은 고객에 의해 아이템을 보호하는 데 이용될 수 있다. 동시에 영업적 환경에서는 태그의 reading을 방해하지 않는다.

둘째, 악의의 모습으로 동작하는 블로커 태그를 말한다. 다시 말하면, DOS 공격을 준비하는 도구로서의 기능을 설명한다. 블로커 태그는 일련번호의 모든 스펙트럼을 읽지 못하도록 차단하거나 특별한 영역(예를 들면, 특별한 제조 회사에 할당된 일련 번호의 집합)을 reader가 읽지 못하도록 차단시킬 수 있다. 이런 형태의 블로커 태그는 비즈니스를 방해하거나 물품 명세서 제어 메커니즘으로부터 상품을 차폐시킴으로써 좀도둑이 침입하는 데 도움을 줄 수 있다.

가. 블로커 태그는 어떻게 동작하나?

블로커는 2k개의 가능한 RFID 태그의 일련번호 모두를 방해(simulation)할 수 있다. 이러한 태그를 “full blocker” 혹은 “universal blocker”라 한다.

Tree-walking 알고리듬의 구조에 의해, 블로커는 쉽게 구현된다. Reader가 다음 비트의 값을 위해 노드 B의 서브트리(subtree) 내에 있는 태그에 질의를 할 때마다, 블로커 태그는 동시에 '0' 비트 혹은 '1' 비트를 방송한다.

개인 프라이버시 보호를 위해, 블로커 태그는 다만 태그의 서브넷만을 효과적으로 블로킹하는 것으로 한정할 수 있다. 이와 같은 블로커를 "partial blocker" 태그 혹은 "선택적인 블로커" 태그라 부른다.

예를 들면, 선택적인 블로커는 단지 root의 왼쪽 서브트리에서 tree-walking을 수행하는 동안만 reader에 응답할 수 있다. 이와 같은 선택적인 차단의 특징은 다만 일련번호에서 '0' 프리픽스를 갖는 태그를 읽는 데 방해하는 효과를 가지고 있다. 이때 '1' 프리픽스를 갖는 태그는 읽혀진다. 이러한 방법으로 선택적인 블로커 태그는 보호를 위한 특별한 영역을 목적으로 할 수 있다.

나. Reader에 친숙한 블로킹 프로토콜

만약에 블로커 태그가 어떤 영역은 블로킹하고, 다른 영역은 그대로 둔다면, 다음과 같은 문제가 일어난다. 예를 들면, 만약에 '0'으로 시작하는 ID는 블록시킨다면, reader는 '1'로 시작하는 ID는 읽는다는 사실은 절대로 피할 수 없다.

어떤 서브트리 내에서 읽기를 시도하지 않는다는 것을 reader에 알려 줄 어떤 방법이 필요하다. 즉 reader는 서브트리가 블록되었을 시점을 알 필요가 있다. 그래서 블록된 서브트리에 갇히지 않고, 트리의 다른 부분을 프로세스 할 수 있다. 서브트리 태그가 존재할 때, 좀 더 효과적으로 동작하도록 tree-walking singulation 프로토콜을 약간 개조한 방법을 생각할 수 있다.

예를 들면, 노드가 주어지면 기본 tree-walking 프로토콜이 서브트리에 있는 모든 나뭇잎에 다음 비트(노드에서 나뭇잎으로 향하는 가지에 있는 레이블)를 방송하도록 요구한다. 우선 reader가 특별한 질의에 응하도록 허용함으로써 프로토콜이 약간 증가할 수도 있다. "이 노드에서 rooted된 서브트리는 blocked 되어 있는가?" 만약에 blocked 되어 있지 않으면, 그때 reader는 표준 next bit 질문을 요구한다.

여기서 이것을 "polite blocking"이라 한다. 왜냐하면, 블로커 태그는 어느 서브트리가 블로킹되어 있다는 것을 선언하기 때문이다.

