

DNSSEC

DNS의 표준은 침해공격의 가능성을 고려하지 않던, 인터넷이 처음 시작되던 25년 전에 정해진 표준 프로토콜이다.

인터넷이 우리 일상의 모든 것을 변화시키면서 침해공격으로부터 DNS 데이터를 보호해야 될 필요성이 점차 증가하고 있다.

DNSSEC은 DNS가 제공하는 다양한 DNS 데이터가 위-변조 침해공격으로 위-변조되어 호스트 PC의 어플리케이션으로 전달되는 것을 방지하기 위해 DNS 프로토콜을 확장하고 보완하는 표준 프로토콜이다.

DNS 데이터의 주요 취약점

- DNS는 UDP 기반의 네트워크 서비스로 패킷 검증에 대한 메커니즘이 없어 피싱(phishing) 등의 스푸핑(Spoofing) 공격에 취약하다.
- 패킷 가로채기(Packet Interception): DNS가 질의/응답 메시지를 주고받을 때 전혀 암호화되지 않은 UDP 패킷을 사용하기 때문에 패킷 가로채기 유형의 위험에 노출되어 있다.
- ID 추측과 질의 예측: DNS 헤더의 ID 필드는 16비트로 구성되어 있으며, 2^{16} 개의 숫자는 대입법을 통하여 충분히 값을 추측할 수 있다.
- 이름 기반 공격: 공격자는 피 공격자의 캐시에 특정 RRs를 위-변조하여 악의적인 데이터를 제공함으로써, 잠재적으로 DNS를 기반으로 하는 모든 환경에 잘못된 판단을 유발하여 영향을 미칠 수 있다.

DNSSEC의 동작 방식

DNS 프로토콜은 질의응답 과정에서 응답된 메시지에 포함된 데이터가 원본 authoritative(해당 도메인에 대한 권한을 가진) 네임서버가 제공한 데이터인지 아니면 위-변조되어 응답된 데이터인지를 구분하는 수단을 가지고 있지 않다. 표준 DNS 데이터 포맷에 따라 응답된 DNS 데이터를 수신한 경우, 리커시브 네임서버의 리졸버는 이 데이터가 위-변조되어 있더라도 이를 구분하지 못하고 캐시에 저장하여 호스트의 질의에 대한 응답 데이터로 제공하게 된다.

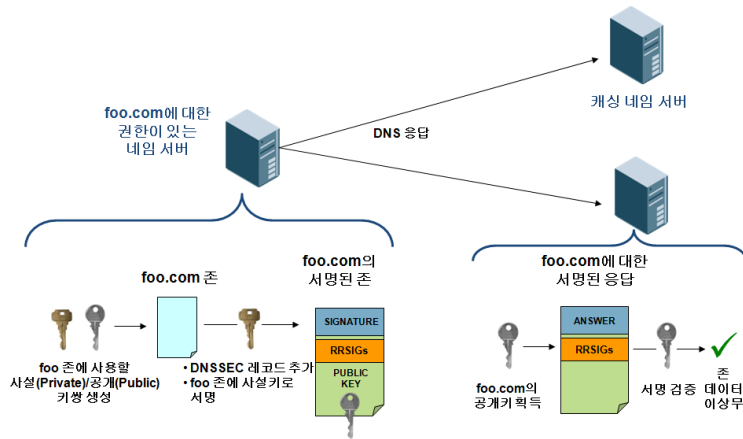


그림 1> DNSSEC 동작방식

DNSSEC은 이들 취약점을 보완하기 위해, DNS의 각 리소스 레코드에 대한 “전자서명(Digital Signature)” 메커니즘을 적용하는 보안 프로토콜을 추가 정의한다. DNSSEC은 공개키 암호화(Public Key Cryptography) 방식의 전자서명을 사용하여 각 리소스 레코드를 전자서명(digital signature)한 후 이를 별도의 리소스 레코드인 RRSIG(Resource Record Signature) 리소스 레코드에 저장한다. RRSIG RR은 질의응답 절차에서 응답 메시지에 함께 포함되어 응답한다. 리졸버는 응답 받은 리소스 레코드에서 함께 동봉된 이 리소스 레코드에 대한 RRSIG RR의 전자서명을 가지고 서명검증 절차를 수행함으로써, 이 데이터가 authoritative 존(zone)의 원본 데이터와 다르지 않음을 검증할 수 있다.

