IPv6 네트워크 환경에서 MCGA를 고려한 통합적인 보안관리 방안

오 하 영[†] · 채 기 준[††] · 방 효 찬[†††] · 나 중 찬[††††]

요 약

32비트의 IPv4 주소고갈의 문제를 해결하고 보안과 QoS를 확실히 보장해 주기 위해 등장한 IPv6는 특성상 128비트로 증가된 주소공간과 네트워크를 효율적으로 관리하기 위한 주소체계, 이웃 탐색 및 주소 자동 설정 등 다양한 서비스 제공을 위해 노드와 라우터간의 주고받는 새로운 메시지들이 많이 추가되었다. 결과 IPv4에서 존재하던 공격은 물론 예측하지 못했던 새로운 공격들이 많이 등장하게 된다. IPv4에서 성공적으로 IPv6로 전환하기 위해 무엇보다 필요한 것은 안전하고 체계적인 보안 정책기반 아래 기존에 동작되고 있는 IPv4 호스트 및 라우터와 IPv6의 안전한 호환성이다. 따라서 관리자는 앞으로 도래 할 IPv6 네트워크 환경을 효율적으로 관리하기 위해서 다양한 측면에서 보안 문제를 도출하여 통합적인 보안 대응 방안을 설계해야 한다. 본 논문에서는 IPv4와 IPv6의 특성을 파악하고, IPv4/IPv6에서의 공격 측면에서 보안 취약성 분석 및 보안 문제를 도출하여 시스템 측면, IPv6 특성별 측면, 개선된 CGA인 MCGA (Modified Cryptographically Generated Address)의 제안을 통해 IPv6에서의 효율적인 보안 관리를 위한 통합적인 대응방안을 제시한다.

키워드 : IPv6 네트워크, 보안, CGA, MCGA

Integrated Security Management with MCGA in IPv6 Network

Hayoung Oh[†] · Kijoon Chae[††] · Hyo-Chan Bang[†††] · Jung-Chan Na[††††]

ABSTRACT

IPv6 has appeared for solving the address exhaustion of IPv4 and for guaranteeing the problems of security and QoS. It occurs the unexpected new attacks of IPv6 as well as the existing attacks of IPv4 because of the increasing address space to 128bits and the address hierarchies for efficient network management and additions of the new messages between nodes and routers like neighbor discovery and auto address configuration for the various comfortable services. For the successful transition from IPv4 to IPv6, we should get the secure compatibility between IPv4 hosts or routers working based on secure and systematic policy and IPv6. Network manager should design security technologies for efficient management in IPv4/IPv6 co-existence network and IPv6 network and security management framework designation. In this paper, we inspected the characteristics of IPv4 and IPv6, study on security requirement for efficient security management of various attacks, protocol, service in IPv4/IPv6 co-existence and IPv6 network, and finally suggest integrated solution about security vulnerability of IPv6 network in considering of analysis of IPv6 system, host and application, IPv6 characteristics, modified CGA(MCGA).

Key Words : IPv6 network, security, CGA, MCGA

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 해결하는 차세대인터넷 프로토콜이다[1,2,3,4]. 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 IPv6 네트워크 환경에서의 효율적인 보안 관리를 위한 보안 요구사항에 대한 연구가 제대로 되지 않았기 때문이다.

따라서 본 논문에서는 IPv4와 IPv6의 특성을 파악하고

※ This research was partially supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2006-C1090-0603-0028) and supported by ETRI(Electronics and Telecommunications Research Institute), Korea.

† 준 회 원 : 이화여자대학교 컴퓨터학과 석사
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
††† 정 회 원 : 한국전자통신연구원 선임연구원
†††† 정 회 원 : 한국전자통신연구원 능동보안기술연구팀 팀장
논문접수 : 2006년 5월 30일, 심사완료 : 2006년 11월 6일

IPv4에서 등장했던 공격들 분석 및 해결책 제안은 물론 IPv4에서 IPv6로 변환하면서 새롭게 등장할 수 있는 다양한 공격들 측면에서의 보안 문제를 고려하여 시스템 측면, 호스트와 어플리케이션 측면, IPv6 특성별 측면, MCGA (Modified Cryptographically Generated Address)를 통해 IPv6에서의 효율적인 보안 관리를 위한 통합적인 대응방안을 제시한다.

본 논문은 다음과 같은 순서로 구성되어 있다. 1장의 서론에 이어서 2장에서는 IPv4/IPv6 혼합망 및 IPv6에서의 보안 취약성 분석 및 보안 문제를 도출한다. 3장에서는 IPv6에서의 효율적인 보안 관리를 위한 통합적인 대응방안을 제시하고 4장에서는 분석과 성능평가 결과를 제시하며 5장에선 본 논문의 결론과 향후 연구 방안에 대하여 기술한다.

2. IPv4/IPv6 혼합망 및 IPv6에서의 보안 취약성 분석 및 보안 문제 도출

2.1 IPv4/IPv6 혼합망에서 발생할 수 있는 공격 측면에서의 보안 취약성

2.1.1 IPv4/IPv6 혼합망에서 유사한 공격 위협

IPv6 네트워크는 의무화된 IPSec을 통해 인증과 기밀성을 제공받을 수 있다. 하지만 IPSec은 키 관리 및 구성의 문제점과 어려움이 있기 때문에 아직 현실화되기 어렵다. 따라서 IPSec이 없다면 IPv4에서 나타난 스니핑 공격(Sniffing), 응용 계층 공격(Application Layer attack), 인증되지 않은 임의의 디바이스 공격(Rogue Devices), 중간 공격(Man-in-the-middle attack), 플러딩 공격(Flooding) 위협은 IPv6에서 그대로 존재 할 수밖에 없다.

2.1.2 IPv6에서 새롭게 등장한 공격 위협[5,6,7]

가. 사전답사 공격(Reconnaissance)

사전답사 공격은 공격자에 의해 실행되는 첫 번째 공격으로 이 공격은 스캐닝과 같은 액티브 네트워크 방식과 검색엔진 또는 공공 문서를 통한 소극적인 데이터 수집 방식 양쪽을 모두 포함한다. IPv4, IPv6에서 공격자 및 방어자 입장을 고려한 사전답사 공격의 특징은 <표 1>와 같다.

나. 허가 받지 않은 접근 공격(Unauthorized Access)

허가 받지 않은 접근 공격이란, IPv4로부터 상속받은 투명 전송 정책(open transport policy)을 이용하는 공격들의 집합을 일컫는다. IP 프로토콜 스택에서, 어떤 호스트가 네트워크상의 다른 호스트에 연결을 설정하는 것을 막을 수 있는 방법은 없기 때문에 공격자는 인터네트워킹 디바이스, 종단 호스트의 상위 계층 프로토콜, 어플리케이션에 연결을 설정하여 허가 받지 않은 접근 공격을 할 수 있다. IPv4, IPv6에서 공격자 및 방어자 입장을 고려한 허가 받지 않은 접근 공격의 특징은 <표 2>과 같다.

다. 헤더 조작 및 단편화 공격(Header Manipulation and Fragmentation)

단편화나 헤더 조작은 공격자가 네트워크 침입 탐지 시스템이나 방화벽과 같은 네트워크 보안 디바이스의 정책을 피해가거나 네트워킹 구조를 직접적으로 공격하기 위해 사용될 수 있다. IPv4, IPv6에서 공격자 및 방어자 입장을 고려한 단편화나 헤더 조작 공격의 특징은 <표 3>과 같다.

라. 3, 4 계층에서의 스푸핑 공격 (Spoofing)

스푸핑 공격은 IP 주소를 수정하고, 다른 장소나 응용 프로그램으로부터 보내진 조작된 트래픽을 나타내기 위해 통신하고 있는 포트 주소를 수정하는 공격이다. IPv4, IPv6에서 공격자 및 방어자 입장을 고려한 3, 4계층 스푸핑 공격의 특징은 <표 4>와 같다.

