Journal of Digital Contents Society Vol. 6. No. 4. December. 2005(pp. 267-272)

유비쿼터스 컴퓨팅 환경에서 RFID 보안 기술에 대한 연구

방기천*

요 약

유비쿼터스 컴퓨팅 환경은 미래 생활을 대변하는 새로운 패러다임으로 IT와 개인 생활에 많은 변화를 일으킬 것으로 기대된다. 그러나 유비쿼터스 컴퓨팅 환경은 방대한 정보를 언제 어디서든 획득할 수 있고, 공유할 수 있어서 보안위협 및 개인의 프라이버시 침해와 같은 역기능의 문제가 심화되고 있는 추세이다. 본 논문에서는 유비쿼터스 컴퓨팅 환경에서 RFID 기술 도입에 따른 역기능을 최소화하기 위한 방안에 대해 연구하였다. 본 논문에서는 유비쿼터스 컴퓨팅 환경의 중요한 부분인 RFID 시스템에서 발생할 수 있는 보안 및 프라이버시 위험요인들과 보안 요구사항에 대해 알아보았다. 그리고 이러한 위험요인에 대해 현재 진행되고 있는 기술적 해결방법들을 살펴보았다.

A Study on the RFID Security Technologies in Ubiquitous Computing Environment

Kee-Chun Bang*

Abstract

The ubiquitous computing environment is a new paradigm that represents the future life and is expected to bring about great changes in IT and in the lives of individuals. However, since a good deal of information can be easily obtained and shared in the ubiquitous computing environment, problems such as a security threat and infringement of privacy are getting serious. The present study is intended to explore some ways to minimize such problems by introducing RFID technology in the ubiquitous computing environment. This study also examines the causes of violation of security and privacy that might occur in the RFID system and requirements for security. In addition, it seeks possible technical solutions to those causes.

Key words : Ubiquitous Computing, RFID, Privacy, Security

1. 서 론

유비쿼터스 컴퓨팅(Ubiquitous Computing)은 제록스 PARC(Palo Alto Research Center) 연구소의 마크와이저(Mark Weiser)에 의해 1988년에 처음으로 제시된 개념이다. 당시 마크와이저는 컴퓨터와 네트워크 및 인간이 융합된 환경을 조성하는 것이 유비쿼터스 컴퓨팅의 목표라고 주장하였다. 전자 공간과 결합된 물리공간은 와이저가 상상 했던 것보다 훨씬 거대한 변혁을 가져오고 있다. 인터넷혁명 이전을 물리공간(1 공간)이라 하면, 인터넷혁명 이후의 공간을 전자공간(2 공간)이라 할 수 있고, 전자공간과 물리 공간이 융합된 제 3의 공간이 유비쿼터스 컴퓨팅 공간으로, 컴퓨터뿐만 아니라 가전 등 다양한 디바이스까지도 네트워크에 접속하여 정보의 제공과 획득이 가능한 공간이다. USN(Ubiquitous Sensor Network)은 필요한 모든 곳에 네트워크 접속하여 정보를 제공하거나 수신할 수 있는 통신 기능을 갖춘 센서를 부착하고 이를 통하여 사물의 인식정보는 물론 주변의 환경정보까지 탐지하여 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 것을 의미한다[1].

RFID(Radio Frequency IDentification)는 이러한 유비쿼터스 컴퓨팅의 실현을 위한 중요한 기술로서, 무선 기술과 소형칩을 이용하여 사람 또는 사물의 인식과 식별이 가능하도록 하며, 이를 바탕으로 사용자 또는 네트워크는 접속 새로운 부가 정보를 생산·수용하게 된다. RFID 기술은 단순히 바코드를 대체할 자동인식 기술의 한 부분이 아니라 네트워크와 사물을 연결하는 유비쿼터스 컴퓨팅 응용의 중간자로서 발전과 활용이 더욱 부각될 것으로 기대된다[2].

