RFID 객체검색서비스 보안 기술

이 신 경* 박 남 제** 최 두 호*** 정 교 일****

◈ 목 차 ◈

1. 서 론

RFID(Radio Frequency Identification) 네트워크는 RFID 검색서비스와 RFID 코드와 관련된 정보를 저장하고 있는 RFID 정보서비스, 그리고 이력정보가 저장된 위치정보를 가진 RFID 이력서비스, 다수의 리더로부터 들어오는 정보를 수집 및 여과하는 미들웨어, RFID 태그로부터 RFID 코드 및 관련정보를 무선주파수로 수집하는 리더, 무선주파수를 이용하여 상품을 식별하기 위한 초소형 IC칩과 안테나가 내장된 태그 등으로 구성된다[1].

본 문서는 RFID 구성요소 중 EPC(Electronic Product Code) 코드에 대한 데이터를 찾고 그 데이터에 대한 접속 승인을 담당하는 RFID 객체검색서비스의 보안에 대하여 설명하는 것으로서, 'ONS Security'[7] 문서를 기본으로 작성되었다.

* 한국전자통신연구원 선임연구원
** 한국전자통신연구원 선임연구원
*** 한국전자통신연구원 선임연구원, 팀장
**** 한국전자통신연구원 책임연구원, 마케팅기술위원

본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업(2005-S-088-04, 안전한 RFID/USN을 위한 정보보호기술) 사업의 일환으로 수행하였음

2. EPCglobal 네트워크와 ONS

2.1 EPC와 ONS

EPC는 EPCglobal에서 정의한 전자 제품 코드로 모든 단일 제품을 유일하게 식별할 수 있도록 고유의 번호인 96bit ID를 가진다. RFID 태그의 마이크로 칩에 내장된 EPC ID는 무한한 양의 동적 데이터가 저장되는 데이터베이스와 연결하여 다양한 정보를 이용할 수 있다. EPC가 필요한 정보를 얻기 위해 직접 해당 정보를 가지고 있는 정보서버(EPC Information Server)에 접근하는 정적인 방법은 막대한 양의 정보들이 매번 새로운 정보들로 업데이트되어 제공되는 동적인 변화에 적응할 수 있는 한계가 있기 때문에 그 해결책으로 제시된 것이 바로 객체검색서비스(ONS) 이다.

ONS(Object Naming Service or Object Name Service)는 글로벌 검색서비스를 제공하는 구성요소로 국내 RFID 네트워크에서는 ODS(Object Directory Service)로도 명명되고 있다. ONS의 주요 기능은 EPC에 대응되는 1개 또는 여러 개의 URL(Uniform Resource Locator; 논리적 주소)를 변환시켜 주며, 이 URL을 이용하여 인터넷 프로토콜(IP)주소를 찾을 수 있다. 이렇게 획득한 정보서버의 IP를 통해 정보서버와의 연결이 이루어지면 여기에서 해당 EPC의 상품이나 케이스, 팔레트 등에 대한 상세 정보를 얻게 된다.

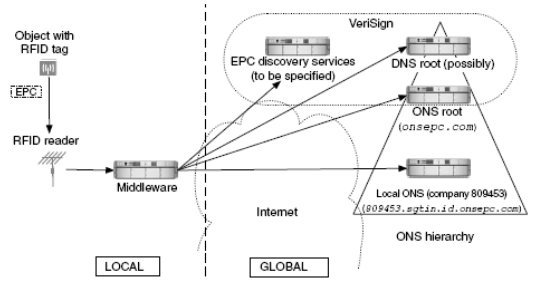
2.2 EPCglobal 표준

EPCglobal에 대한 표준은 유통물류의 국제 표준화 기구인 EAN(Europe Article Number)/ UCC(Uniform Code Council) 산하의 RFID 표준화를 선도하고 있는 'EPCglobal'에서 진행되고 있다. MIT를 중심으로 1999년 Auto-ID 센터를 설립하여 자발적인 RFID 기술연구를 추진하기 시작하여 2003년 EAN/UCC (현재 GS1로 명칭 변경)의 통합단체로 흡수되면서 RFID 기술보급 및 활성화 중심의 현 체제로 전환되었다. 현재 바코드뿐만 아니라 여타 상거래 시스템에 대한 글로벌 표준을 감독/보호하고 있으며 다수의 리더와 태그 제조업체 및 이와 관련된 업체들이 EPCglobal 회원으로 가입하고 있다[2].