〈표 1〉 사전답사 공격 위협

공격 종류	IPv4	IPv6			
	해결책	변화 요소	공격	방어	원인
사전답사 공격 (IPv4) 1. 핑 스캐닝 (Ping sweeps) 2. 포트 스캔 3. 응용 층 취약성 스캔	필터 링, 공격 탐지 기법	IPv6의 확장된 주소	불리	불리	서브 넷 크기 ($2^{64}-2^{8}$) -취약한 호스트를 찾기 위한 포트 스캔 어려움 -공격자를 추적하기 어려움
		인터넷 edge위의 공공 서비스들은 DNS에 가까울 필요가 있음	유리	불리	공격자에게 민감한 호스트들의 주소를 제공될 수 있음
		동적 주소 설정 위한 사설 확장	유리	불리	1.공격자의 인터페이스 ID 변경이 용이하여 공격자 추적 및 호스트 관리가 어려움 2.DDNS의 업데이트 작업의 오버헤드 – 가용성 하락
		기억하기 쉬운 주소 이름	유리	불리	1.관리자 – 할당할 수 있는 많은 주소 공간이 있음에도 불구하고 관리상 이유로 각 노드들 기억하기 쉬운 주소 사용 2.공격자-작은 범위 주소 공간 스캔으로 다른 노드 유추
		네트워크 카드 벤더들을 위한 유명한 IEEE OUI 할당	유리	불리	1.공격자-IEEE OUI-64 주소의 고정 부분 이용하여 작은 범위 주소 공간에 대한 스캔으로 다른 노드유추 2.Ethernet 카드 제조회사의 정보를 이용하여 interface 주소범위 추측 가능
		사설확장 구현	유리	불리	추적 문제 해결을 어렵게 함
		사이트 로컬 멀티캐스트 주소의 사용	유리	불리	공격자는 네트워크상의 key systems 파악하여 공격할 수 있음(ex: all routers – FF05::2, all DHCP - FF05::3)
		통합된 ICMPv6	유리	불리	IPv6에서는 다음과 같음 몇몇의 ICMP메시지들을 허가해야함 Ex) ND ICMP, FM, packet-too-big...

〈표 2〉 허가 받지 않은 접근 공격 위협

공격 종류	IPv4	IPv6			
	해결책	변화 요소	공격	방어	원인
허가되지 않은 접근 공격 (IPv4) 1. 투명 전송 정책 활용	액세스 컨트롤 1. Layer3 : ACLs 2. Layer4	IPv6 주소 체계의 변화 및 포트 정보를 이용한 액세스 컨트롤	유리	불리	1.침입차단시스템은 액세스 컨트롤을 사용하여 인증된 호스트만 내부 네트워크로 접속할 수 있게 하지만, IPv6 노드는 다중 주소를 가짐. 2.IPsec tunneling을 이용하는 경우 IPv6 메시지가 암호화되어 전송되기에 공격자가 침입차단시스템 우회가능
		확장 헤더 (ex: 라우팅 헤더)	유리	불리	공격자는 라우팅 헤더 등의 확장 헤더를 악용하여 침입차단 시스템 보안 정책을 우회할 수 있음 (홉-홉 옵션 헤더, 라우터 알림 옵션 등을 남용)
		ICMPv6	유리	불리	IPv6에서는 IPv4와 같은 엄격한 ICMP 필터링이 불가
		멀티 캐스트 조사	유리	불리	지역-사용 멀티캐스트가 IPv6의 기능으로 통합 됨
		최적의 탐색을 위한 애니 캐스트	유리	불리	인증되지 않은 애니 캐스트 그룹멤버가 거짓 정보를 광고하거나 해당 멤버에 의해 송신자의 주소를 변경할 수 있음 (masquerading, DoS 공격가능)
		투명한 방화벽	유리	불리	IPv6의 방화벽은 IPv4와 다른 IPv6 ICMP메시지와 멀티캐스트 메시지들을 인식할 수 없음

〈표 3〉 헤더 조작 및 단편화 공격 위협

공격 종류	IPv4	IPv6			
	해결책	변화 요소	공격	방어	원인
헤더 조작 및 단편화 공격 (IPv4) * 원래 목적 1.말단 호스트들의 중간 경로상의 가장 작은 데이터 그램에 맞추기 위함 * 공격자의 악용 1.패킷을 단편화 또는 헤더를 조작하여 네트워크 침입 탐지 시스템, 방화벽을 우회함 2.직접적으로 공격	현재 방화벽 및 네트워크 침입 탐지 시스템 -조합된 패킷들을 액세스 컨트롤 규칙이나 공격 패턴에 매칭 시켜봄	중간 노드들에 의한 IPv6 단편화가 없어짐	불리	유리	많은 파편화는 공격자의 공격을 유리하게 만들고 결국 액세스 컨트롤의 규칙을 우회할 가능성을 제시
		중복되는 단편화	유리	불리	공격자 패킷 중복되는 단편화를 침입차단시스템이 필터링 못해 목적지까지 전송되면 목적지는 재조합 시 어떤 패킷이 올바른지 알 수 없어 시스템 교착상태,홀동 발생:시스템 재시동
		IPv6의 최소 MTU (maximum translation unit)는 1280 octets (RFC 2460)	불리	유리	큰 데이터를 작은 단편화 패킷들로 보냄으로써 공격을 막음
		다수 확장 헤더들과 단편화 헤더들의 조합	유리	불리	IPv6기본 헤더 뒤에 따라오는 수 많은 확장 헤더들과 단편화 헤더들로 인해 4계층 프로토콜(TCP, UDP)이 첫 번째에 들어 있지 않기에 문제 발생 가능
					즉, 기존의 4계층 프로토콜 기반 정책을 적용시키기 어려움

〈표 4〉 3, 4 계층에서의 스푸핑 공격 위협

공격 종류	IPv4	IPv6			
	해결책	변화 요소	공격	방어	원인
3, 4계층에서의 스푸핑 공격 * 목적 공격자는 소스 IP주소와 포트들을 수정	진입 필터링 (ingress filtering), 표준의 ACLs	IPv6 3계층 스푸핑	유리	유리	포괄적으로 묶어서 할당할 수 있는 IPv6의 주소 체계 (Globally aggregated nature of IPv6 addresses)를 활용하여 네트워크에서 외부 포인트 구분이 쉬움
		IPv6 4계층 스푸핑	유리	불리	IPv6에서는 관리해야 하는 subnet의 크기가 매우 큼
					진입 필터링을 사용한다고 할 지라도 IPv6주소 체계 성격상 공격자에게 스푸핑 공격을 할 수 있는 기회가 굉장히 커짐
		다양한 터널링 메커니즘	유리	불리	터널링이 시행되는 동안 공격자는 IPv4또는 IPv6의 연결성을 이용하여 다른 IP 버전으로 트래픽을 보내 공격할 수 있음

마. 주소 결정 프로토콜(ARP)과 동적 호스트 설정 프로토콜(DHCP) 공격

주소 결정 프로토콜(ARP-Address Resolution Protocol)과 동적 호스트 설정 프로토콜(DHCP-Dynamic Host Configuration Protocol) 공격은 호스트의 초기화 프로세스나 호스트가 전송을 위해 접근하는 디바이스를 파괴하려는 공격이다. IPv4, IPv6에서 공격자 및 방어자 입장을 고려한 ARP and DHCP 공격의 특징은 <표 5>과 같다.

바. 브로드캐스트 증폭 공격(Broadcast Amplification Attacks - Smurf)

브로드캐스트 증폭 공격은 공격자가 소스의 주소를 희생자의 주소로, 서브 넷의 브로드캐스트 주소를 목적지로 에코-요청 메시지를 보내서, 서브 넷 상의 모든 종단 호스트들은 스푸핑 된 희생자의 주소로 에코-응답메시지로 응답을 보내기 때문에 결국 희생자는 에코-리플라이 메시지로 인해 넘치게 되는 서비스 거부 공격(DoS : Denial of Service) 공

〈표 5〉 ARP, DHCP 공격 위협

Threat Analysis	IPv4	IPv6			
	해결책	변화 요소	공격	방어	원인
ARP and DHCP Attacks * 목적 호스트들이 허가 받지 않거나 공격에 노출된 디바이스와 통신하게 하거나 (예: 공격자의 MAC) 잘못된 네트워크 정보로 구성되게 하는 것	ARP, DHCP에 답변은 인증된 포트만 가능하도록 함,침입차단 시스템	주소 자동 설정 가능 (Autoconfiguration)	불리	유리	DHCP 기능은 주소 자동 설정 기능으로 거의 대체됨
		이웃 탐색 (ND - Neighbor Discovery)	불리	유리	무분별하게 IPv4의 Broadcast로 주고 받는 ARP의 기능을 없애고 IPv6에서는 이웃탐색(ND)시 수신자를 제약하는 multicast로 대체
		주소 자동 설정 메시지 스푸핑	유리	불리	공격자는 IPv6 주소 자동 설정 기능을 악용하여 정상적인 주소 할당을 방해하거나 정상적인 세션을 종료할 수 있음
		이웃 탐색 메시지 스푸핑	유리	불리	이웃 탐색 시 공격자는 디바이스 간 서로 주고 받는 다양한 간청 및 광고 메시지들이 스푸핑 해 디바이스의 이웃탐색 캐쉬 정보를 업데이트 할 수 있음

〈표 6〉 브로드캐스트 증폭 공격 위협

Threat Analysis	IPv4	IPv6			
	해결책	변화 요소	공격	방어	원인
Broadcast Amplification Attacks (smurf)	브로드캐스트 공격이 가능한 서브넷 모니터링	ICMPv6	유리	불리	IPv4에서는 에러보고의 기능에 국한되던 ICMPv4는 IPv6에서는 에러보고는 물론 이웃 탐색, 그룹관리 등 IPv4의 IGMP, ARP, ICMPv4등 많은 기능을 포함하기 때문에 공격자는 이를 악용할 확률이 더 높아짐. 특히 에러보고 메시지 중 하나인 'packet Too Big', 'Parameter Problem' 응답 메시지 등 필터링이 불가능한 ICMPv6 메시지들은 침입차단 시스템이나 액세스 컨트롤의 보안 규칙에서도 허용되기 때문에 서비스 거부(DoS) 공격에 매우 취약
					공격자는 디바이스와 라우터 간의 주고 받는 다양한 간청, 광고(NS, NA, RS, RA) 메시지들을 악용하여 라우터 정보를 수집할 수 있음

격이다. IPv4, IPv6에서 공격자 및 방어자 입장을 고려한 브로드캐스트 증폭 공격의 특징은 <표 6>과 같다[8,9].

