# DNSSEC을 이용한 .KR 도메인네임의 제한적 인증에 관한 연구

임준형* 장현익**
*한국인터넷정보센터(KRNIC) 기술지원부
**한국인터넷정보센터(KRNIC) 주소관리부
e-mail:[jhlim, hijang]@nic.or.kr

# A Study on Restrictive Authentication of .KR Domain Name Using DNSSEC

Joon-Hyung Lim*, Hyun-Ik Jang**
*Dept of Technical Support, Korea Network Information Center
**Dept of Address Management, Korea Network Information Center

요약

DNSSEC은 IETF에서 논의중인 DNS 보안 표준으로서, DNS에 있어 가장 큰 잠재적 위협인 '도메인네임에 대응되는 IP주소의 위변조 위협에 대응하기 위해 논의되고 있는 표준이다. 최근 네트워크 환경에서의 최상의 암호화 기법으로 자리잡은 공개키 암호화 기법을 이용하여, 도메인 Zone에 서명을 하여, 이러한 Zone 메시지를 받아보았을 때, 서명을 검증함으로서, DNS메시지가 중간에 위·변조없이 적정한 소스로부터 왔다는 것을 확인하는 것이다. 본 논문에서는 DNSSEC에서 가능한, 계층적 인증방식을 .KR 하위 도메인네임에서 활용할 수 있는 방안으로서, secure resolver를 이용한 도메인네임의 인증을 제시하였다.

## 1. 서론

'인터넷의 심장'이라 해도 과언이 아닌 DNS(Domain Name System)는 도메인네임을 IP주소로 매핑(mapping) 해주거나, 그 반대의 작업을 수행하며, 인터넷의 접근성을 높혀, 오늘날의 인터넷의 기반을 이루어 왔다. 도메인네임은 인터넷환경으로의 접근성을 극대화시킨 인터넷의 기본적인 주소자원으로서 현재 그 의존도가 나날이 높아지고 있고, 이에 따라 도메인네임 서비스에 대한 보안 위협도 날로 증대되고 있다. DNS에 있어 가장 큰 잠재적 위협은 '도메인명에 대응되는 IP주소의 위변조 위협으로서, 위협이 현실화될 경우, 그 파급효과는 실로 엄청날 수 밖에 없다.[1] 이에 IETF의 DNSEXT 워킹그룹에서는 DNSSEC(DNS Security Extensions) 이라는 DNS보안 표준을 논의중이다. 본 논문에서는 DNSSEC의 계층적 인증방식의 필요성과 이를 .KR 하위 도메인네임에 적절히 적용하는 방안을 제시한다.

## 2. DNS에 대한 보안 위협

가. IP Spoofing

현재의 DNS는 일명 IP Spoofing(IP속임)으로 알려져있는 공격기법에 대해 잠재적인 보안취약점을 모두 가지고 있다. 일반적으로 해커가 자신의 IP주소를 감추기 위해 source IP주소를 spoofing하는 경우도 있으나, DNS의 경우, 캐쉬데이터에 대한 공격, DNS Zone파일에 대한 직접적인 공격 등의 방법으로 일시적, 혹은 장기적으로 중요 도메인네임에 대응하는 IP주소를 위조할 가능성이 있다. [1,4,5]

만약 공격이 성공했을 경우, 사용자가 조작된 데이터를 검증할 수 없는 현재 상황에서는, 변조된 IP주소에 공격자가 유사한 사이트를 열어 두었을 경우 사용자는 아무 의심없이 공격자의 사이트에 자신의 ID, 비밀번호 등 개인정보를 그대로 입력하는 사고가 발생하게 된다.

나. DNSSEC의 등장배경

전세계적으로 인터넷이 사회 중요 기반시설로 인식되고 있는 현재의 상황에서 DNS에 대한 잠재적인 위협은 매우 위험한 일이 아닐 수 없다. 이에 IETF에서는 도메인네임 Zone정보의 위변조 여부를 검증하기 위해 디지털 서명을 이용한 DNS 데이터의 검증표준을 RFC2535를 통해 제안했고, 현재는 대표적인 DNS프로그램인 BIND가 9버전부터 DNSSEC을 기본 스펙에 가장 가깝게 구현해오고 있다.