3. ONS 보안 취약점

3.1 EPCglobal 통신절차

웹이나 메일에서 http://www.naver.com 같은 URL이라는 고유의 식별자를 사용하듯이 EPC를 사용하는 네트워크 시스템에서는 "urn:epc:id:sgtin:809453.1734.108265"와 같은 EPC URI(Uniform Resource Identifier)를 사용함으로써 각각의 객체를 식별한다. 그리고 URL 정보를 숫자로 이루어진 IP 주소로 해석해주는 DNS(Domain Name System)처럼 EPC의 URI를 가지고 있어 요청이 있을 경우 해당 객체의 정보를 찾을 수 있도록 도와주는 시스템이 바로 ONS이다. ONS 시스템을 포함하는 EPCglobal의 통신 절차는 그림과 같다.



(그림 1) EPCglobal 네트워크

ONS의 작동을 간단하게 설명하면, 어떤 한 물품에 대한 정보를 얻기 위해서 EPC는 ONS가 이해할 수 있는 형태의 질의를 이용하게 된다. 태그로부터 읽어 들인 순수한 EPC 정보는 비트 값이기 때문에 로컬시스템의 미들웨어는 이를 URI의 형태로 바꾸어 ONS로 질의를 해야 한다. ONS는 이 질의를 받아 하나 이상의 서비스가 가능한 URL을 반환하게 되고, 로컬의 미들웨어에서는 사용자가 반환된 URL 정보를 이용하여 정보를 가지고 있는 EPCIS로 접속하게 된다. ONS와의 통신절차 및 방법은 기존의 DNS기술을 기반으로 구현되어 있어 ONS를 DNS의 서브시스템으로 분류하기도 한다[2,4].

ONS는 계층구조를 살펴보면 기본적으로 ONS 루트 서버, 사용자의 로컬 호스트에 존재하는 ONS 로컬 서버 및 캐시로 구성된다.

루트 ONS는 기존의 루트 DNS와 유사한 구성을 가지며 서비스 또한 질의된 RFID 코드의 도메인 네임으로부터 RFID 코드와 관련된 EPCIS의 URL을 가지고 있는 로컬 ONS의 주소 값을 제공한다. 루트 ONS는 다시 2계층으로 나뉘어서 관리되며, 계층 1은 루트 ONS의 도메인인 "onsepc.com"이라는 이름으로 된 파일을 가지고 있어 RFID 코드의 분류에 따라 할당된 기관들의 도메인 네임 정보를 저장하고, 계층 2는 ONS 위임서버로 각각의 기관별로 로컬 ONS의 주소를 가진다.

로컬 ONS는 해당 네트워크 내의 EPCIS의 위치정보와 로컬 ONS 상위에 존재하는 루트 ONS의 위치정보가 저장된다[2,4]. 마지막으로 ONS 캐시는 질의한 EPC 정보 및 해당 응답을 저장함으로써 객체검색의 요청이 들어왔을 때 내부의 저장된 정보를 검색하여 존재하면 그 내용을 반환해주고, 그렇지 않다면 상위에 존재하는 루트 ONS에게 해당 질의를 전송한다[4].

이러한 ONS의 기본 처리 절차는 인증 및 암호화 기술이 적용되지 않은 상태에서 로컬 네트워크와 인터넷을 통과하도록 되어 있어 송수신되는 객체 식별정보가 쉽게 노출되거나 분석이 가능하다는 취약점을 내재하고 있다.

