IPv4/IPv6에서 효율적인 보안 관리를 위한 보안 문제 분석

오하영° 채기준
이화여자대학교
hyoh°@ewhain.net, kjchae@ewha.ac.kr

Analysis of Security Vulnerabilities for Efficient Security Management in IPv4/IPv6

Hayoung Oh° Kijoon Chae
Ewha Womans University

요 약

IPv6는 차세대 인터넷을 구축하기 위한 가장 핵심적인 기술로서 풍부한 주소공간을 활용하여 많은 수의 이동전화, 가전제품 등 Post-PC 디바이스의 인터넷 접속 시에 예상되는 주소고갈 문제를 근본적으로 해결하면서 이동성 지원, 보안기능 강화 등 다양한 기능을 제공할 수 있도록 설계된 차세대 인터넷 프로토콜이다. 그러나 국내외로 실제 망 사업자(ISP)들이 현재 인터넷 주소방식인 IPv4의 주소고갈을 목전에 두고 있음에도 불구하고 IPv6 주소방식의 도입을 미루는 이유 중의 하나는 아직 IPv6 네트워크 환경에서의 효율적인 보안 관리를 위한 보안 프레임워크가 구체적으로 정의되어 있지 않기 때문이다. 따라서 본 논문은 차후 궁극적으로 IPv4/IPv6 혼합망 및 IPv6에서의 효율적인 보안 관리를 위한 보안 프레임워크를 설계하기에 앞서 IPv4/Ipv6에서 취약성 분석 및 보안 문제를 도출하고자 한다.

1. 서 론

128 비트의 주소체계를 사용하는 IPv6는 차세대 인터넷을 구축하기 위한 가장 핵심적인 기술로서 풍부한 주소공간을 활용하여 많은 수의 이동전화, 가전제품 등 Post-PC 디바이스의 인터넷 접속 시에 예상되는 주소고갈 문제를 근본적으로 해결하면서 Plug & Play 방식의 편리한 인터넷 제공과 이동성 지원, 보안기능 강화, 서비스 품질보장 등 다양한 기능을 제공할 수 있도록 설계된 차세대인터넷 프로토콜이다. 그러나 국내외로 실제 망 사업자(ISP)들이 현재 인터넷 주소방식인 IPv4의 주소고갈을 목전에 두고서도 IPv6 주소방식의 도입을 미루는 이유는 기존의 IPv4 방식과의 안전한 변환 및 연동이 제대로 지원되지 않았고 아직 IPv6네트워크 환경에서의 효율적인 보안 관리를 위한 보안 요구사항 연구가 제대로 되지 않았기 때문이다[1].

IPv4에서 성공적으로 IPv6로 전환하기 위해서 무엇보다 필요한 것은 안전하고 체계적인 보안 정책기반아래 기존에 동작되고 있는 IPv4 호스트 및 라우터와 IPv6의 안전한 호환성이다.

IPv4/IPv6 혼합망 환경에 적용할 수 있는 실시간 보안 노드 기술 및 보안 정책기반 보안관리 기술이나 IPv4/IPv6 혼합망에 적용이 가능한 실시간 보안게이트웨이시스템, IPv4/IPv6 혼합망 및 IPv6 환경에서 다양한 네트워크 침입을 능동적으로 탐지하고 대응할 수 있는 IPv6 인프라 구축용 라우터 통합보안기술 등 IPv4/IPv6 혼합망 및 IPv6에서의 효율적인 보안 관리를 위한 보안 요구사항 연구가 필요하다.

따라서 본 논문에서는 차후 효율적인 보안 관리를 위한 보안 요구사항을 도출 및 보안 프레임워크 설계를 위해 IPv4/IPv6 혼합망 및 IPv6에서의 취약성을 분석한다.

2. IPv4/IPv6에서 취약성 분석 및 보안 문제 도출

2.1 IPv4와 IPv6에서 유사한 공격 위협[2][3][4]

2.1.1 Sniffing Attack (스니핑 공격)

스니핑은 네트워크를 가로질러 전송 중인 데이터를 캡쳐하는 공격을 일컫는다. 가장 흔한 예로는 TCPdump(지나가는 패킷을 잡는 네트워크 모니터링 툴)가 있는데, 이것은 대부분의 유닉스와 같은 운영체제에 포함되어 있다. 스니핑 공격을 실행하고 있는 공격자는 자주 로그인 보증서를 결정하거나 아직 암호화되지 않은 프로토콜의 민감한 정보를 볼 수 있다.