* 본 연구는 2005년 남서울대학교 교내연구비 지원에 의하여 수행되었음.

※ 제일저자(First Author) : 방기천
접수일 : 2005년 8 월 29 일, 완료일 : 2005년 12 월 1 일
* 남서울대학교 멀티미디어학과 교수
bangkc@nsu.ac.kr

그러나 이러한 RFID 기술의 확산은 개인 신상정보 노출에 따른 개인의 사생활 침해와 같은 역기능의 새로운 문제를 야기할 것으로 우려되고 있다. 이것은 RFID 기술이 정보접근의 매개역할을 하는 태그식별정보가 개인이 알지 못하는 사이에 당사자의 허가 없이 오용될 가능성을 내재하고 있기 때문이다 [3].

기존의 정보시스템의 정보보호를 위해 제시된 기술적, 법·제도적 방안들을 RFID 기술을 위하여 그대로 적용하는 데는 많은 문제점을 갖고 있다. RFID 정보시스템의 경우에 사용되는 태그 식별정보는 개인과는 무관한 것처럼 보이는 개인이 사용하는 제품이나 서비스들의 정보이지만, 이후 처리 과정에 따라 개인화 되어 지금의 개인정보와 유사한 수준의 정보로 까지 추출 될 수 있기 때문이다. 또한 유비쿼터스 컴퓨팅 환경에서는 이렇게 추출된 정보가 고속·광대역 통신 인프라를 통해 바람직하지 않은 목적을 위해 급속히 유포될 수 있기 때문이다.

본 논문에서는 유비쿼터스 컴퓨팅 환경에서 RFID 기술 도입에 따른 역기능을 최소화하기 위한 방안에 대해 연구한다. 유비쿼터스 컴퓨팅 환경에서 개인이 인식하지 못하는 중에 노출되는 개인정보의 침해와 같은 역기능은 RFID 보급에 있어 장애 요인이 될 것이다. 본 연구에서는 2장에서 RFID의 특징과 보안의 취약점을 설명하고 3장에서는 살펴보고 3장에서는 RFID 시스템에서 발생할 수 있는 보안위협에 대해 알아본다. 4장에서는 RFID 보안의 제약사항과 보안위협을 해결하기 위해 제시되고 있는 기법들을 검토하고 5장에서는 결론을 맺는다.

2. RFID의 개요 및 프라이버시 위협

RFID는 사물에 전자 태그(Tag)를 부착하여, 사물이 주위 상황을 인지하고 정보시스템과 실시간으로 정보를 교환하고 처리할수 있는 기술이다. RFID는 리더의 안테나를 통해 접촉하지 않고 태그의 정보를 판독하거나 인식하는 객체인식 기술 중의 하나이다. 다양한 물품에 부착되는 RFID 태그는 칩과 안테나로 구성되고, 칩에는 사물의 유일한 식별코드와 정보를 저장하며 리더의 요청에 의해 또는 상황에 따라 스스로 외부에 자신의 정보를 송·수신하게 되며, 그림 1과 같이 RFID 시스템을 구성하게 된다[4].

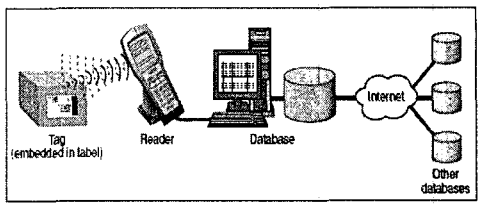

그림 1. RFID 시스템의 구성요소

RFID의 시스템은 크게 태그와 리더기 및 데이터베이스로 구성된다. 태그는 리더기의 요청에 응답하는 트랜스폰더(Transponder)로서 각각의 고유한 시리얼 번호를 저장하고 있다. 리더기는 태그에 정보를 요청하고 수신한 데이터를 판독하여 태그를 인식한다. 데이타베이스는 리더기 태그로부터 수집한 정보를 저장하거나 태그 또는 리더기를 대신하여 복잡한 연산을 수행한 후 서버 리더기에서 수집된 정보의 진위 여부를 판단해주는 역할을 수행한다.