3.2 DNS 보안 취약점

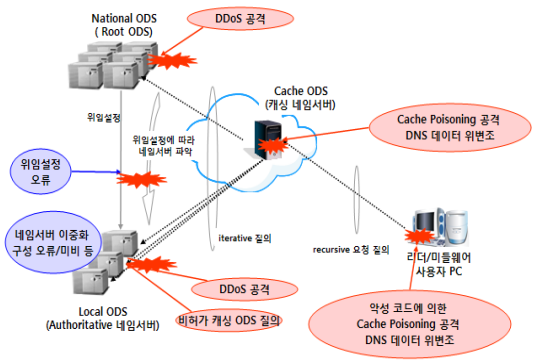
DNS란 우리가 일상적으로 사용하고 있는 도메인 이름의 체계를 뜻하고, 이러한 체계는 도메인 정보를 관리하는 수많은 네임서버 (혹은 DNS 서버)들의 상

호작용에 의해 유지되고 있다. 이러한 네임서버는 현존하는 가장 체계화된 분산시스템으로서 '.'(dot)를 의미하는 13개의 '상위 네임서버'(이하 루트서버)를 기점으로 전 세계에 분산되어 있어 사용자가 인터넷상에 어느 곳에 있든지 빠르고 쉽게 도메인 네임을 사용할 수 있다. 반대로 위와 같은 네임서버는 인터넷의 중요 기반시설로서 보안문제에 의한 사고 발생 시에는 전 세계 인터넷 이용자들을 혼란에 빠뜨릴 수도 있다.

1990년 최초로 DNS의 보안 취약성에 대하여 언급한바 있으나 당시로서는 이를 극복할 수 있는 보안 메커니즘이 없었기 때문에 5년이 지난 1995년이 돼서야 그 내용이 발표되었다.[4] 그밖에도 DNS에 대한 다양한 취약성과 공격은 CERT나 Security Focus와 같은 사이트에 언급되어 있으며 'Top 20 List of Internet Security Vulnerabilities'[16]이나 RFC333:Threat Analysis of the Domain Name System을 통해 알려진 바 있다.

대표적인 DNS의 공격유형은 패킷 가로채기이다. 패킷 가로채기의 가장 간단한 공격은 DNS가 질의/응답 메시지를 송. 수신할 때 암호화되지 않는 UDP(User Datagram Protocol) 패킷을 사용함에 따라 발생하는 위협이다. 패킷을 가로챔으로써 공격자는 가로챈 메시지의 응답 내용을 의도한 목적에 부합되게 변경하여 전송하는 형태로 공격이 가능하다. 이외에도 DNS 프로토콜 자체의 결함을 이용하여 공격하는 것으로 과도한 로드를 걸거나 메모리 조작으로 인해 정상적이 서비스를 불가능하게 만드는 DoS(Denial of Service; 서비스 거부), DDoS(Distribute Denial of Service; 분산서비스거부) 공격이 있으며 DNS 캐시 포이즈닝에 의한 공격 방식이 있다. 캐시 포이즈닝 공격은 호스트 이름의 IP 주소를 변경하여 DNS 캐시에 악의적인 정보가 저장되도록 하고 사용자가 인터넷 접속 시 악의적인 웹사이트에 접속하게 하여 사적인 정보를 훔치는 파밍(Parming) 공격을 유도하게 된다. DNS는 웹 서비스 뿐만 아니라 메일 서비스와도 밀접하게 연관되어 있어 DNS에 장애가 발생할 경우 접속 불안, 속도 저하 등 그 피해가 매우 커질 수 있다. 그럼에도 불구하고 DNS는 이를 제공하는 서버나 클라이언트, 정보를 인증하는 어떤 방법도 가지고 있지 않아 보안 설정이 허술한 것이 사실이다.[4]

더불어 ONS는 보안에 대한 고려 없이 설계된 DNS 기반 기술을 이용하기 때문에 DNS가 가지는 기본적인 보안 위협을 모두 가질 뿐 아니라 RFID 네트워크의 특징으로 기밀성 및 프라이버시, 무결성 및 가용성 측면에서 추가적인 보안위협을 가지고 있다. 대표적인 ODS의 보안위협은 그림과 같다[8].



