안전한 인터넷 기반제공을 위한 DNS 보안 고도화 연구

김학주*, 윤민우*, 임형진*, 정태명**, 송관호***

*성균관대학교 컴퓨터공학과

**성균관대학교 전기전자컴퓨터공학부

***한국인터넷정보센터

A Study On The Advanced DNS Security For Secure Internet-Infrastructure

Hak-joo Kim*, Min-woo Yoon*, Hyung-jin Lim*,

Tai-myung Chung**, Kwan-ho Song***

*Dept of Computer Engineering, SungKyunKwan University

**School of Information & Communication Engineering, SungKyunKwan University

***Korea Network Information Center(KRNIC)

요 약

DNS는 인터넷 자원 관리를 위해 사용되고 있는 분산 네이밍 데이터베이스로써 최근 보안상의 취약점으로 인해 안전한 인터넷 사용에는 한계가 있다고 지적되었다. 따라서 안전한 인터넷 기반 제공을 위해 DNS의 보안 고도화 연구가 진행되었으며 그 일환으로 DNS 보안 확장(DNSSEC)이 대두되었다. 본 논문에서는 DNSSEC에 대한 이론적인 바탕을 토대로 보다 안전한 인터넷 자원 사용을 위한 방안을 연구하고 이의 적용방안과 안정화를 위한 제반 사항을 기술한다.

I. 서론

최근 전 세계적으로 발생하고 있는 상위의 루트 네임 서버들에 대한 공격으로 인해 인터넷 기반시설에 대한 보호가 중요한 문제로 떠오르고 있다. DNS는 인터넷 주소 자원 관리의 핵심 시스템으로서, 전 세계에 분산되어 있는 수많은 네임 서버들 간의 계층적 상호 연동을 통해 동작한다. 하지만, 계층 구조의 최상단 루트서버가 공격을 받아 피해를 입거나, 혹은 상위 레벨 네임서버의 데이터가 위/변조된다면 해당 네임서버는 잘못된 정보로 인한 피해를 입게 되며 특히 공공 및 금융 등 사용자의 자산과 관리된 컨텐츠에 대한 공격은 상상할 수 없는 큰 혼란을 가져올 수 있다[1]. 그러나 서비스 거부 공격(DoS : Denial Of Service) 등 네임서버의 기능을 마비시키기 위한 공격들은 기존의 분산 DNS 구조 자체의 특성과 필터링 기술 등을 통해 적절한 대응 방안의 도출이 가능하지만, 네임서버 데이터의 위/변조 발생 시 이에 대한 적절한 대응방안은 없는 상태이다[2].

따라서 본 논문에서는 DNS의 보안 취약점을 살펴보고 이에 대응하기 위한 방안으로 대두된 DNSSEC에 대한 연구 내용을 다룬다. 더불어 DNSSEC의 적용을 위한 방안을 연구하여 효과적인 DNS 보안 취약점 해결 도모한다.

2장에서는 DNS와 DNS의 보안 취약점에 대해

살펴보고 3장에서는 DNSSEC의 구성 및 동작 등 개괄적인 내용을 살펴보며 4장에서는 DNSSEC의 적용 방안과 적용 시에 부가적으로 고려해야 될 사항들을 기술한다.

II. DNS의 보안 취약점

1. DNS에 대한 위협

DNS는 트리(tree)형의 분산 데이터베이스(distributed database)이다. 클라이언트(client)와 서버(server) 패러다임으로 구성되어 있으며 각 노드는 서브 트리(sub-tree)의 루트 역할을 하여 위임을 통해 권한을 얻은 루트로부터 그 권한이 영향을 미치는 노드들의 영역인 도메인(domain)을 관리한다. 각 도메인은 최소한 1개 이상의 네임서버(name server)를 가져야 한다.