IPv6가 IPsec으로 스니핑을 막는 기본적인 기술을 제공하더라도, 도전받을 것으로 예상되는 키 관리 이슈를 위한 간편함을 제공해 주지는 않는다. IPsec의 전개는 시간을 끌 것이며 스니핑 공격은 계속될 것이다.

2.1.2 Application Layer Attack (응용 계층 공격)

응용 계층 공격은 OSI 모델의 7계층에서 일어나는 모든 공격을 포함한다. 이것은 오늘날 인터넷에서 일어나는 공격들의 집합이며, 현재 존재하는 네트워크의 불안정성을 보여주는 취약점이다. 버퍼 플로우와 같은 일반적인 공격, 웹 어플리케이션 공격, 그리고 바이러스와 웜은 모두 어플리케이션 계층 공격의 카테고리에 속한다. IPv4와 IPv6 양쪽에서, 어플리케이션 레이어 공격은 자연스럽게 존재한다. 만약 프로토콜이 IP 주소에 더욱 강력한 인증을 채택한다면 이런 종류의 공격은 쉽게 추적될 수 있다. 하지만 응용 계층 공격의 책임은 영향을 받는 응용 계층에 있으며 아래 계층에서 일어나는 전송에 존재하지 않는다.

본 논문은 정보통신부 및 정보통신 연구진흥원의 대학 IT연구센터 지원 사업 및 한국전자통신연구원 정보 보호 연구단 위탁연구과제의 연구결과입니다.

2.1.3 Rogue Devices (로그 디바이스)

로그 디바이스는 불량 디바이스다. 로그 디바이스가 손쉽게 허가받지 않은 랩 탑이 될 수 있다고 하더라도, 공격자에게 더 흥미로운 점은 무선 로그 액세스 포인트(rogue wireless access point)인 DHCP나 DNS 서버, 라우터, 스위치 등이다. 이러한 공격은 IPv4에서 매우 흔하며 IPv6에서 크게 바뀌었다. 만약 IPsec이 IPV6에서 좀 더 포괄적인 방식으로 쓰인다면, 디바이스의 인증은 이러한 공격을 다소 완화시킬 수 있다. 802.1x표준이 이 방면에 도움이 될 것이다.

2.1.4 Man-in-the-Middle Attack

IPv4와 IPv6가 자체적으로 보안 메커니즘을 갖지 않기 때문에, 각각의 프로토콜은 보안에 있어 IPsec 프로토콜에 의존한다. 이러한 경향에서 IPv6는 IPsec 프로토콜을 공격하는 Man-in-the-Middle 공격에 의해 야기되는 보안 위협에 노출 될 수 있다. 따라서 공격을 막을 수 있는 툴과 디바이스가 이미 문서화되어 있다. 현재는 공격을 막기 위해, IKE main-mode negotiation을 권장한다. IKEv2가 미래에 이러한 이슈를 해결할 것으로 기대한다.

2.1.5 Flooding Attack (플러딩 공격)

플러딩 공격은 자원을 소비시킬 수 있는 손쉬운 방법이다. 늘어나는 IP 주소가 플러딩 공격에 대한 추적을 어렵게 하더라도, 플러딩 공격의 핵심은 IPv6에서도 그대로 남아있다. 로컬 공격인지 분산된 DoS공격인지에 따라, 호스트가 처리할 수 있는 이상의 또는 링크가 전송할 수 있는 이상의 트래픽을 보내 네트워크 디바이스나 호스트를 플러딩 한다. 새로운 기술이 나오더라도 IPv4에서 플러딩 추적에 쓰였던 기술이 IPv6에서도 사용 가능하다.

2.2 IPv6에서 새로운 공격 위협[2][3][4]

2.2.1 Reconnaissance (사전 답사)

Reconnaissance는 공격자에 의해 실행되는 첫 번째 공격으로 스캐닝과 같은 액티브 네트워크 방식과 검색 엔진 또는 공공 문서를 통한 소극적인 데이터 수집 방식 양쪽을 모두 포함한다.

