인터넷 기반구조의 취약성 분석과 보안 강화 방안

Improving the Internet Infrastructure Security

이희조
Heejo Lee

인터넷의 의존도가 증가됨에 따라 인터넷 마비로 이어지는 보안사고의 위협이 점차 증가되고 있다. 최근의 인터넷 보안 사고로부터 인터넷 기반구조의 보안 문제점들이 부각되고 있으며 관련 연구의 필요성이 제기되고 있다. 그러나 이제까지의 인터넷 보안관련 연구는 기반구조 보호 측면보다는 주로 정보의 보호라는 관점에서 진행되어 왔다. 본 논문에서는 인터넷의 기반구조를 도메인네임 시스템(DNS), 네트워킹 장비, 라우팅 프로토콜, 네트워크 연결 구조로 구분하고 이들에 대한 공격 위험성을 분석하며 보안을 강화하기 위한 방안과 앞으로의 연구 방향을 제시한다.

주제어: 인터넷 기반구조 보호, 도메인 네임 시스템, 라우터 공격, 라우팅 프로토콜 보안, 네트워크 연결 구조, 서비스 거부 공격

Growing dependency on the Internet increases the importance of protecting the Internet from various security threats. Recent incidents show the potential of affecting the entire Internet infrastructure. However, the research in the Internet security has been focused on securing the information instead of securing the Internet infrastructure itself. In this paper, we will introduce the vulnerabilities of the Internet infrastructure with respect to attacking the domain name system (DNS), networking devices, routing protocols, and network topology, respectively. As well, we show the research trends for securing the Internet infrastructure and the directions of future research.

Keywords: Internet infrastructure security, DNS (domain name system), router attack, secure routing protocol, network topology, denial of service attack

I. 서 론

인터넷의 발달은 정보 교류의 가속화와 더불어 많은 편리함을 가져다 주었으며 이제는 생활의 여러 부분에 직접적인 영향을 끼치는 핵심 인프라가 되었다. 또한, 국가의 기반이 되는 금융, 항공, 운송, 에너지, 국방과 관련되는 시스템들이 인터넷과 연동이 되어짐에 따라 인터넷은 국가 전체를 제어하는 신경망 시스템으로 자리를 잡아 가고 있다[19].

인터넷은 초기에 연구 정보 교류를 위한 목적으로 설계되어졌으며 악의적인 사용자를 염두에 두지 않음으로 인하여 보안이라는 관점에서는 많은 취약성이 존재하고 있다. 이를 보완하기 위한 다각적인 시도가 이루어져 왔으나 아직도 많은 연구가 필요로 되고 있다. 또한, 인터넷의 급성장과 더불어 인터넷이 어떤 모습으로 성장해가고 있는지의 전반적인 이해와 이를 바탕으로

이희조: 안철수 연구소

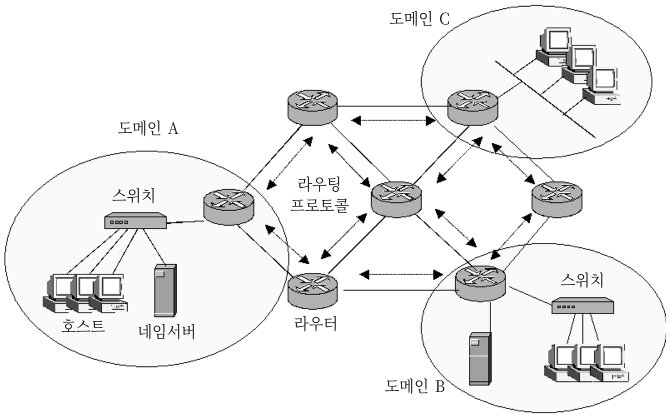


그림 1. 인터넷 기반구조 구성요소

한 보안 강화방안의 연구가 필요하게 되었다.

최근에 발생한 인터넷 보안 사고는 인터넷 기반구조가 공격에 의해 마비될 수 있음을 일깨워 주었다. 이러한 공격의 예로서는 2002년 10월 21일 발생한 루트 네임서버의 분산 서비스거부(DDoS) 공격과 2003년 1월 25일 발생한 SQL 슬래머 웜의 공격이 있었으며, 이들은 인터넷 인프라의 취약성을 보여준 대표적 사건으로 인터넷 전체가 공격에 의해 영향을 받을 수 있음을 보여준 사건이다.

이제까지의 인터넷의 발전 방향은 주로 네트워킹 성능을 높이기 위한 방향으로 발전해 오고 있으며, 이는 보안과 생존성 강화 측면으로는 상반되는 면이 존재한다는 연구 결과가 보고되었다[14]. 또한, 보안을 강화하기 위한 연구는 주로 정보의 보호 관점에서 연구가 진행되어 왔으며, 전반적인 인터넷 기반 구조의 보안 문제에 관한 연구는 미흡한 실정이다[5].

본 논문에서는 인터넷의 기반구조의 특성을 분석하고 보안 취약성을 강화하기 위한 접근 방안을 정리하고자 한다. 또한, 앞으로의 인터넷 기반구조의 보안강화를 위한 연구 전망을 제시한다.

II. 인터넷 기반구조 공격 유형

1. 인터넷 기반구조

인터넷은 다양한 네트워크를 연결하여주는 네트워크의 네트워크로 국경과 지역을 초월하는 거대 네트워크가 되었다. 인터넷 기반 구조를 이루는 요소로는 도메인네임 시스템(DNS: Domain Name System), 네트워킹 장비, 라우팅 프로토콜, 네트워크 연결 구조 등이 있다. 그림 1에서는 이러한 인터넷 기반구조의 구성요소를 바탕으로 인터넷을 단순화하여 보여주고 있다.

인터넷 기반구조의 구성 요소를 크게 구조적 측면과 프로토콜 측면으로 구분할 수 있다. 구조적인 측면의 구성 요소로는 네트워킹 장비와 이들간의 연결로서 이루어지는 네트워크들의 연결 구조가 해당된다. 이러한 구조 위에서 동작이 되는 것이 프로토콜 측면의 구성요소들로 이들은 라우팅 프로토콜과 도메인네임 시스템이 있다. 본 논문에서는 4가지 각각의 구성요소들의 보안 문제점과 강화방안을 차례로 살펴본다.

