특집

EPC 네트워크에서의 네임 서비스에 대한 보안 이슈

이향진, 전길수 (한국정보보호진흥원)

I. 서 론

RFID 기술을 이용한 다양한 형태의 비즈니스 모델 개발 및 시범 사업이 전 세계적으로 활발히 진행되고 있는 가운데, EPCGlobal에서는 관련 기술의 표준화 및 시범 서비스 운영 등을 통해 RFID 관련 산업 전반을 선도하고 있다. 특히, 최근에는 전 세계 주요 DNS 서버를 운영하는 베리사인(VeriSgin)에 EPC 네트워크 운영을 위임함으로써 본격적인 RFID 서비스 제공을 위한 기반을 다지고 있다.

현재 RFID 서비스는 RFID 기술이 가지는 편의성 등으로 인해 세계적으로 널리 보급될 계획에 있고, 모바일 RFID 서비스 등과 같은 추가적인 비즈니스 모델이 개발되고 있다. 그러나 RFID 기술 및 RFID 네트워크가 가지는 다양한 보안 및 프라이버시 침해 위협은 RFID 기술과 서비스 도입에 중요한 장애로 작용하고 있다. 그러므로 본 고에서는 RFID 네트워크의 주요 구성요소 중 하나인 네임 서비스에 대해 분석하고자 한다. 특히, 본 고에서는 RFID 기술 및 비즈니스를 주도하고 있는 EPC Global의 EPC 네트워크에서 제공하고 있는 네임 서비스의 구조를 분석하고 네임 서비스와 관련된 다양한 보안이슈에 대해 논의하고자 한다.

II. EPC 네트워크에서의 네임 서비스

EPC 네트워크에서 제공하는 네임 서비스에는 EPC 네트워크에서 제조업체 등이 제공 · 관리하는 객체정보를 제공하는 EPC Information Service(이하, EPC-IS), 서버에 대한 검색 서비스를 제공하는 Object Name Service(이하, ONS)와 해당 객체에 대한 이력정보를 제공하는 EPC Discovery Service (이하, EPC-DS)가 있다.

다음에서는 ONS 및 EPC-DS가 제공하는 서비스의 내용 및 동작 방식에 대해 설명한다.

1. Object Name Service

ONS는 사용자 어플리케이션으로부터 RFID 태그가 부착된 객체의 RFID 코드에 대한 질의를 받아 해당 코드의 객체정보가 저장되어 있는 EPC-IS 서버의 위치를 반환해

줌으로써 사용자에게 EPC-IS에 대한 검색 서비스를 제공한다. 이는 기존의 DNS (Domain Name Service) 서버가 도메인 네임을 입력 값으로 받아 해당하는 IP 주소를 알려주는 기능과 유사하며, 실제 DNS 기술[1]을 기반으로 구현되고 있다.

EPC 네트워크를 구축한 EPC Global에서는 이와 같은 ONS와 DNS의 유사성으로 인해 전 세계 주요 DNS 서버를 운영하고 있는 베리사인에 EPC 네트워크의 운영을 위임하여 현재는 베리사인에서 EPC 서비스를 시험 제공하고 있다.[2]

1) 구성요소

ONS 네임 서비스 구조는 〈그림 1〉와 같으며[3], 기본적으로 ONS 루트 서버, ONS 위임 서버, ONS 리졸버 및 사용자의 로컬 호스트에 존재하는 ONS 로컬 서버 및 캐시로 구성된다.

• ONS 루트 서버

- 모든 ONS의 최상위 ONS로서 로컬 ONS의 캐시에 EPC 관련 정보가 없을 경우, 사용자의 EPC Coordination 어플리케이션에 의해 가장 처음으로 질의되는 ONS
- 현재, EPC 네트워크의 루트 ONS는 베리사인이 운영하고 있음