사. 라우팅 공격

라우팅 공격은 네트워크의 트래픽을 방해하거나 방향 재설정에 초점을 맞춘다. 공격은 다양한 방식으로 실행되는데, 플러딩 공격, 공격자의 잘못된 경로 재설정 언급, 디폴트 라우터의 메시지 제거 등의 방식을 이용할 수 있으며 공격의 상세한 부분은 사용되는 프로토콜에 따라 다르다.

아. 바이러스와 웜

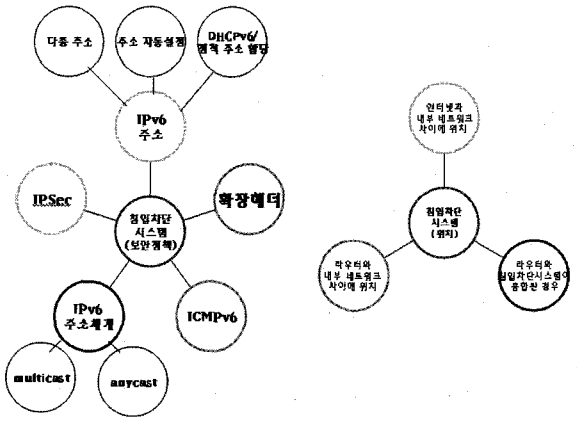
바이러스와 웜은 오늘 날의 IP 네트워킹에 있어 가장 눈에 띄는 공격으로 IPv6의 IPSec이 필수가 되어 보안기능을 제공해준다고 하더라도 완벽히 해결될 수 없는 응용 계층 공격 중 하나다.

3. IPv6에서의 효율적인 보안 관리를 위한 통합적인 대응방안

IPv6는 IPv4에 비해 많은 편리한 서비스를 제공해주지만 2장에서 살펴보았듯이 노드와 라우터간의 주고받는 새로운 추가 메시지가 많아지고 IPv4에선 없었던 새롭고 다양한 공격들에 노출되기 쉽다. 따라서 관리자는 시스템 측면과 IPv6 프로토콜 자체의 특성을 활용한 보안 대응방안을 고려하면서 그것만으로 해결되지 않는 부분은 동시에 데이터의 인증과 무결성 및 기밀성까지 제공해주는 MCGA를 사용하여 더욱 강력한 보안을 제공해 통합적인 관리를 해주어야한다.

3.1 시스템 측면에서의 대응방안

시스템측면에서의 대응방안은 다음 (그림 1)와 같다.



(그림 1) 시스템 측면에서의 대응 방안

3.1.1 침입차단시스템을 이용한 대응방안

침입차단시스템은 각 네트워크에 1개 이상이 설치되며 네트워크 경계에 위치하여 외부의 보안 취약성들로부터 내부의 사설망을 보호하는 보안 정책을 적용하는 시스템이다. 이것은 네트워크 계층의 패킷 필터링 침입차단시스템을 비롯해 전송계층의 서킷 지향적 침입차단시스템, 응용계층의 응용 레벨 프록시 등 여러 계층에서 동작할 수 있으며, 서로 다른 계층에서 혼합하여 운용할 수도 있다. IPv6 침입차단시스템은 IPv4와 기술적으로는 동일하나 IPv6가 되면서 바뀐 주소 표현방식이나 ICMP 메시지, 멀티캐스트 메시지

를 조사 및 추적하기 위해 능력을 강화해야하며 이웃발견 기능, 복제주소 탐색 기능, 주소 자동설정기능 등을 잘 고려해서 보안 정책을 수정 보완해야한다. 또한 확장 헤더를 다룰 때 침입차단시스템에서 어떤 확장 헤더를 허락할 것인지 결정해야 하고 IPv6정책을 IPv4 IP 옵션 정책과 비교 시 종단 호스트 운영체제의 행동도 고려해야한다. 또한 IPv6 서브넷에 존재하는 넓은 범위의 스푸핑 가능한 IP 주소와 함께, 공격이 일어날 때 트래픽의 MAC 소스를 결정하는 메커니즘을 갖기 위해 마지막 홉 역추적을 위한 과정을 문서로 남기고 그 결과 스푸핑 된 IP-to-MAC 주소 결합이나 스푸핑 된 DHCP 메시지 등과 같은 공격을 완화해야한다.

가. 침입차단시스템 보안 정책 설정을 통한 보안 대응방안

(1) IPv6의 주소

a) **다중 주소** : IPv6 호스트는 하나의 인터페이스에 다중 주소가 허용되므로 단일 주소만을 고려하여 만들어진 기존 침입차단시스템의 접근제어 기능은 수정되어야 한다. IPv6 침입차단시스템에서는 글로벌 주소는 허용하고 링크 로컬주소에 대해서는 외부로 나가는 것과 외부에서의 접근을 막아야한다.

b) **비상태형 주소자동설정**(stateless address auto-configuration) : 글로벌 유니캐스트 주소는 라우터가 광고한 프리픽스정보와 IEEE EUI-64 형식의 식별자를 이용하여 설정되고 EUI-64 식별자는 MAC 주소로부터 유도될 수 있기 때문에 IP 주소와 MAC 주소의 맵 핑이 용이하다. 이때, 침입차단시스템은 MAC 주소와 2계층 포트간의 매핑을 지원할 수 있어야한다. 침입차단시스템에서는 이미 내부 네트워크에서 외부 네트워크로 전송되는 패킷들의 MAC 주소와 EUI 주소의 지속성을 체크할 수 있으나 정적으로 할당되는 주소들을 사용하는 경우에는 주소정보가 수동적으로 설정되어 있어야한다.

c) **DHCPv6** : DHCPv6 는 상태정보를 유지하는 주소자동설정 프로토콜이다. DHCPv6 서버들은 설정 파라미터들에 대한 클라이언트들과 IA(Identity association) 클라이언트들과 관련된 클라이언트를 식별하기 위해 DUID(DHCP Unique Identifier)를 사용한다. DHCP 클라이언트는 서버를 식별할 필요가 있는 메시지에서의 서버를 식별하기 위해 DUID를 사용한다. 따라서 침입차단시스템은 DHCPv6를 사용하여 DUID를 설정한 내부 호스트만이 외부 네트워크의 호스트와 연결이 가능하도록 해야 한다.

또한 정적 주소 할당은 IPv4의 정적 주소할당기법과 매우 유사하므로 이를 사용할 경우 IPv4에서의 보안 취약성과 유사하다. DHCPv6를 사용하여 주소를 할당하는 경우, 침입차단시스템은 DHCPv6를 모니터링 하여 주소의 오남용을 방지해야 한다. 또한 비 상태 주소자동설정의 경우, 주소 및 포트의 오남용을 방지하기 위해 [소스 IPv6 주소, 소스 MAC 주소]를 가지고 있는 이웃 간청 메시지(NS), [(소스 IPv6 주소, 소스 MAC 주소), (목적지 IPv6 주소, 목적지 MAC 주소)]를 가지고 있는 이웃 광고메시지를 모니터링 해야 한다. 침입차단시스템은 위의 두 메시지를 모니터링 하여 만약 두 메시지의 정보가 일치되지 않는 경우에는 이전의 저장된 이웃 탐색 엔트리를 분석하여 스위치의 포트 남용을 방지할 수 있다. 즉 침입차단시스템은 같은 MAC 주소를 가진 다른 IP주소의 이웃 탐색 엔트리의 변화를 감지해야한다.