(그림 2) 대표적인 ODS 보안 위협

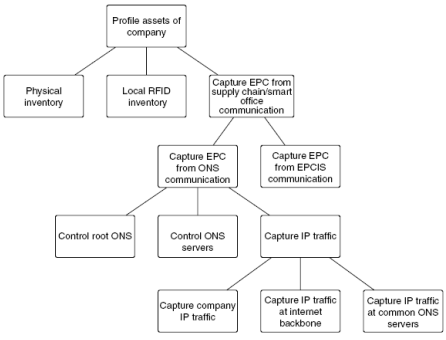
3.3 기밀성과 익명성

EPCglobal 네트워크에서 EPC와 관련된 정보를 이용하기 위한 정보서버와의 통신규격은 전송 계층 보안(TLS; Transport Layer Security protocol)과 같은 프로토콜을 사용하여 안전성을 보장할지 모르지만, 초기 ONS를 통해 질의하고 응답받는 룩-업 과정에서는 인증 및 암호화 과정이 적용되어 있지 않아 누구나 접근하여 송. 수신되는 정보들을 공격할 수 있다. 또한 현재의 처리 절차상에서 EPC는 연속적인 번호체계로 이루어져 있어 일부 객체 클래스와 회사 ID의 조합만으로 제품 브랜드와 종류를 알 수 있어 개인적인 측면이나 제품의 시장흐름을 중요시하는 비즈니스 측면에서 비밀정보로 간주되어야할 정보임에도 불구하고 사용자의 프라이버시를 침해할 수 있는 위험이 있다.

가장 간단한 형태로 RFID 태그가 근처의 리더기에 Electronic Product Code(EPC)인 일련번호를 브로드캐스트하게 된다. 이 일련번호는 AutoID 센터가 주는 번호로 64-128비트 길이를 갖으며 제조업자, 제품 형태 등 바코드에 포함되어 있는 정보들을 담고 있음에 따라, 사용자의 구매제품 혹은 의류항목들을 유일하게 식별할 수 있다. 이에 자신의 드레스 사이즈를 근처에 있는 리더기가 읽을 수 있으며, 누가 어떤 약물을 구매

했는지, 돈이 얼마나 있는지 등이 스캔되어질 수 있으며, 신발 사이즈와 의류정보를 기반으로 기록된 자신의 정보와 위치 정보가 추적될 수 있다[4].

무선 환경에서 태그와 리더 사이의 비인증 접근이나 도청에 대한 보안기술은 여러 가지 방법으로 제안된바 있다. 그러나 이러한 프라이버시 문제를 완화하기 위한 대부분의 솔루션은 태그와 리더사이의 인증이 이루어진 이후의 EPC에 대해서는 어떠한 상황도 고려하고 있지 않다. 아래 그림은 EPC 네트워크상에서 발생할 수 있는 보안취약성에 대한 트리 목록이며 현재로서는 이러한 ONS의 처리 절차상 발생할 수 있는 문제에 대한 어떠한 간단한 해결책도 제시된바가 없다.



(그림 3) EPC 네트워크의 보안 취약성

3.4 무결성과 가용성

ONS에서의 무결성은 EPC에 대한 정보서버의 주소를 넘겨주는 결과에 대한 정보의 정확성을 의미한다. ONS 검색서비스는 서비스를 제공하다보면 중간에 추가적인 ONS 위임 서버를 설정 할 수 있다. 만약 공격자가 이러한 하위 ONS 서버를 제어할 수 있는 경우가 발생하면 로컬 서버와 ONS 위임서버 사이에서 송수신되는 정보서버의 URL은 중간자 공격을 받을 수 있으며 URL에 대한 위, 변조가 밸생할 수있다. 이러한 과정에서 어떤 충분한 인증 방법조차 존재하지 않으면 공격자는 비슷한 도메인에 대해서도 위조된 정보서버의 주소를 전달할 수 있어 단순한 질의문에 대한 위변조일지라도 이에 상응하는 위험은 어플리케이션의 특성과 비즈니스의 영속성에 따라 그 파장이 작지만은 않을 것이다.

또한 EPCglobal 네트워크의 수용이 점점 더 확대되면 될 수록 관련 정보를 찾기 위한 ONS 처리 절차도 잦아지고, 넓어진 접근성 때문에 인터넷 공격으로부터 더 많이 노출된 형태로 서비스를 제공하게 될 것이다. 결국 네트워크상의 특정 서버에 트래픽을 집중시키는 DDoS공격이나 서버의 소프트웨어를 다운시키는 공격들이 유도될 수 있고 EPC 네트워크의 확대에 따라 홈케어, 지능형 냉장고등의 개인을 위한 애플리케이션뿐만 아니라 다양한 인터넷서비스를 이용하는 B2B, B2C 비즈니스까지도 위험을 증가시키는 결과를 가져올 수 있어 가용성에 대한 이슈는 보다 중요하게 고려될 필요가 있다.