RFID 태그는 전원 공급 요소에 따라 수동형(Passive)과 능동형(Active)으로 구분된다. 수동형 태그는 태그 자체적인 전원을 따로 가지고 있지 않기 때문에, 데이터 전송을 위해서는 리더가 보내는 전파를 이용하는 후방산란(Backscatter) 변조 방식을 사용한다. 반면 능동형 태그는 자체적인 전원 공급 장치를 가지고 있기 때문에 리더의 전파를 이용할 필요가 없다. 근본적인 작동 방식에 차이가 있기 때문에 수동형 태그는 가격이 저렴하고 반영구적으로 사용 가능한 장점을 얻을 수 있지만, 인식 거리가 짧다는 단점을 가지고 있으며, 능동형 태그는 자체 전원 공급 장치로 인해 단가가 올라가 고 태그의 수명이 제한되는 단점이 존재한다.

RFID 태그는 이 밖에도 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 가능형이 있다. 쓰기 가능한 메모리를 탑재한 경우, RFID 태그의 ID 정보를 reader/writer라 부르는 무선통신 장치에 의해 써넣기가 가능하다. 이 밖에 도 RFID 태그는 무선자원을 사용하기 때문에 주파수 대역에 따라 구분할 수도 있다.

RFID 시스템을 이용하면, 상자 속에 태그가 부착된 상품 인식이 가능하기 때문에, 상품의 재고 관리나 물류 관리에 이용된다. 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.

RFID 시스템은 전파를 이용하는 특성상 태그, 리더기, 데이터베이스간의 통신 과정에서 개인의 프라이버시 침해 위험이 높다. 특히 태그와 리더기간의 통신은 RF 신호를 사용하기 때문에 주고 받는 내용을 쉽게 도청할 수 있다.

3. RFID 보안 위협의 특징 및 보안 위협 유형

3.1 RFID 보안 위협의 특징

USN 환경에서의 보안공격 및 침해 대상은 표 1에서와 같이 컴퓨터에 저장된 정보나 데이터 또는 통신 인프라가 아닌, 사물이나 신체 등 개인의 모든 정보가 된다. 또한 보안공격 및 침해의 범위는 개인의 컴퓨터에 국한되지 않고, 개인의 사적인 모든 공간이 될 것이다. 따라서 태그 및 센서 정보의 무단 누출, 위/변조, 오동작, 개인화 정보의 불법 수집 및 유통과 같은 것에 대한 정보보호 보완대책이 필요하다.

RFID 보안위협의 특성은 보안위협 대상이 모든 USN에 의하여 연동되는 모든 장치로 공격 및 피해 범위가 광범위하게 될 경우가 많아지며, 통신 환경에 대한 신뢰성을 보장할 수 없게 된다. 또한 사물에 부착된 태그와 리더 사이의 정보 흐름에 대한 도청으로 태그에 저장된 정보와 소유자의 개인정보의 노출 등 기밀성을 침해하는 위협이 크게 증가할 것이며, RFID 등에 수록된 정보를 변조시키거나 위조하는 등의 위협도 증가할 것이다[5].

USN 환경에서는 태그 리더 영역, 미들웨어 영역, 서비스 인프라 영역에서 USN 서비스의 안전성을 제공할 수 있는 정보보호 기술 개발과 함께 개인 프라이버시를 적극적으로 보호하고 사물의 자동 인식, 이력 추적 등 RFID/USN 서비스를 안전하게 제공할 수 있는 초경량 정보보호 기술 및 시스템 개발이 요구되며, 손상된 태그나 센서가 야기 시키는 유해 트래픽을 식별 위협을 조기에 탐지할 수 있도록 네트워크 모니터링 체계 확대가 필요하다.

