KIPS Tr. Comp. and Comm. Sys.
Vol.4, No.8 pp.259~270 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2015.4.8.259

Automated Method for the Efficient Management of DNSSEC Singing Keys in Korea

Myung Hee Choi† · Seung Joo Kim††

ABSTRACT

In this paper, we study and implement ways for users to easily apply and manage the DNSSEC in a domestic environment. DNSSEC is the DNS cache information proposed to address the vulnerability of modulation. However, DNSSEC is difficult to apply and manage due to insufficient domestic applications. In signing keys for efficient and reliable management of DNSSEC, we propose proactive monitoring SW and signing keys. This is an automatic management s/w signing key for DNSSEC efficient and reliable management and to provide a monitoring of the signing key. In addition to the proposed details of how DNSSEC signing key update and monitoring progress smoothly, we expect that the present study will help domestic users to apply and manage DNSSEC easily.

Keywords : Automatic Management S/W, BIND, DNSSEC, KEY Roll-over, KSK, Monitoring, ZSK

국내 DNSSEC 서명키의 효율적인 관리를 위한 자동화 방안

최 명 희† · 김 승 주††

요 약

본 논문은 DNSSEC 적용을 국내 환경에 맞게, 사용자들이 보다 쉽게 적용 및 관리할 수 있는 방법에 대해 연구하고 구현하였다. DNSSEC은 DNS 캐시 정보가 위·변조되는 취약점을 해결하기 위해 제안된 것으로, DNSSEC 적용 및 관리에 어려움이 있어 국내 적용이 미비한 편이다. 이에 DNSSEC의 효율적이고 안정적인 관리를 위한 서명키 자동관리 SW와 서명키 모니터링을 제안하고자 한다. 더불어 제안한 사항을 실제 구축하여 DNSSEC 서명키 갱신과 모니터링이 원활하게 진행되는지 살펴보고, 본 연구가 향후 국내 DNSSEC 사용자들이 보다 쉽게 DNSSEC를 적용·관리하는 데 도움이 될 것으로 기대한다.

키워드 : 자동관리 S/W, BIND, DNSSEC, 키 갱신, KSK, 모니터링, ZSK

1. 서 론

우리는 스마트폰 혹은 컴퓨터로 인터넷에 접속하여 각종 정보를 검색하고, 뉴스 등을 확인하며, 마우스 클릭으로 많은 일을 하고 있다. 이처럼 인터넷은 우리 삶에 많은 부분을 차지하고 있고, 우리 삶에 끼치는 긍정적인 요소가 높이 평가되었지만 근래에는 사이버 범죄 등의 부정적인 요소가 급증하고 있다. 이로 인해 안정적인 인터넷 서비스에 대한 요구가 증가하고 있으며, 안정적인 인터넷 서비스를 영위하기 위하여 인터넷의 근본인 DNS에 대한 보안 취약점인 캐시 정보의 위·변조를 막기 위한 DNSSEC (DNS Security Extension)에 대한 세부적인 연구가 필요하다.

현재 DNSSEC는 유럽 국가들을 중심으로 많이 적용되어 운영되고 있으나, 아시아 국가들의 도입률이 현저히 낮은 추세이다. 2014년 APNIC(Asia-Pacific Network Internet Center) 통계에 따르면, OECD 가입국의 DNSSEC 도입률을 비교한 결과는 Fig. 1과 같으며, 한국이 최하위에 랭크되었다[1]. 국내 DNSSEC 적용률이 2% 이하로 타 OECD 국가들에 비해 낮음을 알 수 있다.

국내 DNSSEC 도입률을 높이기 위해서는 DNSSEC에 대한 인식 제고도 필요하지만 무엇보다도 DNSSEC 기반의 DNS 데이터의 서명 및 검증을 위해 필요한 서명키(KSK, ZSK)의 효과적인 운영 및 관리 방안 마련이 필요하다. ICANN(Internet Corporation for Assigned Name and Numbers) 또한 SSAC(Security and Stability Advisory Committee)에서 DNSSEC 서명키 교체(Rollover)에 관한 보안 및 안정적

† 정 회 원 : 한국인터넷진흥원 선임연구원,
고려대학교 정보보호대학원 석사수료
†† 종신회원 : 고려대학교 사이버국방학과 교수,
고려대학교 정보보호대학원 교수
Manuscript Received : May 8, 2015
First Revision : June 15, 2015; Second Revision : July 6, 2015
Accepted : July 6, 2015
* Corresponding Author : Kim Seung Joo(skim71@korea.ac.kr)

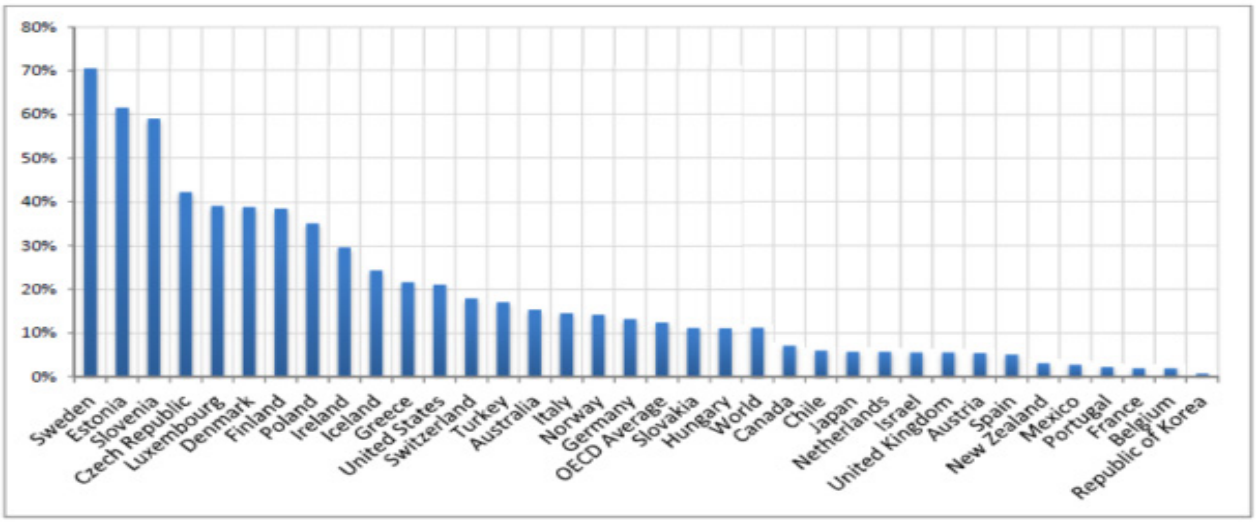


Fig. 1. Present Condition of Country DNSSEC(2014)

인 관리 방안에 대한 권고문을 2013년 11월에 발표하였다[2]. 추가적으로 2013년 6월에는 '.biz' DNSSEC 서명키가 잘못되어 'isc.biz' 도메인에 대한 DNSSEC 유효성 확인이 불가한 일이 발생하였다[3].

본 논문에서는 기존 DNSSEC 적용에 대한 문제점을 살펴보고, 이를 개선하기 위한 DNSSEC 서명키 자동화 메커니즘 및 모니터링을 제안한다. 더불어 나라별 DNSSEC KEY 길이 및 교체 주기가 상이하기 때문에 국내 환경에 맞는 DNSSEC 서명키 생성 및 관리 방안을 도출하고자 한다.

본 논문은 다음과 같이 구성되어있다. 2절은 관련 연구로서 DNSSEC에 대한 동작원리, 국제표준, 국내외 도입 현황 및 필요성 등에 대해 살펴보고, 3절에서는 DNSSEC의 도입 시 고려사항 및 문제점 등에 대해 살펴본다. 4절에서는 문제점을 해결할 수 있는 서명키 자동 생성 메커니즘 및 모니터링을 제시하고, 5절에서는 본 제안의 결과와 향후 연구 방향에 대하여 기술한다.

2. 관련 연구

2.1 DNSSEC 개요

1) DNS 취약점

전산시스템에 대한 해킹 공격이 심화되고 있는 현재, DNS도 예외는 아니다. 리커시브 네임서버의 캐시 데이터를 위·변조함으로써 정상적인 인터넷 접속을 방해하는 공격 형태도 나타나고 있다.

가장 대표적인 사례는 1997년 미국에서 발생한 사건으로, 당시 인터넷 도메인 관리 최상위 기관이었던 InterNIC의 웹사이트에 대한 웹 접속 트래픽이 제3의 웹사이트로 전환되도록 DNS 캐시 포이즈닝(cache poisoning)을 유발한 사건이다. 이 사건은 AlterNIC의 설립자였던 유진 카시푸레프(Eugene Kashpureff)에 의해 발생했다. 그는 당시 InterNIC이 인터넷의 상위 도메인을 독점하고 있는 것에 대한 강력한 항의의 표시로써, DNS 보안 취약점을 이용하여 InterNIC 사이트에 접속하는 트래픽을 AlterNIC 사이트로 전환하게 만들어버렸다. 이 사건은 DNS 프로토콜의 취약점을 실제로 드러낸 사건으로서, 이 취약성을 활용하여 웹 접속 트래픽을 마음먹은 대로 제3의 서버로 전환시켜버리는 것이 가능하다는 것을 여실하게 보여주었다. DNS 취약성이 본격적으로 이슈화되기 이전의 네임서버들은 DNS 메시지 ID를 순차적으로 증가하는 값을 사용하도록 구현하고 있었다[4].