4. ONS 보안기술

ONS 보안기술로는 ONS 계층구조 설계를 수정하는 것 이외에도 VPN(Virtual Private Network)을 이용하거나 DNSSEC등 ONS의 보안 위협을 완화하기위한 다양한 방법이 연구되고 있다.

4.1 네트워크 구조 변경

EPC의 기밀성은 VPN을 이용한 네트워크의 구조와 DNS의 서버 계층의 설계 변경을 통해 다소 그 위험성을 감소시킬 수 있다. 로컬에 위치한 서버에서의 모든 ONS 질의는 VPN을 통해 루트 ONS에 전송하고, 루트 ONS 통해 다른 글로벌 지역의 서버로 전송되어 검색이 이루어지는 형태로 네트워크를 구축하는 방법이다.

VPN은 공중 통신망 기반시설을 이용하여 시작 지점에서 목표 지점까지 외부로부터 어떠한 영향도 받지 않고 안전하게 정보를 전송할 수 있는 가상의 터널을 이용한 연결로서, 사전에 약속된 특별한 프로토콜로 세션을 구성, 타 사용자나 외부로부터 안전하게 보호받는 기술이다. 이와 같은 네트워크 구조에서 공격자는 외부 시스템으로 전송되는 정보를 획득한다고 할지라도, 해당 정보가 어느 제품에 대해 혹은 어떤 지역에 질의된 것인지 추측할 수 없게 된다. 또한 네트워크를 기업 내부로 한정하여 해당 기업에 대해서만 사용하는 경우

관련 정보는 외부로 유출되지 않고 무결성 및 가용성에 대한 위협도 내부 공격자만으로 제한될 수 있다.

그러나 이러한 네트워크 구조의 경우 EPC 네트워크 자체의 이용목적을 만족시킬 수 없으므로 실질적인 보안대책으로 적용하기는 어렵다. 또 다른 방법은 ONS와 정보서버의 캐싱 시간을 연장함으로써 인터넷을 통한 질의 자체를 감소시키는 방법이다. 이는 정보서버가 얼마나 많이 이용되는지 그리고 새로운 정보에 대한 요구사항 등 응용 시나리오에 따라 그 유효성의 차이가 발생할 수 있다.

4.2 엑스트라넷에서의 가상사설망 이용

VPN을 이용한 모든 EPC 질의를 중앙의 서버로 집중시키는 방법은 신뢰하는 사업 파트너와 엑스트라넷을 구성함으로써 그 활용 범위를 확장시킬 수 있다. 이렇게 확장된 엑스트라넷을 통해 모든 기업은 중앙의 ONS 검색을 이용하고 또 다른 ONS 질의는 다른 지역으로 전달되게 된다. 그러나 이러한 방법은 정보서버와 ONS 검색 서비스를 제공하는 모든 네트워크 구성 객체들 간에 VPN을 설치하기 위한 키 관리에 문제가 있어 네트워크를 확장하는데 무리가 있어 보인다.

더욱이 EPC 네트워크가 활성하고 되고 RFID 리더의 사용이 점점 증가하게 되면 엑스트라넷을 떠나 지역 네트워크 자체의 부담도 증가하게 되어 결국 엑스트라넷을 통한 VPN의 확장은 정보의 무결성과 ONS의 가용성보다 기밀성에 대한 보안 위협이 증가할 것이다.

4.3 The Onion Routing

ONS 시스템에 질의를 전송하는 패킷과 해당 패킷이 전송된 소스를 매치시킬 수 없도록 인터넷 트래픽을 변형하고 섞는 방법으로 TOR(The Onion Routing)로 대표되는 Onion Routing 기법이 활용될 수 있다. Onion Routing은 인터넷에서 익명성을 보장하는데 가장 널리 사용되는 기술로, 인터넷에서 특정 패킷의 발신을 누가 했는지의 여부를 숨길 수 있다. Onion Routing에서 Onion은 한 메시지가 겹겹이 암호화되어 가장 바깥쪽 암호화 층을 풀어야만 안쪽이 보이는 양파와 비슷한 암호화 기법의 특성을 묘사한 것이다. 이러한 용도가 있기 때문에 이 기술이 미국을 비롯한 외국에서는 굉장히 많이 쓰이고 있지만, 국내에서는 그 개념조차 생소할 정도로 많이 알려져 있지 않은 실정이다[6]. 더욱이 이 방법 또한 기밀성을 제공하기는 하지만 EPC 네트워크의 가용성을 만족시키는 못하고 있다.