2. 인터넷 기반구조 공격 유형 분류

인터넷의 기반구조에 대한 공격으로는 직접공격, 서비스 거부공격, 프로토콜 스푸핑 공격, 간접공격으로 구분할 수 있다.

- 직접 공격: DNS 서버와 라우터 등을 직접 침입하는 형태의 공격을 말하며 추후 다른 공격으로 이어질 수 있는 특징을 지닌다.
- 서비스거부 공격: 서버나 라우터 그 자체, 혹은 네트워크에서 처리할 수 있는 용량 이상의 과다 트래픽을 유발하여 정상적인 서비스가 계속될 수 없도록 하는 공격 유형을 말한다.
- 프로토콜 스푸핑: TCP/IP와 기타 라우팅 프로토콜의 인증 취약점을 이용하는 속임수 공격으로 접근이 허가된 정상적인 사용자의 IP 주소를 도용하여 공격을 수행하는 형식이다.
- 간접공격: 이미 공격을 당한 시스템을 에이전트로 하여 다른 시스템을 공격하는 방식으로 인터넷 웜, 트로이 목마, 컴퓨터 바이러스 등을 함께 이용하기도 한다.

다음 장에서 인터넷 기반구조의 각 구성 요소별 취약성 분석과 이를 강화하기 위한 방안을 정리한다.

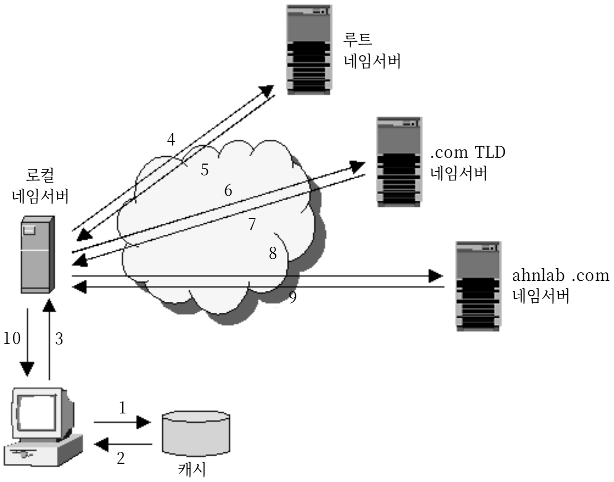


그림 2. 캐시되지 않은 도메인 이름을 찾는 반복 질의과정

Ⅲ. 도메인네임 시스템(DNS)

1. DNS 개요

DNS는 인터넷 기반구조의 필수 응용 프로토콜로 사람들이 인식하기 쉬운 도메인 이름을 IP 주소로 변환시켜주기 위한 분산 데이터베이스 시스템이다.[1] 네트워크에서 인식이 되는 것은 4 바이트 숫자로 표현이 되는 IP 주소밖에 없으므로 www.ahnlab.com와 같이 문자열로 표현이 되는 도메인 이름을 IP 주소로 변환해 주는 시스템이 필요하고 이 역할을 하는 것이 DNS이다. 인터넷의 주요 어플리케이션인 웹과 이메일 등은 DNS와의 연동이 필수적이다. 그림 2에서는 사용자 컴퓨터에서 도메인 이름에 대한 질의에 대해 IP 주소를 찾기 위해 계층구조 형태로 구성되어진 네임 서버를 찾아가는 과정을 도식화 하고 있다.

전화를 사용할 때 전화번호부의 역할을 인터넷에서는 DNS가 하고 있다[12]. 즉, 전화는 숫자로 된 전화번호밖에 인식하지 못하므로 기억하고 있는 이름을 이용하여 전화번호를 찾게 된다. 전화번호를 찾는 방식은 이름과 전화번호를 적어둔 수첩이나 전화번호부, 혹은 114 등이 있으며, 이러한 역할을 인터넷에서는 호스트 내의 캐시(Resolver Cache), 로컬 네임서버, 루트 네임서버 등이 하고 있다. 이러한 DNS 시스템이 동작하지 않는다면 인터넷은 무용지물이라 할 수 있다.

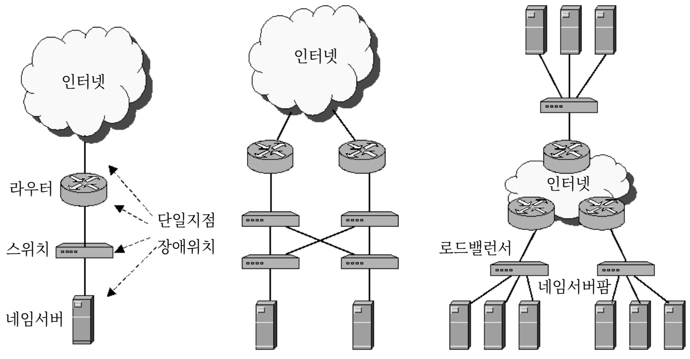
2. DNS 공격 유형

DNS에 문제가 발생하는 경우 인터넷에 미치는 영향은 매우 크다. 특정 도메인을 담당하는 네임서버에 문제가 발생하여도 해당 도메인에 대한 네트워킹 뿐 아니라 전체 DNS에 영향을 끼칠 수 있게 된다. 2002년 1월 24일 Microsoft 네임 서버의 문제로 인해 루트 네임서버에 질의가 급증한 현상은 이를 잘 나타내 주고 있다[4]. 또한, 최상위 네임 서버인 루트 네임서버에 문제가 발생할 경우 전체 인터넷이 마비가 될 수 있음을 일깨워준 사건은 2002년 10월 21일 발생한 13대의 루트 네임서버에 대한 DDoS 공격에서 알 수 있다. 이때는 7~8대의 루트 네임서버에 장애를 일으켰으며 1시간 동안 공격을 하다 멈추었으나 지속되는 경우 공격의 특성상 대응이 어렵고 치명적일 수 있다는 것을 알게 하여 주었다.

DNS에 대한 공격 유형을 크게 4가지로 분류할 수 있으며, 이는 네임 서버의 침입, 네임 서버에 대한 서비스 거부공격, DNS 스푸핑 공격, 내부 네트워크의 정보 유출 등으로 구분할 수 있다[10].