2005년 상반기에 발생한 캐시 포이즈닝 피해는 주로 Microsoft Windows 서버의 DNS 서버에서 발생하였다. Microsoft Windows NT/2000 서버의 DNS 네임서버가 캐시 DNS로 동작할 때, 위·변조된 응답 데이터를 검출하여 대처하는 기능을 제공하는 DNS 캐시 오염(cache pollution) 방지기능이 디폴트로 동작하지 않기 때문에 그 피해가 발생하였다. 이에 비해 Windows 2003 서버는 캐시 오염 방지 기능이 디폴트로 동작하므로 피해가 없었다. 이 사례에서 Windows DNS를 사용하는 캐시 DNS에서 .COM에 대한 네임서버 정보가 위장된 네임서버로 변경되어 반영되고 있는 것이 발견되었다. 이 침해 사건은 오래된 버전의 DNS 버전을 사용하고 있거나, 캐시 포이즈닝 방지 기능이 적용되지 않은 캐시 DNS의 경우, 간단한 형태의 공격으로 말미암아 캐시 포이즈닝 피해를 볼 가능성이 있다는 점을 상기하도록 하였다[5].

2011년 브라질에서 ISP를 대상으로 하는 DNS 캐시 포이즈닝 공격이 발생하여 3~4백만의 ISP 서비스 이용자가 G-mail, Youtube, MS Hotmail 접속 시 악성 프로그램 설치 웹사이트로 유도되는 사건이 발생하였다[4].

위 사건들은 오래된 DNS 버전을 사용하고 있거나, 캐시 포이즈닝 방지 기능이 적용되지 않은 캐시 DNS의 경우, 간

단한 형태의 공격으로 말미암아 캐시 포이즈닝이 발생할 가능성이 있다는 점을 상기시켰다.

2) DNSSEC 개념

DNSSEC는 DNS의 근본적인 보안 취약점을 극복하기 위해 개발되었다. DNSSEC는 응답 메시지의 각 Section에 설정되는 리소스 레코드 데이터 자체를 보호하기 위해, 리소스 레코드에 대하여 전자서명 메커니즘을 적용하는 표준 방안을 제공한다.

DNSSEC가 적용되는 핵심적인 데이터 보호 부분은 응답 메시지의 각 Section에 설정되어 응답되는 리소스 레코드 데이터로 Table 1과 같다.

Table 1. The Resource Record of DNSSEC

리소스 레코드(RR)	개요
DNSKEY	도메인 존의 공개키 데이터를 저장하여 제공하기 위한 RR
RRSIG	존 안에 있는 RRset에 대한 개인키의 전자서명한 결과값을 갖는 RR
DS	DNS 고유의 위임체계에 따라 보안 측면의 인증된 위임체계를 구성하기 위한 데이터를 저장하는 RR
NSEC/NSEC3	DNS 데이터 부재 인증을 위해 정의된 RR

DNSSEC가 적용되었을 때, {IP 착발신 주소, UDP 착발신 포트번호, DNS 메시지 트랜잭션 ID}가 일치한다 하더라도, 응답 메시지의 Answer Section에 설정된 응답 리소스 레코드는 이와 함께 제공되는 서명 데이터(RRSIG RR)를 사용하여 서명검증을 통해 이 데이터가 위·변조된 여부, 권한(Authoritative) 네임서버가 서명한 원본 데이터인지를 검증해낼 수 있게 된다. 이 서명 검증에 의한 데이터 위·변조 여부의 검증 기능은 리커시브 네임서버로 하여금 각 수신되는 응답 메시지의 데이터를 조사하고 검증하여 위·변조된 데이터와 안전한 데이터를 분류하여, 캐시에 관리하는 것을 가능하게 한다[4].

3) DNSSEC 키 갱신(Roll-Over)

DNSSEC에서 사용되는 키들은 영구적으로 사용되는 것이 아니기 때문에 키 교체가 필요하다. 키들의 롤링 프로세스에 관여하는 존 관리자들은 반드시 이전 버전의 존 데이터가 캐시에 저장되어있는지 확인해야 한다. 이러한 캐시 데이터들을 무시할 경우, 클라이언트들이 서비스를 제대로 받지 못하게 된다. 예를 들어, 기존의 키로 서명된 존 데이터들을 검증하려고 할 경우에 기존의 키가 캐시에 존재하지 않는 상황에서, 또는 그와 반대의 상황에서 해당 존 데이터는 위조된(bogus) 데이터로 취급된다.

인증키는 보안 설정된 리졸버(Resolver)가 검증한 공개키로서 리졸버(Resolver)가 DNS 데이터 인증에 사용하게 되는 공개키를 말한다. DNSSEC에서 사용하는 키는 KSK(Key Signing Key)와 ZSK(Zone Signing Key)이다. KSK는 오직 DNSKEY RR set에 대한 서명만 수행한다. 대상 영역의 하나 또는 여러 개의 키를 서명한 개인키에 대응하는 인증키(공개키)로 KSK의 대응 개인키는 도메인 영역의 ZSK 데이터를 갖는 DNSKEY RR set을 서명한다.

ZSK는 도메인 영역이 소유하고 있는 RR 모두에 대해 서명하며, 위임 설정에 사용되는 Glue recode(NS 및 이와 관련된 A/AAAA- IPv4인 경우 A레코드, IPv6인 경우 AAAA 레코드)는 서명하지 않는다. ZSK의 대응 개인키는 도메인 존이 '소유하는' 모든 도메인의 RR set을 대상으로 서명한다.

서명키 갱신은 주기적으로 진행되며, 현재 사용하는 키와 다음 주기에 사용할 키를 미리 발행(Pre-publish)하여 주기적으로 교체한다[6].

서명키 갱신 시 Fig. 2와 같이 일정 기간 동안 2개의 서명키가 설정되어있어, 새로운 서명키 교체에 따른 서비스 장애는 발생하지 않는다.

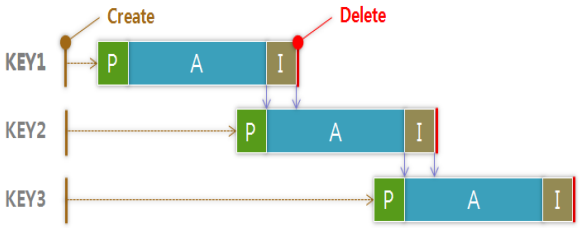


Fig. 2. The Roll-over of DNSSEC Key

위 Fig. 2는 서명키 갱신 절차를 보여주는 것으로, 'Create'는 키가 생성된 상태이며, 'Publish'는 키가 존에 포함되었지만, 서명이 이루어지지 않은 상태를 말한다. 'Activate'는 키가 존에 포함되어 해당 키로 서명이 이루어지는 상태이며, 'Inactive'는 키가 존에 남아있지만 새로운 키로 대치되어 대치된 키로 서명이 이루어지지 않은 상태이고, 'Delete'는 키가 존에서 삭제된 상태이다.

4) 국내외 DNSSEC 키 크기 및 갱신주기 비교

우리나라의 경우 ZSK의 키 크기는 1,024bit로 교체주기는 약 3개월이고, KSK의 경우 키 크기는 2,048bit로 교체주기는 약 12개월이다. 서명키 크기는 컴퓨팅 연산 능력 발전에 따라 권고 사이즈가 향후 변경될 수 있다[7].

미국 NIST의 권고사항의 경우, ZSK의 키 크기는 1,024 bit이고 알고리즘은 RSA-SHA1, 갱신주기는 약 한 달(30일)이다. KSK는 2,048bit로 알고리즘은 ZSK와 동일하며, 갱신주기는 약 12개월이다.

스웨덴의 경우에는 ZSK의 키 크기는 1,024bit로 주기는 1개월이다. KSK는 2,048bit로 유효기간은 2년이다[8].

키 크기별 키 교체주기의 경우 KSK는 부모 존의 DS RR 교체가 필수이다. 캐시 DNS 서버의 서명검증용 레코드 캐싱 상태를 고려하여 작업이 필요하며, ZSK는 부모 존과 상관없이 교체 가능하다.

2.2 DNSSEC 국제 표준

DNS의 근본적인 문제인 보안 취약성을 극복하고 보안성을 부여하기 위한 DNSSEC 표준은 1993년 제28차 IETF회의에서 처음 논의되었다. IETF에서는 DNSSEC 워킹그룹을 중심으로 DNS에 대한 보안 확정 표준을 개발하였다. 1999년 RFC2535 표준 문서를 시작으로, DNSSEC 프로토콜이 최종적으로 완성된 것으로 여겨졌다. 그러나 RFC2535 문서로 대표되는 DNSSEC 표준을 실제 적용하는 데 보안상의 문제점과 적용 운영상의 문제점이 드러나 새로운 표준문서인 RFC4033, RFC4034 및 RFC4035을 2005년에 완료하였다.