4.4 DNSSEC

DNS의 보안취약성을 극복하기 위해 DNS 데이터에 대한 인증과 무결성 서비스를 제공하는 것이 바로 DNS 보안 확장(DNSSEC: DNS Security Extensions)이다. DNS 보안 확장은 도메인 접속정보의 위, 변조를 방지하기 위하여 네임서버 정보에 공개키 기반 구조(PKI:Public-Key Infrastructure)를 이용하여 서명・검증하는 보안기술로서 이 기술을 적용할 경우 사용자가 인터넷접속 시 도메인 질의 후 받은 응답이 실제로 요청한 DNS 서버로부터 왔는지 중간에 위, 변조 되었는지 여부를 검증할 수 있어 신뢰성 있는 인터넷 접속을 가능하게 한다.[8]

DNS 보안 확장의 구성요소를 살펴보면 초기 버전은 비밀 키를 이용하여 두 서버간의 상호 인증이 이루어지는 TSIG(Transaction Signature)와 RR(Resource Record)set과 연관되어 암호학적으로 생성된 전자서명을 통해 데이터 발신 인증과 무결성을 제공하는 두개의 서로 다른 독자적인 프로세스로 구성되어졌다. 새로운 버전에서의 DNS 보안 확장은전자서명과 서명검증 절차를 지원하기 위한 신규 리소스 레코드인 RRSIG(Resource Record Signature), DNS-Key(DNS Public Key), DS(Delegation Signer), NSEC(Next Secure)를 정의하였다.[5]

DNS 보안 확장은 프로토콜 측면에서 안전하고 신뢰성을 보장할 수 있는 방법이긴 하지만 키 관리 및 키 제어 문제, 그리고 많은 다양한 조직의 트러스트를 구축하는 것 등의 어려움이 있어 그 효과에 비해 많은 나라에서 채택되어 사용하고 있지는 않은 실정이다. 그렇기 때문에 인터넷을 사용하는 모든 업체에서 DNS 보안 확장을 선택한다면 ONS에 대한 무결성은 보장될 수 있다. ONS의 가용성 문제는 DNS 보안 확장을 활용함으로써 추가적인 보호가 이루어지지는 않고 있으며 서명에 대한 검증으로 서버에 대한 부하 증가만 가져올 수 있다.

5. 결 론

EPC를 포함하는 RFID는 유통구조의 비용절감을 위해 설계된 구조이기 때문에 그 탄생배경부터 보안이나 프라이버시 측면은 고려 대상이 아니었다. 그렇기 때문에 현재의 EPC 네트워크는 많은 보안 위협을 가지고 있으며 특히 ONS의 검색 서비스는 기밀성 및 프라이버시, 무결성 및 가용성 측면에서 보안이슈가 제기되고 있다.

DNS에 기반을 둔 ONS 보안 취약점은 현재의 보안 기술에 의해 부분적으로 완화될 수 있지만 기본적인 네트워크 설계 자체에 대한 변경을 요구하기도 한다. TOR와 같은 트래픽 익명 서비스는 ONS의 사용과 정보 서버를 접근하는데 있어 프라이버시 문제의 해결책을 제시하고 있고, ONS 정보의 무결성은 DNS 보안 확장을을 통해 보완이 가능하지만 ONS와 정보서버의 가용성은 좀 더 연구가 이루어져야할 부분이다.

수많은 제품에 대하여 서로 다른 정보를 저장하고 이를 접근하기 위한 글로벌한 네트워크 시스템에 대한 구현은 비즈니스의 확산에 따라 자연스럽게 진행되는 방향일지도 모른다. 그렇지만 그러한 요구에 맞춰 보안과 프라이버시를 해결할 프로토콜과 분산 해시 테이블을 근거로 한 P2P(Peer to Peer) 시스템과 같은 ONS의 대체 모델을 설계할 필요성이 있다.