- 네임 서버의 침입: 네임 서버로 운영되는 시스템을 침입함으로서 네임 서버를 제어할 수 있는 권한을 획득하는 형태의 공격을 말한다. 이러한 네임서버의 제어권을 획득하는 경우 해당 네트워크에 대한 공격 등 다른 공격으로 이어질 수 있게 된다.
- 서비스 거부공격: 네임 서버에 대한 서비스 거부공격은 해당 도메인에 대한 DNS 동작이 불가능해 지고, 결과적으로는 해당 네트워크의 인터넷 서비스를 마비시키게 된다. 또한, 외부 네트워크에서도 해당 도메인 정보를 얻지 못하여 접근이 용이하지 않게 되며, 지정된 캐시 기간이 만료되면서 해당 도메인에 대한

[1] DNS에서는 도메인 이름을 IP 주소로 변환해 주는 정방향 질의(“A” Query)와 더불어 IP 주소로부터 도메인 이름을 변환해 주는 역방향 질의(“PTR”Query)도 가능하다.



(a) 단일구조 (b) 고가용성 이중구조 (c) 복수지역 중복구조

그림 3. 네임 서버의 구성 방식

접근이 불가능하게 된다.

- DNS 스푸핑 공격: DNS 프로토콜의 인증의 취약성을 이용한 공격으로 크게 네임 서버를 속이는 공격과 네임 서버에 질의를 요청한 클라이언트를 속이는 공격으로 구분이 된다. 네임 서버를 속이는 공격은 가짜 자원 레코드(resource record, RR) 를 네임서버에 저장하도록 함으로써(cache poisoning) 질의의 응답으로 변조된 값이 전달이 되게 하는 경우를 말한다. 클라이언트에 대한 속임수는 요청된 질의에 대해 네임 서버가 응답하기 이전에 가짜 응답 정보(fake reply)를 클라이언트에게 보내는 경우를 말한다.
- 정보 유출: 네임 서버에 저장된 정보가 통째로 유출되는 경우 공격자는 네트워크 연결 구조와 같은 내부 네트워크 정보를 획득할 수 있게 된다. 예를들어, 도메인 데이터베이스 정보가 1차 서버에서 2차 서버로 이동(zone transfer) 하는 내용이 침입자에게 유출되는 경우 이러한 정보는 내부 네트워크로의 침입과 같이 다음 단계의 공격에 활용이 되어질 수 있다.

DNS에 대한 공격은 해당 네트워크 전체에 영향을 끼치고 다른 네트워크에 대한 추가 공격에 활용될 수 있는 등의 위험성이 존재한다.

3. DNS 보안 강화

DNS의 보안을 강화하기 위한 방안으로는 프로토콜 보안 강화, 네임서버로 유입되는 트래픽 제어, 서버와 네트워크 구조 강화, 네임서버 분산 및 복제기술 등이 있다.

- 프로토콜 보안강화: DNS 프로토콜에 인증 및 데이터 무결성을 강화하기 위한 것으로 IEFT에서 추진하고 있는 DNSSEC[6]이 있다. 디지털 서명 방식을 이용하여 보안을 강화한 것으로 클라이언트와 네임서버 자체가 안전하지 않은 경우 여전히 보안 취약성이 존재하게 된다.
- 네임서버 트래픽 제어: 네임서버의 앞단에서 네임서버로 유입되는 트래픽을 제어하는 것으로 TCP/UDP 53번 포트 외에 불필요한 트래픽 차단(packet filtering)하고 처리 가능한 용량의 트래픽 유입만을 허가(rate limiting) 함으로써 네임서버에 대한 침입과 서비스 거부공격을 방어할 수 있게 된다.
- 서버와 네트워크 구조 강화: 네임서버가 위치한 네트워크에 단일지점 장애위치(single point of failure)가 없도록 구성함으로써 서비스 거부공격과 고장에 대해 생존성을 높이고 지속적인 서비스 제공이 가능하도록 한다.
- 네임서버 분산 및 복제기술: 네임서버의 구성을 대용량 단일서버보다 소용량 다중서버로 DNS 서버 팜을 구성하여 안정성을 높일 수 있다. 또한, 루트 네임서버와 같이 전체 인터넷의 성능과 직결되고, 문제 발생시 전체 인터넷에 치명적인 영향을 끼치는 네임 서버는 여러 지역에 분산해 둠으로서 성능을 향상시키고 더불어 네트워크의 장애나 공격에 저항력을 높이게 할 수 있다.

네임서버를 구성함에 있어서 잦은 오류중에 하나는 단일지점 장애위치를 가진 치명적인 구조로 네임서버 인프라를 구성하는 경우이다. 단일지점 장애위치란 이들 중 한곳만 정상동작을 하지 못해도 서비스 전체가 마비되는 치명적인 지점을 말한다. 이러한 단일지점 장애위치로는 네임서버들이 모두 하나의 서브네트워크에 존재하는 경우나 하나의 네트워킹 장비에 모든 네임서버들이 연결되는 경우나 네트워크에 단일 링크로 연결되는 위치가 존재하는 경우 등에 나타난다. 이러한 예로 Microsoft가 4대의 네임서버를 동일 서브넷에 구성하여 두었다가, 2002년 1월에 라우터 설정 실수로 인해 모든 네임서버가 인터넷 연결이 끊긴 경우에서 라우터가 단일지점 장애위치가 된다.