1990년, Bell 연구소의 벨로빈(Steven M. Bellovin)이 자신의 논문에서 최초로 언급한 DNS 보안 취약성을 바탕으로 DNS가 갖는 보안 취약점에 대한 연구가 진행되었다. 벨로빈이 논문에서 밝힌 최초의 DNS의 취약성은 원격사용자가 r-commands를 통해 시스템 접근 시, 호스트 네임 정보를 통한 사용자의 인증 과정에서 발생할 수 있는 버클리 r-commands의 취약성에서 기인한 것이었다. 그러나 rlogin의 명령어를 통한 DNS 시스템 공격 시뮬레이션 결과는 DNS 데이터베이스에 대한 허가되지 않은 악의적인 변경과 캐쉬 오염 등의 공격이 이름 기반의 사용자 인증 문제와 도메인 네임 시스템에 대한 접근 권한 문제, 변경된 정보에 대한 진위 여부 검증 불가 등과 같은 DNS 시스템이 갖는 근본적인 취약성을 지적했다[3].

2. DNS의 보안 취약점

이 절에서는 DNS가 갖는 보안적인 취약점에 대해 설명하겠다.

■ 패킷 가로채기

패킷 가로채기는 가장 간단한 공격유형으로, DNS가 전체 질의/응답 메시지를 주고받을 때, 전혀 암호화되지 않은 UDP 패킷을 사용하기 때문에 악의를 가진 공격자가 공유 네트워크나 중간 전달 네트워크에서 패킷 가로채기 능력만 가지고 있으면 이와 같은 공격을 실행하여 쉽게 악용할 수 있다. 이 취약점은 이름 기반 공격과 같은 좀 더 복잡한 공격을 시도하기 위해 사용되기도 한다.

■ ID 추측과 질의 예측

DNS 헤더의 ID 필드는 16비트로 구성되므로, 이 필드에 들어갈 수 있는 값의 총 개수는 2^{16}밖에 되지 않으므로 대입법(Brute force search)을 통해서 충분히 값을 추측해 낼 수 있다. 또한 리졸버가 질의했을 것이라 예측되는 QNAME과 QTYPE을 이용하여 위조된 데이터를 메시지 내에 삽입할 수 있다.

■ 이름 기반 공격

악의적인 공격자가 네임서버의 권한을 획득한 후 해당 네임서버의 캐쉬와 존 파일 정보를 잘못된 정보로 오염시키는 공격이다. 이 공격이 실행된 후에도 DNS는 존 트랜스퍼를 통해 오염된 정보를 다른 네임서버로 전파하기 때문에 잘못된 네임정보가 인터넷에 퍼지게 된다. 이 공격은 DNS의 정상적인 동작을 통해 전파되기 때문에 발견이 어렵다는 특징이 있다.

위에서 설명한 취약점 이외에도 신뢰받는 서버로 위장, 도메인 네임에 대한 인증된 거부 등의 취약점이 존재한다[4].

3. DNS 보안 위협에 대한 대응안

DNS 인프라는 이를 사용하고자 하는 모든 사용자들에게 접근 가능하게 하는 것을 전제로 하고 있다. 앞 절에서는 이와 같은 DNS에 위협을 주는 취약점들에 대해 분석하였다. 이러한 DNS의 보안상 취약성은 아래와 같은 DNS 메커니즘의 특성에 기인한 것이다.

■ 신뢰할 가치가 없는 소스에 대한 신뢰

■ 이름 기반의 인증 과정

■ DNS 동작 과정상의 부가적인 데이터에 대한 신뢰

이러한 DNS 취약성을 이용하여 악의의 사용자들이 침해를 시도하는 목적은 제공되는 서비스를 불가능하게 하거나 서버 이름이나 데이터의 위/변조를 통해 어떤 목적을 달성하기 위한 의도이다. 이러한 위협의 원인과 목적에 대한 대응안으로서 DNS에서 전송 데이터에 대한 위조, 변조에 대한 무결성(integrity)을 제공하고 DNS 데이터에 대한 기원 인증(data origin authentication)과 같은 메커니즘이 필요하다.

III. DNS Security Extensions

1. DNSSEC이란 무엇인가?

DNS 보안 확장(DNS Security Extension, DNSSEC)의 주목적은 DNS의 취약성을 극복하기 위해 DNS 데이터에 대한 인증과 무결성 서비스를 제공하여 DNS에 보안 요소를 추가하는 것이다. 이를 위해 DNSSEC 프로토콜은 KEY, SIG, NXT 등 새로운 자원레코드(RR:Resource Record) 유형의 정의와 각 구성요소들의 안전한 상태(secure status)에 대한 요구사항들을 정의한다[5].

