안전한 도메인 네임 시스템 관리를 위한 관리 정보 개체 정의에 관한 연구

이만희, 장행진, 박형우, 변옥환
한국전자통신 연구원

A Study on Defining Management Information Base for Domain Name System Security Extensions

Man-Hee Lee, Haeng-Jin Jang, Hyung-Woo Park, Ok-Hwan Byeon
Electronics and Telecommunications Research Institute

인터넷에서 호스트의 인터넷 주소와 이름을 상호 매핑해주는 도메인 네임 시스템은 호스트 수가 급증함에 따라 그 중요성 또한 증대되고 있다. 최근 인증 기능을 제공하는 도메인 네임 시스템이 제안됨에 따라 이를 이용하여 진보된 서비스를 제공하려는 연구가 활발히 진행중이다. 한편 도메인 네임 서버를 기존 네트워크 관리 체계 내에서 관리하기 위한 관리 정보 개체는 이미 정의되어 있었다. 하지만 인증 기능을 제공하는 도메인 네임 서버 관리 정보 개체에 대한 연구는 진행되지 않고 있다. 본 논문에서는 인증 기능을 제공하는 도메인 네임 시스템을 관리하기 위한 관리 정보를 정의하고 이를 구현하기 위한 안전한 도메인 네임 서버 관리 모델을 제시한다.

1.서론

도메인 네임 시스템(Domain Name System, DNS)은 인터넷에서 널리 사용되는 서비스중 하나이다 DNS는 시스템에 할당되어 있는 32비트 크기의 인터넷 주소와 암기하기 쉬운 호스트의 이름을 상호 매핑해주는 전세계적인 분산 시스템이다[8,9]. 그러나 인터넷 사용이 확대됨에 따라 DNS 서비스의 중요성 또한 증대되고 있지만, 오히려 인증기능이 없는 DNS의 보안 취약성을 이용한 해킹 사고가 증가하고 있다.

인증기능을 가지는 *DNSSE(DNS Security Extensions)*은 IETF의 DNS Security 워킹그룹에 의해서 정의되었다. 이 모델은 DNS 서버와 네임 정보를 요청하는 프로그램인 리졸버(resolver)간의 인증된 통신, DNS 서버간의 안전한 존 파일 전송, Public Key의 안전한 분배 기능 등이 정의되어 있다[3,4,11] 이 모델은 DNS가 단순한 주소 매핑 서비스가 아닌 전세계를 대상으로 하는 안전한 정보 제공 시스템으로 사용될 수 있는 기회를 제공하였다. 그 예로 DNS를 이용한 Public Key Infrastructure(PKI)가 있다. 즉, 이미 구성되어 있는 DNS의 전세계적인 트리 구조를 이용하여 전자상거래 등에서 필요한 사용자 인증 공개키 분배를 구현하는 것이다[5,12].

한편 Simple Network Management Protocol(SNMP)를 이용해서 DNS 서버를 관리하기 위한 DNS MIB(Management Information Base)는 1994에 정의되었다[1,2,10]. 이 MIB은 DNS 서버의 환경 정보, 서비스 통계 정보, 존 전송 정보 등을 정의한다. 그러나 DNS의 인증기능 강화로 DNS 서버의 운영 환경 및 방법 등도 많이 달라졌다. 더욱이 SNMP를 이용한 어플리케이션 통합 관리에 대한 표준화 작업이 진행중인 시점에서 *DNSSE MIB*에 대한 조속한 연구가 필요하다[6,7]

본 논문에서는 SNMP를 이용하여 DNSSE 서버를 관리하기 위한 DNSSE MIB을 정의한다. DNSSE MIB는 기존 DNS MIB을 포함하고, DNSSE 서버의 환경 정보, 서비스 통계 정보, 기존 DNS와의 공존을 위한 관리 정보 등을 정의하였다. 그리고 서비스 시작, 중단, 에러 등이 발생했을 때 관리자에게 경고를 보내는 trap 메시지도 정의하였다 그리고 이를 이용한 DNSSE 서버 관리 모델을 제시한다.