Polite 블로킹의 다른 형태는 서브트리 태그가 구현하고 있는 정책을 reader에게 알려 주는 것이다. 이렇게 하기 위하여, 우리는 먼저 열거한 정책 레이블 0, 1, …, k인 표준 영역에 대응한 각각의 "virtual" 태그 일련번호 t, t+1, …, t+k의 조그만 한 영역을 설계하여 사용한다. 프라이버시 정책 i를 구현하였다는 것을 나타내기 위하여, 블로커 태그는 일련번호 t+i를 갖는 태그의 존재를 시뮬레이션 할 수 있다.

다. 비용 요구 사항

블로커-태그 접근 방식은 구현 비용이 매우 적기 때문에 아주 매력적이다.

첫째, 일반적으로 consumer-product RFID 태그는 전혀 변경될 필요가 없다. RFID 태그는 값이 비싼 암호 방식을 원하지 않는다. 이는 전체 시스템 코스트 항목으로서 아주 중요한 사항이다.

둘째, 블로커 태그 자체가 매우 싸다. 블록 태그는 본질적으로 아주 적은 회로 변경을 동반한 한 두 개의 표준 RFID 태그로 구성된다.

셋째, 부수적으로 요구되는 구현이 아주 적다. 패스워드는 각 표준 RFID 태그를 관리하기 위해 필요하며, 그리고 프라이버시 영역을 변경하도록 권리를 부여하기 위해 필요하다. 이것은 이미 설명한 "kill" 명령을 위해 설명한 것과 같다.

2. 프라이버시 보호도구로서의 블로커 태그

고객의 프라이버시 보호를 위해 널리 이용되는 도구로서 매력을 확인시켜 주기 위해, 블로커 태그는 재고 관리와 같은 정상적인 RFID 기반 상업과정은 조금도 방해하지 않는 방식이다. 이 관점에서, universal 블로커 태그는 의도에 반대되고 있다.

프라이버시 개선을 목적으로, universal 블로커

태그 대신에 선택적인 블로커 태그 사용을 요구한다. 이는 프라이버시 보호를 위해 한 개 혹은 그 이상의 영역의 특별한 명령을 가지고 있다. 따라서 "프라이버시 영역"은 선택적인 블로커 태그에 의해 보호될 태그 일련번호(restricted number)로 구성된다. 선택적인 블로커 태그는 reader가 프라이버시 영역으로서 블로커 태그에 의해 규정된 영역에 들어갈 때마다 reader의 tree-walking 알고리듬 수행을 방해한다. 그리고 이외의 영역에서는 reading이 허용되며, 블로커 태그는 inactive 상태로 남는다.

프라이버시 영역과 태그 일련 번호의 동적 변경을 이용하여, 상인 및 고객이 동시에 만족할 수 있는 프라이버시 정책의 영역(natural range)을 구현하는 것이 가능하다. 우리는 사용하는 환경에 의존하여 프라이버시 영역 내외로 움직일 수 있는 일련번호를 갖는 시스템을 상상할 수 있다.

프라이버시 영역에 상응하는 선택적인 블로커-태그는 아주 간단하게 구현할 수 있으며, 이는 single 노드의 서브트리로 구성된다. 예를 들면, 그러한 영역이 일련번호 트리의 오른쪽 반으로 간단하게 구성된다. 즉 모든 일련번호가 leading bit가 1인 것을 의미한다.

예로, 어떤 슈퍼마켓에서는 leading bit가 '1'인 일련번호로 구성되는 프라이버시 영역을 갖는 블로커 태그를 사용하고 있다. 슈퍼마켓에서 패키지 각각은 재고 상품 관리 목적으로 사용될 유니크한 일련번호를 갖는 RFID 태그를 가지고 있다. 사전 프로그램에 의해, 제품이 슈퍼마켓 내부 혹은 창고에 있을 때 RFID 태그의 일련번호는 '0' bit로 시작한다. 이 때, 블로커 태그는 태그의 reading을 방해하지 않는다.