그러나 유럽지역에서 DNSSEC를 본격적으로 적용할 때, DNSSEC 표준에서의 NSEC RR에 의해 도메인 존 내부의 도메인 네임과 리소스 레코드 설정 내역이 모두 공개될 수 있다는 점이 개인정보 보호 관련 법률에 위배될 수 있다는 이유로 DNSSEC 적용을 거부하는 이슈가 발생하였다. 실제로 DNSSEC 표준 내용 중 NSEC RR에 의해 DNSSEC가 적용된 도메인의 내부 설정 내역이 용이하게 파악되었다. 이 문제를 존 목록화(Zone Enumeration) 이슈 또는 “Zone Walking” 이슈라고도 한다. 실제 영국과 독일 등은 이러한 개인정보 보호 문제를 이유로 DNSSEC의 자국 도메인에 대한 적용을 유보하는 정책적 태도를 취하고 있다.

IETF DNSEXT 워킹그룹에서는 NSEC RR에 의해 존 목록화(Zone Enymberation) 문제를 해소하기 위한 추가 표준화 작업이 진행되었다. 이는 기존의 NSEC RR을 대신하여 존 목록화 문제를 일으키지 않고 있는 NSEC3 RR의 표준규격이다[6]. 위에서 언급한 대표적인 DNSSEC 국제 표준은 Table 2와 같다.

Table 2. The RFC of DNSSEC

구분	표준명	설명
RFC4033	DNS Security Introduction and Requirements	DNSSEC 개요
RFC4034	Resource Records for the DNS Security Extensions	DNSSEC 리소스 레코드
RFC4035	Protocol Modifications for the DNS Security Extensions	DNSSEC 프로토콜
RFC6014	Cryptographic Algorithm Identifier Allocation for DNSSEC	DNSSEC 암호 알고리즘 추가 요건 변경

2.3 DNSSEC 국내외 도입 현황

1) DNSSEC 국내 도입 현황

국내에서는 DNSSEC 도입을 위하여 2006년에 DNSSEC 시험 시스템을 구축하여 기술적 검증을 실시하여, 2007년에는 2단계 도메인인 ‘safedns.kr’에 DNSSEC 기술을 시범 적용하였다. 2008년에는 DNSSEC 도입을 위한 요구사항 및 필요사항 도출 및 분석을 위한 연구를 진행하였으며, 2009년에는 키 관리 및 존 서명 기본 정책을 수립하였다. 2011년에는 ‘go.kr’을 시작으로 순차적으로 총 31개 국가 도메인 영역에 DNSSEC 서명을 적용하여 2012년 9월에 완료하였다. 2012년에 한국인터넷진흥원 도메인(kisa.or.kr)에 대한 DNSSEC 적용을 시작으로 본격적으로 .kr 도메인에 대한 DNSSEC 실 서비스를 실시하였다[9].

2014년에는 국내 DNSSEC 확대 적용을 위하여 국가도메인 등록대행자와 함께 DNSSEC 시범사업을 추진하였으며, 2014년 12월 기준으로 DNSSEC가 적용된 국가도메인은 2만여 개다.

국내에도 DNS에 대한 보안 중요성이 확산됨에 따라 DNSSEC를 적용한 도메인이 2013년 12월 기준 100개 미만이었으나, 2014년 12월 기준 2만 개로 급증한 것으로 파악된다. 또한, 앞으로도 DNSSEC를 적용한 도메인의 지속적인 증가가 예상된다.

2) DNSSEC 국외 도입 현황

2005년 말 스웨덴은 자신의 최상위 국가도메인인 .SE 도메인에 DNSSEC를 적용하였다. 유럽대륙의 RIR(Regional Internet Registries)인 RIPE NCC는 자신의 도메인과 리버스 도메인(Reverse domain)에 대하여 DNSSEC를 적용하였다. 이외에도 ISC(Internet System Consortium. Inc.)에서는 DNSSEC를 운영할 수 있도록 하는 네임서버 SW인 BIND DNS를 제작, 배포하고 DNSSEC를 적용하였다.

2008년 백악관 예산집행부(OBM)를 시작으로 .gov의 DNSSEC 도입 및 .gov의 연방정부기관 도메인 전체에 DNSSEC를 도입하도록 요구하는 지침을 미국정부에서 배포하였다. 2009년 .org(Public Interest Registry)에 DNSSEC를 서명하였으며, 2010년 7월 15일 IANA가 관리하는 루트 도메인 Zone에 DNSSEC를 서명함으로써 DNSSEC의 궁극적인 적용이 가능해졌다.

2011년 베리사인(Verisign)에서 관리하는 .com 및 .net에 DNSSEC를 적용하였으며, 2012년 미국 ISP인 Comcast가 자사의 캐시 DNS 서버에 DNSSEC 검증기능을 활성화하였다. 2013년에는 글로벌 DNS 서비스 제공 중인 Google Public DNS 서비스의 DNSSEC 검증기능을 활성화하여 DNSSEC 서비스를 이용할 수 있게 되었다.

그뿐 아니라 인터넷주소관리기구(ICANN)에서 2012년부터 진행되고 있는 신규 일반최상위도메인(gTLD) 신규 신청 시 DNSSEC 도입을 의무화하였다. 즉 신규 일반최상위도메인 신청 및 관리기관 획득을 위해서는 해당 최상위도메인의 권한 서버에 DNSSEC를 서명해야 하며, DNSSEC 운영 계획을 제출해야 한다[4].

2.4 DNSSEC 도입 필요성

DNS의 보안 신뢰성 강화를 위한 DNSSEC의 도입 적용은 단순히 도메인 네임 시스템에 대한 위·변조 공격에 대한 대응이라는 소극적 측면만 있는 것이 아니라, 날이 갈수록 증가하고 있는 인터넷 기반 전반에 대한 보안강화 요구 충족을 위한 인프라 차원의 기반 환경을 마련한다는 적극적인 측면을 내포하고 있다.

이러한 적극적인 측면이 DNSSEC의 도입 적용이 궁극적으로 필요한 이유라고 볼 수 있다. 중요한 데이터를 다루게 될 응용 애플리케이션들은 안전한 통신을 위해 각종 인증체계가 필요하게 되며, 이러한 인증을 위한 공개키와 같은 보안 인증용 데이터가 도메인 네임 시스템을 통해 신뢰성을 가지면서 안전하게 배포될 수 있으려면, 도메인 네임 시스템이 DNS 데이터에 대한 위·변조 검증체계를 기본적으로 제공할 수 있어야만 한다. DNSSEC는 전자서명 메커니즘을 도메인 네임 시스템에 적용함으로써 데이터를 안전하게 배포할 수 있는 안전하고 보편적인 개방형 데이터베이스 체계를 제공할 것이다.

DNSSEC 적용 등을 통한 DNS의 보안성 강화는 DNS 자체의 보안성에만 그치는 것이 아니라 DNS를 활용할 수 있는 다양한 응용 애플리케이션의 보안성 강화를 위한 기반 환경을 제공하는 역할을 하게 될 것으로 예상된다[6].

3. DNSSEC 적용 시 문제점

3.1 리졸버(Resolver) 신뢰앵커(Trust Anchor) 설정 문제

DNSSEC는 권한 DNS의 서명된 도메인 존으로만 구성되는 것이 아니라, 캐시 DNS에서의 서명검증을 통해 데이터 위·변조 검증 동작을 포함한다. 권한 DNS의 서명된 존에 설정되는 각 DNSSEC 리소스 레코드 데이터들은 모두 리졸버(Resolver)에서의 서명검증 절차가 효율적으로 진행될 수 있도록 정의되고 설정된다.

캐시 DNS에서의 리졸버(Resolver)가 수행하는 서명검증 절차는 신뢰앵커 설정이 없이는 진행될 수 없다. 신뢰앵커는 서명검증 절차에서 신뢰 판단을 하는 기준점이라고 할 수 있다. 리졸버(Resolver)의 서명검증 절차가 정상적으로 수행될 수 있으려면 리졸버(Resolver)의 신뢰앵커가 전체 인터넷 도메인 존에 설정된 것이 가장 이상적이다.

DNSSEC 적용에서 캐시 DNS에서의 리졸버(Resolver)의 신뢰앵커 설정 및 관리는 서명검증에서 핵심적인 요소이다. 만일 이 신뢰앵커의 갱신이 제대로 이루어지지 않을 경우, 서명 검증이 실패하여 신뢰앵커가 설정된 도메인 영역과 데이터를 비교하고 있음으로써 서비스 접속 불능 상태가 유발될 수 있다. 따라서 리졸버(Resolver)의 신뢰앵커 설정과 관리가 안정적이고 쉬운 방식으로 이루어질 수 있는 체계를 마련하는 것이 필요하다. 2013년 IETF에서는 신뢰앵커 설정과 관리에 관한 메커니즘에 대해 표준화 작업을 완료하였고, BIND 9.7 이후 버전부터 적용하고 있다[6].