본 논문은 아래와 같이 구성된다 다음 절에서는 DNS MIB을 살펴보고 3절에서는 *DNSSE*의 특징을 살펴본다. 4절에서는 DNSSE를 관리하기 위한 DNSSE MIB를 정의한다. 마지막으로 결론에서는 맺는 말과 앞으로의 연구 방향을 소개한다.

2. DNS 서버를 위한 관리 개체

본 절에서는 DNS MIB을 살펴보겠다. 이 MIB은 크게 dnsServConfig, dnsServCounter, dnsServOptCounter, dnsServZone의 4가지 그룹으로 분류된다.

표 1. DNS MIB

Group Name	Object	
dnsServ Config	ImplementIdent, Recurs, Uptime, ResetTime, Reset	
dnsServ Counter	AuthAns, AuthNoNames, AuthNoDataResps, NonAuthDatas, NonAuthNoDatas, Referral, Errors, RelNames, ReqRefusals, ReqUnParses, OtherErrors	
dnsServ OptCounter	Self	AuthAns, AuthNoNames, AuthNoDataResps, NonAuthDatas, NonAuthNoDatas, Referrals, Errors, RelNames ReqRefusals, ReqUnParses, OtherErrors
	Friends	〃
dnsServ Zone	Table	Name, Class, LastReloadSuccess, LastReloadAttempt, LastSourceAttempt, Status, Serial, Current, LastSourceSuccess
	SrcTable	SrcName, SrcClass, SrcAddr, SrcStatus

dnsServConfig는 서버 버전, uptime 시간 등의 DNS의 일반적인 configuration에 대한 정보이고 dnsServCounter는 DNS가 request에 대해 응답한 response의 형태에 따른 서비스 통계 정보이다. dnsServOptCounter는 자신의 DNS가 설치된 시스템에서 발생한 DNS request와 access control에 등록된 외부 시스템에서 발생한 DNS request에 대해 응답한 response의 형태에 따른 서비스 통계 정보이다 dnsServZone는 DNS 서버가 authority를 가지는 zone에 대한 정보인 dnsServZoneTable과 외부 네임 서버로부터 전송 받은 zone에 대한 정보인 dnsServZoneSrcTable로 이루어진다.

3. 인증기능을 제공하는 DNS 모델

DNS Security 워킹 그룹은 안전한 네임 서비스를 보장하는 DNS 모델을 제안하였다[4]. 이 모델은 공개키 분배 기능, 데이터 인증기능, 트랜잭션과 리퀘스트 인증기능을 제공한다. 이 모델의 가장 큰 특징은 공개키 알고리즘을 사용하여 네임 정보와 함께 인증서 역할을 하는 SIG Resource Record(RR)를 전송하는 것이다.

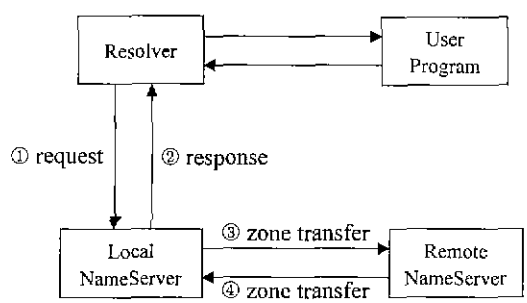

그림 1. 도메인 네임 시스템 구성도

리졸버와 네임서버간의 인증 방법은 다음과 같다 DNS의 모든 RR은 인증자의 비밀키로 sign한 SIG RR를 가지며 일반 RR이 전송될 때 이를 인증하는 SIG RR을 함께 전송한다 수신측에서는 인증자의 공개키로 수신된 RR의 인증을 확인한다 (그림 1,②). 만약 DNS가 존 정보의 동적 변경 기능을 지원한다면 리졸버에서 네임서버로 전송되는 request도 같은 방법으로 인증해야 한다(그림 1,①)[3,11]. DNS 서버간의 zone 전송에서도 zone file 자체에 대한 Signature를 생성하여 zone file과 같이 전송하면 인증된 zone file을 전송이 가능하다(그림 1,③④).