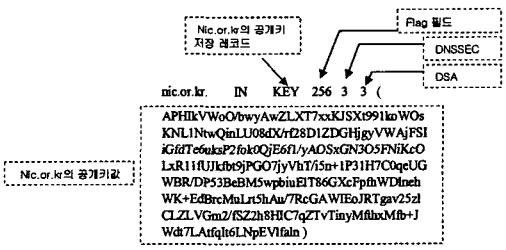
## 3. DNSSEC의 이해

가. 새롭게 추가된 Resource Record

DNSSEC을 위해 기존 DNS에서는 볼 수 없었던 Resource Record인 KEY, SIG, NXT 레코드가 추가되었다.[1,5]

a. KEY 레코드

KEY레코드는 해당 zone파일에 대한 암호 키쌍(key-pair)을 생성한 뒤, 그 중 공개키(public key)를 저장하는 레코드로, flag, key타입, 암호화알고리즘을 알려주는 세 개의 필드와 공개키값이 저장된다.




b. SIG 레코드

SIG레코드는 특정 RR(Resource Record)에 zone에 대한 개인키(private key)로 서명한 결과값을 저장하는 레코드로, KEY 레코드에 저장된 공개키값으로 복호화할 경우 키 값에 위변조가 없었을 경우 정상적으로 복호화 된다.

```
$ORIGIN .
$TTL 86400      ; 1 day
nic.or.kr       IN    SIG   KEY 3 3 86400 20020328043910 (
                            20020226043910 10203 or.kr.
                            AB9SqHR2lvMQCbeLKqCvD+LEIYzCFiCMo22xTi4eswm
                            bWmetXIN42s= )
```

위의 예시의 경우 SIG레코드는 KEY 레코드에 서명한 결과값을 갖는다.

c. NXT 레코드

일반적인 DNS환경에서는 Zone에 없는 도메인에 대한 질의에 대해서는 '해당 도메인없음(NXDomain) 응답을 한다. 하지만, DNSSEC이 적용된 경우 NXDomain응답에도 서명이 필요한데, 반복되는 NXDomain응답에 일일이 서명을 하는 것은 비효율적이므로, 아래와 같이 각 레코드별로 NXT레코드를 추가하여 '존재하지 않는 도메인 영역'을 표시한다.

```
example.nic.or.kr.   3600  IN   A     192.168.1.10
example.nic.or.kr.         3600 NXT   test.nic.or.kr. ( A SIG NXT )
                           3600 SIG   NXT 3 4 3600 20020328072526 (
                                      20020226072526 26922 nic.or.kr.
                                      AMthzvksFOvkMVftpV4VAiZAzqRaY92y
                                      ZzBH i/aZpkU5jSp1WscK8r0= )
```

박스안의 예는 사전적 순서로 example.nic.or.kr과 test.nic.or.kr사이에 오는 도메인명은 존재하지 않는다는 것을 한 개의 레코드로 표현한 것이다.

예를 들어, 호스트명 security는 사전적으로 example과 test사이에 위치하므로, 질의시, 해당 NXT레코드를 돌려주어 security 도메인은 존재하지 않는다는 것을 알려준다. 이 정보는 질의한 네임서버에 캐싱(caching)되어 향후 다른 존재하지 않는 도메인 질의시 캐시된 로컬 데이터에서 응답을 수행한다. [2,4]

## 4. DNSSEC의 계층적 인증 체계

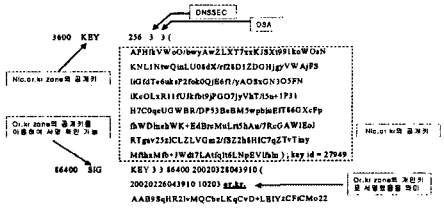
서명된 Zone파일이 운영중인 DNS서버가 공격자에 의해 완전히 침해당할 경우, 공격자가 새로운 키를 생성할 수 있고, 이를 이용해 조작된 zone을 완전히 새롭게 서명한다면 해당 Zone에 대한 무결성은 보장될 수 없다. [4]