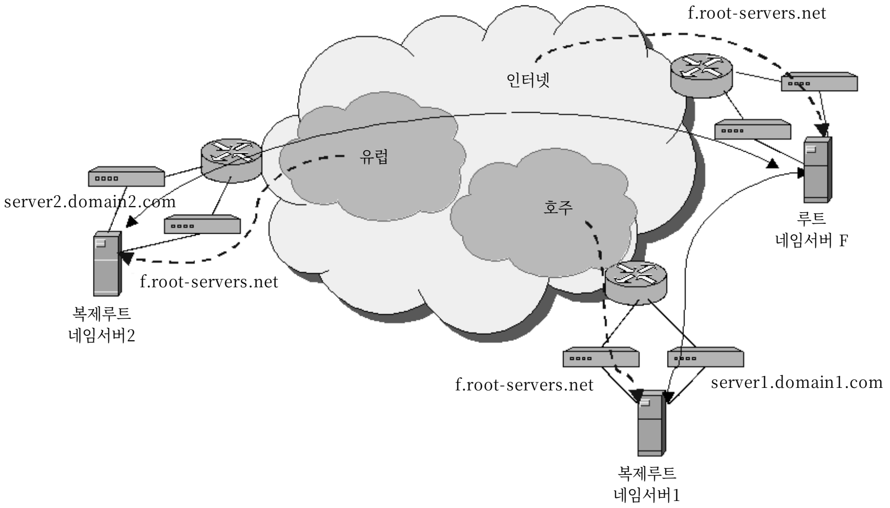


그림 4. 루트 네임서버의 복제기술

그림 3의 (a)에서는 단일지점 장애위치의 예를 나타내주고 있으며, 그림3의 (b)에서는 이러한 단일지점 장애를 없애기 위한 고가용성 이중구조 구성의 예를 보여주고 있다. 또한, 그림3의 (c)에서는 지역적로도 분산이 되어 복수지역에 네임서버들을 중복하여 구성하는 예시를 보여주고 있다.

루트 네임서버는 전세계에 13개의 네임서버가 존재하고 있으며, 캐시되지 않은 모든 DNS 질의의 시작지점 이기 때문에 루트 네임서버가 동작하지 않으면 인터넷 전체가 마비가 된다. 이러한 루트 네임서버의 중요성으로 인해 위험 분산을 위하여 루트 네임서버의 복제기술을 시도하고 있다[22]. 맨처음 복제에 성공한 것은 13개의 루트 네임서버 중에서 F-루트서버로 2002년 11월에 이를 운영중인 ISC(Internet Software Consortium)에서 APNIC에 제공한 경우이다. 미국에 있는 F-루트 서버는 현재 호주, 유럽 등으로 복제되어 가고 있다. 루트 네임서버의 복제기술을 이용하면 같은 루트 네임서버의 IP 주소로 질의가 되어도 지역마다 가까운 복제 네임서버를 찾아가게 되므로서 응답시간이 줄어들어 DNS 성능을 향상시킬 수 있으며, 또한 고장이나 공격에 대한 피해를 최소화할 수 있게 한다.

그림 4에서는 두개의 네트워크 인터페이스를 이용하여 루트 네임서버를 복제하는 기술을 표현하고 있다. 같은 주소의 루트 서버에 대한 요청도 지역에 따라 가까이 있는 복제 서버로 질의가 가도록 설정된 경우이다. 이러한 환경을 구성하기 위해서는 V장에서 소개가 되어지는 BGP 라우팅 프로토콜을 이용할 수 있다. 복제 루트서버가 존재하는 AS에서는 루트서버의 네트워크가 연결되어 있음을 BGP 업데이트 메시지를 통해 발송하게 되면, 주변에 가까이 있는 네트워크에서 루트서버로 접근하는 경우에 근처 복제 서버로 라우팅이 이루어 진다.

IV. 네트워킹 장비

1. 네트워킹 장비 개요

인터넷은 여러 네트워크를 연결하는 네트워크의 네트워크이다. 이러한 네트워크를 형성하기 위해서는 네트워킹을 위한 장비를 이용하게 된다. 주요 네트워킹 장비로는 라우터, 스위치, 브릿지 등이 있다. 이중에서도 라우터는 네트워크들 간의 연동을 위해 TCP/IP 프로토콜에 기반을 하여 네트워크 사이에 패킷을 전달하는 역할을 함으로써 인터넷의 기반구조를 이루는 주된 요소가 되고 있다.

인터넷의 기반이 되는 라우터에 대한 공격은 네트워크에 전반적인 영향을 끼칠수 있으므로 공격의 주된 목표가 되고 있다[3]. 본 장에서는 네트워킹 장비 중에 라우터에 대한 공격과 이의 영향력을 분석해 보고, 라우터의 보안을 강화하기 위한 방안을 살펴본다.

2. 라우터 공격 유형

라우터의 공격 유형은 특정 라우터에 대한 직접적인 공격과 라우터간의 라우팅 정보 교환을 위한 라우팅 프로토콜의 취약성을 이용한 간접 공격이 있다. 라우팅 프로토콜의 공격은 다음 장에서 별도로 다루도록 하며, 본 장에서는 라우터에 대한 직접적인 공격을 중심으로 기술하도록 한다.

라우터의 직접적인 공격의 유형으로는 라우터를 침입하여 라우터 기능의 제어하는 것과 라우터에 대한 서비스 거부공격이 있다. 이러한 공격의 유형은 다음과 같이 패킷 드롭, 잘못된 경로로 패킷 전달, 특정 네트워크 인터페이스 차단, 패킷 훔쳐보기, 서비스 거부공격

등이 있다.

- 패킷 드롭: 라우터에 도착한 패킷을 드롭하도록 하는 경우 패킷은 목적지에 도달하기 전에 유실이 된다. 특정 네트워크에서 오가는 패킷을 전체를 드롭하거나 일부를 드롭하는 경우로 나눌 수 있다. 일부의 패킷만 드롭되어도 TCP의 성능에 매우 큰 영향을 끼치며[16], 오동작하는 라우터를 찾아내기 어려운 특징이 있다.
- 잘못된 경로로 패킷 전달: 정상적인 라우팅 경로와 다르게 패킷을 전달하는 경우이다. 이때, 최적의 라우팅이 되지 않아 네트워크 속도 지연이 발생하거나, 특정 링크에 패킷이 집중되므로서 트래픽 혼잡이 가중되고 결과적으로 네트워크가 마비되는 서비스 거부 공격 현상이 발생할 수 있다[5].
- 특정 네트워크 인터페이스 차단: 라우터에 연결된 네트워크 인터페이스의 기능을 정지시킴으로써 특정 네트워크를 인터넷에서 차단할 수 있게된다. 모든 네트워크 인터페이스를 차단하는 경우 라우터에 연결된 네트워크들 사이에는 네트워크 단절현상이 발생한다.
- 패킷 훔쳐보기: 라우터를 제어하여 특정 네트워크로 가는 패킷을 모니터링 할 수 있다. 공격자는 모니터링 하고자 하는 패킷들의 라우팅을 자신이 제어하는 특정 네트워크로 보내지도록 함으로써 패킷 모니터링을 할 수 있다. 또한, 도달한 패킷들은 다시 재전송하여 목적지까지 보내게 되면 일반 사용자는 인식하지 못하는 사이에 특정 네트워크 전체가 모니터링이 될 수 있게 된다. 이 경우 라우팅 경로가 변경되어 해당 패킷들의 도달 시간이 일부 지연될 수 있으나 모니터링 되고 있는 것을 발견하기는 쉽지 않다.
- 서비스 거부공격: 다양한 형태의 서비스 거부공격을 라우터를 목표로 공격을 할 수 있다. 이 경우 라우터가 정상적인 기능을 하지 못하거나 라우터로 과다한 트래픽이 집중되어 패킷 손실율이 급증하게 된다. 결과적으로는 네트워크가 차단되는 현상이 발생한다.