참 고 문 헌

[1] 한국인터넷진흥원, “RFID 검색시스템 구축 및 운영 지침서 V1.2”, 2006.12

[2] 오세원, 표철식, 채종석, “RFID 표준화 및 기술동향”, 전자통신동향분석, 제 20권 제 3호, p.56-66, 2005년 6월.

[3] 정한영, 이상훈, “인트라넷 환경에서 MND -ONS 시스템 구축”, 한국정보과학회 가을 학술발표논문집, Vol34, No.2, 2007년

[4] 한국정보보호진흥원, “RFID 객체 검색 서비스 보안을 위한 인증모델연구”, 암호이용기반구축보고서, 2005

[5] TTA, “DNS 보안 확장 개요 및 리소스 레코드 형식”, DTTAS.KO-01.0098, 2006. 12

[6] Group Foxtrot, FREEDOM OF SPEECH ON THE INTERNET, Korea Advanced Institute of Science and Technology

[7] Benjamin Fabian, Oliver Gunther, and Sarah Spiekermann, “ONS Security”, RFID HandBook:Applications, Technology, Security, and Privacy, 2008

[8] 나정정, ″RFID디렉토리시스템 보안기술“ RFID/USN 보안컨퍼런스, 2008

◐ 저 자 소 개 ◑

이 신 경

1999년 전남대학교 전산학과 졸업

2001년 전남대학교 전산학과 석사

2000년 12월~현재 한국전자통신연구원 정보보호연구본부 선임연구원

관심분야 : 정보보호, 센서 네트워크, 보안관리

Email : neuron@etri.re.kr

박 남 제
2000년 동국대학교 정보산업학과 졸업
2003년 성균관대학교 정보보호학과 석사
2008년 성균관대학교 컴퓨터공학과 박사
2003년 04월~현재 한국전자통신연구원 정보보호연구본부 선임연구원
현재) 관세청 사이버밀수단속 세관원
한국산업기술평가원 평가위원
지식경제부 핵심애로기술지원 기술지도전문가
한국정보통신인력개발센터 자격검정 전문위원
모바일RFID포럼 표준기획분과위원,정보보호분과 간사
미국인명연구소(ABI) 자문연구위원회 전문위원
영국캠브리지국제인명센터(IBC) Vice President
한국인터넷정보학회 편집위원
ITU-T SG17 Q.9 Co-Editor
한국과학기술자네트워크(KOSEN) 전문위원
관심분야 : 정보보호, 암호이론. 모바일 컴퓨팅, 센서네트워크
Email : namjepark@etri.re.kr, namjepark@gmail.com

최 두 호
1994년 성균관대학교 수학과 졸업
1996년 한국과학기술원 수학과 석사
2002년 한국과학기술원 수학과 박사
2002년-2007년 한국전자통신연구원 선임연구원, 팀장
2006년 09월~현재 ITU-T X.1171(X.nidsec-1) 에디터
관심분야 : RFID/USN, 정보보호, 위상수학
Email : dhchoi@etri.re.kr

정 교 일
1981년 한양대학교 전자공학과 졸업
1983년 한양대학교 전자공학과 석사
1997년 한양대학교 전자공학과 박사
1982년-현재 한국전자통신연구원 책임연구원, 마케팅기술위원
현재) 국가정보원 정보보호시스템 인증위원
ITU-T(국제전기통신연합) SG17 연구위원
TTA(한국정보통신기술협회) 국제표준화전문가
한국전자지불산업협회 IC카드포럼 의장
Asia IC Forum 표준화위원장
행정자치부 전자주민증 자문위원
ISO TC215 전문위원
TTA(한국정보통신기술협회) TC1 의장
IC카드연구센터 전자여권표준기술개발단 단장
모바일RFID포럼 정보보호분과위원장
홈네트워크시큐리티포럼 의장
대검찰청 디지털수사 자문위원
대한전자공학회 상임이사
한국정보보호학회 부회장
한국디지털포렌식학회 부회장
한국인터넷정보학회 이사
관심분야 : 정보보호, Biometrics, 국가기반보호, 신호처리
Email : kyoil@etri.re.kr