제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

DNS 서비스 보안 문제점과 대응 기술 현황

한영주*, 김동수*, 정태명**
*성균관대학교 전기전자 및 컴퓨터 공학과
** 성균관대학교 정보통신공학부
e-mail : {yjhan, dskim}@imtl.skku.ac.kr
tmchung@ece.skku.ac.kr

The Threats to DNS Service and the Trend in DNS Security Technology

Young-ju Han *, Dong-soo Kim * and Tai-myoung Chung**
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
** School of Information and Communication Engineering, Sungkyunkwan University

요 약

DNS는 인터넷 주소 자원 관리의 핵심으로 다양한 인터넷 서비스의 근간이 되는 중요한 자원이다. 인터넷의 급속한 발전과 함께 사이버 공격의 다양하고 지능적인 발전으로 인해 DNS에 대한 위협이 날로 증가하고 있다. 이에 본 논문에서는 현재 DNS의 보안 문제점을 살펴보고 이러한 보안 문제점을 해결할 수 있는 보안 기술로써 DNS 프로토콜 보안 기술과 DNS 서비스 보안 기술에 대해 논의한다. DNS 서비스 보안은 DNS 프로토콜 보안과 네트워크 전반에 걸쳐 이루어지는 통합 보안 관리 시스템과의 상호 연계를 통해 극대화 될 수 있다.

1. 서론

DNS(domain name system)란 IP 주소와 이에 상응하는 계층적 이름 체계를 사상하여 주는 거대한 분산 네이밍 시스템으로써, 인터넷 주소 자원 관리의 핵심이다[1].

최근 인터넷을 기반으로 하는 컴퓨터 네트워크 발전과 더불어 사이버 공격은 해를 거듭할수록 급증하고 있으며, 악의적인 사용자들에 의한 정보 접근, 정보 조작, 시스템 무기력화 등 고의적이며 불법적인 시도가 주류를 이루고 있다. 최근에는 2002년 10월에 발생했던 13개의 루트 서버에 대한 서비스거부공격과 같이 인터넷 관리 기반 시설에 대한 공격 또한 증가하고 있어 DNS에 대한 보호가 이슈로 떠오르고 있다[2].

만약 공격자가 DNS 서버를 속이거나 혹은 실제로 DNS 서버의 통제권을 갖게 되면, 공격자는 호스트 네임과 주소의 해석들을 악의적인 목적을 위해 조작할 수 있기 때문에 DNS 서버가 해커들의 공격의 대상이 되기 쉬우며, 이러한 공격으로 인해 DNS 서버가 피해를 입게 되면, 사용자들은 인터넷을 이용할 수 없거나 IP 주소를 이용하여 접근해야 하는 불편을 초래하여 큰 혼란을 가져오게 된다.

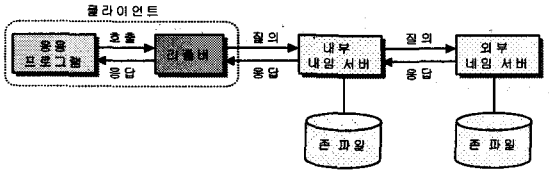
본 논문에서는 DNS 서비스의 정상적인 동작을 위협하는 DNS 보안 문제점에 대해 살펴보고, 일련의 사이버 공격으로부터 DNS를 안전하게 보호할 수 있는 DNS 보안 기술의 동향 및 대책을 살펴보고자 한다.

2. DNS 개요

DNS란 기본적으로 호스트 네임과 호스트의 IP 주소를 사상하기 위한 전역적이고 계층적인 분산 데이터베이스로써, 도메인 네임으로 색인화되어 있다[3]. 도메인 네임이란 인터넷을 사용하는 사람들이 IP주소를 기억하기 어렵기 때문에 기억하기 쉽도록 의미 있게 만든 이름으로, 계층 구조를 이루고 있어서 존(zone) 혹은 도메인과 같은 형태로 분산되어 관리된다. 인터넷을 사용하는 응용들은 내부적으로 실제로 원하는 컴퓨터를 찾기 위해서 IP 주소를 사용하기 때문에 이 IP주소와 도메인 네임을 사상하는 DNS 서비스는 인터넷의 중요한 기반 서비스이다.