DNSSEC에서 제공하는 서비스는 아래와 같다.

1) 데이터 기원 인증과 데이터 무결성 보장

DNSSEC은 DNS 데이터에 대해 인증과 무결성을 제공한다. 이 두 가지 기술은 DNS의 RRset들과 연관되어 암호학적으로 생성된 전자서명을 통해 제공된다. 데이터 기원 인증과 무결성 제공 서비스는 DNS 데이터에 대한 통신 과정의 위/변조와 이름 기반 공격 등의 위협으로부터 종단간의 신뢰성 있는 DNS 서비스를 보장한다.

이를 위해, DNSSEC은 새로운 형태의 자원레코드인 SIG RR과 KEY RR을 정의한다. KEY RR은 공개키 암호 방식의 공개키/개인키 쌍 중 공개키를 저장하며 SIG RR은 각각의 RRset에 대해 개인키로 서명된 디지털 서명 데이터를 저장한다. NXT RR은 존재하지 않는 이름(name)에 대한 "음의 응답(negative reply)"에 대해 발생할 수 있는 캐쉬오염과 같은 추가적인 취약점을 방지하기 위하여 존재하지 않는 이름이나 자원레코드 유형에 대한 인증을 지원한다.

2) 트랜잭션과 요청 메시지 인증

전자서명을 사용한 기원인증 및 무결성 서비스는 존 내에 존재하거나 존재하지 않는 자원 레코드에 대한 보호기능을 제공하지만, 실제 트랜잭션이나 요청의 메시지 헤더 등에 대한 보호는 제공하지 않는다. 만일 DNS의 헤더 비트가 악의적인 의도로 서버에 의해 잘못 설정되었다면, 이것을 발견할 수 있는 방법은 존재하지 않는다. 이와 같은 문제는 트랜잭션 인증 메커니즘인 TSIG나 SIG(0)를 사용함으로서 해결할 수 있는데, 이를 통해 리졸버는 수신된 메시지가 자신이 질의를 보낸 서버로부터의 응답이고, 전송 과정 중에 위조 혹은 변조되지 않았다는 것을 확신할 수 있다.

요청 메시지에 대한 인증이 DNS 서버에 대해 아무런 기능도 제공하지 않지만 이 메커니즘은 안전한 트랜잭션(transaction) 및 동적 업데이트(dynamic update)에도 사용할 수 있다[6].

2. DNSSEC의 구성

1) 새로운 RR

■ KEY RR

DNSSEC은 DNS 자원레코드 묶음(RRsets)을 서명하고 인증하기 위해 공개키 암호방식을 사용한다. 여기서 사용되는 공개키가 DNSSEC 인증 과정에서 사용되기 위하여 KEY 자원레코드에 저장된다. 존은 자신이 권한을 갖고 있는 RRsets를 비밀키를 사용해서 서명하고, 비밀키에 대응하는 공개키를 KEY RR에 저장한다. 리졸버는 이 존의 RRsets를 인증하기 위해서 생성된 서명과 공개키를 사용할 수 있다.

■ SIG RR

개인키를 이용해 생성된 서명(signature)은 SIG 자원레코드에 저장되고 DNSSEC 인증 과정에서 사용된다. 예를 들면, 존은 자신이 권한을 가지고 있는 RRsets를 개인키로 서명하고, 그 결과값인 서명을 SIG RRs에 저장한다. 리졸버는 이 서명을 가지고 존의 RRsets를 인증할 수 있다.

SIG RR은 서명에 대한 유효기간을 명시하고 있으며, 서명을 증명하는데 사용될 수 있는 공개키를 식별하기 위해서 "algorithm"과 "signer's name", "key tag"를 사용한다.

SIG RR의 서명은 RRset 외에 트랜잭션을 보호할 수도 있다. 이러한 경우, "Type Covered" 필드 값이 0으로 설정되는데, 이러한 SIG RR을 SIG(0)이라고 한다.