3.2 네트워크 장비의 DNSSEC 질의응답 패킷 차단 가능성

DNSSEC를 적용하는 경우, DNSSEC 질의 또는 응답 메시지가 중간의 네트워크 장비로 차단될 수 있다. DNSSEC 표준을 인식하지 못하는 방화벽 장비와 NAT 기반 네트워크 장비가 DNSSEC를 사용한 질의응답 메시지를 차단할 수 있기 때문이다. 이 경우, DNS 질의응답 자체가 실패할 수 있다.

방화벽이나 NAT 장비에서 DNS 응답 메시지 크기가 512바이트 이상인 경우 차단될 수 있다. 이러면 DNS 질의응답이 실패하거나, 또는 최종 응답이 지연될 수 있다. 이를 위해 DNS 질의응답 경로 상에 존재하는 방화벽이나 NAT 장비에서의 DNS 메시지 제한에 따른 패킷 필터링 정책이 있는지 점검하고 개선할 필요가 있다[6].

3.3 DNSSEC를 악용 가능한 DDoS 공격

DNS 프로토콜은 질의 메시지와 응답 메시지로 질의응답 절차가 이루어진다. 이를 패킷 크기 측면에서 볼 때, DNS 질의 메시지는 질의대상 도메인 네임(QNAME)과 질의 리소스 레코드 타입(QTYPE)을 지정하는 작은 바이트의 크기를 갖는 메시지이다. 대상을 지정하는 Question Section, 응답 대상 리소스 레코드를 포함하는 Answer Section, 그리고 Authority Section과 Additional Section 등에 리소스 레코드를 포함하여 질의 메시지에 비해 통상 2배 이상의 크기를 갖는 메시지가 된다. 2006년 상반기에는 네임서버를 공격대상으로 삼지는 않지만, 제3의 특정 호스트를 공격하는 데에 네임서버를 공격의 수단으로 악용하는 방식의 공격이 실제로 시도되었으며, 이를 “Reflected Attack” 또는 “Reflector Attacks”라고 한다. DNS 질의 메시지를 하나 발송했을 때, 그 응답 메시지는 질의 패킷에 비해 2배 이상의 크기를 갖는 응답 패킷으로 증폭되어 되돌아오게 된다. 이러한 트래픽 측면에서의 DNS 질의응답 과정의 증폭(amplification) 효과를 악용하는 공격 방식이다. UDP 기반의 DNS 메시지는 최대 512바이트의 크기를 가질 수 있다는 한계점을 안고 있다. DNS 응답 메시지가 512바이트 길이를 가지고 있는 경우, 이 메시지의 IP 패킷 길이는 약 540바이트가 된다. 이에 공격자는 EDNS0의 OPT RR을 질의메시지에 사용하여, 최대 UDP 페이로드 크기(payload size)를 4,096바이트로 설정함으로써 최고 4,096바이트의 크기를 갖는 응답 메시지로 서비스 거부 공격을 시도한다. 약 70바이트 정도에 불과한 DNS 질의 IP 패킷으로 4,196바이트에 달하는 응답 IP 패킷들을 유도해낼 수 있으므로, 약 60배의 트래픽 증폭효과를 얻을 수 있기 때문이다. 이때, 공격자가 10Mbps 정도의 DNS 질의 패킷을 생성하여 송출할 수 있다면, 공격 대상 호스트에는 약 600Mbps 이상의 DNS 응답 패킷 트래픽이 폭주하여 집중되게 된다[10].

3.4 DNSSEC 적용 관리 비용 증가

DNSSEC의 적용은 도메인 네임 시스템의 관리에서 전반적인 비용 증가를 유발한다. 기존의 도메인 네임 시스템의 경우, 사용자 레벨의 도메인 존을 설정한 네임서버의 경우에는 최초 구성 후 변경사항이 없는 경우 그대로 방치되는 경우가 대부분이다. 이는 사이트별로 설치된 캐시 DNS의 경우도 마찬가지이다. 네임서버 소프트웨어는 초기 구축 당시의 버전 그대로이고, 설정 또한 기본 설정만으로 유지된다.

그러나 DNSSEC가 일단 적용되면, 전에는 사용하지 않았던 서명키를 생성하고 이를 보안정책에 따라 관리해야 하며, 도메인 존을 생성하거나, 도메인 이름을 추가 또는 변경, 삭제할 때마다 존 파일을 서명해야 한다. 데이터의 변경이 없을 때에도 서명된 존의 서명 유효기간이 만료되기 이전에 시간을 맞추어 재서명을 해주어야 한다. 생성된 서명용 키는 존 서명용 키 쌍과 키 서명용 키 쌍을 구분하여 관리해 주어야 한다. 이러한 작업은 도메인 존 내에서만 이루어지고, 또한 적절한 주기를 정해 서명키 자체의 갱신과 외부의 상위 부모 도메인 관리자의 협조가 필요한 작업(DS RR: 위임정보의 갱신)으로 이루어지기도 한다. 그뿐만 아니라, 혹시 서명검증에 문제가 발생하면 서비스 접속 장애가 발생할 수 있으므로, 존의 키 갱신 등의 변경 사항이 있을 때, 리졸버(Resolver)의 상태를 고려하면서 작업 계획을 수립해야 한다. 이런 작업 중에 실수가 발생하면 리졸버(Resolver)에서 서명검증이 실패하는 경우가 발생하고, 이때에는 이로 인한 서비스 접속 장애가 발생할 수 있다. 한마디로 그대로 내버려두어도 문제가 없던 네임서버가 까다로운 보안 관리를 필요로 하는 시스템으로 변모하게 된 것이다. 이렇듯 전반적으로 요구되는 관리 사항은 기존 네임서버 관리체계일 때보다 관리비용이 증가되는 결과를 가져온다.

DNSSEC의 필요성을 인식하고, 자신의 도메인 존에 DNSSEC를 적용하여 서명하려는 경우, 그 서명 자체가 중요한 것이 아니라, 서명된 존을 어떻게 안정적으로 유지 관리할 것인가를 먼저 검토하여 관리체계를 만들어야 한다. 관련된 관리체계 없이, 서명된 존을 반영하여 구축한 경우, 시간이 지나 서명의 유효기간이 만료됨에도 불구하고 그대로 방치한다면, 유효기간 만료 시점부터 그 사이트의 메일 서비스, 웹사이트 접속 등의 관련 도메인 네임을 사용하는 인터넷 서비스가 모두 접속 불능 상태에 빠질 수 있다. 물론 이 경우는 DNSSEC를 지원하는 캐시 DNS에 의해 서비스되는 호스트들에게 그러한 사태가 발생함을 의미한다. 이런 일을 예상치 못한 시스템 관리자들은 혼란에 빠질 수 있다. DNSSEC를 지원하지 않는 일반 캐시 DNS를 사용하는 호스트들은 서비스 접속에 이상이 없지만, DNSSEC 지원 캐시 DNS를 사용하는 호스트들은 서비스 접속 불능 상태를 겪게 된다. 이 두 현상 사이의 차이점이 캐시 DNSSEC 지원 여부라는 점을 직관적으로 파악하기가 어려우므로 문제의 원인을 파악하는 데 장시간이 소요될 수 있다. 이러한 문제는 비단 사용자 레벨의 도메인 존에만 국한되지 않고 국가 최상위 도메인의 경우에도 관리상의 실수로 인해 이러한 서비스 장애가 유발될 수 있다. 국가 최상위 도메인 존의 관리 실수는 그 피해 범위가 해당 국가 최상위 도메인 이하의 모든 도메인 영역에 미치게 된다.

결론적으로 DNSSEC 적용은 단순히 네임서버에서의 도메인 존의 서명이라는 작업을 의미하는 것만은 아니다. 서명된 도메인 존에서 안정적이고 철저한 관리를 지속적으로 해나갈 수 있는 관리체계의 정비 마련이라는 요소가 더 중요하다. 관리체계가 마련되지 않은 채 DNSSEC를 적용했을 때, 혹시 발생할 수 있는 관리상의 실수 하나가 예상치 못한 장애 사태를 유발할 수 있다. 이는 권한 DNS 관리에만 국한되지 않고 캐시 DNS의 신뢰앵커 설정 관리도 해당된다. 특히 ISP와 같은 수많은 사용자 호스트가 캐시 DNS로 사용되고 있는 캐시 DNS에 DNSSEC 지원 기능을 활성화할 때, 신뢰앵커 설정 및 관리체계는 제일 먼저 해결해야 할 숙제인 것이다[6].

4. DNSSEC 서명키 자동화 구현

앞 절에서 제시된 DNSSEC의 문제점 중 본 논문에서는 DNSSEC 적용 관리 비용에 대한 해결책을 제시하고자 한다. 국내 DNSSEC 도입률을 높이기 위해서는 무엇보다도 DNSSEC 운영 및 관리가 용이하여야 하며, 이에 따른 비용이 최소화되어야 한다. 무엇보다도 DNSSEC 서명키가 주기적으로 자동 생성되어 해당 도메인에 대한 서비스 연속성이 확보되어야 하며, 관련 업무 담당자의 업무 효율성을 증대시켜야 한다. 이를 위하여 DNS 담당자들이 DNSSEC를 보다 쉽게 도메인에 적용 및 관리할 수 있도록 서명키 자동화 및 모니터링을 구현하고자 한다.