DNS는 존 파일이라 일컫는 데이터 베이스, 네임서버라 칭하는 서버 그리고 리졸버(resolver)라 일컫는 클라이언트로 구성된다[3]. 존 파일은 분산 데이터 베

이스로써 IP 주소와 사상할 수 있도록 전체 데이터베이스 중 일부분에 해당하는 도메인 네임을 정의한 자원 레코드들을 저장하고 있다. 네임서버는 이러한 존 파일을 갖고 있으며 리졸버에게 정보를 제공한다. 리졸버는 질의를 생성하여 네트워크를 통해 네임서버로 질의를 전송하는 라이브러리 루틴을 의미한다. 네임서버는 특정 도메인 영역에 대한 권한을 가지고 그 도메인 영역에 대한 질의에 대해서 서비스를 제공한다. 네임서버는 관리의 편리함과 안정성을 제공하기 위해 흔히 마스터(master) 네임서버와 슬래이브(slave) 네임서버의 형태로 운영된다. [그림 1]은 DNS의 동작 과정을 나타낸다.



[그림 1] DNS의 동작 과정

DNS는 다음과 같은 네 가지 기능을 수행한다.

■ 이름 분석(resolution)

네임서버는 반복 질의 혹은 재귀 질의 방식을 통해 자신이 권한을 갖고 있는 영역에 대한 데이터뿐만 아니라, 권한을 가지고 있지 않은 데이터에 대해서도 리졸버에게 알려 줄 수 있는 기능을 가지고 있다.

■ 역 질의(inverse query)

네임서버는 도메인 네임을 IP 주소로 사상하는 것이 아닌 역으로 IP 주소를 가지고 도메인 네임을 찾을 수 있는 역 질의를 제공한다.

■ 캐싱(caching)

캐싱은 이름 분석 과정에 있어서 빠른 탐색을 지원하기 위한 기능으로 네임서버는 이름 분석이 끝나는 시점에서 그 정보를 임시 저장하여 나중 질의에 재사용할 수 있다.

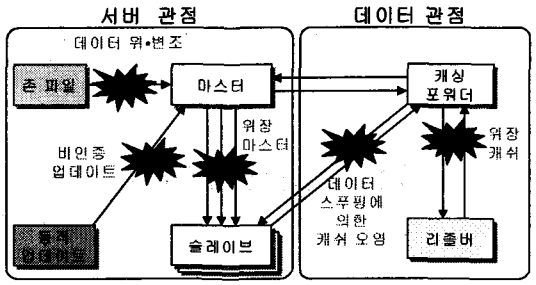
■ 존 전달(zone transfer) 및 동적 갱신

존 전달은 슬래이브와 마스터 네임서버 사이에 일어난다. 슬래이브는 존 파일을 생성 및 변경할 수 없고, 일정 주기로 마스터 서버로부터 존 파일을 다운받아 자신의 존 파일을 갱신한다. 이러한 과정을 존 전달이라 일컬으며 이러한 존 전달이 관리자에 의해 수동적으로 이루어지지 않고 자동적으로 지원되는 것을 동적 갱신이라 한다.

3. DNS의 보안 문제점

3.1 DNS 프로토콜 보안 문제점

DNS 프로토콜에서 가장 중요한 자원은 존 파일에 자원 레코드의 형태로 관리되고 있는 도메인 네임에 관한 정보이다. 도메인 네임을 관리하는 자원 레코드가 악의적인 사용자에 의해 변경되거나 삭제되었을 경우 인터넷을 사용하려는 많은 사용자에게 큰 혼란을 야기시킬 수 있다. 이와 같이 도메인 네임 정보를 파괴하려는 DNS에 대한 위협은 [그림2]와 같이 크게 서버 관점과 데이터 관점으로 나뉠 수 있는데, 서버 관점에서 존 파일의 데이터 위 변조(corrupting data)와 동적 갱신 시의 비인증 갱신(unauthorized updates), 그리고 슬래이브에게 마스터로 위장하여 접근(impersonating master)하는 위협이 있다. 데이터 관점의 위협은 위장 캐쉬(cache impersonation) 공격과 데이터 스푸핑(data spoofing)에 의한 캐쉬 오염(cache poisoning) 위협 등이 있다[4][5].