■ NXT RR

기본 DNS 프로토콜에 따르면, 리졸버가 질의한 메시지의 QNAME이나 QTYPE에 존이 가지고 있지 않은 데이터에 대한 값이 설정되어 요청되면, 서버는 리졸버에게 음의 응답을 반환하도록 규정되어 있다. 하지만 이와 같은 메커니즘은 실제 존재하는 데이터에 대해서도 사고나 혹은 악의적 의도에 의해서도 같은 응답을 반환하게 될 가능성이 존재한다. 이 경우 잘못된 음의 응답이 캐쉬 될 가능성도 있어 복합적인 DNS 취약성을 유발시킬 수 있으므로 강력한 존재 부정 메시지 인증 메커니즘을 요구하게 된다. NXT RR은 자신이 속하는 소유자 명이 어떠한 유형의 자원 레코드들을 가지고 있는지 나타내고, 정규형 이름순서(canonical order)에 따르는 다음 번 이름을 가리킨다. 즉, NXT RR은 존 내에 특정 소유자 명이 존재하는지, 그리고 그 소유자 명에 특정 유형의 RRsets이

존재하는지를 증명하는 데 사용된다.

2) 신뢰사슬(chain of trust)

DNSSEC에서는 인증이 이루어지는 대상 도메인에 대해 네임서버 간의 유기적인 연결을 통하여 신뢰사슬 메커니즘을 도입한다. 신뢰사슬 메커니즘의 기본 개념은 해당 네임서버의 공개키를 상위 존으로 트랜스퍼하여 전달하고 전달된 공개키는 상위 존의 개인키로 암호화하여 다시 원래의 존으로 트랜스퍼한다는 것이다. 이것은 공개키의 노출 시에 발생할 수 있는 보안 위협을 감소시키기 위한 것이다.

아래의 [그림1]은 신뢰사슬 메커니즘을 보여준다.

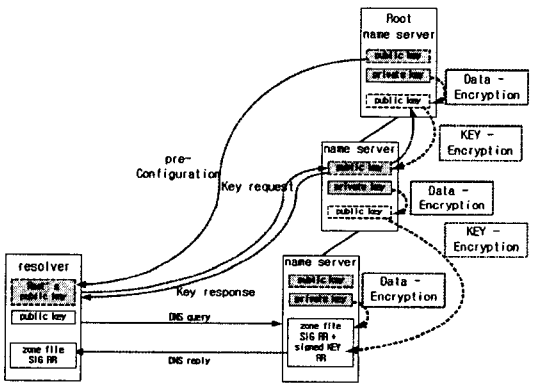

그림 1 신뢰사슬 메커니즘

신뢰사슬 메커니즘은 상위 네임서버로의 반복적인 암호화를 거쳐 결국 루트서버로부터 해당 서버까지 인증 사슬이 형성되며 이로 인해 응답의 요청을 보내는 리졸버는 DNSSEC을 지원하기 위하여 항상 루트의 공개키를 설정해야 한다는 전제가 붙는다[7].

그러나 신뢰사슬은 공개키의 안전성 문제로 인한 키 롤오버(rollover) 시에 많은 부하가 발생한다는 문제점을 안고 있다.

3. DNSSEC의 동작

DNSSEC의 동작은 아래와 같이 4가지 과정으로 분류된다.

- 존에 대한 서명
- 요청에 대한 정보 제공
- 요청 결과에 따른 분석
- 응답에 대한 메시지 인증

DNSSEC의 운영 시에 가장 많은 비중을 차지하는 동작과정은 응답 메시지에 대해 메시지를 인증하는 과정이다.

[그림2]는 신뢰사슬이 적용된 리졸버가 네임서버를 대상으로 질의를 보냈을 경우, 어떻게 응답 메시지에 대한 복호화를 수행하는 지에 대한 과정을 보여준다.