4.1 DNSSEC 서명키 자동 메커니즘 구현

DNSSEC 적용 도메인 존에 대한 서명키 관리 비용을 최소화하기 위하여 서명키 관리 자동화 기능을 구현한 도구를 개발하였다. DNSSEC 적용 도메인 존에 대한 서명키 관리자동화 도구의 구현은 서명키 관리 서버(DNSSEC Master)들과 웹 서버에 구현한다. DNSSEC 서명키 관리 서버에서 DNSSEC 적용 존에 대한 DNSSEC 서명과 신규 서명키 생성, 그리고 서명키 정보 유효기간 만료 서명키의 삭제(서명 예정일 한 달 이상 경과 키 대상) 및 백업의 과정을 진행한다. 또한, 이 과정을 통해 정리되는 서명키 정보는 JSON 데이터 타입으로 웹 서버로 전달되어 서명키 관리 서버별로 존재하는 서명키 현황을 직관적으로 판단하기 쉬운 간트 차트(Gantt Chart) 형식의 웹 페이지로 조회할 수 있도록 구현하였다.

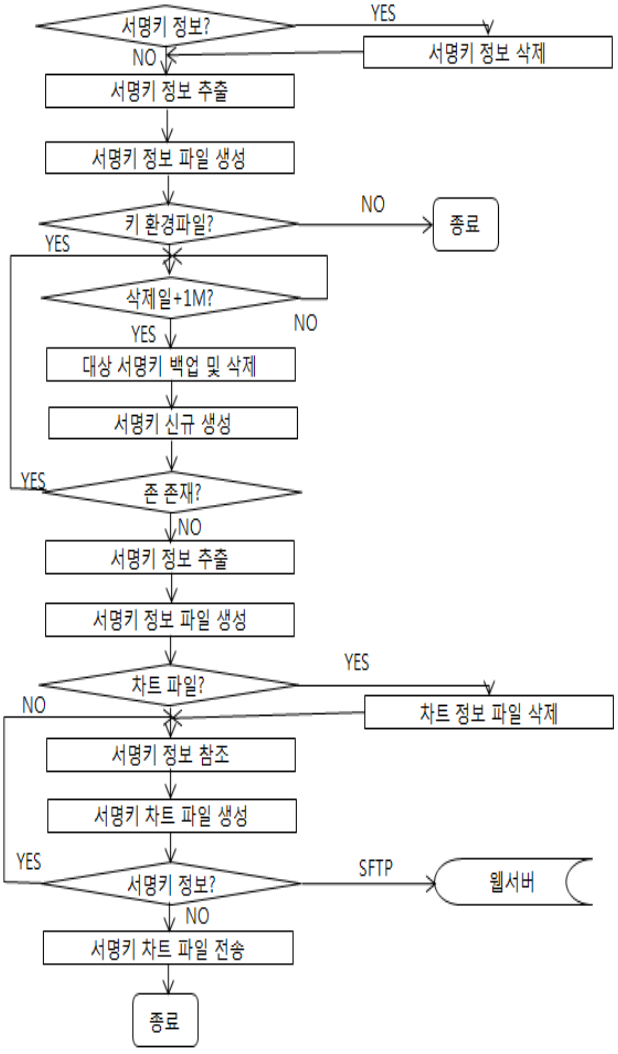


Fig. 3. The Process of Key Auto-management

Fig. 3은 서명키 자동 생성 및 모니터링에 대한 프로세스를 도식화한 것으로, 처음에 서명키가 있는지 여부를 파악하고 해당 서명키 정보를 추출하게 된다. 만일 서명키 정보가 있다면 기존 정보를 삭제하고 새로 추출하여 파일을 생성한다. 그다음에 키 환경 파일의 존 정보 및 서명키 정보를 확인하며, 키 환경 파일이 없다면 종료되고 키 환경 파일이 있으면 서명키 정보 중 맨 마지막 서명키의 삭제일을 맵핑하여 삭제일보다 1개월 이상 남아있으면 추가 확인해야 할 존이 있는지 여부를 확인 후, 없다면 키 정보를 추출하고 서명키 정보 파일을 생성하게 된다. 이때 마지막 서명키의 삭제일이 1개월 미만으로 남았으면, 대상 서명키를 백업한 후 삭제하고 신규로 생성한다. 이를 통해 서명키 사용이 말소되기 전까지 서명키를 새로 생성함에 따라 안정적으로 DNSSEC 서명키를 생성하여 관리할 수 있다.

DNSSEC 서명키 자동 생성 스크립트는 Table 3과 같으며, 서명키 자동화 메커니즘 구현에 있어 중요한 요소이다.

Table 3. The Automatic S/W of DNSSEC KEY Generation

```
k=0
 kdata=$(echo ${ilines[(i*kcnt)+(kcnt-1)]} | tr "|" "\n")
 for y in $kdata
 do
      ((k++))
      case "$k" in
           '2') #zone nam
              zname=$y;;
           '5') #key publish date
              pdate=$y;;
           '6') #key activate date
              adate=$y;;
           '7') #key inactive date
              idate=$y;;
           '8') #key delete date
              ddate=$y;;
      esac
 done
 dpdate='date +%Y%m%d%H%M%S  -d "${pdate:0:8} +3month
 ${pdate:8:2}:${pdate:10:2}:${pdate:12:2}"'
 dadate='date +%Y%m%d%H%M%S  -d "${adate:0:8} +3month
 ${adate:8:2}:${adate:10:2}:${adate:12:2}"'
 didate='date +%Y%m%d%H%M%S  -d "${idate:0:8} +3month
 ${idate:8:2}:${idate:10:2}:${idate:12:2}"'
 dddate='date +%Y%m%d%H%M%S  -d "${ddate:0:8} +3month
 ${ddate:8:2}:${ddate:10:2}:${ddate:12:2}"'

 #echo "${EXE_PATH}/dnssec-keygen -3 -r /dev/urandom -b
 1024 -n ZONE -P $dpdate -A $dadate -I $didate -D $dddate
 ${zname}." >> $LIB_PATH/keygen.cmd
 result='${EXE_PATH}/dnssec-keygen -3 -r /dev/urandom -b
 1024 -n ZONE -P $dpdate -A $dadate -I $didate -D $dddate
 ${zname}.'
 #echo "${zname} zone new file keygen is ${result}" >> $LIB_
 PATH/keygen.result
 echo "${EXE_PATH}/dnssec-keygen -3 -r /dev/urandom -b
 1024 -n ZONE -P $dpdate -A $dadate -I $didate -D $dddate
 ${zname}." >> $LIB_PATH/runcmd.kgen
 echo "rm -f ${ZONE_PATH}/dnssec/${dname}/${result}.*" >>
 $LIB_PATH/recovery.rm
 #printf "%s Zone create data is [publish:{%s}, activate:{%s},
 inactive:{%s}, delete:{%s}]\n" "$zname" "$dpdate" "$dadate"
 "$didate" "$dddate"

 chown                                          named:named
 ${ZONE_PATH}/dnssec/$dname/${result}.*
```

4.2 DNSSEC 서명키 모니터링 구현

DNSSEC가 적용된 도메인 존에 대하여 Fig. 3과 같이 서명키 관리서버에서 생성된 서명키 정보(JSON 데이터 타입)를 전달받아 기존에 차트 파일이 있으면 삭제하고 신규 생성한다. 모니터링은 Fig. 4와 같이 도메인 존의 서명키 현황(적용일시, 활성일시, 비활성일시, 삭제일시, 키 ID)을 간트차트로 변환하여 서명키의 생성주기(Life Cycle)를 쉽게 파악할 수 있도록 구현한다.

DNSSEC 서명키 모니터링 웹서비스의 특성상, 도메인 존에 대한 DNSSEC 적용 시 서명키 관리에 드는 제반 정보를

```
[root@signer chartdata]# cat signer_ackr.js | more
jQuery(window).ready(function () {

    var gantt = JSGanttChart.create({
        types: {
            ksk: {
                name: "Key signing key",
                color: "#CC0000" // red
            },
            zsk: {
                name: "Zone signing key",
                color: "#C79810"  // yellow
            }
        },
        elements: [
            {
                id: "ackrksk1",
                keyidx: "31260",
                name: "Key Signing Key 1",
                startDate: "01 May 2014 01:00",
                endDate: "21 August 2017 01:00",
                type: "ksk",
                elements: [
                    {
                        id: "ackrksk1pdate",
                        name: "publish date",
                        startDate: "01 May 2014 01:00",
                        endDate: "01 May 2014 01:00",
                        percentageDone: 100
                    },
                    {
                        id: "ackrksk1adate",
                        predecessors: ["ackrksk1pdate"],
                        name: "activate date",
                        startDate: "01 May 2014 01:00",
                        endDate: "21 August 2017 01:00",
                        percentageDone: 23.82
                    }
                ],
                percentageDone: 23.82
```

Fig. 4. The Creation of Singing Key Chart File

웹 기반의 사용자 인터페이스 기능으로 구현 개발하는 것이 중요하다. 또한 DNSSEC 서명키의 교체(Roll-over)와 관련하여 교체 시점이 잘못되었을 경우, 서명 인증에 문제가 발생할 수 있다. 이러한 문제를 고려하여 서명키를 적용 단계별로 구성하여 DNSSEC 서명키를 쉽게 구분할 수 있도록 간트 차트를 사용하여 가독성 높게 구성하였다.