표 1. 구성 요소별 주요보안 취약점과 보안 요구사항

구 분	보안 취약점 및 보안 요구사항
RFID	- 태그정보의 위/변조, 리더(Reader)기 위장, DOS 공격 - 제 3자의 타인정보 유출 - 개인정보 보호 침해 및 신용정보 해킹
USN	- 악의적 공격자로부터의 태그정보의 접근시도 - Reader기의 도청 - 데이터에 대한 기밀성과 무결성의 위/변조 - RFID/USN 노드간의 상호 인증 오류

3.2 RFID 보안 위협의 유형

RFID 기술은 활용상의 방안 등으로 볼 때 개인의 프라이버시 침해위험이 매우 높다. 미국의 EPIC (Electronic Privacy Information Center)는 RFID를 이용하는 환경에서의 프라이버시 위험요인을 표 2와 같이 분석하고 있다. 또한, RFID 태그 시스템에서 보호되지 않은 태그는 도청(Eavesdropping), 트래픽 분석(Traffic analysis), 스푸핑(Spoofing) 혹은 서비스 거부 공격(Denial of service) 등의 공격에 취약하다 [6].

표 2. EPIC의 RFID 프라이버시 위험요인

구 분	설 명
숨겨진 태그장소	- RFID 태그들이 소유주인 개인들이 알지 못한 상황에서 사물들과 문서에 내장되어질 수 있음. - 무선전파는 섬유, 플라스틱, 다른 물질들을 쉽게 조용하게 통과할 수 있기 때문에 지갑, 쇼핑백, 옷가방 등에 들어있는 사물 또는 옷에 부착된 RFID 태그들을 읽을 수 있음.
전세계 모든 사물들을 위한 유일한 식별자	- 전자제품코드(EPC)는 지구상에 있는 모든 사물에 유일한 ID를 가지게 할 수 있음. - 유일한 ID 번호의 사용으로 개별 물리적인 사물이 판매 또는 이전 시점에서 신원이 확인되고 구매자 또는 소유자와 연결될 수 있는 전세계적인 사물 등록 시스템의 창조가 가능.
대규모 데이터 통합	- RFID 배치는 유일한 태그 데이터를 포함하고 있는 대량 데이터베이스의 개발을 요구 - 이들 기록들은, 특히 컴퓨터 메모리와 프로세스 능력이 확장되면서, 개인신원확인 데이터와 연결될 수 있음.
숨어있는 리더	- 인간 또는 사물이 모여져 있는 어떤 환경에서도 보이지 않게 섞여질 수 있는 리더들에 의해 태그들은 시야의 제한없이 멀리서 읽혀질 수 있음 - RFID 리더들은 이미 실제로 바닥 타일들에 내재되어 소비자들이 언제 또는 "스캔"되고 있는지 없는지에 대한 인식을 불가능하게 하고 있음
개인추적과 개인정보 프로파일	- 개인적인 신원이 유일한 RFID 태그 넘버와 연결되어 있다면 개인들이 인식하지 못하는 사이에 프로파일(profile)되고 추적당할 수 있음

○ 도청공격(Eavesdropping) : 태그와 리더사이의

통신은 무선 방식이기 때문에 누구든지 태그에 접근하여 태그의 출력 값을 얻을 수 있어, 인가되지 않은 리더가 적절한 접근 제어기능이 없는 태그에 접근하여 프라이버시를 침해할 수 있음. 도청자가 사용자의 지갑 혹은 가방의 내용물을 스캔할 수 있음.