4. DNSSE 서버를 위한 관리 개체 정의

본 절에서는 DNSSE 서버를 관리할 수 있는 두 개의 MIB 그룹인 dnsServSecConfig, dnsServSecCounter과 3가지 trap 메시지를 정의하고 이를 이용한 DNSSE 서버 관리 모델을 제시한다.

먼저 dnsServSecConfig 그룹은 DNS 서버의 인증 관련 환경 정보를 저장하는 그룹이다.

표 2. dnsServSecConfig 그룹

Object Name	Max Access	Description
Secure	RO	RFC2065를 구현하는지? True(1), False(0)
SecureSet	RW	0 : 일반 DNS 서버로 수행, 1 : DNSSE 서버로 수행
DynUpdate	RO	RFC2136를 구현하는지? True(1), False(0)
DynUpdateSet	RW	0 : 일반 DNS 서버로 수행, 1 : dynamic update 지원 DNSSE 서버로 수행
SignInterval	RW	zone file의 모든 RR을 re-sign하는 interval
SignUptime	RO	마지막으로 sign한 후 경과한 시간(초)
SignReset	RW	0 : 서버의 다른 상태, 1 : signing, 2: 모든 RR을 sign, 3 : running

SecureSet, DynUpdateSet은 안전성과 동적 존 정보 변경을 제공하지 않는 대부분의 DNS 서버와 연동하기 위해 이 기능들을 제어하는 개체이다. 그리고 RFC2065는 주기적으로 DNSSE 서버의 모든 RR을 re-sign하기를 권고하는데 이 주기를 SignInterval로 정의하였고, sign한 후의 시간을 SignUpTime로 정의하였다. SignInterval의 max-access는 Read-Write로써 관리자가 re-sign 주기를 제어할 수 있다 SignReset는 sign 주기와 관계없이 임의로 모든 존 정보를 sign할 수 있는 관리 정보이다 이 그룹의 개체들은 DNSSE 서버 관리자로 하여금 쉽게 DNSSE 서버의 인증기능을 변경하고 운영할 수 있도록 해준다

dnsServSecCounter 그룹은 DNSSE 서버의 서비스 통계 정보를 저장하는 그룹이다

표 3 dnsServSecCounter 그룹

Object Name	Max Access	Description
SigRequest	RO	sign된 request 개수
ErrSigRequest	RO	인증 실패한 request 개수
SigAns	RO	sign하여 응답한 response 개수
SigXfer	RO	sign하여 전송한 zone transfer 횟수
SigXferIn	RO	sign되어 전송된 zone transfer 횟수
ErrSigXferIn	RO	인증 실패한 zone transfer 횟수

위 개체들은 DNSSE 서버의 서비스 통계, 서비스 부하 정보를 관리자에게 제공할 수 있으므로 DNSSE 서버 관리에 매우 유용할 것으로 예상된다.

마지막으로, DNS 서버가 발생시킬 수 있는 trap message를 정의하였다

표 4 Trap Message

Message Type	Description
WarmStart	DNSSE 서버가 서비스 시작할 때 발생
SignOvertime	SignUpTime>SignInterval인데도 re-sign이 일어나지 않을 때 발생
WarmStop	DNS 서비스가 중단되었을 때 발생

기존 DNS MIB에는 trap message가 정의되어 있지 않았지만 향후 DNS 서비스의 중요성을 고려해 볼 때 서비스 시작, 중단, SignOvertime trap message는 DNS 서버를 안정적으로 관리하는데 반드시 필요하다

이 DNSSE MIB을 지원하기 위해서는 서버 내에 인증 운영을 동적으로 변경할 수 있는 인증 제어 기능과 trap 발생을 위한 모니터링 기능이 반드시 필요하다. 그러므로 다음과 같은 DNSSE 서버 관리 모델이 필요하다.