구현된 DNSSEC 서명키 모니터링 웹서비스의 중요한 기능은 다음과 같다. DNSSEC 적용 도메인을 관리하는 서버의 조회 기능, 등록된 서버에서 관리하는 도메인 존의 조회 기능 및 관리 서버별 도메인 존의 서명키 유효기간 조회 기능을 갖추고 있다.

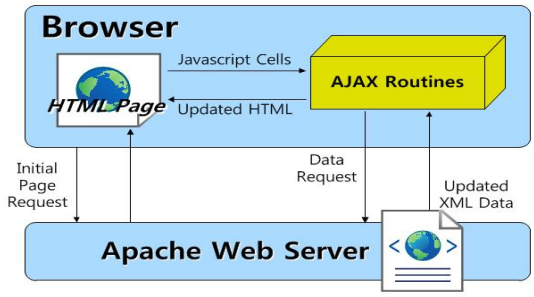


Fig. 5. The Web Server of DNSSEC Key Monitoring

Table 4. Web Development Environment

구분	설명
웹서버 운영체제	Solaris 5.10
웹 서버	Apache 2.2.21
데이터 교환 방식	JSON
사용 개발 도구 및 기법	html, Javascript, Ajax, JQuery 1.11.0

DNSSEC 서명키 모니터링 웹서비스의 구성 및 개발환경은 Fig. 5와 Table 4와 같다. 해당 구성을 기반으로 서명키 모니터링 웹서비스를 개발하였다.

DNSSEC 서명키 모니터링 웹서비스의 특성상, 도메인 존에 대한 DNSSEC 적용 시 서명키 관리에 드는 제반 정보를 웹 기반의 사용자 인터페이스 기능으로 구현 개발하는 것이 중요하다. 또한 DNSSEC 서명키의 교체(Roll-over)와 관련하여 교체 시점이 잘못되었을 경우, 서명 인증에 문제가 발생할 수 있다. 이러한 문제를 고려하여 서명키를 적용 단계별로 구성하여 DNSSEC 서명키를 쉽게 구분할 수 있도록 간트 차트를 사용하여 가독성을 높였다.

구현된 DNSSEC 서명키 모니터링 웹서비스의 주요 기능은 다음과 같다. DNSSEC 적용 도메인을 관리하는 서버의 조회 기능, 등록된 서버에서 관리하는 도메인 존의 조회 기능 및 관리 서버별 도메인 존의 서명키 유효기간 조회 기능을 갖추고 있다.

DNSSEC 서명키 모니터링 웹서비스는 DNSSEC 서명키를 관리하는 대상 서버의 목록과 선택된 관리 서버의 도메인 존의 목록을 선택할 수 있다.

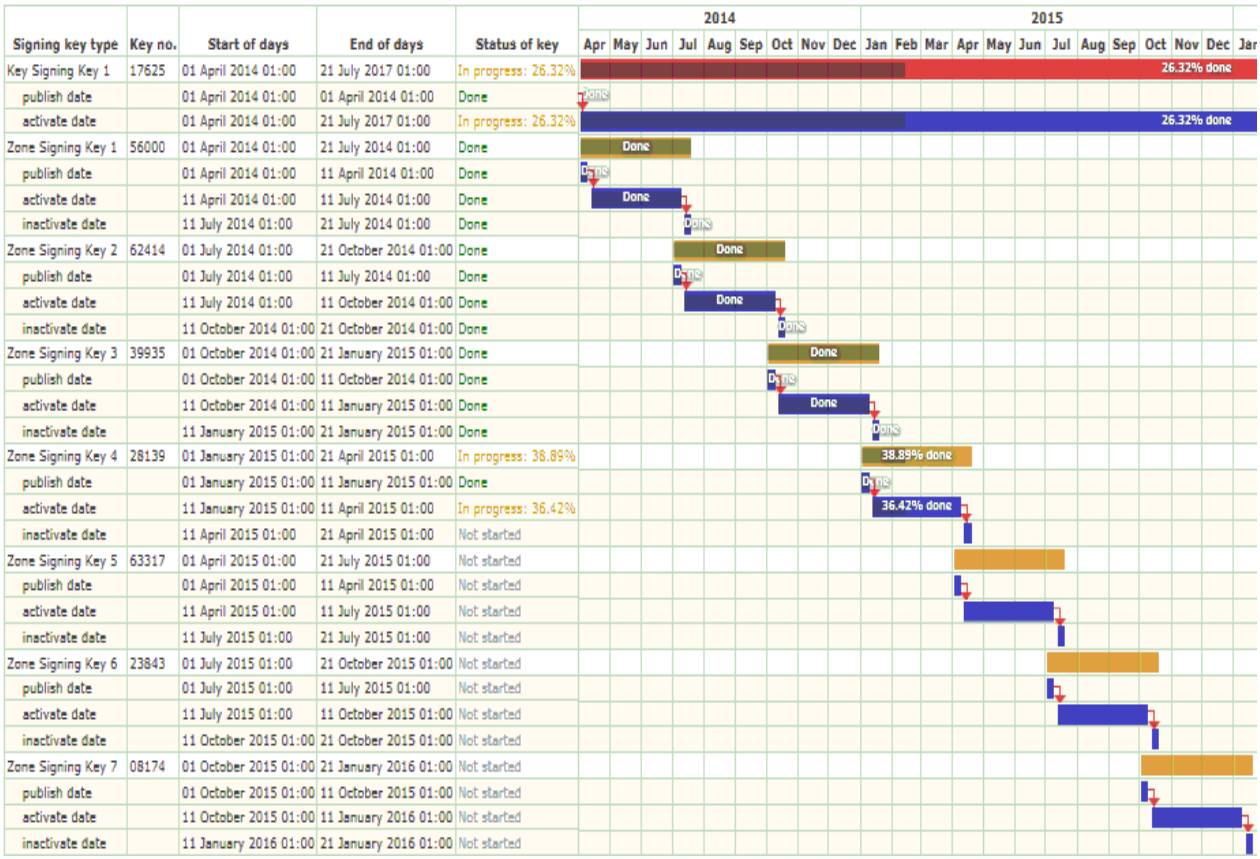
DNSSEC를 적용한 서버와 도메인 존을 선택한 후 검색버튼을 누르면 현재 도메인 존의 서명키 현황을 Fig. 6과 같이 살펴볼 수 있으며, 차트 구성 주요 항목은 Table 5와 같다.

Table 5. Main Details of the Chart

구분	설명
Signing key type	서명키 종류(KSK: Key Signing Key, ZSK: Zone Signing Key)와 키의 생성주기 구분 (적용일시: Publish date, 활성일시: Activate date, 비활성일시: Inactivate date)
Key no.	서명키 생성 시 부여되는 키 ID
Start of days	서명키 생성주기(적용, 활성, 비활성)의 시작일시
End of days	서명키 생성주기(적용, 활성, 비활성)의 종료일시
Status of key	서명키의 현재 시점 기준 진행 상태를 비율(%)로 표기
Gantt chart	서명키의 상태를 월별 기준으로 진행 상태를 진행바(Progress bar) 형태로 표시

4.3 DNSSEC 서명키 자동 메커니즘 및 모니터링 효율성

DNSSEC 서명키 관리자동화 도구는 자동으로 DNSSEC 적용 도메인 영역에 대한 서명키를 생성하고 유효기간이 지난 서명키에 대해 백업과 삭제 처리를 한다. 또한, 해당 도구는 등록대행자를 포함한 DNSSEC 적용 도메인 DNS 관리자들이 서명키의 상태를 쉽게 파악하고 적용할 수 있도록 쉘 스크립트로 작성하여 DNS를 관리하는 데 편의성을 도모하였다. 대부분의 홈페이지의 경우, 도메인 관리자, 유지보수 및 운영자가 달라 이에 대한 업무 연속성이 보장되지 않는