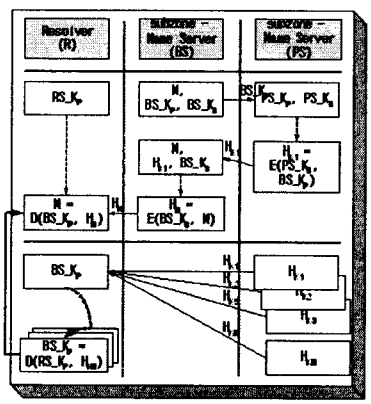

그림 2 응답메시지 인증과정

무결성 보호를 위해 SIG RR을 사용하여 RRset을 인증함과 동시에 SIG RR에 대한 유효성 검사가 끝나고 나면 서명된 데이터는 재조립되어 인증된 응답메시지로써 리졸버에 의해 인정받는다.

4. DNSSEC에 대한 고려사항

DNSSEC은 공개키 암호화 방식을 사용하여 메시지에 대한 무결성과 신뢰할만한 근원지 인증을 수행한다. 그러나 DNS의 특성상 많은 패킷이 짧은 시간에 일어나는 경향이 있는데, DNSSEC의 적용은 각 패킷마다 새로운 RR의 포함으로 인한 메시지 크기 증대와 암호화 및 복호화로 인한 처리시간(processing time)의 증가가 적용에 있어 문제가 되고 있다. 더욱이 키 롤오버에 따른 트래픽 증가와 신뢰사슬 형성 시에 키의 전송으로 인한 트래픽 증가 등은 네트워크 상의 과부하를 더욱 증폭시킨다. 따라서 이를 해결하기 위해 많은 연구가 진행되고 있는데 그 중 DS RR의 적용과 KSK(Key Signing Key)/ZSK(Zone Signing Key)의 적용은 인증에 필요한 정보의 변경을 가져오기 때문에 주목해야 한다.

1) KSK/ZSK

이것은 DNSSEC의 초기 테스트에서 입증된 키

의 사용과 분배 측면의 성능향상에 기반하며 KSK는 존의 KEY RR을 대상으로 암호화를 수행하는 공개키를, ZSK는 존을 구성하는 파일의 데이터를 표현하는 자원레코드에 대한 암호화를 수행하는 데 사용된다. KSK는 DS RR을 생성하거나 신뢰성을 인정받은 하위 존을 위해 리졸버로의 키 분산을 위해서 사용된다. 이것은 해당 존에 속하는 키를 롤오버(roll-over)할 경우, 기능상의 분류에 따라 유효기간을 다르게 줌으로써 롤오버 처리 과정이 짧아지며 그로 인해 처리 속도를 향상시켜준다. 관리자의 입장에서는 해당 KEY RR이 KSK인지 ZSK인지를 구분해야 할 경우가 있다. 이를 만족시키기 위해 KSK 플래그 비트를 설정함으로써 보다 쉽고 빠르게 KEY RR의 기능을 분류할 수 있다. 그러나 이 KSK 비트가 절대적인 기능의 분류를 나타내지는 않는다[8].

2) DS RR

DS RR의 존재는 존의 위임을 나타내는데, 그에 해당하는 RDATA는 위임되거나 하위 존에 대한 권한을 갖는 서버를 나타낸다. 실제 수행 결과치를 볼 때 인터넷에서 일어나는 위임의 10-30%가 서로 다른 NS RR을 갖게 되며 이로 인해 아래와 같은 문제점들이 발생할 수 있다. 따라서 상위와 하위 존 사이에 통신을 줄일 수 있는 새로운 접근 방식이 요구된다[9].