• ONS 위임 서버

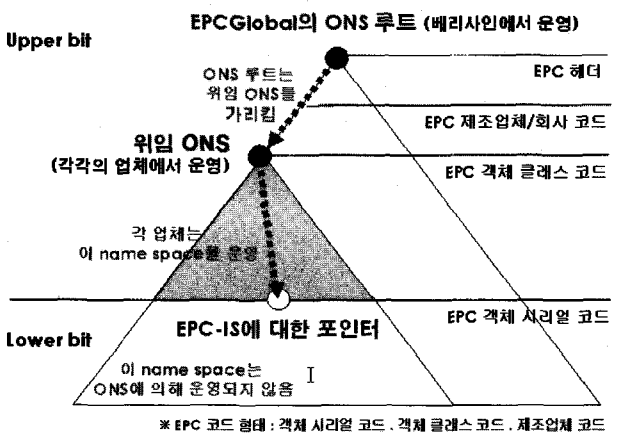
- ONS 네임 서비스 계층구조에서 ONS 루트 서버의 하위 서버로서 EPC 코드에 대한 EPC-IS의 URL을 제공

• ONS 리졸버

- ONS에 접근하기 위한 인터페이스를 가지고 있는 모듈로서, 특정 객체의 EPC 코드에 대한 EPC-IS의 URL을 찾기 위한 과정인 레졸루션을 수행
- DNS API와 서비스가 사용자 어플리케이션에 노출되지 않는 다양한 방법을 제공하고 인터페이스를 표준화하는 통합된 API를 제공

• ONS 캐시

- DNS 캐시와 동일하게 이전에 질의한 EPC 코드 정보 및 해당 질의에 대한 응답을 저장, 관리함



〈그림 1〉 ONS 네임 서비스 구조

- 다만, 존재하는 DNS 캐시를 통해 캐시된 정보를 내부적으로 관리하는 캐시로 기존 DNS 캐시를 이용하기 위한 ONS API를 이용

2) ONS 질의 · 응답 메시지

ONS는 기존의 도메인 네임서버가 도메인 네임을 입력 값으로 받아 해당하는 IP 주소를 알려주는 기능과 유사하므로 기존 DNS 기술을 기반으로 구현된다. 이러한 ONS 질의 · 응답을 위해서 DNS 자원레코드 NAPTR (Naming Authority Pointer)가 이용된다.[4]

Domain	TTL	Class	Type	Order	Pref	Flags	Service	Regexp	Replacement

〈그림 2〉 NAPTR 자원레코드 포맷

다음은 NAPTR 자원레코드의 각 필드별 설명이다.

- Domain : 질의하는 대상의 호스트 이름
- Class : 인터넷인 경우 'IN'으로 설정
- Type : NAPTR 자원레코드인 경우 '35'로 설정
- TTL (Time to live) : 자원레코드가 참조되어 캐쉬에 저장된 경우, 해당 자원레코드의 캐쉬 저장 유효기간
- Order, Pref(Preference) :
  - DNS는 정렬(ordering)을 보장하지 않으므로 NAPTR 자원레코드가 바른 순서로 배열되기 위해 사용되는 필드
  - 유효한 값을 반드시 가져야 하며, 번호가 낮을수록 먼저 처리됨
  - Pref. 필드는 Order 필드와 함께 자원레코드의 정렬에 이용
- Flags : 필드 해석에 대한 제어를 위한 필드, 'u'로 설정된 경우 URL을 의미
- Service : 'Regexp' 필드에 나오는 주소에 대한 서비스 제공 방식

  ex) OIS+html의 경우, 'Regexp' 필드의 값은 OIS의 주소를 의미하고, 웹(html) 형태로 서비스가 제공됨을 의미
- Regexp : EPC IS에 대한 URL
- Replacement 필드 : EPC network에서는 사용되지 않음

3) ONS 질의 · 응답 메시지의 예

ONS 응답은 여러 개의 URL을 가질 수 있으므로 하나 이상의 NAPTR 자원레코드 형태가 될 수 있다. 〈그림 3〉는 ONS 레졸루션의 결과 질의에 대한 응답의 예로, 서비스 형태는 EPC-IS 이며, EPC-IS의 URL 주소는 'http:// exapmle/cgi-bin/epcis'이다. 기타, Regexp 필드의 '^.*$'는 match anything, '!'는 구분자이다.