[그림2] DNS에 대한 위협

이러한 위협이 발생하게 되는 근본적인 원인은 DNS 프로토콜에서 존 파일 및 질의 응답 메시지의 무결성에 대한 검증과 리졸버와 네임서버 간 혹은 네임서버 간의 신뢰 관계를 부여할 수 있는 인증 메커니즘의 부재에서 찾을 수 있으며 이에 대한 DNS 프로토콜 차원에서의 보안 강화가 필요하다.

3.2 DNS 서비스 보안 문제점

공격자는 공격을 시작하기 전에 목표 네트워크 및 호스트에 관한 많은 정보를 DNS 서버를 통해 얻을 수 있을 뿐만 아니라, DNS 서버는 네트워크에 침입하기 위한 통로로 이용될 수 있기 때문에 DNS 서버가 해커들의 공격의 대상이 되기 쉽다. 또한 서비스 거부 공격 및 분산 서비스 거부 공격에 의한 DNS 서버의 중단은 HTTP, FTP, SMTP등의 프로토콜을 통한 Web, 파일전송, 전자우편과 같은 필수 인터넷 서비스의 정상적인 운영을 불가능하게 하므로 그 손실은 막대하다.

이러한 공격 패턴을 살펴보면 실제 DNS 서버로 사용되고 있는 BIND나 MS DNS Server들의 프로그램 취약점을 이용한 버퍼 오버플로우 공격을 통한 서비스 거부 공격이 대다수이다[6][7].

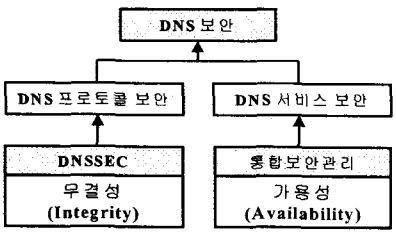
현재 DNS 서비스 파괴를 목적으로 하는 공격뿐만 아니라 다른 서비스에 대한 공격으로 인해 받는 간접적인 피해 또한 무시할 수 없다. 2003년 1월 25일에 일어난 인터넷 대란은 MS SQL 서버의 취약점을 이용하여 확산된 SQL_Overflow 웜으로 인하여 국내외 인터넷 망이 마비되는 초유의 사태였다. 이 웜의 확산 과정에서 생성되는 대량 패킷으로 인한 트래픽 폭증은 회선 장애와 서비스 지연을 일으켰고, KT DNS 서버의 서비스가 지연됨에 따라 재시도 질의가 급증함으로써 서버의 CPU 과부하를 초래하여 결국 국내 인터넷 서비스가 정지되었다[8]. 이 경우 SQL_Overflow 웜이 DNS 서버 자체를 공격하지는 않았으나 다른 서비스의 취약점을 통해 간접적으로 DNS 서버에게 치

명적인 영향을 줄 수 있다는 것을 반증하는 예이다.

DNS 서비스는 네트워크 기반 서비스이므로 이러한 직·간접적인 공격의 파급 효과는 네트워크 전반에 걸쳐 악영향을 미치기 때문에 네트워크 보안을 위한 근본적인 대안이 필요하다. 이러한 공격에 대한 대응은 DNS 프로토콜의 보안 강화로는 해결될 수 없기 때문에 네트워크 차원에서의 보안 강화가 필수적으로 요구된다.

4. DNS 보안 기술

3장에서 서술한 DNS보안 문제점을 해결하기 위해서는 [그림3]에서 나타낸 것과 같이 DNS 프로토콜 보안과 DNS 서비스 보안이 함께 이루어져야 한다. 이 장에서는 각각의 보안 기술에 관해 살펴본다.