■ 존의 apex에서의 저장되는 키의 양의 증가

■ KEY RR에 대한 빈번한 업데이트 필요성

■ 키 롤오버 메커니즘에 의해 키의 중복이나 분실의 위험성의 증가

■ 상위 존으로부터의 DNSSEC KEY RR이 아닐 경우 해당 패킷을 제거

■ 상위 존에서의 KEY RR 에 대한 실행시간 고려하지 않음

존이 위임을 통해 구분되는 경우에 있어서도 키의 신뢰성을 유지하기 위해 DNSSEC에서는 상위 존과 하위 존 사이에 신뢰 사슬 구조를 형성하게 된다. 신뢰 사슬 구조는 RFC2535에서도 존재하지만 기존의 구조에서는 키의 암호화를 위해 상위 존과 하위 존 사이의 상호 키 교환으로 인한 트래픽 상의 오버헤드와 위임이 일어날 경우 권한을 인정받은 존을 구성하기 위해 필요한 모든 키가 저장되어야 하는 저장 공간상의 오버헤드가 DNSSEC의 적용에 있어서 효율성을 저하시킨다. DS RR은 하위 존의 KSK를 포인팅 함으로써 그 KSK에 대한 신뢰성을 보장하며 하나의 DS RR을 이용해 존에서 사용되는 모든 키에 대한 신뢰성 보장이 가능하기 때문에 공간상의 오버헤드를 줄일 수 있다. 더불어 기존의 신뢰사슬에서는 하위 존의 키가 상위 존에 전송되어 암호화된 후 다시 하위 존으로 반환되기 때문에 최소 2N개의 트래픽이 요구되지만 DS RR을 사용하게 되면 상위 존의 DS RR이 하위 존의 키를 포인팅하고 있으므로 N개의 트래픽이 요구된다. 그러나 ZSK에 대한 해쉬 함수 처리로 인해 하나의 존 안에서 수행하는 복호화 횟수는 2배 이상 증가하여 처리 과정상의 오버헤드는 증가하게 된다.

IV. DNSSEC 적용방안

지금까지 DNS의 보안을 위한 DNSSEC 프로토콜에 대해 살펴보았다. DNSSEC은 DNS에 공개키 기반의 보안 메커니즘을 적용하여 보다 안전하고 신뢰성 있는 인터넷환경을 사용할 수 있도록 하는 것이 목적이지만 아직까지 도입에는 많은 어려움을 안고 있다. 따라서 적용 시에 반발작용을 최소화시킬 수 있는 효율적인 적용방안의 도입이 필요하다.

1. 적용을 위한 고려사항

DNSSEC의 적용은 아직 과부하 등 프로토콜의 자체적인 문제점과 새로운 인프라의 적용으로 인한 반발작용이 문제가 되고 있다. 더구나 DNSSEC의 경우 기술적인 운용능력이 전무해 기술적인 측면과 도입에 필요한 자원 마련에도 많은 어려움이 예상된다.

2. 존의 상태변화에 따른 점진적인 적용

이 절에서는 DNSSEC의 도입을 위해 대상 존의 상태[10]의 변화를 통한 단계적인 적용방안을 모색한다.

1) from Unsecured zone to Locally-secured zone

이 단계에서는 DNSSEC 적용의 필요성을 갖고 있으며 DNSSEC 적용에 필요한 시스템적, 네트워크적인 자원을 보유하고 있는 공공기관이나 단체의 노력이 필요하다. DNSSEC은 아직까지 자체적인 문제점을 완벽히 해결하지는 못했기 때문에 앞으로도 당분간은 계속적인 연구와 개선노력이 필요하기 때문이다. 이러한 공공기관이나 단체에서는 DNSSEC을 적용하는데 있어 자신이 권한을 갖는 존 내에서 DNSSEC을 우선적으로 적용함으로써 개선노력에 필요한 환경을 조성하고 이의 효

용성을 입증하며 그에 대한 정책적인 지원을 끌어내는 노력도 필요하다.

현재의 안전하지 않은 존에서 지역적으로 안전한 존을 구성하기 위해서는 우선 해당 기관의 내부에 DNSSEC 적용에 필요한 자원을 확보하고 DNSSEC을 적용하는 노력이 필요하다. 여기에는 위에서 설명한 DNSSEC 적용을 위한 기술적인 고려사항을 모두 반영한 시스템의 준비가 선행되어야 하며, 더불어 DNSSEC을 지원할 수 있으면서도 해당 기관에서 기존에 수행하고 있던 DNS 동작 역시 지원이 가능해야 한다. 그러나 이러한 노력은 해당 기관의 입장에서도 후에 전체적으로 안전한 존으로의 이전을 위한 좋은 바탕이 된다. 우선 관리자 측면에서의 기술력의 집적은 차후에 보다 단위가 큰 환경에서의 적용에 발생할 수 있는 기술적인 문제에 대해서 해결할 수 있는 능력을 사전에 배양할 수 있게 되며 해당 존의 최상위 서버에서 관리하고 있는 키를 새로 편입하게 되는 존의 상위에 등록만 하면 되기 때문에 키의 분배 문제에도 그리 많은 노력을 필요로 하지 않아 전체적으로 안전한 존으로의 이전이 간단해진다.