Signing key type	Key no.	Start of days	End of days	Status of key
Key Signing Key 1	17625	01 April 2014 01:00	21 July 2017 01:00	In progress: 26.32%
publish date		01 April 2014 01:00	01 April 2014 01:00	Done
activate date		01 April 2014 01:00	21 July 2017 01:00	In progress: 26.32%
Zone Signing Key 1	56000	01 April 2014 01:00	21 July 2014 01:00	Done
publish date		01 April 2014 01:00	11 April 2014 01:00	Done
activate date		11 April 2014 01:00	11 July 2014 01:00	Done
inactivate date		11 July 2014 01:00	21 July 2014 01:00	Done
Zone Signing Key 2	62414	01 July 2014 01:00	21 October 2014 01:00	Done
publish date		01 July 2014 01:00	11 July 2014 01:00	Done
activate date		11 July 2014 01:00	11 October 2014 01:00	Done
inactivate date		11 October 2014 01:00	21 October 2014 01:00	Done
Zone Signing Key 3	39935	01 October 2014 01:00	21 January 2015 01:00	Done
publish date		01 October 2014 01:00	11 October 2014 01:00	Done
activate date		11 October 2014 01:00	11 January 2015 01:00	Done
inactivate date		11 January 2015 01:00	21 January 2015 01:00	Done
Zone Signing Key 4	28139	01 January 2015 01:00	21 April 2015 01:00	In progress: 38.89%
publish date		01 January 2015 01:00	11 January 2015 01:00	Done
activate date		11 January 2015 01:00	11 April 2015 01:00	In progress: 36.42%
inactivate date		11 April 2015 01:00	21 April 2015 01:00	Not started
Zone Signing Key 5	63317	01 April 2015 01:00	21 July 2015 01:00	Not started
publish date		01 April 2015 01:00	11 April 2015 01:00	Not started
activate date		11 April 2015 01:00	11 July 2015 01:00	Not started
inactivate date		11 July 2015 01:00	21 July 2015 01:00	Not started
Zone Signing Key 6	23843	01 July 2015 01:00	21 October 2015 01:00	Not started
publish date		01 July 2015 01:00	11 July 2015 01:00	Not started
activate date		11 July 2015 01:00	11 October 2015 01:00	Not started
inactivate date		11 October 2015 01:00	21 October 2015 01:00	Not started
Zone Signing Key 7	08174	01 October 2015 01:00	21 January 2016 01:00	Not started
publish date		01 October 2015 01:00	11 October 2015 01:00	Not started
activate date		11 October 2015 01:00	11 January 2016 01:00	Not started
inactivate date		11 January 2016 01:00	21 January 2016 01:00	Not started

Fig. 6. Monitoring Result

경우가 있다. 이때 DNSSEC 서명키 갱신이 진행되지 않는다면 도메인 서비스가 불가할 수 있다.

그러나 해당 서명키 관리자동화 도구를 DNSSEC 적용 도메인 존에 사용한다면, 서명키 갱신이 연속적으로 진행됨에 따라 홈페이지 및 기타 관련 서비스에 대한 가용성을 확보할 수 있다.

DNSSEC 서명키를 수동을 설정한다면 Table 6과 같이 서명키를 하나씩 각각 설정해야 한다. 해당 서명키의 유효기간이 완료되기 전에 DNS 담당자는 서명키별로 생성 시기, 활성화 시기 및 삭제 시기 등을 점검하고 신규 생성하여야 한다.

Table 6. The Program of DNSSE Key Generation

구분	Program
KSK	dnssec-keygen -3 -r /dev/urandom -b 2048 -n ZONE -P 20120917104303 -A 20120917104303 -f KSK co.kr.
ZSK	dnssec-keygen -3 -r /dev/urandom -b 1024 -n ZONE -P 20140601010000 -A 20140611010000 -I 20140911010000 -D 20140921010000 co.kr.

최종적으로 DNSSEC 자동화 서명키 생성의 효과를 살펴보고자 BIND 기반의 DNSSEC 자동화 키 관리 도구에 의해 키 관리를 하는 도메인과 수동으로 키를 생성하여 관리하는 도메인을 각각 2개씩 선정하였다. 본 실험 DNS 환경은 Table 7과 같으며, 실험은 DNS 및 DNSSEC 프로젝트를 10년 이상 수행한 DNS 전문가에 의해 진행되었다.

Table 7. Test Environment of DNSSEC Key Generation

구분	세부 버전
운영체계	Linux 2.6.32-220el6
DNS S/W	BIND 9.8.0-P1

Table 8. The Application Result of DNSSEC Automatic Model

구분	미적용	적용
DNSSEC 설정 빈도	4	1
DNSSEC 설정 소요 시간(회당)	1시간	2시간
DNSSEC 설정 점검 빈도	3	2
DNSSEC 설정 점검 소요 시간(회당)	7~8분	2~3분
DNSSEC 설정 오류	1	0

총 4개의 도메인에 대하여 ZSK 교체주기를 3개월에서 24시간(1일)으로 변경하여, 3주간 DNSSEC 서명키를 생성하였다. 그리고 이를 각각 설정하는 데 1시간 및 2시간이 소요되었다. Table 8을 살펴보면 처음에는 DNSSEC 서명키

설정 자동 모듈 및 모니터링을 적용하는 데 시간이 더 소요되었다. 하지만 BIND 기반의 DNSSEC 자동화 키 관리도구로 키를 생성한 경우에는 한 번의 설정으로 도메인과 네임서버 정보가 변경되지 않는 한, 지속적으로 서명키가 생성e되므로 별도의 서명키 관리가 필요 없으나, 수동으로 키를 생성한 경우에는 서명키의 유효기간이 완료되기 전에 인력과 시간을 들여 지속적으로 서명키를 생성해야 한다.

3주간의 실험 기간 동안 생성된 키의 숫자는 Fig. 7과 같다. 처음에는 도메인별로 총 7개의 ZSK를 생성하였으며, 서명키 자동화 생성 도구를 적용한 도메인의 경우, 마지막 서명키의 삭제일을 확인하여 7일차부터 매일 하나의 키를 자동으로 생성함을 볼 수 있다.

더 확실한 자료를 얻기 위해 2015년 6월 25일부터 일주일간 DNS 전문가 18명을 대상으로 서명키 생성 및 모니터링 Tool 적용 실험을 진행하였다. 본 실험은 앞의 실험과 동일하게 ZSK 교체주기 24시간(1일)으로 하여 7일간 진행되었다. 참여 연령대는 30대와 40대가 각각 8명으로 가장 많았으며, 20대와 50대가 각각 1명씩 참가하였다. DNS 관련 근무 기간은 평균 5.6년으로, 참여군의 88.8%은 DNSSEC에 대하여 알고 있거나 아주 잘 알고 있었다.

Table 9. The Application Result of DNSSEC Automatic Model

구분	미적용	적용
DNSSEC 설정 빈도	2	1
DNSSEC 설정 소요 시간(회당)	1시간	1.5시간
DNSSEC 설정 점검 빈도	2	1
DNSSEC 설정 점검 소요 시간(회당)	12분	6분
DNSSEC 설정 오류	1	0

실험 결과는 Table 9와 같으며, 두 실험을 통해 DNSSEC 서명키 모니터링을 사용하면 무엇보다도 사용자가 편리하게 DNSSEC 서명키 사용 현황을 살펴볼 수 있음을 알 수 있었다. 현재 사용하는 서명키가 몇 번째 생성한 서명키이고, 사용 주기가 얼마나 남아있는지 등 이를 웹으로 구현된 시스템을 통해 한눈에 살펴볼 수 있다. 일일이 키 파일을 'cat' 명령어를 통해 Fig. 8과 같이 하나하나 살펴보지 않아도 된다.

```
[root@signer cokey]# cat Kco.kr.+007+04007.key
; This is a zone-signing key, keyid 4007, for co.kr.
; Created: 20120917104634 (Mon Sep 17 19:46:34 2012)
; Publish: 20150301010000 (Sun Mar  1 10:00:00 2015)
; Activate: 20150311010000 (Wed Mar 11 10:00:00 2015)
; Inactive: 20150611010000 (Thu Jun 11 10:00:00 2015)
; Delete: 20150621010000 (Sun Jun 21 10:00:00 2015)
```

Fig. 8. Singing Key Confirmation Process

이는 시스템을 잘 모르는 사용자에게는 매우 불편하며, 생성된 모든 서명키를 확인해야 하기 때문에 시간도 많이 소요된다. 관리해야 할 도메인이 많다면 이를 확인하는 시간은 기하급수적으로 늘어날 것이다. Table 8에서와 같이 모니터링을 통해 서명키를 살펴보면 시간이 많이 절약됨을 알 수 있다. 더불어 본 논문에서 제시한 모니터링을 사용한다면 보다 쉽게 생성된 여러 도메인의 모든 서명키를 살펴볼 수 있으므로 효율적이다. DNSSEC 서명키 모니터링을 사용하면 무엇보다도 사용자가 편리하게 DNSSEC 서명키 사용 현황에 대해 살펴볼 수 있다. 현재 사용하는 서명키가 몇 번째 생성한 서명키이고, 사용 주기가 얼마나 남아있는지 등 이를 웹으로 구현된 시스템을 통해 한눈에 살펴볼 수 있다.