(2) IPv6의 주소체계

a) **멀티캐스트 주소**(multicast address) : 공격자는 모든 라우터를 나타내는 주소(FF05::2)와 모든 DHCP 서버를 나타내는 주소(FF05::3)를 목적지 주소로 사용하여 플러딩 공격을 하거나, IPv6의 사이트 범위를 갖는 멀티캐스트 주소를 이용하여 공격할 라우터에 대한 스캔 작업 없이 모든 라우터에 대한 서비스 거부 공격을 할 수 있다. 따라서 침입차단시스템은 외부로부터 멀티캐스트 주소에 접근할 수 없도록 네트워크 경계 지역에 위치하여 필터링해야하며 스캔을 포함한 공격의 위험을 경감시키기 위해 경계 라우터에서 내부 IPv6주소를 필터링해야하고 주요 시스템에는 추측이 어려운 IPv6주소를 할당해야한다. 또한 침입차단시스템은 이웃탐색 및 주소자동설정의 원활한 기능을 위해 최소한의 링크 로컬 멀티캐스트(예 : FF02::/10) 트래픽만 허용해야 한다. 특별히 브로드캐스트 증폭 공격에 대하여 RFC 2463[10]에서 말했듯이 서비스 거부 공격을 막기 위해 ICMPv6 메시지가 IPv6 멀티캐스트 목적지 주소나 링크 계층 멀티캐스트 주소 또는 링크 계층 브로드캐스트 주소를 가진 패킷에 대한 응답으로 생성되어선 안 된다.

b) **애니캐스트 주소**(anycast address) : 인증되지 않은 애니캐스트 그룹 멤버는 거짓 정보를 광고하거나 해당 멤버에 의해 송신자의 주소를 변경할 수 있는 보안취약성으로 위장공격 및 서비스 거부 공격이 가능하기에 침입차단시스템은 허용이 안 된 애니캐스트 요청은 필터링해야한다.

(3) IPSec (IP Security)

IPSec 터널링을 이용하는 경우 내부 IPv6 메시지가 암호화되어 전송되기 때문에 침입차단시스템에서는 패킷의 접근제어를 할 수 없어 공격자는 침입차단시스템을 우회할 수 있다. 따라서 암호화된 패킷을 복호화 할 수 있는 분산 형 침입차단 시스템의 사용과 인증 및 무결성 만 제공해주는 AH(Authentication Header)만 적용한 암호화 패킷은 침입차단시스템이 상위 계층의 정보를 기초로 패킷에 대한 접근제어를 하도록 하기 때문에 권장된다.

(4) ICMPv6

ICMPv6는 IPv4에서보다 더 IPv6 작동의 필수적인 부분으로 많은 기능을 제공해 주지만 공격자에게 공격의 기회를 더 주는 것이 사실이다. 따라서 현재 ICMP 필터링에 대한 최고 방안은 계속해서 논쟁 중이며 엄격한 ICMP 필터링이 최고 대안이라는 의견이 일반적으로 받아들여지고 있다. 그러나 이런 전면적인 거부는 IPv6에서 네트워크의 마비를 일으킬 수 있기 때문에 는 불가능하다. 따라서 IPv6에서 ICMPv6에 대한 침입차단시스템의 보안 정책은 ICMPv4에서의 보안정책은 물론 ICMPv4에서의 보안정책에서는 없었던 특징도 반영해야하므로 ICMPv4 정책이 ICMPv6로 어떻게 변환되었는지 비교, 대조하는 것이 중요하다.

(5) 확장 헤더

a) **단편화 헤더** : IPv4 침입차단시스템은 단편화된 패킷을 teardrop 공격 등으로부터 보호하기 위해 IP 패킷을 재조립하고 단말 시스템에게 완전한 정상적인 패킷을 전달했다. 하지만, IPv6에서는 패킷의 단편화 및 재조립이 단말 시스템에서만 가능하기 때문에 IPv6 침입차단시스템은 단편화된 패킷이 정상인지 비정상인지 알 수 없고 재조립할 수도 없다. 따라서 관리자는 IPv6 침입차단시스템이 정상적인 단편화 헤더를 가진 외부 패킷을 필터링하지 않도록 주의하여 설정하고 단편화된 패킷을 재조립하여 필터링을 적용할 수 있어야 한다. 특히 IPv6는 다양한 확장헤더와 단편화의 조합으로 4계층 프로토콜이 첫 번째 패킷에 포함되지 않을 수도 있기에 4계층 프로토콜을 기반으로 보안 정책을 가진 침입차단시스템은 파편을 재조립해야한다. 또한 서비스 공격인지 판별하기 위해 유일한 식별자로부터 온 파편의 숫자에 대한 조사 및 공격자가 파편의 흐름을 생성하는 경우 이를 탐지하기위해 소스 서브 넷 매칭을 포함해야한다. 서비스 공격 및 우회 공격을 막기 위해 플로우의 마지막 패킷을 제외하고 1280 octet이하의 모든 파편은 버려야한다.

b) **라우팅 헤더** : 공격자 A는 라우팅 헤더를 이용해 먼저 접근 가능한 내부 서버 B를 경유해 접근할 수 없었던 내부 서버 C를 공격할 수 있다. 즉 공격자는 라우팅 헤더를 이용하여 라우팅 헤더목적지 주소 기반의 접근 제어를 하는 침입차단시스템의 필터링을 우회할 수 있기 때문에 IPv6 침입차단 시스템은 type 필드 값이 0인 라우팅 헤더를 갖는 패킷은 차단하도록 필터링 규칙을 설정하고 최종 목적지 주소와 라우팅 헤더의 주소 필드 값을 비교할 수 있는 필터링 규칙을 설정해야 한다. 또한 종단 호스트는 수신된 패킷의 라우팅 헤더에 포함된 최종 목적지 주소가 자신의 주소가 아닌 경우에는 패킷을 폐기해야한다.

c) **인식하지 못하는 헤더**(Unknown Header)/**목적지 옵션 헤더**(Destination option header) : RFC 2460[10]에서는 목적지 옵션 (Destination Option)을 가진 패킷을 목적지에서만 처리되도록 하고 있으나, 강력한 보안 정책은 인식하지 못하는 헤더들 또는 목적지 옵션들을 갖는 패킷들을 침입차단시스템이나 필터링에 의해 폐기되게 한다. 침입차단 시스템은 모든 확장 헤더 체인을 처리하며 인식하지 못하는 헤더를 갖는 패킷을 폐기하기 때문에 정상 헤더임에도 불구하고 침입차단시스템이 인식하지 못해서 폐기되는 것을 방지하는 보안 정책이 필요하다.

나. 침입차단시스템의 위치에 따른 대응방안

(1) 침입차단 시스템이 라우터와 내부 네트워크 사이에 위치

침입차단시스템이 라우터와 내부 네트워크 사이에 위치해 있기 때문에 IPv6의 특징인 주소자동설정이 사용된다면 침입차단시스템은 네트워크 계층에 투명하게 운영되어 호스트로부터의 라우터 간청메시지와 그에 대응하는 라우터로부터의 내부 네트워크로의 라우터 광고응답메시지를 차단해서는 안 된다. 만약 침입차단시스템이 라우터와 내부 호스트간의 교환되는 메시지를 필터링한다면, 침입차단시스템 자신이 라우터 광고메시지들에 응답할 수 있어야하고 주기적으로 라우터 광고메시지를 내부 호스트들에게 전송해야 한다. 내부 네트워크가 DHCPv6를 운영하고 있다면 이러한 설정은 매우 중요하다. 또한 내부 네트워크 내의 IPv6 멀티캐스트 그룹에 참가하고 있는 멤버가 존재한다면 침입차단시스템은 MLD (Multicast Listener Discovery)프로토콜을 지원해야 한다.

(2) 침입차단 시스템이 인터넷과 내부 네트워크 사이에 위치

침입차단시스템이 인터넷과 내부 네트워크 사이에 위치해 있기 때문에 침입차단시스템은 라우터에서 사용되는 동적 라우팅 프로토콜에 대한 필터링 기능을 지원해야한다. 그러나 IPSec이 사용될 때에는 BGP가 보안 라우팅 업데이트를 위해 MD5 Hash를 사용하기 때문에 정적인 라우팅 기법을 사용해야한다.

(3) 라우터와 침입차단시스템이 통합된 경우

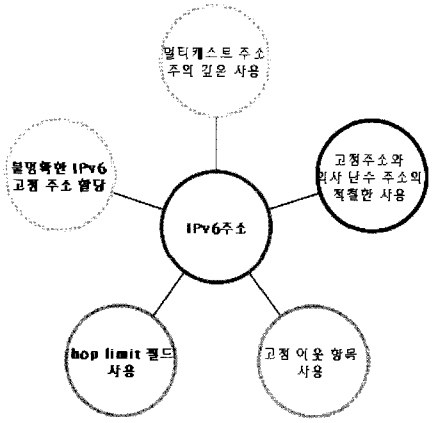
라우터와 침입차단시스템이 통합된 경우는 좀 더 복잡하고 더 많은 보안문제에 직면할 수 있다. 이러한 설정은 작은 사무실의 환경에서 사용되는 구조로 위의 (1)과 (2)의 고려사항을 모두 만족해야한다.