이외에도 다른 네트워크를 공격하기 위한 중간 경로로 활용하거나 라우터의 다양한 기능을 이용하여 추가 공격에 활용이 될 수 있다.

3. 라우터 보안 강화

라우터는 대표적인 네트워킹 장비이지만 설정 변경이 자주 필요치 않은 특성으로 인하여 문제가 발생하지 않는 이상 방치되는 경우가 많이 있다. 위에서와 기술한 바와 같이 실제 주요 서버들에 대한 공격 보다 네트워크 전반에 걸쳐 훨씬 큰 영향을 끼칠 수 있으므로 라우터의 보안 관리를 더욱 세밀히 할 필요가 있다. 라우터의 보안을 강화하기 위한 방법으로는 다음과 같다.

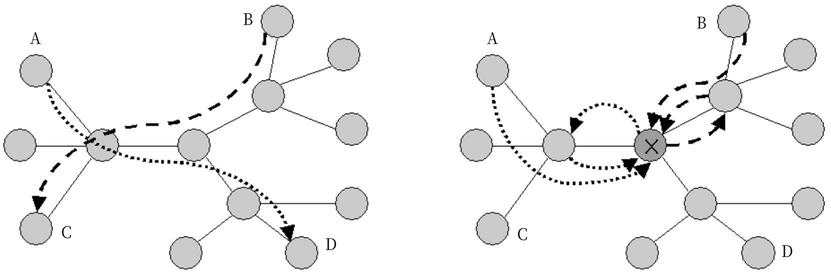
- 라우터 암호 관리: 라우터의 암호는 외우기 쉽도록 매우 간단한 암호를 사용하거나, 모든 라우터에 같은 암호를 사용하는 경우가 있다. 특히 라우터 업체에서 초기 설정해둔 암호를 그대로 사용하는 경우는 외부의 침입에 쉽게 노출이 되게 된다. 이러한 예로는 "router", "network", "admin"과 해당 도메인 이름 등을 암호로 사용하는 경우 등이 있다. 따라서, 정기적으로 암호를 변경하는 규칙을 설정하고 관리자들간에 오프라인으로 공유하는 등의 라우터 암호관리 규칙을 점검하여야 한다.
- 라우터 OS 취약성 강화: 라우터에 사용되는 OS는 장비 업체 자체 개발한 OS나 Unix 계열 운영체제를 수정한 경우가 있으며, 이들의 보안 취약성으로 인해 라우터의 관리자 권한을 획득할 수 있게 된다. 따라서, 해당 라우터 제조사에서 배포하는 버그 패치와 OS 업그레이드를 정기적으로 수행토록 한다.
- 라우터 접근 제어: 라우터에 관리를 위해 접근할 수 있는 터미널의 IP 주소를 지정하도록 한다. 접근 제어 규칙을 설정해 두지 않는 경우 세계 어느 곳에서나 접근 시도가 가능하므로 공격 당할 확률이 그만큼 높아지게 된다. 라우터 마다 다양한 접근 제어 방법을 제공하고 있으므로 해당 사이트의 관리에 적절한 접근 제어 방법과 규칙을 설정하도록 한다.
- 불필요한 기능과 프로토콜 제거: 라우터에 기본적으로 설정이 되어있는 기능과 네트워크 프로토콜 중에 사용하지 않는 기능은 제거하도록 한다.
- 유해 트래픽 제어: 네트워크의 경계에 있는 라우터에서 불필요한 유해 트래픽을 차단하도록 한다. 유해 트래픽으로는 사설 IP 주소의 패킷, 브로드캐스트 주소의 패킷, 소스 주소가 변조된 패킷 등을 차단한다[8]. 또한, 같은 패킷이 반복적으로 나가고 들어오는 경우 라우팅 루프[2]나 인터넷 웜의 공격일 가능성이 있으므로 이를 필터링하는 방법 등이 있다[17].

V. 라우팅 프로토콜

1. 라우팅 프로토콜 개요

라우팅 프로토콜은 네트워크의 변화에 따라 라우팅 정보를 교환하여 라우팅 테이블을 동적으로 업데이트 해주는 역할을 한다. 매번 새로운 네트워크가 추가되거나 제거 될 때 마다 모든 네트워크에서 수동으로 라우팅

[2] 인터넷에서는 라우팅 루프가 종종 발견되고 있으며, 주된 원인으로서는 라우터들간에 라우팅 정보 불일치에서 기인하는 것으로 보고되었다[9]. 라우팅 루프에 빠진 패킷은 TTL=0가 되면서 사라지게 되며, 이러한 라우팅 루프는 트래픽 혼잡을 가중시키고 네트워크 성능에 저해 요인이 되고있다.



(a) A→D, B→C 라우팅 경로 (b) X에서 C, D 라우팅 테이블 변조결과

그림 5. 라우팅 정보 변조로 인한 라우팅 루프 형성

경로를 변경하지 않아도 가장 최적의 라우팅 경로를 찾아 라우팅 테이블을 업데이트 하게 된다.

이러한 라우팅 프로토콜로는 단일 관리 도메인(AS: Autonomous System) 내에서의 라우터간 네트워킹을 위한 IGP(Interior Gateway Protocol)와 여러 도메인 사이의 라우팅을 위한 EGP(Exterior Gateway Protocol)로 나뉘어 진다. IGP의 예로는 OSPF와 RIP가 대표적이며, EGP로는 BGP(Border Gateway Protocol)가 표준 프로토콜로 사용이 되고 있다[15].

본 장에서는 인터넷 연동의 기반이 되는 BGP 기반의 공격에 대한 위험성을 분석하고 이를 강화하기 위한 방안을 살펴본다.