가. 신뢰 사슬(Trust Chain)

DNSSEC에서는 이와같은 독자 서명시 위협을 방지하기 위해 상위 Zone의 개인키로 하위 Zone의 공개키에 서명함으로서, 상위 Zone이 하위 Zone을 인증할 수 있는 방법을 사용할 수 있다. (예:

OR.KR Zone이 NIC.OR.KR Zone을 인증)

아래 예로 제시한 nic.or.kr zone파일의 경우, nic.or.kr zone의 공개키를 or.kr의 개인키로 서명한 결과값(SIG이하)을 포함하고 있다.[2,4]




즉, 이 경우, 만약 공격자가 해당 zone의 주 DNS서버를 완전히 장악하고, 모든 키쌍을 새로 생성해 zone을 변경후 새로이 서명했더라도 새로 생성된 공개키를 부모 zone인 or.kr zone으로부터 새로 서명받지 않으면 상위의 부모zone과의 신뢰사슬(Trust chain)은 끊어지게 된다.

## 5. .KR 도메인에 대한 신뢰사슬의 적용방안

신뢰사슬(trust chain)이란 DNSSEC을 이용해 최상위 부모 zone(parent zone)부터 하위의 자식 zone(child zone)까지 계층적으로 zone안의 레코드들을 확인(verify)해주는 구조를 의미한다.

### 가. 신뢰사슬(Trust Chain)의 한계

신뢰사슬을 완벽하게 구성하여, 계층적인 인증을 가능케하기 위해서는, 전세계 13개의 최상위 root DNS서버에대한 DNSSEC의 적용과 그에 따른 하위 zone에 대한 서명 서비스가 필요하다. 하지만, 아직까지는 DNSSEC이 최상위의 DNS서버에는 적용되지 않았으며, 운영시 문제점 파악을 위한 테스트베드의 운영만 진행되고 있다.[4]

### 나. 제한된 신뢰사슬의 적용 방안

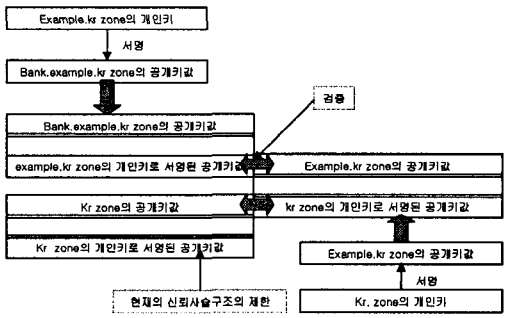
전세계의 최상위 Root DNS서버에 DNSSEC이 적용이 안된 상태에서도 그 하위단의 가능한 zone에서 DNSSEC을 적용하여 '제한된 신뢰사슬'을 구성할 수 있다. 예를 들어, 우리나라의 경우 .kr 도메인부터 DNSSEC을 적용하여 그 하위 zone (co.kr , or.kr 등.)으로 확대 적용해 나갈 수도 있다.

단지, .kr 상위의 zone인 "."(dot) DNS서버로부터 .kr에 대한 인증을 받을 수만 없을 뿐 .kr 이하로는 신뢰사슬의 구성이 가능하다.

### 다. DNS 인증서비스 제공 방안

a. secure resolver의 이용

강도높은 인터넷 보안이 필수적인 인터넷뱅킹, 쇼핑몰 등의 사이트의 경우 DNSSEC에서 제공하는 신뢰사슬을 구성할 경우, 일반적으로 사용되는 공개키기반 인증서 이외에도, 해당 사이트의 도메인네임에 대한 인증을 다시 한번 받을 수 있다.