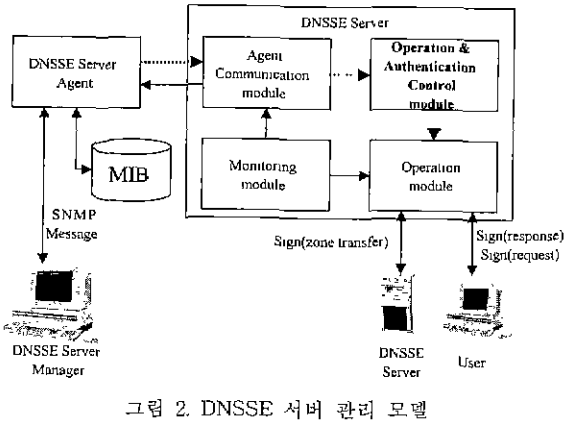

그림 2. DNSSE 서버 관리 모델

5. 결론

본 논문에서는 이미 정의된 DNS MIB과 인증기능을 제공하는 DNS 모델을 살펴보았고, 이를 SNMP를 이용하여 관리하기 위해 추가되어야 할 관리 개체들을 정의하였다.

dnsServSecConfig는 안전한 DNS 서버와 다른 서버와의 연동, 인증을 위한 제어 기능을 제공한다 dnsServSecCounter는 서버의 인증된 질의, 응답 및 zone 전송 횟수에 대한 통계 정보를 제공한다 그리고 3가지 trap 메시지는 관리자로 하여금 서버의 중요 상태를 실시간으로 연락 받도록 하여 안정적인 DNS 서버 관리를 가능하게 한다. 그리고 이 이 DNSSE MIB을 지원하는 DNSSE 서버 관리 모델을 제시하였다.

앞으로의 연구 과제로는 본 논문에서 제시한 MIB을 구현하는 DNSSE 서버를 구현하고, 나아가 이 서버들을 효율적으로 관리할 수 있는 메니저 시스템 개발하는 것이다.

[참고문헌]

[1] R. Austein and J. Saperia, "DNS Server MIB Extensions", RFC1611, May 1994.

[2] J Case, M. Fedor, M. Schoffstall, and J Davin, "Simple Network Management Protocol", STD 15, RFC 1157, SNMP Research, Performance Systems International, Performance Systems International, MIT Laboratory for Computer Science, May 1990.

[3] D. Eastlake, "Secure Domain Name System Dynamic Update", RFC2137, April 1997.

[4] D. Eastlake, and C. Kaufman, "Domain Name System Protocol Security Extensions", RFC 2065, January 1997

[5] O. Gudmundsson, D. Eastlake, "Storing Certificates in the Domain Name System", internet-draft, January 1998.

[6] C. Kalbfleisch, "Applicability of Standards Track MIBs to Management of World Wide Web Servers", RFC 2039 by IETF Network Working Group , November 1996.

[7] M.H. Lee, H.J. Choi, Y.H. Ham, and H.W. Park, "A Shared Memory Model for Management of WWW Server", 한국정보처리학회 춘계학술발표논문집, 1998.

[8] P. Mockapetris, "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[9] P. Mockapetris, "Domain Names - Implementation and Specification", STD 13, RFC 1035, USC/Information Sciences Institute, November 1987.

[10] M.T Rose, "The Simple Book: An Introduction to Management of TCP/IP- based internets", published by Prentice Hall, ISBN 0-13-812611-9

[11] P. Vixie, S. Thomson, Y Rekhter, and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[12] 임찬순, 김재우, 장행진, 박형우, "안전한 도메인 네임 시스템 모델 설계", 한국정보처리학회 추계학술발표논문집, 제4권 제2호, pp.1056-1060, 1997