○ 트래픽 분석(Traffic analysis) : 태그의 내용이 보호되고 있다 하더라도, 예측되는 태그의 응답 값은 태그와 태그 소유자의 신원(Identity)을 연결시킬 수 있는 정보를 제공해 줌. 태그 가 유일한 식별정보를 노출하지 않는다 하더라도 태그의 응답 값에 대한 분석을 통해 태그를 소지한 사용자를 추적할 수 있음. 이 공격은 RFID 태그가 의류, 제품 등에 부착하여 사용자를 추적할 수 있는 위치 프라이버시(Location Privacy)에 대한 위험요인임

○ 스푸핑(Spoofing) 공격 : 스푸핑 공격이란 외부의 악의적 침입자가 자신이 사전에 지정한 코드가 작동되도록 함으로써 사용자의 권한을 획득하는 해킹 기법. 일반 사용자의 태그를 스푸핑한 공격자는 자동화된 체크 아웃 혹은 보안 시스템을 속일 수 있으며, 스푸핑된 데이터로 값싼 물품과 비싼 물품을 교체할 수 있음.

○ 서비스거부(Denial of Service) 공격 : RFID 시스템자원에 대한 정상서비스를 방해하기 위해공격으로, RF 신호 채널을 방해하거나, 임의의 다른 수단으로 태그를 무력화시키는 등이 해당됨.

○ 세션 가로채기(Hijacking), 재생(Replay) 공격, 중간자 공격(Man In the Middle Attack) : RFID 리더와 태그사이의 상호인증을 위한 인증 프로토콜 수행 시 발생할 수 있는 공격들로, 인증된 세션을 가로채는 세션 가로채기 공격, 공격자가 검증자에게 이전에 수행되었던 프로토콜 부분 중 일부분을 다시 실행시키는 재생 공격, 공격자가 인증 프로토콜 수행 중간 에 자신의 정보를 삽입하는 중간자 공격 등이 있음.

○ 물리적(Physical) 공격 : 태그의 메모리는 내용을 노출시키게 하는 물리적 공격에 취약함. 즉 스마트카드에 적용될 수 있는 프로브공격, TEMPEST공격 등의 물리적 공격이 RFID 태그 메모리에도 적용될 수 있음. 이러한 공격에 강인한 메모리가 RFID 태그에 사용되기에는 비용이 너무 비싸진다는 문제점이 있음. 또한, 향후 스마트카드처럼 암호알고리즘을 지원하는 태그가 설계되는 경우, 스마트카드에 적용될 수 있는 전력해석(Power Analysis), 타이밍 해석(Timing Analysis) 등의 사이드채널공격(혹은 부채널 공격)에 대한 위험요인도 존재할 수 있음.

4. RFID 보안의 제약사항 및 보안 기법

4.1 RFID 보안의 제약사항

RFID 태그 중 가격이 싸며 작은 태그 중의 하나는 Atmel TK5552이다. 이 태그는 992비트의 저장공간을 가지고 있으며, 데이터 전송 비율은 약 초당 100kB이다. 또한, 메모리의 내용에 대한 읽기/쓰기를 허용하고 $1.0로 판매가 되고 있다. 그러나 향후 보편적으로 사용될 RFID 태그는 US$0.05~US$0.1의 가격범위에 있기 때문에 강력한 암호화 기법을 사용하는 것은 현실적으로 가능하지 않다. 낮은 가격의 범위를 벗어나지 않으면서 보안 및 프라이버시 위험을 고려한 태그 및 리더의 설계가 중요한 문제가 되고 있다. 저렴한 RFID 태그는 기본적으로 패시브 형태의 사용을 요구하고 있으며, 저렴한 태그의 비용 요구사항(5센트 이하)은 태그가 사용할 수 있는 전력, 처리시간, 저장 공간, 게이트 수 등의 자원을 제한한다. 5센트의 태그를 만들기 위한 IC 칩 비용은 2센트를 넘으면 안되며 이는 게이트 수를 7.5K~15K 게이트로 제한한다. 현재 100비트의 EPC 칩은 약 5~10K 게이트를 요구함에 따라, 안전성 측면에서 요구되는 게이트의 수는 2.5K~5K를 넘어서면 안 되는 제약조건을 갖고 있다[7]. CRYPREC 보고서에 따르면 대칭키 암호알고리즘의 구현이 6~13K게이트로 알려져 있으며 대칭키를 기반으로 설계할 수 있는 해쉬 함수도 유사한 수의 게이트가 요구될 것으로 기대된다. 더 적은 게이트 수가 요구되는 Tiny Encryption Algorithm이 저렴한 RFID 태그에 앞으로는 사용될 수 있는 가능성이 있으나 현재 사용하기에는 비싸다.