3.1.2 호스트와 어플리케이션에 대한 보안 유지를 통한 대응방안

호스트와 어플리케이션에 대한 보안을 유지해야한다. 적절한 시기에 패치를 하고 호스트를 잠그는 것이 IPv4에서 중요했더라도, IPv6의 초기에 이것들은 더욱 중요한 의미를 갖는다. 왜냐하면 많은 호스트 침입탐지 시스템이 IPv6에서 아직 널리 지원되지 않기 때문이다. 추가적으로, IPv6의 초기 도입 시기에는 몇몇 호스트가 적절하게 보안되지 않을 가능성이 높다. 따라서 위태로운 호스트가 다른 종단 호스트마저 위태롭게 하지 않도록 호스트 보안 유지에 초점을 맞춰야 한다.

3.2 IPv6 특성 별 대응방안

IPv6 특성 측면에서의 대응방안은 (그림 2)과 같다.



(그림 2) IPv6특성 측면에서 대응방안

3.2.1 불명확한 IPv6 고정 주소 할당에 따른 대응방안

관리자는 관리상의 이유로 시스템에 (::10, ::20, F00D)와 같은 기억하기 쉬운 호스트 주소를 할당하기 쉽다. 하지만 공격자는 이를 악용하여 공격할 희생자 네트워크의 취약성을 쉽게 파악하고 정보를 스캐닝 툴의 데이터베이스에 넣을 수 있기 때문에 관리자는 표준에 따르되 중요한 시스템에 대해서는 자신만 알고 공격자는 추적하기 힘든 불명확한 고정 주소를 사용해야한다.

3.2.2 멀티캐스트 주소의 주의 깊은 사용에 따른 대응방안

IPv6는 공격자로 하여금 네트워크의 핵심 자원을 식별하고 그것을 공격할 수 있게 하는 멀티캐스트 주소를 지원한다. 이러한 주소들은 사용에 있어 노드 영역의 주소, 링크 영역의 주소, 사이트 영역의 주소를 갖는다. 예를 들어, 모든 라우터(FF05::2)와 모든 DHCP 서버들 (FF05::3)은 사이트-특정 주소를 갖는다. 이러한 셋업이 합법적인 사용이더라도, 이것은 간단한 플러딩 공격이나 다른 어떤 것에 의해 공격자에게 시스템의 공적인 리스트를 넘겨준다. 그러므로 내부 네트워크에서 주의 깊게 사용하고 네트워크 경계에서 필터링하며 바깥으로부터 도달 불가능하게 만들어야한다.

3.2.3 고정주소와 의사난수 주소의 적절한 사용에 따른 대응방안

고정주소의 공격 취약성을 극복하기 위한 의사난수 주소를 사용한 프라이버시 확장이 이점이라 하더라도, 프라이버시 확장은 또한 관리자가 문제 추적을 하거나 네트워크를 관리하는데 해결을 어렵게 한다. 따라서 프라이버시 확장을 주의 깊게 구현해야한다. 만약 네트워크가 잘못된 행동을 하는 호스트를 갖고 있고 호스트의 주소를 주기적으로 변화시킨다면, 호스트를 정확히 추적하는 것 또는 문제가 한 호스트에서 발생했는지 여러 호스트로부터 발생했는지 결정하는 것은 매우 어렵다. 따라서 내부 네트워크에서는 관리자만이 알 수 있는 MAC 주소 기반의 고정 주소를 사용하고, 인터넷으로 향하는 트래픽을 위해 의사난수 주소를 사용해야한다.

3.2.4 고정 이웃 항목 (static neighbor entry) 사용에 따른 대응방안

이웃탐색 기능에는 이웃 탐색 메시지의 남용을 탐색하는 기능이나, 메시지의 전송을 보호하기 위한 기능 없기에, 최고 실행 후보로 중요한 시스템에 대해 고정 이웃 항목을 사용해야한다. 매우 민감한 환경에서, 시스템이 디폴트 라우터를 위해 고정 항목을 가지고 있으면 공격자로부터 많은 전형적인 이웃 탐색 공격을 피할 수 있다.

3.2.5 hop limit 필드 사용에 따른 대응방안

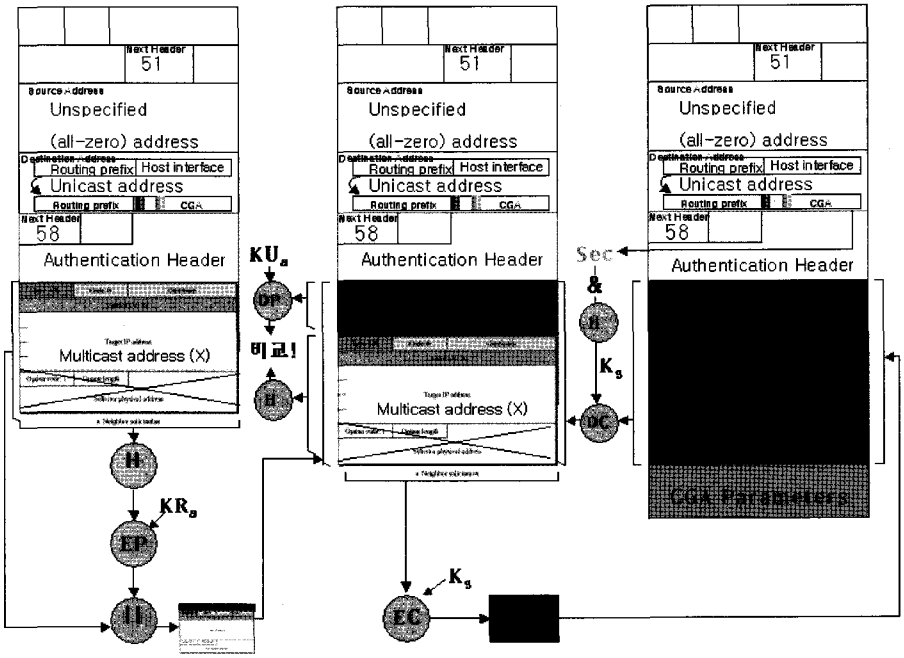
공격으로부터 네트워크 디바이스의 프로토콜 스택을 보호하기 위하여 hop limit을 사용해야한다. 예를 들어, 기본적인 기술은 올바른 동일 계층 간의 hop limit값은 255이다. hop limit값은 라우터를 거치면서 감소하기 때문에 적절한 hop limit의 사용으로 다른 네트워크 구조에서로부터 오는 스푸핑 된 패킷을 막을 수 있어야 한다.

3.3 개선된 CGA(MCGA)를 통한 대응방안

IPv6의 128비트는 라우터의 프리픽스 64비트와 노드의 MAC주소를 기반으로 만들어지는 인터페이스 64비트로 이루어진다. CGA는 궁극적으로 IPv6의 128비트의 주소 중 인터페이스 64비트를 암호화해서 안전한 통신을 제공하는 것이다. 하지만 IETF의 SEND(Securing Neighbor Discovery) 워킹 그룹에서 제안한 기존 CGA[11]는 공개키를 이용한 전자서명을 통해 인증(authentication)은 제공해주지만 메시지의 기밀성(confidentiality)을 보장하지 못하고 재전송 공격(replay attack) 및 DDoS와 같은 폭발공격을 막지 못한다. 따라서 (그림 3)과 같은 MCGA를 생성을 통해 호스트는 안전한 이웃탐색 서비스 및 비 상태 주소 자동생성 서비스 등을 위해 IPv6 기본헤더 뒤에 붙는 ICMPv6 메시지에 기밀성을 제공하고. 재전송 공격 및 분산 서비스 공격, IP-MAC Binding 공격과 같은 폭발 공격을 막을 수 있다. 이것은 (그림 4)과 같은 한층 발전된 동적인 Sec과 Mask값을 이용하여 송신자는 대칭 키(symmetric key)를 만들어 ICMPv6메시지를 암호화하고 주소 소유자의 공개 암호키의 암호를 이용한 해쉬 함수 계산 시 송신자의 MAC address값과 TimeStamp 값을 추가하여 IPv6주소의 인터페이스를 생성하여 수신자에게 전달하기 때문이다.