[그림 3] DNS 보안 영역 및 대책

4.1 DNS 프로토콜 보안 기술: DNSSEC

DNSSEC(DNS Security)이란 DNS의 보안 강화를 위한 DNS 프로토콜의 확장으로 IETF의 DNSSEC WG(working group)을 거쳐 현재는 DNSEXT WG에서 진행 중인 기술 분야이다. DNSSEC의 기본 목적은 네임서버의 존 파일로부터 받은 데이터에 대해 무결성과 인증을 제공하는 것이다. 이는 공개키 암호화를 사용하는 전자서명 기술을 통해 제공된다[9]. DNSSEC은 다음과 같은 세 가지 서비스를 제공한다.

- 키 분배
- 데이터 근원 인증 및 무결성
- 트랜잭션 및 요청 인증

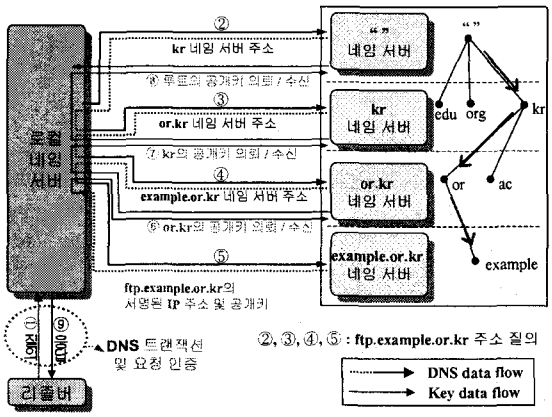
키 분배 서비스는 도메인 네임마다 공개키를 부여하며, 이 공개키를 이용하는 공개키 알고리즘에 의해 네임서버가 관리하는 존 파일의 데이터에 대한 신뢰성을 검증할 수 있는 기능을 제공한다.

데이터 근원 인증 및 무결성 서비스는 DNSSEC의 핵심으로써, 존 파일내의 자원 레코드 집합을 전자서명 기술을 이용하여 서명함으로써 리졸버와 네임서버 간의 신뢰성을 보장할 수 있다. 이는 캐쉬 오염과 같은 DNS 공격을 방어할 수 있는 메커니즘이다.

트랜잭션 및 요청 인증 서비스는 DNS 요청 및 응답 메시지의 헤더를 인증할 수 있는 서비스를 제공함으로써 리졸버나 네임서버가 수신한 응답 메시지가 자신이 보낸 질의에 대한 응답인지 혹은 자신이 질의를 요청한 서버로부터의 응답인지를 검증할 수 있게 해준다. DNSSEC은 이러한 보안 기능을 제공하기 위해 KEY, SIG, NXT의 3가지 자원 레코드를 정의하고 있다.

ftp.example.or.kr의 이름 분석 과정을 살펴보자. 로컬 네임서버의 재귀적 질의를 통해 얻은 응답에는 example.or.kr의 비밀키로 서명 된 ftp.example.or.kr의 IP 주소, 해당 IP 주소를 풀 수 있는 example.or.kr의 공개키 그리고 이 공개키를 or.kr의 비밀키로 서명한 정보가 들어있다. 로컬 네임서버는 수신한 example.or.kr의 공개키로 IP 주소를 풀어 데이터의 무결성을 검증하는데, 이 공개키를 검증하기 위해서는 or.kr의 공개키가 필요하다. 마찬가지로 or.kr의 공개키를 검증하기 위해서는 kr의 공개키가, kr의 공개키를 검증하기 위해서는 루트의 공개키가 필요하다. 결국 재귀적 질의를 통해 얻은 IP주소의 무결성을 검증하기 위해서는 루트 네임서버의 공개키로 kr에서부터 example.or.kr까지 각 네임서버의 공개키를 검증해야 하며 최종적으로 검증된 example.or.kr의 공개키로 수신한 IP 주소의 무결성을 검증할 수 있다. 또한, 리졸버와 로컬 네임서버사이의 트랜잭션 인증은 특별한 서명을 추가하여 제공된다. 이와 같이 DNSSEC에서의 정보 검증은 최상위 루트서버로부터 DNS 체계에 따라 순차적으로 이루어지기 때문에 DNSSEC이 완전하게 적용된 환경에서는 공격자가 루트서버부터 하위 말단의 네임서버까지 모두 속이지 않는 한 DNS 정보의 완전한 위·변조는 불가능하게 된다.