2) from multiple Locally-secured zones to Globally Secured zone

몇몇 존에서 DNSSEC의 적용을 위한 노력을 통해 지역적으로 안전한 존을 구성한 후에는 이와 같은 존들을 연계하여 전체적으로 안전한 존의 상태로 옮겨가는 노력이 필요하다. 이러한 노력은 대체로 국가적인 TLD(Top Level Domain)나 그에 버금가는 규모의 TLD에서 이루어져야 한다. 만일 이러한 통합의 움직임이 그보다 하위의 존에서 일어나게 될 경우, 후에 보다 큰 규모의 통합이 필요하게 될 경우 전체적으로 키를 재분배하고 위임관계를 형성해야 하는 어려움이 따르기 때문이다. 물론 통합의 움직임이 일어나는 시기에 기반 기술의 보급 지연이나 자원의 문제 등의 문제가 있을 때는 여러 단계에 걸친 통합의 움직임이 시도될 수도 있다.

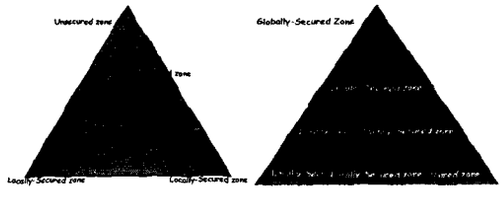

그림 3 존 상태변화에 따른 적용방안

이 과정에서 또 하나 고려할 수 있는 것이 이미 존재하고 있는 지역적으로 안전한 존의 위치에 대한 고려이다. 이것은 DNS 시스템의 구성에 있어 이미 상하관계를 이루고 있는 안전하지 않은 존들과 서로 별개의 도메인에 속하는 존들의 경우를 생각할 수 있으며 이러한 위치관계를 고려하여 체계적인 정책이 수립되어야만 한다. 이 과정을 통해 보다 효율적인 적용을 꾀할 수 있을 것이다.

■같은 도메인 내의 상하관계를 이루고 있는 존

같은 도메인 내에서 이미 상하관계를 이루고 있는 존이라면 DNSSEC의 적용은 훨씬 간단해진다. DNSSEC의 적용을 위한 주요 작업 중 키 분배나 존에 대한 사인 등이 간단하게 해결되기 때문이다. 따라서 이러한 상태의 존들을 우선 통합하는 작업이 필요하다. 이 경우 앞에서 설명한 것과 같이 도메인에서 사용할 apex 키를 생성하고 이를 존 트랜스퍼를 이용하여 하위 네임서버에 전송한 후 그 네임서버가 속한 존을 서명하기만 하면 된다.

■상이한 도메인에 속하는 존

같은 도메인 내에서 상하관계를 이루고 있던 존들이 보다 큰 규모의 지역적으로 안전한 존으로의 이전이 끝나게 되면 서로 다른 도메인에 속하는 존 사이에 DNSSEC 통합을 추진해야 한다. 서로 상이한 도메인 내에서 각각 DNSSEC을 적용한 경우에는 통합을 하려는 존 사이에 사전에 협상이 이루어져야 한다. 따라서 이러한 협상에 대한 내용도 정의되어야만 하는데 여기에는 키의 교환, 암호화 알고리즘의 통일, TTL, 등 인증에 사용되기 위한 모든 인자들이 그 대상이 된다. 전체적으로 안전한 존으로의 움직임은 보다 큰 규모의 지역적으로 안전한 존으로의 이전단계의 반복이라고 볼 수 있으며 이를 위해서는 형성되어 있는 지역적으로 안전한 존이 통합의 움직임이 있는 상위의 존의 적절한 위치에 포함되며 그로 인해 키의 공유와 분배 및 신뢰사슬의 형성이 필요하다. 이는 DNSSEC의 구현을 위한 준비가 되어있는 지역적으로 안전한 존에서는 비교적 간단한 일이 될 것이다. 그러나 아직 준비가 되어있지 않은 안전하지 않은 존이 이러한 통합작업에 참여하게 된다면 그러한 존들은 지역적으로 안전한 존으로의 1차적인 단계를 스스로 거쳐야 하므로 여기에서 기존에 형성되었던 지역적으로 안전한 존들과의 관리능력면이나 운영계획, 관리 정책 및 보안 정책의 수립 등 보다 큰 노력이 필요하다.