가. MCGA 주소 생성

MCGA를 생성하는 데는 64비트의 라우터의 서브넷 프리픽스(subnet prefix), 랜덤 수인 modifier, 주소 소유자의 public key, Collision Count, MAC address, TimeStamp, 폭발공격을 막기 위한 동적인 Mask Num와 security parameter



(그림 3) MCGA의 원리

(Sec) 이렇게 8가지의 값을 고려한다. 한층 강화된 공격을 막기 위해 먼저 선택된 Mask 값에 해당하는 길이의 해쉬 함수 값을 구한 뒤 그 Mask 값과 Sec 값을 고려한 규칙을 만족시키는 modifier를 구하고 궁극적으로 IPv6 주소의 128 비트 중 64비트의 해쉬 결과인 인터페이스를 구한다. MCGA 주소를 생성하는 절차는 다음과 같다.

(1) 먼저, (그림 4)에서 Sec 값과 Mask 값을 선택 및 subnet prefix를 확인한다.

Sec = 1,2,3,4, Mask = 1,2,3,4,5, subnet prefix = fe80::

(2) 128 비트 값을 가지는 modifier를 만든다.

Modifier:

89a8 a8b2 e858 d8b8 f263 3f44 d2d4 ce9a

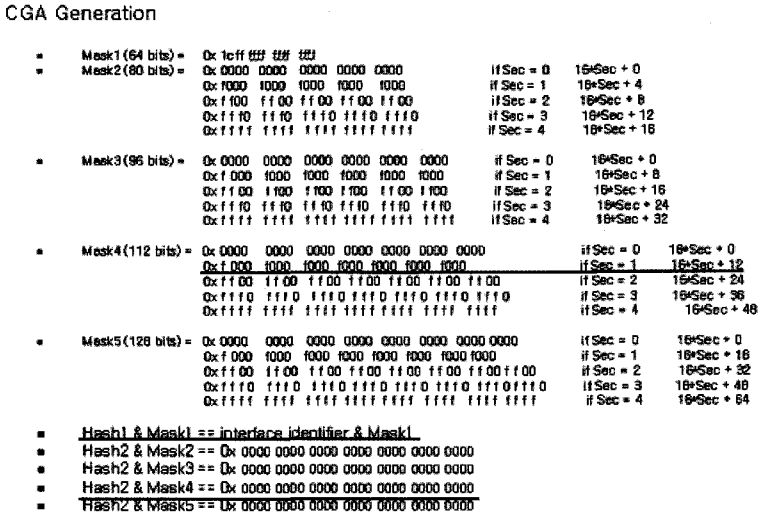
(3) 앞에서 만들어진 modifier 값을 오른쪽에 왼쪽으로 입력하고 주소 소유자의 public key와 함께 연결한다.

Modifier:

89a8 a8b2 e858 d8b8 f263 3f44 d2d4 ce9a

Public key:

305c 300d 0609 2a86 4886 f70d 0101 0105 0003 4b00 3048 0241
00c2 c2f1 3730 ·····
·····0001



(그림 4) Sec값과 Mask값 의 형식

결과 Modifier, Public key의 연결 값인 Hash2 함수의 입력 값은 다음과 같다.

89a8 a8b2 e858 d8b8 f263 3f44 d2d4 ce9a 0000 0000 0000 0000 00
305c 300d 0609 2a86 4886 f70d 0101 0105 0003 4b00 3048 0241
00c2 c2f1 3730 ·····
·····0001

(4) Mask 값을 4로 선택했기 때문에 modifier, public key를 입력 값으로 하여 $Hash_{112}$를 수행한다. 또한 Sec값을 1로 선택했기 때문에 (그림 4)에서 밑줄 그어진 다음을 만족 시켜야한다.

Mask1 (64 bits) = 0x 1cff ffff ffff ffff
Mask4 (112 bits) = 0x f000 f000 f000 f000 f000 f000 f000 if Sec=1, 16*Sec + 12

Hash1 & Mask1 == interface identifier & Mask1
Hash2 & Mask4 == 0x 0000 0000 0000 0000 0000 0000 0000

Hash2 = 436b 9a70 dbfd dbf1 926e 6e66 29c0 = $Hash_{112}$ (modifier, public key) -> 16*Sec +12 = 28 가 0로 시작되지 않음

(5) 위에서 생성된 Hash2의 값(Hash2 = 436b 9a70 dbfd dbf1 926e 6e66 29c0 = $Hash_{112}$ (modifier, public key)) 중 밑줄 친 16*Sec 값만큼의 가장 왼쪽의 값과 16*Sec 값에 해당하는 Mask값을 비교하여 모두 0이 되면 다음 단계를 수행하고, 0값이 안 나오면 modifier값을 증가시킨 후 다음 단계를 진행한다. 위 (4)의 결과는 Sec 값이 1이고 Mask 값이 4일 때 16*Sec +12 값이 0이 안 나온 경우이다. 따라서 modifier 값을 하나 증가시킨 후 다음 단계를 진행한다.

Modifier:
89a8 a8b2 e858 d8b8 f263 3f44 d2d4 ce9b
-> (3)에서 a로 끝났던 Modifier가 1증가하여 b로 끝남을 알 수 있음

Hash2 = 0fst 01ca 080b 0388 0d09 02df 0suq= $Hash_{112}$ (modifier, public key)
-> 16*Sec +12 = 28 가 0로 시작됨, 따라서 이 modifier가 선택됨

(6) 앞에서 만들어진 modifier 값과 subnet prefix 값을 오른쪽에 왼쪽으로 입력하고 public key와 함께 연결한다. Hash1을 구할 때는 subnet prefix도 고려한다.

Modifier:
89a8 a8b2 e858 d8b8 f263 3f44 d2d4 ce9a

Public key:
305c 300d 0609 2a86 4886 f70d 0101 0105 0003 4b00 3048 0241
00c2 c2f1 3730 ·····
·····0001

Subnet prefix:
fe80

결과 다음과 같다.
89a8 a8b2 e858 d8b8 f263 3f44 d2d4 ce9a fe80 0000 0000 0000 00
305c 300d 0609 2a86 4886 f70d 0101 0105 0003 4b00 3048 0241
00c2 c2f1 3730 ·····
·····0001

(7) 앞의 과정이 수행된 후 비 상태 주소 자동 설정 시 주소 중복 탐색 과정 중 주소 충돌 시 필요한 Collision Count를 0으로 세팅한다.

(8) subnet prefix, modifier, public key, Collision Count, MAC address, TimeStamp, Mask Num 값을 SHA-1 Hash함수의 입력 값으로 넣고 암호화를 수행한다. 이렇게 생성된 값 중 가장 왼쪽의 값인 64비트를 Hash1 값으로 한다.

Hash1 = fd4a 5bf6 ffb4 ca6c = $Hash_{64}$ (subnet prefix, modifier, public key, Collision Count, MAC address, TimeStamp, Mask Num)

(9) 앞에서 생성된 Hash1의 값 가운데 첫 번째에서 세 번째 비트까지는 security parameter (Sec)의 값을 넣고, 가운데 'u'와 'g'의 비트를 넣어 최종 인터페이스 ID를 생성한다.

f d 4a 5bf6 ffb4 ca6c
1111 1101
0011 1100
3 c 4a 5bf6 ffb4 ca6c <- MCGA = 인터페이스 ID

(10) 앞의 라우터의 subnet prefix와 인터페이스 ID를 연결하여 최종 IPv6의 128비트의 주소를 생성한다.

(11) 만약 Collision Count가 3번 이상 발생하게 되면 더 이상 주소 생성을 중단하게 에러 메지시를 전송하게 된다.

나. MCGA 주소 검증

MCGA를 생성한 소유자는 해쉬 결과 생성된 자신의 주소 MCGA를 메시지를 통하여 상대방에게 유니캐스트나 멀티캐스트를 이용하여 전송하게 된다. 수신자는 주소의 소유권을 검증하기 위해서는 주소를 소유하고 있는 주소 소유자의 public key를 알고 있어야 한다. 메시지를 수신한 호스트는 주소에 대한 소유권을 검증하기 전에 Collision Count를 검사하여 3번의 충돌이 일어났는지 검사하여 충돌이 일어난 주소라면 의미 없는 주소이기 때문에 MCGA를 이용하여 암

호화된 주소를 풀지 않는다. 하지만, 충돌이 일어나지 않았다면 MCGA를 이용하여 암호화된 주소를 체크하게 된다. 수신자는 SHA-1을 사용하여 subnet prefix, modifier, public key, Collision Count, MAC address, Mask Num, TimeStamp 값을 연결하여 Hash1의 값을 생성한다. 생성된 값의 가장 왼쪽 64비트의 값을 가지는 Hash1을 만든다. 이렇게 생성된 Hash1의 값과 주소의 인터페이스 ID 값과 비교 하고 차이가 나타나는 'u','g'와 최초 3비트인 Sec값은 무시한다. 만약에 64비트가 다르다면 MCGA는 실패하게 된다. 두 값이 같다면 Sec값을 읽는다. modifier와 public key 값을 연관하고, SHA-1알고리즘을 실행한다. Mask값이 4라면 (그림 4)과 같이 실행한 값의 왼쪽 112 비트의 값이 Hash2의 값이 된다. 마지막으로 MCGA 주소를 생성할 때와 같은 Hash2의 규칙을 적용하여 해당 비트의 위치 값이 0과 같은지 비교해 본다. 모두 0이면 성공적이고 0과 같지 않다면 공격자에 의해 중간에 공격당했기 때문에 MCGA과정은 실패한 것이다.