DNSSEC은 DNS 리소스 레코드 데이터를 암호화(encryption)하는 것은 아니다. 공개키 암호화(Public Key Cryptography) 방식은 암호화 메커니즘과 전자서명 메커니즘을 제공한다. 이 중에서 DNSSEC은 암호화 메커니즘이 아닌 전자서명 메커니즘만을 DNS에 적용한다. DNS의 리소스 레코드 데이터는 인터넷 전체에 대한 “공개 데이터(public data)”이기 때문에, DNSSEC을 인식하지 못하는 기존 리졸버들도 이 데이터를 질의하여 조회하는데 문제가 없어야 한다.

공개키 암호화 방식의 전자서명은 데이터를 암호화하는 것이 아니라 데이터의 소유자가 이 데이터를 작성했음을 증명하는 방법을 제공한다. 이는 반대로 이 데이터가 중간에서 누군가에 의해 임의로 변조되었을 때, 이 데이터가 변조되었음을 검출할 수 있는 수단이기도 하다.

DNSSEC은 이와 같은 전자서명의 특성을 DNS 체계에 적용한 표준 프로토콜이다. Authoritative 네임서버의 authoritative 도메인 존은 존의 데이터에 대한 권한이 있는 소유자(owner)다. 따라서 공개키 암호화 방식의 개인키(private key)와 공개키(public key)의 소유자는 도메인 존으로 설정된다. 공개키의 소유자가 네임서버나 단위 리소스 레코드가 아니라 도메인의 존인 것은, DNS 체계에서 위임과 관리권한이 존 구역에 의해 구분된다는 것을 생각하면 쉽게 이해할 수 있을 것이다. DNSSEC 프로토콜은 권한 있는 도메인 존의 데이터가 중간에서 위-변조되지 않고 각 리졸버에게 명확히 전달되는 것을 보장하기 위한 표준이다. 이는 보안 측면에서 “데이터 발신 인증(data origin authentication)”과 “데이터 무결성(data integrity)” 수단을 제공한다.

현재 추진되고 있는 차세대 인터넷은 높은 수준의 보안 안전성을 필요로 한다.

차세대 인터넷 환경은 DNS에 대해서도 그 근본적 보안 취약점을 극복하여 신뢰할 수 있는 데이

터블 차세대 인터넷 응용 어플리케이션에 제공할 수 있는 안전한 기반 인프라 시스템으로의 진화가 요구되고 있다.

DNSSEC 구성 요소 및 구조 모델

DNSSEC은 새로운 DNS가 아니라 기존의 DNS에 대한 추가 확장 프로토콜이다. 따라서 DNSSEC은 기존 DNS 프로토콜에서 정의된 구성요소를 그대로 유지하며, 각 구성 요소별로 DNSSEC 지원을 위한 확장사항을 규정하였다.