DNSSEC을 적용한 동작 과정은 [그림4]와 같다.



[그림4] DNSSEC을 적용한 동작 과정

4.2 DNS 서비스 보안 기술: 통합 보안 관리

DNSSEC은 서비스 거부 공격 방어와 같은 네트워크와 관련된 DNS 서비스 보안 기술을 제공하지 않는다[9]. 서비스 거부 공격은 비전문가에 의해 탐지되기가 어려울 뿐 아니라 대체로 IP 스푸핑을 사용하여 공격 근원지를 찾기가 쉽지 않은 특성 때문에 대응이 쉽지 않다. 현재 네트워크 보안을 위해 침입 탐지 시스템, 방화벽, VPN과 같은 보안 시스템들이 운영되고 있으나, 서비스 거부 공격과 같이 실시간 대응이 필요한 공격에 대해서는 각 보안 시스템들의 유기적인 협동이 필요하다. 따라서 빠른 대응과 보다 능동적인 대응을 위해서는 각 보안 시스템들을 유기적으로 연관시켜 손쉽게 관리 할 수 있어야 하는데, 이를 제공하는 것이 바로 통합보안관리 기술이다[10]. 통합보안관

리는 각 보안 시스템들의 정책과 보안 관리에 필요한 정보들을 중앙에서 관리하거나 적절한 분배를 통해 보안 시스템들 간의 자율적 대응이 가능하게 한다. 이를 통해 얻을 수 있는 통합보안관리시스템의 장점은 다음과 같다.

- 보안 정책의 전체적인 파악
- 정책의 무결성 보장
- 정책복구 용이
- 정책 제어 기능의 확장
- 보안관리의 자율성과 안전성 제공

현재 통합보안관리시스템에 대한 대표적인 관련 연구로는 Check Point사의 SVN(secure virtual network)과 NAI Lab의 CITRA(cooperative intrusion traceback and response architecture)를 들 수 있다.

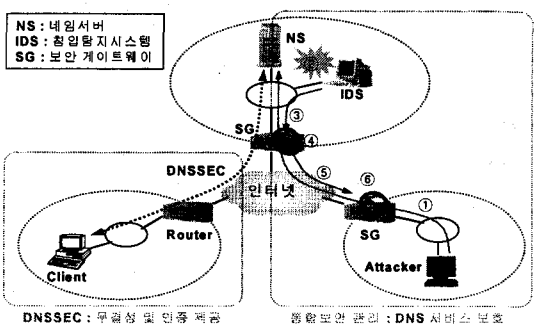
Check Point사의 SVN은 Check Point사의 Firewall-1/VPN-1 제품을 중심으로 사용자 인증 시스템, 정책 관리 시스템이 통합된 전사적 네트워크 보안 환경을 제공한다. OPSEC(Open Platform for Security)은 이러한 SVN 환경 내의 보안 제품들 간의 상호 동작성과 통합을 지원하기 위한 것으로 보안 기능을 위한 몇 개의 프로토콜과 API의 집합으로 구성되어 있다[11].

CITRA는 각 보안 관리 영역의 유기적인 협력을 위해 IDIP(intruder detection and isolation protocol)란 프로토콜을 기반으로 침입탐지시스템, 방화벽, 호스트 그리고 기타 보안 시스템들의 협력을 통해서 공격을 역추적하여 실제 근원지를 식별, 근원지 가까운 곳에서 공격을 차단할 수 있는 기능을 제공한다[12].