또한, 대칭키 암호에 비해 더 많은 게이트 수가 요구되는 공개키 암호를 RFID에 사용하기 위해서는 더 비싼 비용이 소요될 것으로 기대할 수 있다. 현재 NTRU社는 NTRU 공개키 암호기법을 RFID와 비접촉형 스마트카드에 적용한 솔루션 GenuID를 개발하였으며, 비접촉형 스마트카드에 NTRU 암호기법을 구현 할 경우 약 $2의 비용이 소요될 것으로 예측하고 있다. 그러나 NTRU 공개키 암호도 저렴한 RFID 태그에서 이용할 수 있는 리소스 이상을 사용하기 때문에 현재 5센트 이하의 저렴한 RFID태그에 적용할 수는 없고 더 비싼 스마트 태그에서 사용하여야 한다.

4.2 RFID 보안 기법

(1) AutoID 센터의 Kill Tag 기술

사용자의 프라이버시를 보호하는 일반적인 방법으

로 AutoID센터가 제안한 Kill command 기법이 있다. 이 방법은 8비트의 패스워드를 포함한 kill command를 전송해 사용자에게 태그가 주어지기 전에 태그의 기능을 정지시키는 기법이다. 태그의 기능이 정지됨으로써 사용자의 프라이버시를 보호하는 방법이지만 kill command가 적용된 뒤에는 재사용이 불가능하기 때문에 이 방법은 넓은 응용환경을 지원하지 못하는 단점을 가지고 있다. 예를 들어, 지속적인 물리적 접근통제, 소유물에 대한 도난방지, 무선 현금 카드 등의 활용에서는 사용자가 태그를 소지하고 있는 동안 태그가 작동되어야 하기 때문이다.

(2) Faraday Cage 기술

이 방법은 전파 신호가 투과되지 않도록 하는 금속 혹은 망으로 만들어진 컨테이너 (Faraday Cage)를 이용한다. 현재 미국의 mobileClock社는 태그의 내용을 허가되지 않은 리더가 읽는 것을 방지하기 위해 라디오 신호가 투과되지 않도록 하는 "mClock"제품을 판매하고 있다. Faraday Cage방법도 사용자의 프라이버시를 보호해주는 부분적인 해결책이라 할 수 있다.

(3) Active Jamming 기술

이 방법은 근처에 있는 RFID 리더의 기능을 막거나 혹은 방해할 수 있는 라디오 신호를 브로드캐스트 하는 디바이스를 이용하는 것이다. 이 디바이스가 라디오 신호에 대한 전파방해를 수행함으로써 태그가 노출하는 정보를 보호할 수 있다. 그러나 이러한 접근법은 근처에 있는 모든 RFID 리더가 작동되지 않도록 방해할 수 있기 때문에 매우 강력한 해결책이라 할 수 있다.

(4) MIT의 해쉬-락 기술

MIT는 저렴한 비용(5센트 이하)의 태그에서 리소스 제한문제를 해결하면서 인가 받은 리더에게만 태그 정보를 전송하기 위한 방법으로, 해쉬-락 방법을 제안하였다. 이 방법은 낮은 비용의 태그의 리소스 제한을 해결하기 위해 태그에 하드웨어적으로 최적화되어 구현된 해쉬함수만을 가정하고 있다.