카운터에서 RFID 태그 reader가 구매로 고객에 제품(item)이 넘겨질 때, tag-specific key를 아이템의 RFID로 전송된다. 이것은 태그의 일련번호의 leading bit를 '1'로 되도록 유도한다. 슈퍼마켓은 블로커 태그로부터 자유롭게 물건을 제공한다. 이것은 카운터에서 쇼핑백에 넣거나 스티커를 아이템 위에 붙이는 방법이 있다.

고객이 슈퍼마켓의 쇼핑에서 집으로 돌아 왔을 때, 쇼핑백에서 상품을 끄집어 내거나 privacy-enhancing 스티커를 제거함으로써 프라이버시 영역에서 unmask 된다. 고객이 "smart" 냉장고에 물건을 넣으면, 냉장고에 부착된 RFID 태그 reader가 내용을 읽어 들인다. 이때, 연동된 컴퓨터는 물건 재고를 파악하여 다음에 구매하여야 할 물건의 목록을 프린트한다.

이와 같은 간단한 방식을 자연스럽게 AutoID 센터의 EPC-code 시스템으로 통합시킬 수 있다. EPC code는 96bit이며, 다음과 같이 나누어져 있다.

① 8bit header; ② 28bit "EPC 매니저" 코드는 태그를 소유하는 조직이 사용; ③ 24bit "object-manager" 코드는 EPC 매니저에 의해 결정되는 object 등급용으로 사용; ④ 36bit 일련번호는 object를 유일하게 구분하기 위해 사용한다. 따라서 표준 "프라이버시 bit"로 설계된 object manager code bit의 하나를 가짐으로써 지금까지 설명한 프라이버시 구조를 구현할 수 있다. 모든 블로커 태그는 그때 유일한 EPC 매니저 코드에 할당할 수 있다.

3. 악의적으로 이용 가능한 블로커 태그

블로커 태그가 어떻게 악의적으로 사용되는가를 설명하고, 그러한 행동에 대한 방어에 대해서 분석한다. 블로커 태그가 다중 ID의 시뮬레이션에 의해 의도된 RFID reader 프로토콜을 방해하는 방향으로 잘못 사용될 수 있다. 블로커 태그의 합법적인 프라이버시 응용은 multiple id를 방해하지만, 악의의 블로커 태그는 ID의 허용된 프라이버시 영역의 경계를 지키지 않는다. 이러한 universal 블로커 태그의 본성은 악의적이다.

RFID reader는 프라이버시 영역에서 의도된 블로커 행위와 조화를 이루도록 설계되어 있다. 그러나 기본적인 기능은 프라이버시 영역 외에서는 태그를 읽을 수 있다. 따라서 악의의 블로커 태그는 RFID reader 프로토콜에 대해 DOS 공격으로 주어진다. 그러한 공격은 간단하게 서비스를 교란하도록 설계되어 있다. 여기서는 모든 영역의 RFID 간섭 전략보다 DOS에 초점을 둔다.

악의의 블로커 태그의 기능은 actual 태그를 방해

하는 프라이버시 태그와 유사하다. 검출에도 불구하고, 공격은 성공되며, 주위에 있는 actual 태그는 reader에 의해 구별되지 못한다.

선택적인 악의의 블로커 태그는 좀더 정교할 수도 있다. 이는 검출을 피하기 위하여 태그의 특정 부분 방해를 시도할 수도 있다. 이처럼 분산 공격에도 불구하고, 속임수를 당한 태그의 수는 singulation 프로토콜을 지연시킬 만큼 충분히 클 수도 있다.