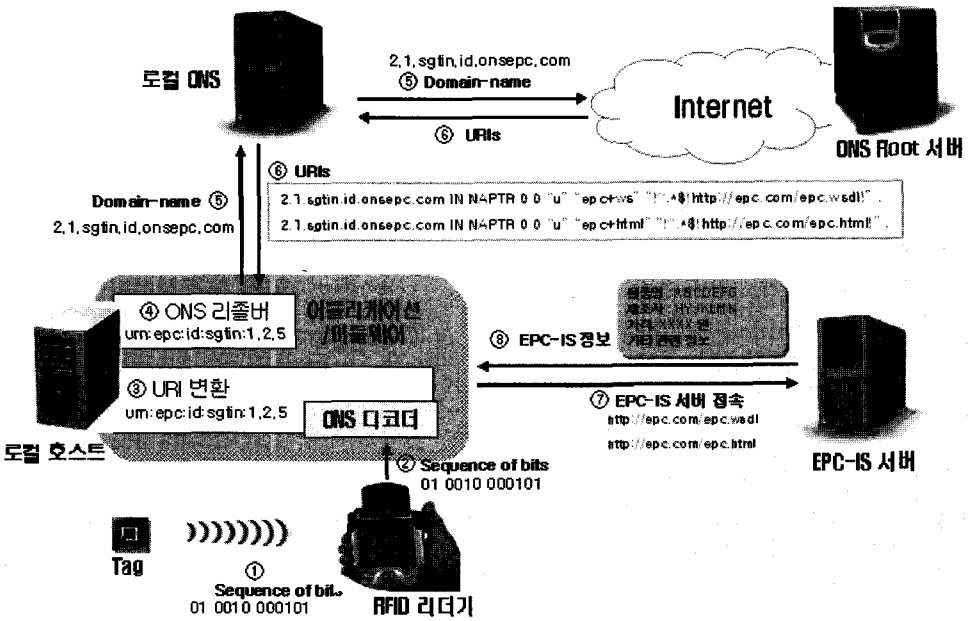
Order	Pref	Flags	Service	Regexp	Replacement
0	0	u	EPC+epcis	!^.*$!http://example.com/cgi-bin/epcis!	.

〈그림 3〉 ONS 응답 메시지의 예

4) ONS 질의 · 응답 과정

ONS 질의 · 응답 과정은 〈그림 5〉와 같으며, 각 과정에서의 세부 동작은 다음과 같이 수행된다.[5]

① RFID 태그 정보를 RFID 리더기가 읽음
② RFID 리더는 읽어 들인 RFID 태그 정보를 로컬 호스트로 전송
③, ④ 로컬 호스트는 전송받은 태그정보를 로컬 ONS 리졸버에 전송하고 로컬 ONS 리졸버는 전송받은 태그 정보를



〈그림 4〉 ONS 레졸루션 과정 (EPC SGTIN 코드)

URI 형태로 변환

- 전송받은 태그 정보 : 01 0010 000101
- URI 형태로 변환 : urn:epc:id:sgtin:1.2.5

⑤ 로컬 ONS 리졸버는 URI 형태를 도메인 이름 형태로 변환하여 ONS 질의를 구성

- URI를 도메인 이름 형태로 변환 : 2.1.sgtin.id.onsepc.com

※변환 방법 : 'urn:epc:' 삭제→시리얼번호 제거→역순으로 정렬 →':' 을 '.'으로 변환→남은 문자열에 '.onsepc.com' 추가

⑥ ONS(로컬 및 루트) 서버에서 하나 이상의 EPC IS 서버의 URL들의 리스트를 포함한 응답을 로컬 호스트(실제적으로 로컬 호스트 내에 있는 로컬 ONS 리졸버)에 반환

⑦ 로컬 ONS 리졸버는 NAPTR 자원레코드 형태로 온 DNS의 응답으로부터 URL 리스트를 획득하여 이를 로컬 호스트에 전송하면, 로컬 호스트는 해당 URL의 EPC IS 서버에 접속

- 로컬 ONS 리졸버가 로컬 호스트에 제공하는 EPC-IS URI
  : http://epc.com/epc.wsdl 혹은 http://epc.com/epc.html