기술에 대하여, IPv6 reconnaissance는 IPv4에서의 reconnaissance와 두 가지 중요한 점에서 다르다. 첫째로, ping sweep이나 port scan이 서브넷 상의 호스트 확인에 사용될 때, IPv6의 주소 체계가 굉장히 커졌기 때문에 이들은 IPv6에서 훨씬 수행하기 어렵다. 둘째로, IPv6에서 새로이 등장한 멀티캐스트 주소는 누구든 알 수 있기 때문에 편리함을 주는 한편 공격자로 하여금 좀 더 쉽게 Key 시스템(라우터, Network Time Protocol servers 등)을 찾을 수 있게 한다. 추가적으로, IPv6 네트워크는 적절히 작동하게 위하여 좀 더 ICMPv6에 의존한다. ICMPv6의 공격적인 필터링은 네트워크 기능에 부정적인 효과를 끼칠 수 있다.

2.2.2 Unauthorized Access (허가 받지 않은 접근)

허가 받지 않은 접근이란, IPv4로부터 상속받은 open transport policy를 이용하는 공격들의 집합은 일컫는다. IP 프로토콜 계층에서, 어떤 호스트가 네트워크상의 다른 호스트에 연결을 설정하는 것을 막는 것은 없다. 공격자는 이러한 점에 착안하여 인터네트워킹 디바이스& 종단 호스트의 상위-계층 프로토콜&어플리케이션에 연결을 설정한다.

접근 제어 기술의 필요성은 IPsec이 호스트 접근 제어를 쉽게 해주더라도 IPv4에서나 IPv6 양쪽에 모두 있다. 방어자는 공격자가 종단 호스트 상의 서비스에 대해 공격 경로를 얻는 것을 방해하기를 원한다. IPv6로의 이전에 따른 접근 제어 능력의 변화는 계층 3 헤더에서 필터링 되는 정보를 변화시켰을 뿐 아니라, IPv6의 주소 시스템과 라우팅 시스템이 형성되는 방식도 변화시켰다. 이러한 멀티플 IPv6 주소들은 로컬 서브넷(링크-로컬 → FE80::/10), 조직체(사이트-로컬 → FC00::/16 or FD00::16), 또는 대규모 인터넷(글로벌 unicast 주소 이진수 001인 프리픽스의 집합)에서의 통신에 중요한 의미를 가진다. 이러한 범위의 주소 사용이 라우팅 시스템과 결합될 때, 네트워크 설계자는 IPv6 주소 배정과 라우팅을 이용한 종단 노드로의 접근을 제한할 수 있다.

2.2.3 Header Manipulation and Fragmentation

파편화(fragmentation)와 헤더 매니퓰레이션 공격은 NIDS나 stateful firewalls와 같은 네트워크 보안 디바이스를 피해가는 수단이나 네트워킹 infrastructure를 직접적으로 공격하기 위해 사용될 수 있다.

많은 문제점이 있었던 중간 디바이스에 의한 파편화가 IPv6에서는 금지되어 있다[RFC 2460]. 따라서 IPv6에서, 오버랩(oerlapping)된 파편은 공격으로 보일 수 있으며, 제거될 수 있다. 하지만, 만약 종단 운영체제가 오버랩된 패킷을 수락한다면, IPv4 파편화 공격과 유사한 목적을 위해 IPv6 보안 디바이스 정책을 우회하려고 파편화된 패킷을 이용하는 공격자를 막을 수 있는 방법이 없다. 추가로, 공격자는 여전히 순서를 읽은 파편을 네트워크 기반의 IDS를 우회하는데 사용할 수 있다.

2.2.4 Layer3,4 spoofing (3,4 계층 스푸핑)

다양한 타입의 IP 공격을 가능케 하는 핵심 요소는 공격자의 능력(IP 주소를 수정하고, 다른 장소나 응용 프로그램으로부터 보내진 조작된 트래픽을 나타내기 위해 통신하고 있는 포트 주소를 수정하는 능력)이다. 널리 알려진 완화 방법에도 불구하고 "Spoofing"이라 불리며 흔히 사용되고 있다.