2. 라우팅 프로토콜 공격 유형

라우팅 프로토콜은 초기 설계에서 인증과 데이터 무결성 등의 보안을 고려하지 않아 보안 취약성이 존재하고 있다. 라우팅 프로토콜을 이용하는 공격으로는 라우터에 침입 후에 위조된 라우팅 정보를 발송하는 형태의 라우터를 이용하는 공격과 라우팅 프로토콜의 보안 취약성을 이용한 스푸핑 공격 등이 있다. 이러한 방식으로 라우팅 프로토콜을 공격하는 유형은 다음과 같다.

- 라우팅 정보의 전달 방해: 라우팅 정보가 동기화 되지 않아 라우터 간에 상이한 라우팅 정보를 가짐으로써 라우팅 루프가 발생하거나, 패킷이 중간에서 갈 곳을 잃어 유실되게 된다.
- 라우팅 정보의 위조: 위조된 라우팅 정보를 라우터들에 전달하게 되어 라우팅 테이블이 비정상적인 경로를 따르도록 된다. 앞장의 라우터 공격에 의한 잘못된 경로로 패킷 전달하는 경우와 유사하지만 보다 넓은 영역에 피해를 줄 수 있는 특징을 지닌다.
- 라우팅 메시지 재전송 공격: 정상적인 라우팅 메시지를 저장해 두었다가 재전송하는 형태의 공격 (replay attack) 이다. 이러한 방법으로 라우팅 정보를 변조할 수 있으며, 이 경우 프로토콜의 인증이 강화가 되어도 정상적인 경우와 구분이 용이하지 않은 특징을 지닌다.

위와 같은 라우팅 프로토콜을 이용한 공격의 결과로 라우팅 경로상에 루프가 형성되어 라우팅 중에 패킷이 유실되거나 특정 네트워크에 트래픽 부하 집중으로 서비스 거부현상이 발생하고 논리적으로 망이 분리가 될 수 있으며 네트워크 전체가 마비되는 현상이 발생할 수 있다(그림 5 참조).

라우팅 프로토콜을 이용하여 라우팅 경로를 변경하는 방식으로 서비스 거부공격을 하는 경우 유해 트래픽이 아닌 정상적인 트래픽이 한 지점으로 몰려드는 형태의 공격이 되므로, 일반적인 서비스 거부공격에 비하여 근원지 추적과 대응이 훨씬 어렵게 된다.

라우팅 프로토콜을 이용한 공격의 특징으로는 해당되는 네트워크 뿐 아니라 타 네트워크나 전체 네트워크를 마비시키는 증폭효과를 가지게 된다.

3. 라우팅 프로토콜 보안 강화

인터넷 연동의 기반인 BGP의 인증과 무결성을 강화하기 위하여 BGP Scalable Transport(BST)[18] 프로토콜과 Secure BGP[11] 프로젝트가 진행되고 있다.

- BST Protocol: Packet Design 사에 의해 고안된 BGP Scalable Transport(BST) 프로토콜은 현재의 BGP를 그대로 사용하면서 BGP가 하위 프로토콜로 TCP 대신 보안이 강화된 BST 프로토콜을 사용하도록 하는 방식이다[18]. 현재 ANSI-C 소스코드를 배포하고 있으며 FreeBSD 환경에서 GateD BGP를 이용해 구현할 수 있다. 라우터에 구현하기 위해서는 메시지 전달방식에서 BST를 사용하도록 수정이 필요하다.
- Secure BGP: 현재의 BGP-4의 보안 취약성을 강화하기 위해 Secure BGP(S-BGP) 프로젝트가 추진되고 있다[11]. S-BGP는 공개키 기반구조(PKI) 상에

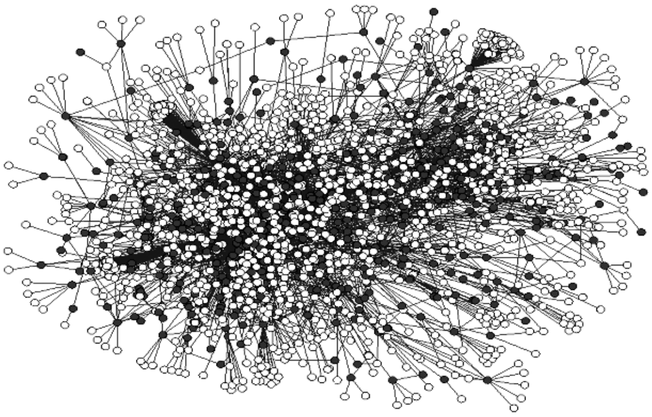
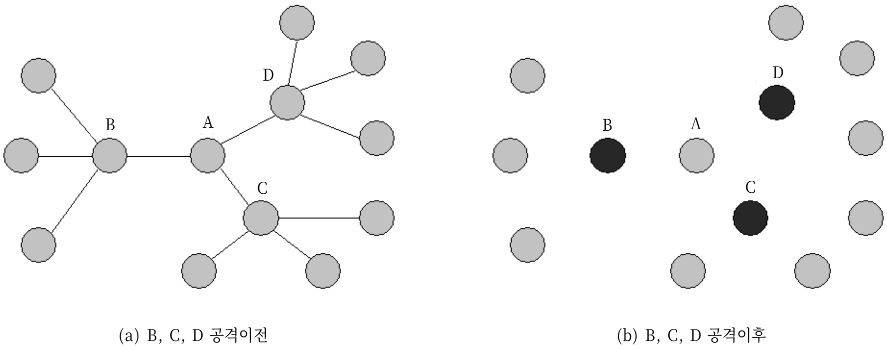


그림 6. 인터넷 AS 연결구조 그래프[3)]



(a) B, C, D 공격이전

(b) B, C, D 공격이후

그림 7. 네트워크의 연결 구조에 따른 치명적 공격

서 운영이 되며 라우터에 S-BGP가 구현되어야 한다. 현재 표준화를 추진 중에 있으며 GateD 4.0.2에 시험 구현이 되어있다.

VI. 네트워크 연결구조

1. 네트워크 연결구조 개요

네트워크의 연결구조(network topology)는 노드와 이들을 연결하는 링크로 구성이 되며 이는 그래프 형태로 표현이 될 수 있다. 노드는 흔히 라우터나 혹은 도메인(AS) 단위로 표현이 된다(그림 6 참조).