시스템의 초기화 과정은 다음과 같다. 태그를 잠그기 위해 태그 소유자는 태그의 metaID로랜덤 키의 해쉬값 metaID=hash(key)를 저장한다. 태그를 잠근 뒤 소유자는 key와 metaID를 백엔드 데이터베이스에 저장하게 되며 metaID값이 할당되자마자 태그는 잠금 상태로 된다. 이 방법은 일방향 해쉬함수의 역원을 구하는 어려움에 기반 하여 인가되지 않은 리더가 태그 의 내용을 읽어내는 것을 방지하는 방법이다. 하지만, metaID가 ID대신 여전히 식별자의 역할을 수행하기 때문에 사용자가 추적 될 수 있는 문제를 완벽하게 해결하지 못한다.

(5) MIT의 Silent Tree Walking 기술

이 방법은 리더에서 태그로 가는 전방향(Forward) 채널의 강인한 신호에 대한 도청자로부터 안전하게 하는 방법이다. Binary tree walking anti-collision 알고리즘은 리더가 태그 ID의 각 비트를 브로드캐스트하기 때문에 전방향 채널에 존재하는 도청공격에 취약한 문제점이 있다. MIT가 제시한 Silent tree walking 알고리즘은 이러한 안전하지 않은 태그의 ID를 리더가 브로드캐스트 하지 않아, 도청공격에 안전하면서 binary tree walking 알고리즘과 유사한 수행속도를 갖도록 변형한 변형기법이라 할 수 있다.

(6) RSA사의 Re-Encryption 기술

RSA사의 Ari Juels et al. 이 태그가 부착된 지폐를 이용 시 발생할 수 있는 프라이버시 위험을 해결하는 하나의 방법으로, 제안한 Re-Encryption 기법은 태그가 노출할 수 있는 정보를 보호하면서 법 집행기관이 지폐를 추적할 수 있는 기술이다. RFID칩을 지폐에 내장하게 되면, 인식기 근처를 통과시키는 것만으로 많은 양의 지폐의 진위를 정확히 판별할 수 있다. 또한 지폐의 유통과정이 그대로 기록돼, 돈세탁이나 불법자금 유통까지도 추적이 가능하다.

이에 유럽은행(ECB)는 2005년까지 Euro 지폐에 RFID 태그를 부착하는 계획을 제안하였으나 기술적으로 상세한 해결방안은 공개하지 않은 상태에 있다. 최근 일본 히타치는 연성이 강한 0.03㎜ 두께의 초소형 RFID칩(뮤칩)을 개발하여, 유로(Euro)화에 내장시키는 프로젝트를 유럽중앙은행(ECB)과 진행 중인 것으로 알려져 있다. 이전의 MIT의 해쉬-락 기법은 고정된 키 값을 해쉬한 metaID값을 사용함으로써 ID에 대해 일정 고정된 값을 유지하기 때문에 지폐 추적문제를 방지하지 못한다. Re-encryption 기술은 태그가 전송하는 ID의 암호문의 형태를 계속적으로 변경하는 것으로 ElGamal 암호기술을 이용하여 설계할 수 있다.

(7) RSA사의 Blocker Tag 기술

Blocker 태그란 RFID 태그 위에 붙이는 것으로 RFID 리더장치를 혼란시켜 태그의 데이터 송신을 무효로 함으로써 개인이나 상품에 관한 데이터를 추적할 수 없게 설계한 통신방해 기술이다. Blocker가 태그에 부착되어 있을때 데이터 추적으로부터 보호될 수 있으며, Blocker 태그가 제거될 때, 태그는 평상시처럼 사용될 수 있다. 이 방법은 기본적으로 RFID 리더가 사용하는 Singulation 프로토콜을 선택적으로 블로킹하는 방법에 기반하고 있다. 많은 Singulation 프로토콜이 있지만 실제적으로 915Mhz

에서 이용되는 Tree walking 방식을 기반 하여 블로킹 하는 방법을 말한다. 13.56MHz에서 작동되는 태그는 Singulation 프로토콜로 ALOHA 프로토콜을 이용하며, Tree walking 방법에서와 유사하게 ALOHA 블록커 태그를 만드는 것이 가능하다.