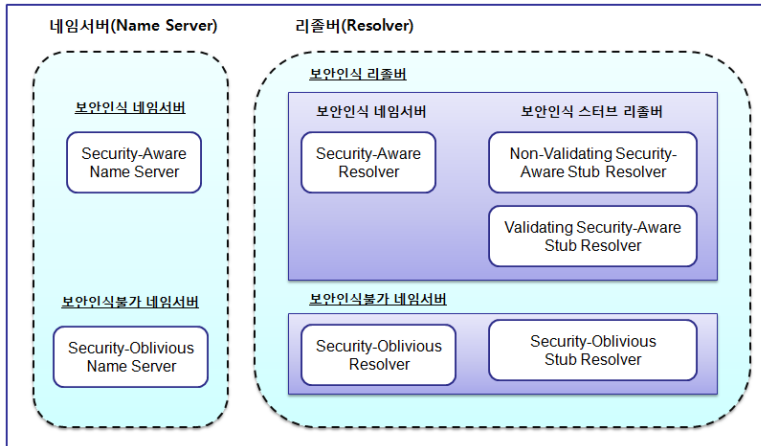


그림 2> DNSSEC 표준에서 DNS 구성요소 중 네임 서버와 리졸버 구분

DNSSEC 표준은 네임서버와 리졸버의 DNSSEC 지원 구현을 필요로 한다. 그러나 DNSSEC은 기존 도메인 네임 시스템에 보안사항을 추가 적용하는 확장 표준으로 기존의 DNSSEC을 인식하지 못하는 네임서버와 리졸버가 인터넷 상에 오랫동안 상존하게 된다. DNSSEC 표준은 기존 DNS 표준만을 인식하는 네임서버와 리졸버가 DNSSEC을 지원하는 네임서버/리졸버와 함께 공존할 수 있고 장기적으로는 DNSSEC 기반의 DNS 체계로 발전할 수 있도록 개발되었다.

따라서 DNSSEC을 지원하는 네임서버/리졸버는 DNSSEC을 인식하지 못하는 기존 네임서버/리졸버와 문제없이 통신할 수 있다. 다만 DNSSEC을 인식하지 못하는 기존 네임서버/리졸버는 기존 DNS 표준의 보안취약점을 그대로 내포하게 된다.

DNS 서버 SW의 DNSSEC 지원현황

표 1> DNSSEC 지원 서버 SW 비교

DNS 서버 S/W	제작/배포	무료배포	DNSSEC 지원	Interface
BIND 9	ISC	○	○	Command line
NSD	Nlnet labs	○	○	Command line
Microsoft DNS	Microsoft	X (운영체제 번들)	일부 지원	GUI, Command line
Infoblox	Infoblox	X (상용)	○	GUI
Adonis	Bluecat Networks	X (상용)	○	GUI
ANS/CNS	Nominum	X (상용)	○	GUI

DNS 표준으로 자리매김한 BIND 9과 NSD는 현재 DNSSEC 표준을 완벽히 지원한다. 그러나 텍스트 형태의 환경설정 파일과 명령어를 통해 설정해야 되는 어려움이 있다. Windows 2008 R2는 일부 GUI와 명령어를 통해 DNSSEC을 적용할 수 있지만 모든 루트 도메인과 ccTLD에서 표준으로 적용하고 있는 NSEC3 표준안을 지원하지 못하고 있다.

그 외 상용 DNS 전용 솔루션들의 경우 GUI를 통해 모든 DNSSEC 표준안을 지원한다.

DNSSEC의 역사

DNS의 주요 보안 취약점은 1990년 스티브 벨로빈(Steven Bellovin)에 의해 발견되었다. 그러나 당시 이 치명적인 취약점을 바로 보완할 방법이 없어서, 취약점 공개로 인해 DNS의 취약점을 악용한 공격이 시작될 수 있다고 판단하였다.

- 1995: 스티브 벨로빈이 DNS 보안에 관련하여 작성한 문서와 DNSSEC이 IETF의 주요 논의대상에 포함됨
- 1999: IETF에서 RFC2535를 발표하여 BIND9에서 DNSSEC을 이용할 수 있도록 개발됨
- 2001: RFC2535의 Key 처리에 대한 운영상의 문제점이 발생하여 DNSSEC 추진이 어려워질 수 있어 RFC2535는 3개의 Draft 문서로 다시 쓰여짐
- 2002~2003: Draft가 재정리되어 BIND9는 새로운 DNSSEC 표준을 적용할 수 있게 됨
- 2005. 3: 3개의 신규 RFC가 발표됨

DNSSEC의 적용 이슈

- 루트 DNS의 공개키와 개인키 쌍에 대하여 하드웨어, 소프트웨어, 시스템 등에 분배 및 사용하는 문제
- 루트 존에 DNSSEC을 적용하는 시기와 국부적으로 운영 및 적용되어 있는 DNSSEC의 관리
- 시스템 리소스 요구사항 검토: DNSSEC 운영상에 추가적인 저장공간, CPU 및 네트워크 대역폭 등이 필요
- DNSSEC 적용에 따른 추가적인 운영자의 노력이 요구됨

다양한 이슈에도 2000년대 후반부터 루트 도메인과 최상위 도메인 등이 DNSSEC를 적용하고, 각국의 관련 기관들이 도입을 적극지원 및 주도하고 있다.