이러한 일련의 과정들이 진행되고 나면 메시지를 보내는 송신자의 주소에 대한 소유권이 인증되는 것이다. 즉 송신자는 메시지원본, public key, 기타 보조의 매개변수를 포함한 메시지가 암호화된 MCGA 주소를 수신자에게 전송하게 되고 수신자는 MCGA의 Sec 값을 가지고 대칭키를 만들어 암호화된 MCGA를 풀어보고 인증 과정이 성공적으로 끝나게 되면 송신자가 가지는 public key를 알 수 있다. 마지막으로 메시지 내의 인증을 public key를 이용하여 열어봄으로써 송신자의 주소 소유권을 인증하게 된다.

4. 분석과 성능평가

IPv4에서 성공적으로 IPv6로 전환하기 위해서 관리자는 IPv4/IPv6 혼합망 및 IPv6에서 등장할 수 있는 다양한 공격을 고려해 보고 취약성을 분석하여 효율적인 보안 관리를 위한 보안 요구사항 및 통합적인 대응방안 설계를 해야 한다. (그림 5)는 공격 종류에 따른 보안 요구사항과 통합적인 대응방안을 분석결과이다. 결과 IPv6에서 효율적인 보안 관

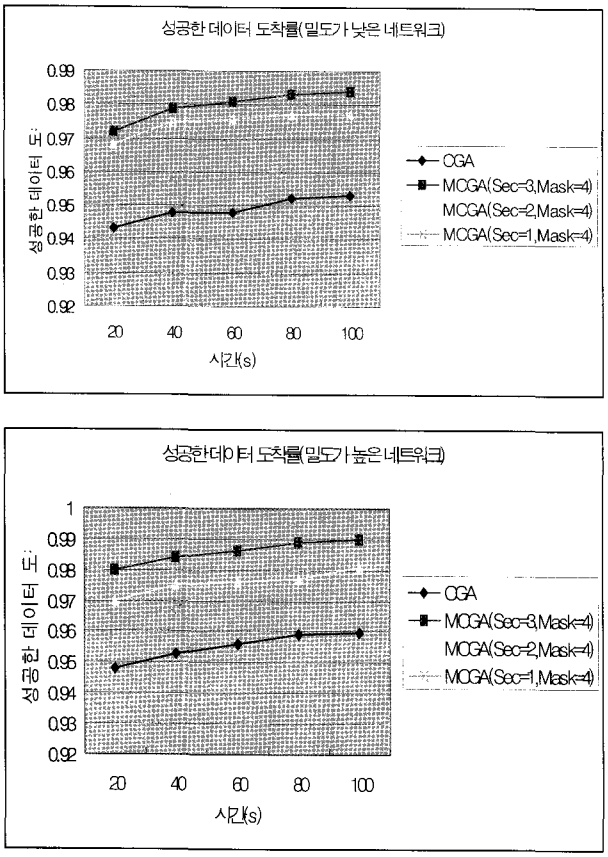
X 해결 불가능 ◬ 완벽한 해결은 불가능 ◌ 해결 가능성 존재 ○ 해결 가능

통합적인 대응방안 / 공격 종류	시스템		관리자의 (IPv6 특성 별) 주의 깊은 사용	CGA	개선된 CGA
	침입 차단 시스템(보안정책)	호스트와 애플리케이션 (적절한 패치와 호스트 잠금)			
사전 답사 공격	◬ 공격자의 연결성 완전히 막음 불가	◬ 공격자의 연결성 완전히 막음 불가	◌ 불명확한 IPv6 고정 주소 할당	◬ 인증, 무결성	○ 인증, 무결성, 암호화
허가되지 않은 접근 공격	◌ global address는 허용, link-local address는 외부로 나가는 것과 외부에서의 접근을 막아야 함	◬ 인증되지 않은 디바이스의 접근을 구분하기 어려움	◬ 인증되지 않은 디바이스의 접근을 구분하기 어려움	○ 인증, 무결성	○ 인증, 무결성, 암호화
헤더 조작 및 단편화 공격	◌ 단편화된 패킷을 재조합 해 필터링 적용	◬ 공격자 우회 가능	○ 관리자의 불필요한 IPv6 확장 헤더 사용 남용 자제	○ 인증, 무결성	○ 인증, 무결성, 암호화
3, 4계층에서의 스푸핑 공격	○ 3, 4계층 정보를 고려한 보안 정책	X 해결 불가능	◌ hop limit 필드 사용	◬ 인증, 무결성	○ 인증, 무결성, 암호화
ARP와 DHCP 공격	◌ ICMPv6의 필수 메시지 제외하고 불필요한 것은 침입차단시스템에서 필터링	◌ ARP, DHCP에 답변은 인증된 포트만 가능케 함	◌ 고정 주소와 의사 난수 주소의 적절한 사용해 공격자에게 주소 노출 줄임	◬ 인증, 무결성	◌ 인증, 무결성, 암호화
브로드캐스트 증폭 공격		X 해결 불가능	○ 목적지 주소가 멀티캐스트인 경우 응답 메시지 생성하지 않도록 함	◌ 인증, 무결성	◌ 인증, 무결성, 암호화
라우팅 공격	◌ 디폴트 라우터의 주기적인 광고 메시지에 주의한 보안 정책	◌ 디폴트 라우터의 주기적인 광고 메시지에 주의한 보안 정책	◌ hop limit 필드 사용	◬ 인증, 무결성	◌ 인증, 무결성, 암호화
바이러스와 웜	X 해결 불가능	◌ 주기적인 호스트 패치와 호스트 잠금으로 치료 가능성 존재	X 해결 불가능	◬ 인증, 무결성	◬ 인증, 무결성, 암호화
이웃 탐색에서의 공격들	◌ ICMPv6의 필수 메시지 제외하고 불필요한 것은 침입차단시스템에서 필터링	X 해결 불가능	◌ 중요한 시스템에 고정 이웃 항목을 사용하여 전형적인 공격 피함	◌ 인증, 무결성	○ 인증, 무결성, 암호화
주소 자동 설정에 관한 공격들		X 해결 불가능	◬ 라우터 광고 메시지를 안전하게 전달하기 힘듬	◬ 인증, 무결성	○ 인증, 무결성, 암호화
복제 주소 탐색에 관한 공격들		X 해결 불가능	◬ 주소 중복에 대한 공격자의 허위 답변 막기 힘듬	◬ 인증, 무결성	○ 인증, 무결성, 암호화
폭발 공격	X 해결 불가능	X 해결 불가능	X 해결 불가능	X 해결 불가능	○ 동적인 Sec, Mask 비트 값 활용
재전송 공격	X 해결 불가능	X 해결 불가능	X 해결 불가능	X 해결 불가능	○ TimeStamp

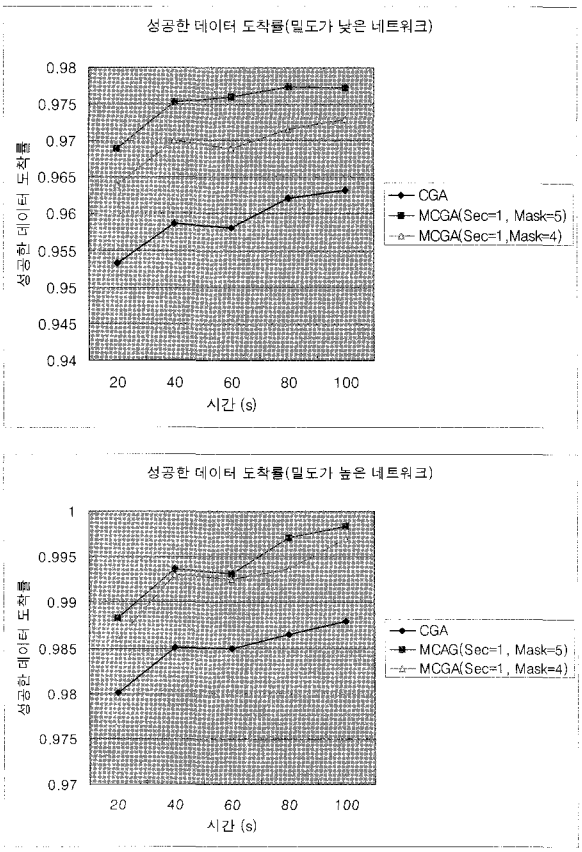
(그림 5) 공격 종류에 따른 보안 요구사항 및 통합적인 대응방안 분석

리를 위해서는 관리자가 크게 시스템 측면과 IPv6 프로토콜 자체의 특성으로 인해 새롭게 등장한 요소들을 고려해야하며 동시에 데이터의 인증과 무결성 및 기밀성을 제공하는 MCGA를 사용하여 더욱 강력한 보안을 제공해 주어야함을 알 수 있다.