근래에 와서 인터넷의 모습이 어떤가와 어떻게 변화해 가고 있는지를 파악하기 위한 연구가 활발히 진행이 되고 있다. 첫번째 주목할만한 결과로는 인터넷 연결구조의 특성 중에 노드와 이에 연결된 링크 수인 디그리(node degree)의 분포는“ Power ”규칙을 따르고 있음을 밝혀낸 연구가 있었다[7].

하지만 이러한 몇 가지 특징만으로는 인터넷의 모습을 설명하는데는 아직도 부족함이 많다. 인터넷의 노드-디그리 분포 특성을 가지고 그래프를 역으로 만들어 보면 본래의 인터넷의 구조와 새로 만들어낸 그래프와는 여전히 큰 차이가 있음을 알 수 있다[13]. 이러한 인터넷의 구조적 특징을 파악하려는 연구는 최근에 활발히 진행이 되고 있다[21].

2. 네트워크 연결구조와 보안

네트워크는 연결 구조의 특성에 따라 네트워크의 성능 뿐만 아니라, 고장이나 공격에 대한 저항력이 달라지

[3)] Oregon RouteViews의 1997년 11월 BGP 라우팅 테이블로부터 추출한 인터넷의 AS 연결구조[20]를 Pajek 소프트웨어를 이용하여 그래프로 표현하였다.

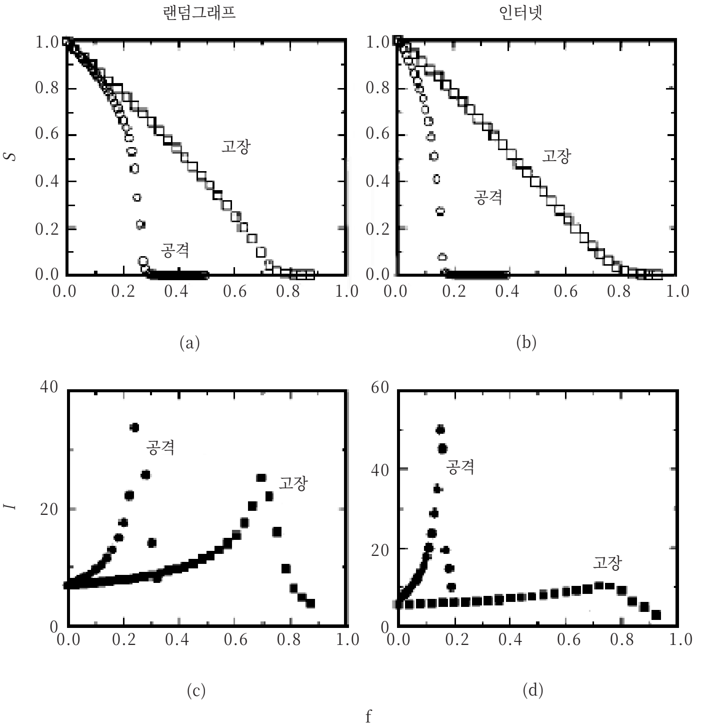


그림 8. 랜덤 그래프와 인터넷의 고장과 공격의 영향 비교

게 된다[1]. 이제까지는 네트워크의 고장에 대한 연구가 주로 진행이 되어 왔으나 공격에 의한 영향을 밝히려는 연구가 최근에 많이 진행이 되고 있다[1],[2],[14].

고장(fault)은 랜덤한 분포를 따르게 되며, 이에 반하여 공격은 공격자의 의도에 따라 취약한 노드를 선별하여 공격할 수 있는 특징을 지닌다. 그림 7에서는 한 노드를 공격하는 경우 노드 A에 대한 공격이 가장 치명적이며, B, C, D 세 노드를 공격하는 경우 전체 네트워크가 완전히 분리가 되는 결과가 된다. B, C, D 노드의 집합이 그래프에서는 모든 링크를 커버하기 때문에 VC(Vertex Cover)라 한다. 인터넷은 전체 AS의 18%만으로 VC를 이룰 수 있으므로[13] 이러한 VC 노드에 대한 공격은 매우 치명적일 수 있다.

인터넷 연결 구조의 특성은 3-D가 가장 대표적인 부분으로 이들은 Degree, Diameter, Dynamics 이다. 각각에 대한 인터넷의 특징은 다음과 같다.

- “Degree” 특성: 인터넷 연결구조는 앞에 언급된 “Power”규칙을 따르고 있으며 이는 디그리가 큰 노드 몇 개에 디그리가 1~2인 노드가 많이 붙어있는 “Heavy-Tail” 분포특성을 가진다[7]. 실제로 인터넷의 도메인들은 노드 디그리가 1이나 2인 경우가 전체의 70%를 차지하고 있으며, 평균 노드 디그리는 3.7이다. 새로운 노드는 디그리가 큰 노드에 붙는 경향이 있다[2].
- “Diameter”특성: 인터넷을 라우터 단위로 보면 두 호스트간의 평균 거리는 9이고, 도메인(AS) 단위로 보았을 때 두 도메인 간의 평균 거리는 3.7 정도이다[2].
- “Dynamics”특성: 인터넷이 진화해온 과정으로부터 Dynamics 특성을 알면 앞으로의 인터넷이 어떻게 변화해 갈 지를 예측할 수 있게 된다. 인터넷의 변화특성은 노드의 수는 시간이 지남에 따라 지속적으로 증가하고 있고, 노드 디그리는 증감이 변화하고 있고, 노드간의 평균거리인 Diameter는 감소하고 있다. Diameter가 감소하면 라우팅 경로가 짧아지게 되므로 네트워크의 지연시간이 감소되는 효과가 나타난다. 이는 네트워크가 성능 위주의 성장을 하고 있음을 의미하며, 인터넷의 연결구조 자체는 공격에 점점 더 취약해 지고 있음을 알 수 있다[14].