DNSSEC 도입 고려사항

DNSSEC의 적용은 DNS의 관리에 있어 전반적인 비용 증가를 유발한다.

기존 DNS의 경우, 사용자 레벨의 도메인 존을 설정한 네임서버는 최초 구성 후 변경사항이 없으면 그대로 방치하는 경우가 대부분이다. 이는 사이트 별로 설치되어 있는 리커시브 네임서버의 경우도 마찬가지다. 네임서버 소프트웨어는 초기 구축 당시의 버전 그대로이고, 설정 또한 기본 설정만으로 유지된다.

그러나 DNSSEC이 일단 적용되면 이야기는 달라진다. 전에는 사용하지 않았던 서명용 키를 생성

하고 이를 보안정책에 따라 관리해야 하며, 도메인 존 생성과 도메인 네임 추가/변경/삭제시마다 존 파일을 서명해야 한다. 데이터의 변경이 없을 때도 서명된 존의 서명 유효시간이 만료되기 전에 재 서명을 해야 한다. 생성된 서명용 키는 존 서명용 키쌍과 키 서명용 키쌍을 구분하여 관리해야 하고 적절한 주기로 키를 갱신해야 한다. 이런 작업이 도메인 존 내에서만 이루어지지 않고 외부의 상위 도메인 관리자의 협조가 필요하기도 한다.

뿐만 아니라 서명검증에 문제가 발생하면 서비스 접속 장애가 발생할 수 있으므로 존의 키 갱신 등의 변경 사항이 있을 때, 리졸버의 상태를 고려하면서 작업 계획을 수립해야 한다. 이런 작업 중에 실수가 발생하면 리졸버에서 서명검증이 실패하는 경우가 발생하고 이로 인해 서비스 접속 장애가 발생할 수 있다.

한마디로 그대로 방치해도 문제가 없던 DNS에 까다로운 보안 관리를 필요로 하게 된다.

DNS 전용 솔루션

기존 DNS에 DNSSEC을 적용 및 관리 운영하는 것이 쉽지 않아진다. 보안/시스템/비즈니스환경/프로세스 등 다양한 조건을 고려해야 한다. DNS 전문 관리팀과 운영인력이 있는 경우 큰 어려움이 없겠지만, 그렇지 않은 경우 관리의 효율성/가용성/보안 등의 사항을 고려하여 전용 DNS 솔루션 도입도 권장할만하다.

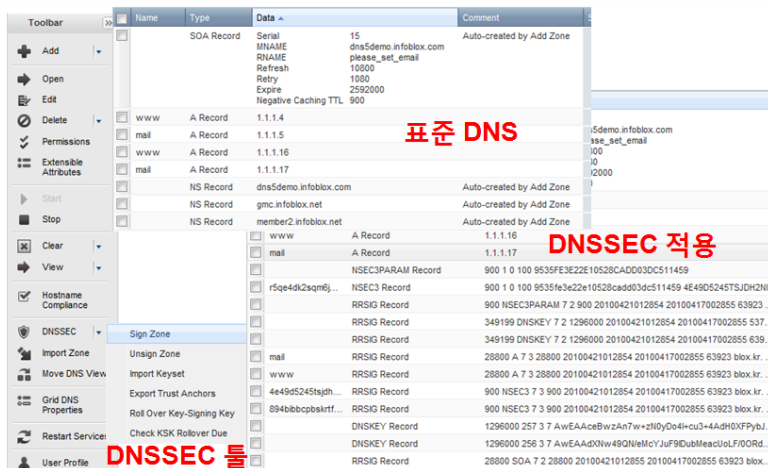


그림 3> Infoblox의 DNS 전용 어플라이언스

이번 호에서는 DNSSEC이란 무엇이며, 탄생 배경/목표/이슈 사항과 적용시 고려사항 등을 살펴보았다. 다음 호에는 국가/기관별 DNSSEC 도입 현황과 우리나라의 DNSSEC 적용 로드맵을 소개한다. 마지막으로 DNSSEC 적용시 참고할 수 있는 자료와 툴에 대해 알아보겠다.

[솔루션 문의]

㈜오픈베이스 시스템사업본부 infrasales@openbase.co.kr