3. 기타 고려사항

DNSSEC의 적용은 아직까지도 어려운 문제에 직면하고 있는데 그것은 DNSSEC의 적용에는 시스템과 네트워크 자체에 많은 부하가 발생한다는 것이다. 시스템에 발생하는 부하는 관리자 차원에서의 추가적인 설정, 존 파일 크기의 증대 등의 문제도 있지만 그로인해 발생하는 네트워크 트래픽의 증가는 DNSSEC이 한 프레임의 크기는 작지만 한꺼번에 여러 프레임이 전송된다는 특징을 갖는 확장된 프로토콜이라는 점에서 치명적이라 할 수 있다.

따라서 트래픽에 대한 분석을 통한 DNSSEC 안정화 작업은 DNSSEC 적용을 위한 바탕이 되는 중요한 작업이라 할 수 있다. 이것은 네트워크 엔지니어링이나 관리 측면에서 해당 트래픽에 대한 통계 데이터를 제공하여 보다 완전한 네트워크 시스템 구현을 위한 바탕이 될 수 있을 것이다. 더불어 잘못된 설정으로 인한 보거스 트래픽의 발생에 대한 발견 및 분석과 바이러스나 보안 공격에 대한 분석 및 새로운 보안정책 형성에 도움을 줄 수 있을 것이다.

V. 결론

본 논문에서는 DNS에 위협을 주는 프로토콜 자체의 취약성을 분석하였고, 이를 극복하기 위한 요구사항으로서 IETF에서 제안하고 있는 DNS 보안 확장 기술에 대한 요소기술을 분석하고 적용방안에 대해 논하였다.

DNSSEC의 적용에는 아직까지 프로토콜 자체적인 문제점과 여건 조성의 어려움 등이 문제시되고 있으나 시스템과 네트워크 기술의 발전에 따라 과부하를 수용할 수 있는 요건이 갖추어지고 DNS의 보안의식이 확대되어 가면 DNSSEC의 적용은 인터넷 자원 관리의 중요한 요소 중 하나가 될 것이다. 앞으로는 DNSSEC 적용의 확대와 함께 기타 다른 보안 요소들과의 연계에 대한 연구를 통하여 DNSSEC의 적용으로 인한 부담을 줄이고 보다 완벽한 보안 인프라 구축을 위한 방안에 대해 계속적인 연구가 이루어져야 하겠다.

참고문헌

[1] 안철수연구소 기술기획실, "SQL Overflow 웜 이 기술 분석 보고서", 2003년 1월.

[2] 배문식, "PKI를 이용한 DNS 보안 동향", 정보통신정책연구원, 2003년 4월 24일.

[3] Steven M. Bellovin, "Using the Domain Name System for System Break-ins", Proceedings of the fifth UNIX Security Symposium, pp. 199-208, June 1995.

[4] D. Atkins, R. Austein, "Threat Analysis of the Domain Name System", IETF network working group, Oct. 2003.

[5] D. Eastlake, "Domain Name System Security Extension", RFC 2535, March 1999.

[6] B. Wellington, "Secure Domain Name System Dynamic Update", RFC3007, Nov. 2000.

[7] R. Gieben. "Chain of Trust - The parent-child and keyholder-keysigner relations and their communication in DNSSEC", Master's thesis, University of Nijmegen, Dec. 2000.

[8] Johan Ihren, "An Interim Scheme for Signing the Public DNS Root", IETF internet draft, Feb. 2003.

[9] Olafur Gudmundsson, "Delegation Signer Resource Record", IETF DNSEXT working group, Dec. 2002.

[10] E. Lewis, "DNS Security Extension Clarification on Zone Status", RFC3090, Mar. 2001.