※로컬 호스트는 해당 URI에 접속한 후, 객체 시리얼번호(5)를 이용하여 해당 객체에 대한 정보를 획득

⑧ EPC-IS는 로컬 서버가 요청하는 serial number에 해당하는 객체정보를 제공

2. EPC Discovery Service

EPC-DS는 EPC 네트워크에서 EPC 태그를 가진 객체에 대한 추적 및 이력관리 서비스를 제공하는 네임 서비스의 일종으로, EPC와

관련된 데이터에 대한 검색엔진과 유사하다. 이 서비스는 EPC와 관련된 개체의 정보가 여러 EPC-IS 서버에 저장되어 있는 경우, 정보가 저장되어 있는 모든 EPC-IS 서버들의 URL 정보를 사용자에게 전송함으로써 사용자가 해당 개체의 이력을 추적할 수 있도록 한다.

이와 같이 EPC-DS는 ONS와 같은 네임 서비스를 제공하지만 EPC-IS의 프레임워크 및 프로토콜을 사용한다는 점에서 ONS와의 차이를 보이고 있다. 특히, ONS는 신뢰된 서버여야 하지만, EPC-DS는 지역적, 기능적으로 제한된 범위에서 사용될 수 있으므로 보편적으로 신뢰된 서버일 필요가 없다.

III. 네임 서비스 관련 보안 이슈

ONS는 보안에 대한 고려 없이 설계된 DNS 기반기술을 이용하므로 패킷 가로채기(Packet intercetion)나 캐시 오염(Cache poisoning) 및 서비스 거부 공격(Denial of Service) 등과 같은 DNS가 가지는 기본적인 보안 취약성을 모두 가진다.[6] 뿐만 아니라, ONS는 EPC 네트워크의 기본적인 특징으로 인해 기밀성 및 프라이버시, 무결성 및 가용성 측면에서 다음과 같은 보안 이슈가 제기되고 있다.[7]

• 기밀성 및 프라이버시 측면

- ONS의 동작과정에는 인증 및 암호화 기술이 적용되지 않으므로 송수신되는 EPC 정보가 쉽게 노출될 수 있음
- 특히, 클래스 레벨에서의 질의인 경우에도 공격자는 이러한 정보를 수집하여 특정 EPC-IS에서 관리하는 객체의 종류 등을 알아내는 등의 공격이 가능
- 또한, ONS는 인증능력이 없으므로 브라우징(Browsing)과 사전공격(Dictionary Attack)에 취약하여 기업의 모든 상품정보가 EPC-IS에 접속하지 않고도 ONS에 의해 누출될 수 있음
- ONS 질의 시, EPC 코드의 객체 시리얼 번호까지의 검색이 가능한 경우, 공격자는 EPC-IS에 접근하지 않고 ONS 질의만으로도 업체에서 관리하는 모든 객체 정보를 확인할 수 있음

• 무결성 측면

- ONS는 DNS와 같이 서버의 환경설정 및 레졸루션 방법에 따라 중간에 추가적인 ONS 서버를 설정할 수 있는데, 공격자가 이러한 중간 ONS 서버를 제어할 수 있는 경우, 로컬 호스트와 ONS 사이에서 송수신되는 EPC-IS의 URL에 대한 중간자 공격(man-in-the-middle attack)이 가능

• 가용성 측면

- DNS에서의 DoS 공격과 마찬가지로 ONS에서도 DoS 공격으로 인한 가용성이 주요 이슈임
- 특히, EPC 네트워크가 널리 확대되면, 홈케어, 지능형 냉장고 등의 개인을 위한 어플리케이션뿐만 아니라 다양한 B2B, B2C 비즈니스에 적용될 수 있으므로 ONS의 가용성에 대한 이슈는 DNS에서 보다 더욱 중요하게 고려되어야 함

Ⅳ. 네임 서비스 보안을 위한 보안 기술

앞서 논의된 ONS에서의 보안을 위해 DNS 보안취약성을 고려하여 설계된 DNS 보안확장(DNS Security Extension, DNSSEC) 표준[8,9,10]의 적용이 계획되고 있다.

DNS 보안확장(DNSSEC, DNS Security Extension)의 기본 목적은 DNS의 보안 취약성을 극복하기 위해 DNS 데이터에 대한 인증과 무결성 서비스를 제공하여 기본적인 DNS에 보안 요소를 추가하는 것이다. 이를 위해 DNSSEC 프로토콜은 DNS의 기본 구성요소를 상속하면서 추가적인 보안을 위해 새로운 자원레코드 유형을 정의하고, 각 구성요소들의 안전한 상태에 대한 요구사항들을 정의한다.