IPv4와는 다르게, IPv6에서 3계층 스푸핑 공격을 완화할 수 있는 방법 중 하나는 IPv6 할당은 네트워크의 서로 다른 포인트에서 쉽게 요약하는 것과 같은 방식으로 이루어지기 때문에 ISP가 고객을 보호해 줄 수 있는 필터링을 허락 한다[RFC 2827]. 하지만 이 방식은 표준 행동을 요구당하지 않으며, 오퍼레이터 영역에서 의식 있는 구현을 요구한다. 4계층 스푸핑 공격은 어떤 점에서 변하지 않았다. 왜냐하면, 4계층 프로토콜이 스푸핑과 관련하여 IPv6에서 변하지 않았기 때문이다. 단지 IPv6에서 서브넷의 크기가 더 커졌으며, 그 때문에 RFC 2827과 같은 필터링에서도 공격자가 거대한 범위의 주소를 스푸핑을 할 수 있다.

2.2.5 ARP and DHCP Attack

ARP와 DHCP 공격은 호스트 초기화 프로세스나 호스트

가 전송을 위해 접근하는 디바이스를 파괴하려 시도하는 공격이다. 이 공격은 일반적으로 로그 디바이스나 위협받은 디바이스 또는 스푸핑 된 통신을 통해, 호스트의 bootstrap (=booting) 대화를 파괴를 포함한다.

IPv6에서, 불행히도, DHCP나 ARP와 동등한 보안 기능이 상속되지 않았다. 왜냐하면 IPv6에서 제공되는 DHCP와 유사한 기능인 "stateless autoconfiguration" 은 DHCP에 대해 실행 가능한 대안을 제시할 수 없고, 할당된 DHCP 서버는 IPv6에서 흔하지 않으며 심지어 현재의 서버 운영 체제에서 널리 사용되지도 않기 때문이다. 따라서 "stateless autoconfiguration" 메시지는 스푸핑될 수 있으며, 스푸핑은 디바이스에 대한 접근을 거부하기 위해 사용될 수 있다. 이 공격을 완화하기 위해, "신뢰하는 포트 개념이 router-advertisement 메시지와 관련하여 사용되어야 한다.

2.2.6 Broadcast Amplication Attack (Smurf)

브로드캐스트 증폭 공격(스머프 공격)은 서브 넷의 브로드캐스트 주소를 목적지로 하여 에코-요청 메시지를 보내고 소스의 주소를 희생자의 주소로 속일 수 있는 능력을 가진 DoS공격 툴이다. 서브 넷 상의 모든 종단 호스트들은 spoof된 주소(희생자의 주소)로 에코-응답 메시지를 응답을 보내고 희생자는 에코-리플라이 메시지로 인해 넘치게(flood)된다.

IPv6에서 IP-지향 브로드캐스트의 개념은 프로토콜로부터 제거되었고, 이러한 공격을 완화시키도록 설계된 특별한 언어가 프로토콜에 삽입되었다. 특별히 스머프 공격에 대하여 RFC 2463은 ICMPv6 메시지가 IPv6 멀티캐스트 목적지 주소나 링크-계층 멀티캐스트 주소 또는 링크-계층 브로드캐스트 주소를 가진 패킷에 대한 응답으로 생성되어선 안 된다고 기술한다. 만약 종단 노드가 RFC 2463에 따른다면, 스머프와 다른 amplification 공격은 IPv6에서 문제가 되지 않을 것이다.

2.2.7 Routing Attacks

라우팅 공격은 네트워크의 트래픽을 방해하거나 방향 재설정에 초점을 맞춘다. 공격은 다양한 방식으로 실행되는데, flooding 공격, rapid announcement, removal of routers, bogus announcement of router등의 방식을 이용할 수 있다. 공격의 상세한 부분은 사용되는 프로토콜에 따라 다르다.