이러한 통합관리 시스템을 이용하여 네트워크 전반에 걸친 서비스를 보호할 수 있으며, 이를 통해 임의의 사이버 공격으로부터 DNS 서비스의 가용성을 보장할 수 있다.

4.3 DNS 보안 구조

앞서 설명된 기술들이 적용되어 DNS 프로토콜 자체 보호와 DNS 서비스 보호를 위한 보안 구조가 [그림 5]에 나타나 있다.



[그림 5] DNS 보안 구조

DNS 서비스 보호를 위해 통합보안 관리 기술이 적용되어 DNS 서비스를 보호하는 절차는 다음과 같다.

①공격자의 침입 및 공격
②IDS에서 침입 탐지
③침입 차단 정책, 역추적 정책 전달
④침입 차단
⑤근원지 역추적
⑥협력 관계 보안 게이트웨이에 의한 침입 차단

5. 결론

사이버 공격이 증가하고 다양해짐에 따라 DNS가 관리하고 있는 인터넷 주소 자원이 사용자가 인터넷을 통해 사용하는 많은 서비스에 필수적이고 핵심적인 자원이기 때문에 보다 안전하게 관리되고 보호되어야 한다. 이러한 DNS의 보안 기능을 강화하고자 하는 기술로는 DNSSEC이 있다. 이는 기존 DNS에서 제공하지 않는 데이터에 대한 인증 및 무결성을 제공하여 네임서버가 관리하는 존 파일 데이터의 신뢰성을 향상시킬 수 있다. 또한 비인가된 사용자로부터의 존 전달이나 동적 갱신을 방지할 수 있다. 그러나 현재 사이버 공격의 형태를 살펴보면 이러한 프로토콜의 보안 강화만으로는 공격자에 의한 위협으로부터 완전히 벗어날 수 없다. 따라서 DNS 프로토콜 보안 강화와 더불어 통합보안관리 시스템을 이용한 네트워크 차원에서의 대응이 함께 이루어져야 한다.

현재 DNSSEC의 경우 BIND9를 통해 구현되어 사용되고 있지만, 향후 보다 강화되고 안정화된 DNS 보안을 위해 암호화된 DNS 정보의 추가로 인한 데이터량의 증가와 서명 및 키 관련 추가 연산에 의한 부하를 해결해야 하며, 통합보안관리 시스템의 경우 DNS 서비스 보안을 적용하기 위한 정책 수립 및 운영에 대한 대책이 수립되어야 할 것이다.

참고문헌

[1] Albitz, P. and Liu, C., *DNS and Bind 2nd Ed.*, O'Reilly & Associates, January 1997.

[2] R. Lemos, "Net attack-how it was squashed", CNET News.com, October 2002.

[3] P. Mockapetris, "Domain Names – Concepts and Facilities", RFC 1034, November 1987.

[4] P. Vixie, "DNS and BIND Security Issues", ISC, May 1995.

[5] S. M. bellovin, "Using the Domain Name System for System Break-ins", Proceedings of 5th USENIX UNIX Security Symposium, June 1995.

[6] "CERT* Advisory CA-2002-31:Multiple Vulnerabilities in BIND", CERT, November 2002.

[7] "CERT* Advisory NL- S-02-77:Buffer overruns in SQL Server 2000", CERT, July 2002.

[8] *SQL_Overflow 웜의 분석 보고서*, 안철수연구소 기획기술실, January 2003.

[9] D. Eastlake, "Domain Name System Security Extensions", RFC 2535, March 1999.

[10] 김동수, 정태명, "중앙 정책 관리를 통한 방화벽 통합 관리 시스템의 개발", 한국통신망운용관리학술대회(KNOM) 2000, May 2000.

[11] *Secure Virtual Network Architecture : A Customer-focused White Paper*, Check Point Software Technologies Ltd., November 2000.

[12] D. Schnackengerg, H. Holliday, R. Smith, K. Djahandari and D. Sterne, "Cooperative Intrusion Traceback and Response Architecture (CITRA)", DISCEX '01. Proceedings, June 2001.