예를 들어, bank.example.kr 이라는 도메인네임을 사용하는 사이트의 경우, bank.example.kr zone의 공개키는 example.kr. zone의 개인키로 서명되고, example.kr. zone의 공개키는 kr. zone의 개인키로 서명되므로, 이 사이트에 접속하는 클라이언트측의 도메인네임을 resolution할 수 있는 resolver에 key 검증기능을 추가해 이상의 신뢰사슬에 따라 bank.example.kr의 공개키를 검증할 수 있다.

이러한 secure resolver가 해당 공개키가 검증되었을 때만, 요청된 도메인네임을 resolution하여, 결과값을 클라이언트에게 돌려준다면, 도메인네임에 대한 위변조 공격에 대응할 수 있다.[1,2,6]

b. secure resolver의 적용 방안

.kr 도메인 이하라고 한정을 해도 한순간에 운영중인 모든 DNS서버에 DNSSEC이 적용되기에는 무리가 있기 때문에, 이러한 secure resolver는 추가적인 보안설정을 필요로하는 인터넷 사이트에서, 접속해오는 클라이언트에게 내려받게 하여, 해당 사이트의 도메인네임의 검증에 사용하게 할 수 있다.

## 6. 결 론

서론에서 언급한바와 같이 인터넷 기반요소인 DNS의 잠재적인 zone정보의 위변조 보안 취약점은 매우 위험한 결과를 초래하므로, 이를 대응하기 위해 DNSSEC이 논의되고 있다.

본 논문에서는 공개키 암호화 알고리즘을 이용하여 Zone정보의 유효성(validity)을 검증하는 DNSSEC의 실제 활용방안을 제시하였다. 인터넷 쇼핑몰이나, 금융업무 관련 사이트의 경우, 이미 유효성판단 및 트랜잭션 암호화를 위해 공개키 기반의 인증서를 이용하고 있지만, 본 논문에 제안된 '신뢰사슬' 구조 역시 기존의 인증서 인증체계와도 비슷하여 이것을 제대로 활용한다면, 도메인네임에 대해서도 그 유효성을 추가적으로 검증받을 수 있다.

현재의 DNSSEC의 문제점은 Zone정보가 커지면 커질수록 zone전체에 서명하는데 시스템의 부하와 시간이 많이 걸린다는 점과, DNS 메시지의 크기가 증가하여, 대규모 트래픽 발생시, 패킷이 잘려나가 재전송이 빈번하게 발생할 것이라는 것이다. 이러한 어려움은 상위 zone의 DNS 서버 운영시 더욱 커지게 되어, 현재는 IETF에서도 많은 관심이 좀 더 원할한 운영을 위한 테스트베드 운영, 최상위 root DNS서버에 적용을 위한 방안연구, 기존 표준 수정을 통한 효율성 증가 등에 쏠려있다.[3] 하지만 .KR 도메인네임의 경우 .com/net/org 및 최상위 root DNS서버에 비해 zone의 규모나 트래픽이 적으므로, 오히려 더 쉽게 .KR zone을 국내 DNS인증체계상의 최상위 zone으로 하는 제한적인 형태의 KR 도메인 인증체계를 외국보다 먼저 적용할 가능성도 배제할 수 없다.

따라서, 본 논문에 관련된 향후 연구과제 역시 .kr DNS 서버에 DNSSEC의 효과적인 적용방안에 관한 연구와 각 키값을 검증할 수 있는 secure resolver의 디자인 및 적용방안에 관한 내용이 될 것이다.

## 참고문헌

[1] R. Arends, M. Larson, "DNS Security Introduction and Requirements", draft-ietf-dnsext-dnssec-intro-01

[2] D. Eastlake "Domain Name System Security Extensions" , RFC2535

[3] R. Arends, "DNSSEC Opt-In", draft-ietf-dnsext-dnssec-opt-in-01

[4] Paul Albitz & Cricket Liu "DNS and BIND" 4th Ed. O'Reilly

[5] Mockapetris, P., "Domain names - implementation and specification", RFC 1035

[6] R. Conrad, D., "Indicating Resolver Support of DNSSEC", draft-ietf-dnsext-dnssec-okbit-03