보통 DNSSEC 서명키 현황을 살펴보려면 사용자가 키 파일을 'cat' 명령어를 통해 하나하나 살펴보아야 한다. 이는 시스템을 잘 모르는 사용자에게는 매우 불편하며, 생성된 모든 서명키를 확인해야 하기 때문에 시간도 많이 소요된다. 하지만 본 논문에서 제시한 모니터링을 사용한다면 보다 쉽

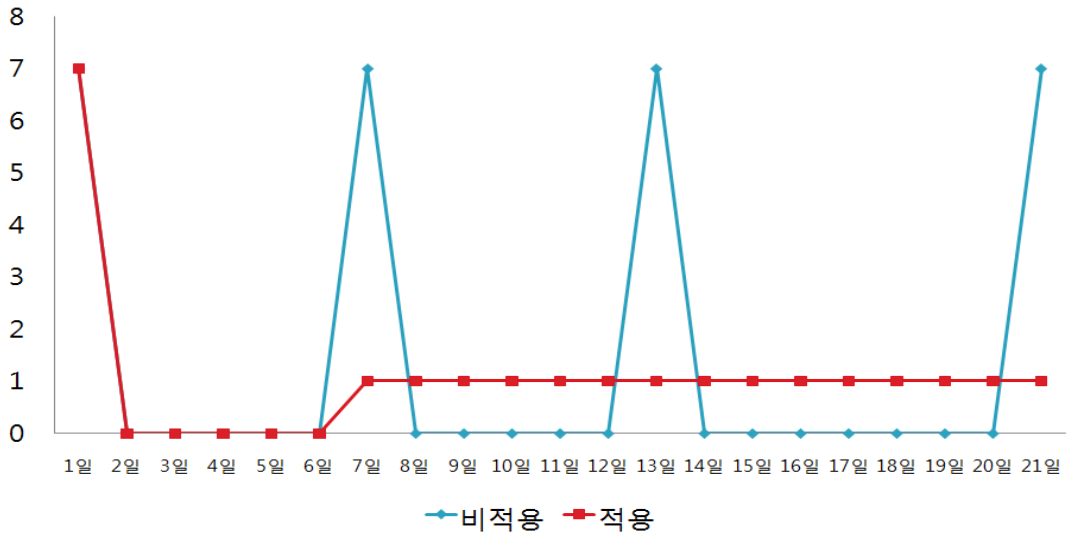


Fig. 7. The Status of Singing Key Creation

게 생성된 모든 서명키를 살펴볼 수 있으므로 효율적이다.

위 실험을 기반으로 한 회사에서 보유한 100개의 도메인에 대하여 2년간 DNSSEC를 적용할 경우, 소요되는 시간은 Table 10과 같다.

Table 10. Run-time Comparison

구분		계산식	소요시간
수동	키 생성	100개 × 60분 × 2년	200시간
	키 모니터링	100개 × 6분 × 4회 × 2년	80시간
자동	키 생성	100개 × 120분 × 1년	200시간
	키 모니터링	100개 × 3분 × 4회 × 2년	40시간

Table 10은 1년 동안 4개의 DNSSEC 서명키를 도메인별로 생성하고, 분기별 서명키 모니터링에 소요되는 평균 시간을 기반으로 도출하였다. 이를 2014년 소프트웨어 고급기술자 노임단가 기준으로 계산하면, 2년간 136만 원 정도 관리 비용을 절약할 수 있다. 3년차부터는 키 모니터링에만 시간이 소요되므로 약 476만 원 정도의 관리 비용 감소 효과를 볼 수 있다. 만일 1만 개 정도의 도메인을 관리하는 호스팅 업체일 경우, 연간 4억 원의 관리 비용을 절감할 수 있다.

5. 결 론

DNS 캐시 위·변조로부터 원활한 도메인 서비스를 하기 위해서는 DNSSEC 적용이 필요하다. 또한 일반 도메인 사용자 및 캐시 DNS 운영자들이 안정적으로 DNSSEC 적용 및 운영을 위해서는 지속적인 관리가 동반되어야 한다. 특히 DNSSEC의 안정적인 운영을 위하여 주기별로 DNSSEC의 서명키 생성 및 교체가 이뤄져야 한다. 하지만 잦은 관련 업무 담당자의 교체 및 운영 업체의 변경 등으로 지속적으로 DNSSEC의 서명키 관리가 어려울 수도 있다.

이에 따라 본 연구는 DNSSEC 적용 후 지속적인 서명키 관리에 따른 문제를 보완하고자 하였다. 따라서 본 논문에서 제안하는 서명키 자동 생성 프로그램은 지속적으로 키를 생성, 적용 및 삭제 프로세스를 통해 안정적으로 서명키 교체를 수행하고, 이후에는 이를 효율적으로 살펴볼 수 있는 모니터링 프로그램을 제안하였다.

DNSSEC 서명키 관리 자동화 프로그램을 통해 키 생성, 적용 및 말소의 일련 프로세스가 지속적으로 반복됨으로써 도메인 및 캐시 DNS 서비스 등의 연속성을 보장받게 되었다. DNSSEC는 도메인 네임서버뿐만 아니라 리커시브 DNS, 캐시 DNS에 다 적용되어야 하므로 해당 자동화 프로그램을 사용할 수 있어 활용도도 뛰어나다.

또한 제안하는 모니터링 프로그램은 시스템에 대한 해박한 지식이 없는 사용자도 보다 쉽게 DNSSEC 서명키 생성, 적용 및 말소 등의 일괄적인 진행 사항을 웹 기반의 간트차트를 통해 한눈에 살펴볼 수 있어, 서명키 교체의 프로세스의 가독성을 충족시켰다.

본 연구에서 제시한 서명키 관리 자동화 프로그램과 모니터링 프로그램은 지속적으로 서비스 연속성이 보장되어야 하는 도메인 사이트 및 캐시 DNS 서버에 해당 프로그램을 적용하여 기존보다 더 안정적이고 효율적으로 서비스를 운영할 수 있게 되었다.

추후 제안하는 프로그램을 국가도메인 등록대행자 및 네임서버 운영자 등에게 제공한다면 보다 쉽게 DNSSEC를 적용 및 관리하는 데 큰 도움이 될 것이다.

IETF에서는 DNSSEC 기반의 DANE 워킹그룹에서 활발하게 이메일 인증 및 본인 확인 등의 연구를 지속적으로 추진하고 있으며, IoT 분야에서도 센서 네트워크의 보안 관련하여 DNSSEC를 적용하여 해결하려는 노력이 HOMENET 워킹그룹을 통해 활발하게 진행되고 있다[11]. 향후 국내에서도 DNSSEC 기반의 IoT 디바이스 인증, 이메일 인증 및 본인 확인 등에 연구가 추진될 수 있으므로 DNSSEC의 안정적 운영·관리에 관한 지속적인 연구가 필요하다.

References

[1] APNIC DNSSEC statistics homepage, APNIC [Internet], http://stats.labs.apnic.net/dnssec.

[2] Security and Stability Advisory Committee(SSAC), "SAC063 Advisory on DNSSEC KEY Rollover in the Root Zone," ICANN, pp.1-34, Nov., 2013.

[3] Internet storm center homepage, SANS Technology Institute [Internet], https://isc.sans.edu/forums/diary/biz+DNSSEC+DNSKEY+is+Invalid/16046.

[4] Dowon Kim, "The Understanding of Internet using-based DNS and DNS Security," *Internet & Security focus*, Vol.9, pp.6-25. KISA, Sep., 2013.

[5] SANS, "March 2005 DNS Poisoning Summary," [Internet], https://isc.sans.edu/presentations/dnspoiso ning.html.

[6] KISA, "DNSSEC Introduction and management of operational guideline," pp.1-227, Nov., 2013.

[7] TTA(Telecommunications Techonlolgy Association), "Domestic DNSSEC demonstration domain name server registration and building instructions," TTAK.KO-10.0315, TTA, Nov., 2009.

[8] Hansang Lee, "The Study for Implementation of DNSSEC and Key Management Method in kr DNS," TM 621.39-9-949, pp.1-101, Yonsei University Graduate School of Engineering, Aug., 2009.

[9] KISA, "DNSSEC Domestic & International Trends and National Action Plans," *ICT Forum Korea*, Aug., 2009.

[10] Verisign, "Anatomy of Recent DNS Reflector Attacks from the Victim and Reflector Point of View," pp.1-16, Apr., 2006.

[11] D. Migault, "Outsourcing Home Network Authoritative Naming Service," homenet WG, pp.1~25, IETF, Feb., 2015.

최 명 희

e-mail : choimh@kisa.or.kr

2008년 한국외국어대학교 정보통신공학과 (학사)

2012년～2013년 한국정보통신기술협회(TTA) 인터넷주소자원(PG211) 위원

2013년 고려대학교 정보보호대학원 정보보호학과(석사수료)

2009년～현 재 한국인터넷진흥원 선임연구원

관심분야 : 도메인, DNS 보안, 네트워크 보안, 사이버 사기 등

김 승 주

e-mail : skim71@korea.ac.kr

1994년～1999년 성균관대학교 정보공학과 (학사, 석사, 박사)

1998년～2004년 KISA(舊한국정보보호진흥원) 팀장

2004년～2011년 성균관대학교 정보통신공학부 조교수, 부교수

2005년～2006년 교육인적자원부 유해정보 차단 자문위원

2007년～2009년 전자정부서비스보안위원회 사이버 침해사고대응 실무위원회 위원

2010년 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원

2012년 선관위 디도스 특별감사팀 자문위원

2002년～현 재 한국정보통신기술협회(TTA) IT 국제표준화전문가

2011년～현 재 고려대학교 사이버국방학과/정보보호대학원 정교수

관심분야 : 보안공학, 암호이론, 정보보증, 보안성 평가 등