몇몇의 프로토콜은 버전이 변하는데도 불구하고 보안 메커니즘을 바꾸지 않았다. BGP(Multiprotocol Border Gateway Protocol)는 도메인 간 라우팅 정보를 나르기 위하여 IPv6에서 확장되었고, 여전히 인증을 위해 TCP MD5에 의존한다. Intermediate System-to-Intermediate System(IS-IS) 프로토콜은 IPv6지원을 위해 드래프트에서 확장되었지만, IS-IS 인증의 기본적인 부분은 변하지 않았다. 기본적으로, IS-IS는 인증 정보를 LSP의 일부로 포함함으로써, LSPs (Link-State Packets)의 인증을 제공했다. 그렇지만 단순한 비밀번호 인증은 암호화되지 않았다. RFC 3567은 IS-IS에 암호화 인증을 추가했고, 이 암호화 인증은 IPv6에서 IS-IS를 보호하기 위해 계속 사용될 것이다.

2.2.8 Viruses and Worms

바이러스와 웜은 오늘 날의 IP 네트워킹에 있어 가장 눈에 띄는 문제로 남아있다.

전통적인 바이러스는 IPv6에서 변한 것이 없다. E-mail 기반의 바이러스나 제거 가능한 미디어를 감염시키는 바이러스가 기대대로 남아있다. 그렇지만, 웜과 바이러스 그리고 취약한 호스트를 찾기 위해 인터넷을 스캔하는 몇몇 종류의 웜은 IPv6에서의 전파를 방해하는 장벽을 만날 것이다. 이러한 변화가 얼마나 의미 있고, 웜 제작자가 전파 효율을 높이기 위해 어떤 기술을 채택할 것인지에 대해서는 더 깊은 연구가 필요하다. SQL slammer-type 웜은 IPv6에서 훨씬 비효율적일 것으로 보인다. 왜냐하면, IPV6에서 감염시킬 호스트를 찾는 능력이 떨어지기 때문이다.

2.2.9 Translation, Transition, and Tunneling

IPv4가 어떻게 IPv6 네트워크로 변환될 지에 대하여 많은 생각과 주의가 기울여져 왔다. 추가적으로, IPv4에서 IPv6로의 이전 기술이 갖는 보안 의미에 대한 평가는 이미 시작되었다.

IPv6 터널링 기술과 방화벽에 관련하여, 만약 네트워크 설계자가 보안 정책을 정의함에 있어 IPv6 터널링을 고려하지 않는다면, 허가받지 않은 트래픽이 터널 내의 방화벽을 돌아다닐 수 있다. 이것은 IM(instant message)와 TCP 80 포트를 사용하는 파일 공유 어플리케이션과 비슷한 종류의 이슈이다.

이제까지 많은 변환 연구에서 행해진 바와 같이, 자동 터널링 메커니즘은 패킷 위조와 DoS 공격에 영향을 받기 쉽다. 이러한 위험은 IPv4에서도 같지만, 공격자가 자원을 착취할 수 있는 가능성을 높인다.

터널링 오버레이는 IPv6에서 6Nonbroadcast multi-access 네트워크로 고려되며, 네트워크 설계자가 이런 사실을 염두에 두고 네트워크 보안 설계를 하기를 요구한다. 네트워크 설계자는 자동 혹은 수동 터널링을 전개할 때 이러한 사실을 명심해야만 한다.

3. 결론

국내외로 실제 망 사업자(ISP)들이 현재 인터넷 주소 방식인 IPv4의 주소고갈을 목전에 두고 있음에도 불구하고 IPv6 주소방식의 도입을 미루는 이유 중의 하나는 아직 IPv6 네트워크 환경에서의 효율적인 보안 관리를 위한 보안 프레임워크가 구체적으로 정의되어 있지 않기 때문이다. 따라서 본 논문은 차후 궁극적으로 IPv4/IPv6 혼합망 및 IPv6에서의 효율적인 보안 관리를 위한 보안 프레임워크를 설계하기에 앞서 IPv4/Ipv6에서 취약성 분석 및 보안 문제를 도출하였다.

4. 참고문헌

[1] R. Atkson, "RFC-1825: Security Architecture for the Internet Protocol", Network Working Group, August 1995

[2] S. Deering, R. Hinden, "RFC-1883: Internet Protocol, Version 6 (IPv6) Specification", Network Working Group, December 1995

[3] 정보통신 및 기술 표준 동향 (TTA 저널 제 29호)

[4] IPv6 and IPv4 Threat Comparison and Practice Evaluation (v1.0), *cisco*