(8) NTT사의 순방향 안전성이 보장되는 기술

NTT사는 태그의 비밀정보가 향후 템퍼링 등에 의해 노출되어도 이전 전송된 데이터가 여전히 안전하다는 것을 보장해 주는 순방향 안전성(Forward Secure)을 보장해주는 방법을 제안하였다. 태그의 안전성 요구사항을 구별불가능성(Indistinguishability)과 순방향 안전성(Forward Security)으로 정의하였으며 이를 만족하는 방법으로 저렴한 비용의 해쉬 체인 메커니즘을 이용하였다.

5. 결 론

유비쿼터스 컴퓨팅 환경은 미래 생활을 대변하는 새로운 패러다임으로 IT와 개인 생활에 많은 변화를 일으킬 것으로 기대된다. 그러나, 지금의 통신 환경이 유비쿼터스 환경으로의 진화함에 따라 이전과 달리 방대한 정보를 언제 어디서든 획득할 수 있고, 공유할 수 있어 보안위협 및 개인의 프라이버시 침해와 같은 역기능의 문제가 심화되고 있는 추세이다. 유비쿼터스 컴퓨팅 사회의 성공을 위해서는 모두의 적극적이고 자발적인 참여와 미래 사회에 대한 두려움이나 부작용을 최소화시킬 때 가능한 일이다.

본 논문에서는 유비쿼터스 컴퓨팅 환경의 중요한 부분인 RFID 시스템에서 발생할 수 있는 보안 및 프라이버시 위협요인들과 보안 요구사항에 대해 알아보았다. 그리고 이러한 위협요인에 대해 현재 진행되고 있는 기술적 해결방법들을 살펴보았다.

이를 통하여 향후 RFID 시스템에서 연구 되어야 할 분야 중의 하나는 저렴한 비용의 RFID에 적용할 수 있는 해쉬함수, 난수 생성기, 대칭키 암호알고리즘, 공개키 암호 알고리즘 등에 대한 개발 및 구현이라는 것을 알 수 있었다. 또한, 이러한 암호화 기법을 이용하는 프로토콜들은 RFID 태그가 스마트카드에 비해 보안 위협에 취약할 것이므로, 프로토콜 설계시 본 논문에서 제시한 보안 위협사항들을 고려하여야 할 것이다. 이러한, 저렴한 비용의 암호화 기법에 대한 하드웨어 구현 또한 전력 소모 및 필요 게이트 수의 최소화를 고려하여 설계해야할 것이다.

참 고 문 헌

[1] Kay Romer and Friedemann Mattern, "The design space of wireless sensor networks," IEEE Wireless Communications, Vol. 11, No. 6, pp. 54-61, Dec. 2004.

[2] 김완석, "RFID의 과제와 전망", IITAITFIND 주간기술동향 제1164호, 2004. 9.

[3] 한국전산원, 전파식별(RFID)보급 활성화를 위한 역기능 및 정보보호 대책 연구, 최종보고서, 2004. 11.

[4] GAO, http://www.gao.gov/.

[5] KAKI, http://http://webzine.kali.or.kr/.

[6] IT리포트, http://www.eic.re.kr .

[7] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, "Cryptographic Approach to Privacy-Friendly Tags," submitted 2003.

방 기 천

1981년 서울대학교 전자공학과(학사)
1988년 성균관대학교 정보처리학과 (석사)
1996년 성균관대학교 전산통계학전공 (박사)

1984년-1995년 MBC 기술연구소
1995년-현재 남서울대학교 멀티미디어학과 교수
관심분야 : 멀티미디어컨텐츠, 멀티미디어 응용, 인터넷 방송 등