특히, DNS 보안확장은 데이터 출처인증과 무결성, 트랜잭션과 요청메시지에 대한 인증 및 키 분배 서비스를 기본적으로 제공하고 있으며, 이를 위해 서명 생성을 위한 키(KEY) 자원 레코드 및 서명값을 저장하는 서명(SIG) 자원 레코드 등을 정의하고 있다.

이 외에도 내부적으로 ONS 계층구조 설계를 수정하거나 VPN을 이용하는 등 ONS의 보안 위협을 완화하기 위한 다양한 방법이 연구되고 있다.[7]

Ⅴ. 향후 전망

최근 시장조사업체인 IDC의 조사에 따르면, RFID 세계시장 규모는 2010년 100억 달러에 달할 것으로 예상될 만큼 빠르게 성장하고 있다. 그러나 RFID 기술 및 RFID 네트워크가 가지는 다양한 보안 및 프라이버시 침해 위협은 RFID 기술 및 서비스 도입을 추진하고 있는 여러 기업들에게 큰 부담으로 작용할 수 있다. 이에 따라 최근 EPC네트워크의 주요 구성요소들에 대한 보안 기술이 연구 · 개발되고 있는데, 특히, EPC 네트워크에서의 네임 서비스에 대한 보안 기술로는 DNS 보안확장의 적용이 가장 확실시 되고 있다. 그러나 DNS 보안확장은 기존 DNS 메커니즘에 인증 및 암호화를 위한 추가적인 요구사항 등의 구현으로 인해 DNS에 로드가 증가하게 되므로 DNS에 비해 10배 이상의 로드가 예상되는 ONS에서의 적용은 쉽지 않을 것으로 예상된다. 그러므로 향후, DNS 보안확장을 보다 효율적으로 ONS에 적용하기 위한 연구가 추가적으로 진행되어야 할 것이다.

참고 문헌

[1] IETF, RFC1035 : *Domain Names - Implementation and Specification*, 1987.

[2] VeriSign, http://www.verisign.com/naming-and-directory-services/supply -chain-services/index.html

[3] Yojiro UO, Shigeya Suzuki, Osamu Nakamura, *Name service on the EPC network*, 2004.

[4] IETF, RFC2915 : *The Naming Authority Pointer (NAPTR) DNS Resource Record*, 2000.

[5] 한국인터넷진흥원, http://www.ods.or.kr, *코드별 레졸루션 과정*, 2005.

[6] IETF, RFC3833 : *Threat Analysis of the Domain Name System*, 2004

[7] Security, Privacy and Trust in Pervasive and Ubiquitous Computing, *Security Analysis of the Object Name Service*, 2005.

[8] IETF, RFC4033 : *DNS Security Introduction and Requirements*, 2005.

[9] IETF, RFC4034 : *Resource Records for DNS Security Extension*, 2005.

[10] IETF, RFC4035 : *Protocol Modifications for the DNS Security Extensions*, 2005.

[11] EPCGlobal, *EPCglobal Object Name Service* 1.0, 2004.

[12] EPCGlobal, http://www.epcglobalinc.org, *EPCglobal Network*, 2004

저자소개

이 향 진

2000년 2월 성균관대학교 전기전자컴퓨터공학부 학사
2002년 2월 성균관대학교 전기전자컴퓨터공학부 석사
2002년 1월 – 현재 한국정보보호진흥원 암호응용팀 연구원
주관심 분야 정보보호, RFID/USN

전 길 수

1991년 2월 서강대학교 수학과 학사
1993년 2월 서강대학교 수학과 석사
1998년 2월 서강대학교 수학과 박사
1998년 10월 – 1999년 9월 서강대학교 기초과학연구소 박사후 연구원
2001년 3월 – 2001년 6월 서강대학교 컴퓨터학과 연구교수
2001년 7월 – 현재 한국정보보호진흥원 암호응용팀장
주관심 분야 암호학, RFID/USN 정보보호, PET