DOS 블로커 공격의 검출은 상대적으로 단순하다. 만약에 감지된 RFID 태그의 수가 어떤 타당성 있는 임계값(예를 들면, 계산대에서 1000개)를 초과하면, 공격이 진행중에 있다고 가정할 수 있다. 이러한 임계값 검출 방법은 간단하고 견고하다. 그 이유는 이것은 악의의 블로커 태그의 정확한 행위에 의존한 검출 방식이 아니기 때문이다. 즉 악의의 universal 혹은 선택적인 블로커 태그는 더욱 정교한 검출 메커니즘을 이용하며, 이것은 규정된 태그 ID 영역의 사용에 의존한다. 예를 들면, reader는 특정 제작자에 관련된 id 영역에서 매번 valid 태그를 나타내는 데이터베이스에 연결되어 있다. 태그 id는 이 영역 내에 있지만 만일 이 영역 내에 있지 않으면 부정으로 간주한다. 만약에 태그 ID가 적어도 부분적으로 불특정하다면, 공격자가 정확한 제품의 ID를 추정한다는 것이 거의 불가능하게 될 것이다.

V. 결 론

개인정보는 현재 정보화 사회에서 중요한 위치를 가지고 있는 웹 콘텐츠를 발전시키고 제공하는 서비스나 상품의 수준을 높이는 데 큰 역할을 하고 있고, 이러한 이용자의 개인정보는 수집자에 의해 데이터베이스화되고 이를 분석하여 마케팅에 활용할 수 있다. 그러나 정보화 사회의 역기능으로, 이용자의 개별적 동의나 인지 없이 개인정보를 무단으로 수집하거나 수집된 정보를 데이터베이스로 구축하여 이차적으로 사용하는 행위 등 여러 가지 문제를 유발시키고 있으며, 이러한 온라인 프라이버시 보호 문제를 해결하기 위해 기술적 및 제도적으로 해결하려는 시도가 이루어지고 있다.

본 논문에서는 이러한 기술적인 해결 방법으로 RFID 태그의 특성을 고려한 RFID 태그와 reader 사이에서 발생하는 프라이버시 문제에 대한 보호 메커니즘을 설명하고, 블로커 태그 개념을 적용한 프라이버시 보호, 즉 프라이버시 영역 설정에 의해 보호 가능한 개념을 나타냈다.

하지만, 다양한 개인 호스트에 저장된 프라이버시 정보의 유출 방지 및 중요한 개인정보 훼손을 차단하기 하기 위한 메커니즘 및 프레임워크 제시가 필요하다. 특히, 개인정보 보호를 위해 기술적인 해결 방법으로는 한계가 있으므로, 개인정보 제공을 위한 프레임워크를 구성하여 개인정보 등급별 프로파일 작성 및 이를 이용하는 개인정보 보호 메커니즘이 필요하며, 이를 통해 마지막으로 개인 정보 프로파일 구성 및 협상 메커니즘을 연구 개발하는 것이 요구된다.

참 고 문 헌

[1] M.K. Reiter and A.D. Rubin “Crouds: Anonymity for Web Transactions,” *ACM Trans. Info. Sysyt. Security 1*, 1998.

[2] D. Inoue and T. Matsumoto, “Rivulet: An Anonymous Communication Method Based on Group Communication,” *IEICE Trans. Fundamental*, Vol.E85-A, No.1, 2002.

[3] S. Sakata, “Security Technology for Mobile and Ubiquitous Communication,” *IEICE Magazine*, Vol.87, No.5, May 2004.

[4] T. Otsuka and A. Onozawa, “Users Privacy in Ubiquitous Network: Anonymous Communication Technique for Ad-hoc Network,” *Technical Report of IEICE ISEC2003-38*, July 2003.

[5] Junichiro Saito and Kouichi Sakurai, “Privacy Protection Using Re-encryption in RFID Tags,” *Technical Report of IEICE ISEC2003-81*, Nov. 2003.

[6] P. Golle, M. Jakobsson, A. Jules, and P. Syverson, “Universal Re-encryption for Mixnets,” 2002, http://www.rsasecurity.com.

[7] A. Juels, “Privacy and Authentication in Low-Cost RFID Tags,” 2003, http://www.resasecurity.com.

[8] A. Jules, R. Rivest, and M. Szydlo, “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,” 2003, http://www.rsasecurity.com.