물론 3, 4계층에서의 스푸핑 공격은 침입 차단 시스템의 3, 4계층 정보를 고려한 보안 정책을 통해 해결할 수 있고 허가되지 않은 접근 공격이나 헤더 조작 및 단편화 공격, ARP와 DHCP공격, 브로드캐스트 증폭 공격, 라우팅 공격 등 기타 다양한 공격들이 기존 IPv4 침입차단시스템의 보안 정책을 고려하고 추가 설정하여 해결 가능성이 존재함을 알 수 있다. 호스트와 애플리케이션의 적절한 패치와 호스트 잠금 역시 ARP와 DHCP 공격, 라우팅 공격을 어느 정도 해결할 수 있고 관리자가 IPv6 자체 특성을 고려하여 주의 깊게 사용함으로써 사전 답사 공격이나 3, 4 계층에서의 스푸핑 공격, ARP와 DHCP공격, 라우팅 공격 등을 비롯한 공격들의 해결 가망성을 알 수 있다. 하지만 데이터의 인증과 무결성, 암호화까지 제공해주는 MCGA는 침임 차단시스템의 보안 정책이나 호스트와 애플리케이션의 적절한 패치와 호스트 잠금, 관리자의 IPv6 특성 별 주의 깊은 사용, 기존의 MCGA에서도 해결되지 않았던 대부분의 공격들을 해결할 수 있음은 물론 기존 방법으로는 막을 수 없던 재전송 공격, 분산 서비스 공격과 같은 폭발 공격까지 해결할 수 있는 가능성이 있기에 의미가 크다. MCGA는 맨 처음엔 낮은 Sec과 Mask값을 선택(예: Sec=1, Mask=4)하여 메시지에 인증 및 무결성, 기밀성을 제공하다가 자신의 정보 전송이 제대로 안 된다던지 상대방으로부터 데이터 도착률의 비율이 점점 작아지면 폭발 공격으로 보고 높은 Sec과 Mask값을 선택(예: Sec=1, Mask=5)하여 통신을 재 시도한다. 즉 동적으로 Sec값과 Mask값을 바꿈으로써 폭발 공격을 막는 것이다. (그림 6)과 (그림 7)은 NS-2 시뮬레이터의 IEEE 802.11 wireless LAN환경에서 폭발 공격 중 하나인 분산공격이 발생했을 때 기존 CGA와 동적인 Sec값과 Mask값을 고려한 MCGA간의 성공적인 데이터 도착률 비교한 것이다. Sec과 Mask값이 높아지면 공격자는 암호화키를 알아내기 위해 맞춰야하는 비트의 수가 많아져 보안성이 증가하기 때문에 성공적인 데이터 도착률이 더 높아짐을 알 수 있다. 또한 밀도가 낮은 네트워크 환경보다 밀도가 높은 네트워크 환경에서 MCGA를 활용할 경우 성공적인 데이터 도착률이 더 높음을 알 수 있다. 물론 바이러스와 웜 공격과 같은 응용 계층 공격은 MCGA를 사용하면서 호스트, 애플리케이션 자체에서의 패치와 병행 시 가장 좋은 해결 방안이라고 볼 수 있다.



(그림 6) Sec변화에 따른 CGA와 MCGA간의 성공적인 데이터 도착률 비교



(그림 7) Mask변화에 따른 CGA와 MCGA간의 성공적인 데이터 도착률 비교

5. 결론 및 향후 연구 과제

IPv4에서 성공적으로 IPv6로 전환하기 위해서 관리자는 IPv4/IPv6 혼합망 및 IPv6의 보안 취약성을 분석하여 IPv6에서의 효율적인 보안 관리를 위한 보안 요구사항 및 통합적인 대응방안 설계를 해야 한다. 따라서 IPv4와 IPv6의 특성, 공격별 측면에서 보안 취약성을 파악하고 궁극적으로 IPv6에서의 효율적인 보안 관리를 위한 보안 요구사항 연구를 고려하여 IPv6 시스템 측면, IPv6 특성 별, MCGA를 통해 통합적인 대응방안을 제시하였다.

향후 과제로는 본 논문에서 분석한 보안 취약성 및 보안 요구사항, 통합적인 대응방안을 바탕으로 IPv4/IPv6 혼합망 및 IPv6에서의 효율적인 보안 관리를 위한 보안 프레임워크를 제안하고 다양한 방법으로 비교, 검증해야할 것이다. 또한 IPv6는 MIPv6, FMIPv6, HMIPv6등 다양한 IP 이동성 관리 프로토콜을 고려하여 설계되어 있기 때문에 노드가 이동하는 환경에서도 안전하게 주소를 자동으로 설정하고 이웃 탐색을 할 수 있는 메커니즘을 고려해 봐야 하며, 공격 라우터가 존재하는 IPv4/IPv6 혼합망 및 IPv6 네트워크 환경도 고려해봐야 한다.

참 고 문 헌

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

[2] R. Hinden, S.Deering, "RFC-2373: IP Version 6 Addressing Architecture", Networking Working Group, July 1998.

[3] Y. Rekhter, P. Lothberg, R. Hinden, S. Deering, J. Postel, "RFC-2073: An Ipv6 Provider-Based Unicast Address Format", Network Working Group, January 1997.

[4] Y. Rekhter, P. Lothberg, R. Hinden, S. Deering, J. Postel, "Internet-draft: An IPv6 Provider-Based Unicast address Format", March 1997 draft-ietf-ipngwg-ipv6-arch-00.txt

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

[6] R. Atkinson, "RFC-1827: IP Encapsulating Security Payload (ESP)", Network Working Group, August 1995

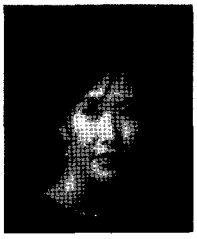
[7] IPv6 and IPv4 Threat Comparison and Practice Evaluation (v1.0), *cisco*.

[8] T. Narten, E.Nordmark, W.Simpson, "RFC-2461: Neighbor Discovery for IP Version 6(IPv6)", Network Working Group, December 1998.

[9] S. Thomson, T. Narten, T. Jinmei, "Internet-Draft: IPv6 Stateless Address Autoconfiguration", May 2005.

[10] A. Conta, S.Deering, "RFC-2463: Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6(IPv6) Specification", Networking Working Group, December 1998.

[11] T. Aura, "RFC-3972: draft-ietf-send-cga-06.txt", March 2005.



오 하 영

e-mail : hyoh@ewhain.net

2002년 2월 덕성여자대학교 전산학과 학사

2001년 11월~2004년 1월 신한금융 지주회사 e-신한

2006년 2월 이화여자대학교 컴퓨터학과 석사

관심분야: 네트워크 보안, 센서 네트워크, 홈 네트워크, 유비쿼터스 컴퓨팅, DDos

채 기 준

e-mail : kjchae@ewha.ac.kr

1982년 2월 연세대학교 수학과 학사

1984년 2월 미국 Syracuse University 컴퓨터학과 석사

1990년 2월 미국 North Carolina State University 컴퓨터공학과 박사

1990년 9월~1992년 2월 : 미국 해군사관학교 컴퓨터학과 조교수

1992년 3월~현재 이화여자대학교 컴퓨터학과 교수

관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능분석, 센서네트워크, 홈 네트워크, 유니쿼터스 컴퓨팅

방 효 찬

e-mail : bangs@etri.re.kr

1995년 2월 홋카이도 공업대학교 경영공학과 학사

1997년 2월 홋카이도 공업대학교 기계시스템공학과 석사

1997년~1999년 한국통신 운용연구단 전임연구원

2000년 8월~현재 : 한국전자통신연구원 선임연구원

관심분야 : 교환망 프로토콜 설계, 네트워크 관리, 네트워크보안

나 중 찬

e-mail : njc@etri.re.kr

1986년 2월 충남대학교 계산통계학과 이학사

1989년 2월 숭실대학교 전자계산학과 공학석사

2004년 3월 충남대학교 컴퓨터과학과 이학박사

1989년~현재 ETRI 능동보안기술연구팀 팀장

관심분야 : 실시간시스템, 네트워크 관리, 네트워크보안