랜덤 그래프와 인터넷의 고장과 공격에 대한 영향력을 비교한 결과는 그림 8에 나타나 있다. 고장이나 공격에 의해 장애가 발생한 노드의 비율을 f로 나타낸다. S는 전체 인터넷 노드에 비하여 연결이 유지된 클러스터 중 가장 큰 클러스터 크기의 비율이다. 따라서 S의 초기값은 1 이며 f=1일 경우 S=0이 된다. *I*은 가장 큰 클러스터의 평균 경로 길이(Diameter) 이다. *f*가 증가함에 따라, 인터넷은 고장에 대해서는 랜덤 그래프에 비해 S가 감소하는 비율이나 *I*이 증가하는 비율이 완만한데 비하여 공격에 대해서는 매우 급격한 양상을 보

이고 있다. 이는 인터넷이 고장에는 극복이 잘되는 구조인 반면, 특정 노드에 대한 공격에는 취약한 구조임을 의미한다.

3. 네트워크 연결구조의 보안 강화

인터넷은 네트워크의 성능이 높아지고 있고 고장에 대한 저항력도 증가가 되고 있으나 특정 노드에 대한 의존도가 높아 의도적인 공격에 대하여는 점점 더 취약해져 가고 있음을 알 수 있었다.

앞으로 인터넷의 연결구조에 대한 연구를 지속하고 인터넷이 변화하는 특성에 대해 더 많은 연구가 필요하다. 이러한 인터넷의 연결구조의 특성과 변화 추세를 파악하게 되면 이러한 특성을 내포하는 연결구조의 모델을 적립하고 이 모델을 이용하여 성능과 고장과 공격에 대하여 저항력이 높은 연결구조와 네트워크 발전 방향을 도출해 낼 수 있을 것으로 기대한다.

Ⅶ. 결 론

본 논문에서는 인터넷 기반구조를 DNS, 네트워크 장비, 라우팅 프로토콜, 네트워크 연결구조의 4가지 관점에서 보안 취약성을 분석하고 보안 강화방안을 정리하였다. 인터넷의 모습은 하루하루 발전해 나가고 있으며 IT 기술과 더불어 다양한 모습의 진화가 예상되고 있다. 현재까지도 짧은 시간에 급 팽창한 인터넷의 모습과 특성을 분석하기 위한 연구를 진행 중에 있으나 많은 연구가 더 필요한 실정이다. 또한, 인터넷 기반구조 자체의 보안의 취약성이 나타나고 있으며 기반구조의 보안문제를 시급히 해결하기 위한 방안의 연구가 필요하다. 더불어 공격 형태는 더욱 지능적으로 발전해 나가고 있으므로 인터넷 기반구조의 보안성 강화에 대한 다양한 연구개발이 필요한 것으로 전망된다.

[참고문헌]

[1] R. Albert, H. Jeong, A. Barabasi, "Error and Attack Tolerance of complex networks," Nature, Vol. 406, Jul. 2000, pp. 378-382.

[2] R. Albert, A. Barabasi, "Statistical mechanics of complex networks," Reviews of Modern Physics, Vol. 74, No. 1, Jan. 2002, pp. 47-97.

[3] K. A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, R. A. Olsson, "Detecting disruptive routers: a distributed network monitoring approach," Proc. of IEEE Symp. on Security and Privacy, May 1998, pp. 115-124.

[4] N. Brownlee, K. Claffy, E. Nemeth, "DNS damage-measurement at a root server," NANOG-24, Feb. 2002.

[5] A. Chakrabarti, G. Manimaran, "Internet infrastructure security: a taxonomy," IEEE Network, Vol. 16, No. 6, Nov/Dec. 2002, pp. 13-21.

[6] D. Eastlake, "Domain name system security extensions," RFC 2535, Mar. 1999.

[7] M. Faloutsos, P. Faloutsos, C. Faloutsos, "On power-law relationships of the Internet topology," Proc. of SIGCOMM, Aug. 1999, pp. 251-262.

[8] P. Ferguson, D. Senie, "Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing," RFC 2827, May 2000.

[9] U. Hengartner, S. Moon, R. Mortier, C. Diot, "Detection and analysis of routing loops in packet traces," Proc. of SIGCOMM IMW 2002.

[10] A. Householder, B. King, "Securing an Internet name server," CERT Coordination Center, Aug. 2002.

[11] S. Kent, C. Lynn, K. Seo, "Secure border gateway protocol (S-BGP)," IEEE JSAC, Vol. 18, No. 4, Apr. 2000, pp. 582-592.

[12] Hyogon Kim, "DNS (Domain Name System), ” Unpublished manuscript, 2002.

[13] K. Park, H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internet," Proc. of SIGCOMM, Aug. 2001, pp. 15-26.

[14] S. T. Park, A. Khrabrov, D. M. Pennock, S. Lawrence, C. L. Giles, L. H. Ungar, "Static and dynamic analysis of the Internet ’s susceptibility to faults and attacks," Proc. of INFOCOM, Apr. 2003.

[15] J. W. Stewart III, "BGP4: inter-domain routing in the Internet," Addison-Wesley Networking Basics Series, 1999.

[16] X. Zhang, S. F. Wu, Z. Fu, T. L. Wu, "Malicious packet dropping: how it might impact the TCP performance and how we can detect it," Proc. of IEEE Symp. on Security and Privacy, May 1998, pp. 263-272.

[17] Cisco White Papers, "Strategies to protect against distributed denial of service attacks (DDoS)," Feb. 2000.

[18] Packet Design, "BGP scalable transport (BST) protocol," 2003, http://www.packetdesign.com/company/bst.html.

[19] White House, "The national strategy to secure cyberspace," Feb. 2003.

[20] Oregon RouteViews, "http//moat.nlanr.net/routing/rawdata/," 2002.

[21] Topology Project, http://topology.eecs.umich.edu, 2003.

[22] John Milburn, "Personal communication," 2003.

이 희 조
(Heejo Lee)

1993.2: 포항공과대학교 컴퓨터공학과 학사
1995.2: 포항공과대학교 컴퓨터공학과 석사
2000.2: 포항공과대학교 컴퓨터공학과 박사
2000.3 ~ 2001.2: Purdue Univ. CS 및 CERIAS 연구원
2001.3 ~ 현재: 안철수연구소 CTO, 기술기획실장
관심분야: 네트워크 보안, 인터넷 기반구조 보호기술, 결함포용 컴퓨팅, 병렬 알고리즘
E-mail: heejo@ahnlab.com
Tel: +82-2-2186-6145
Fax: +82-2-2186-6100