주 제

IPv6 침입 탐지 및 차단 기술

한국전자통신연구원 김기영, 정보흥, 장종수

차 례

Ⅰ. 서 론

지난 69년 미국을 중심으로 군사적 목적으로 개발된 알파넷이 바로 인터넷의 전신이라 할 수 있으며, 90년대 들어오면서 활용서비스의 증가와 함께 사용자가 폭발적으로 증가함으로써 실제적으로 인터넷 시대의 문을 열었다. 그러나 21세기로 접어들면서 계속되는 사용자의 증가와 인터넷에 연결되는 장치들의 증가로 인하여 인터넷 주소 공간의 유한성이 큰 문제로 대두되었다.

국내 이용자 수의 경우만 보아도 2003년에 2,922만명, 2004년 3,158만명, 2005년 3,301만명으로 크게 증가하였고 앞으로 무선 인터넷 통신망과 인터넷 정보가전 등의 새로운 서비스의 등장으로 인해 2010년까지에는 추가로 2억개 이상의 IP 주소가 필요할 것이라는 전망이 나오고 있다. 최근 들어서 PC 뿐 아니라 가전, 자동차, 센서 등 모든 기기들이 하나의 네트워크로 연계되어 유비쿼터스 네트워크가 실현되는 환경이 구축되면서 더욱더 절실히 요구되는 상황이다.

이러한 상황에서 지금까지 사용하고 있던 IPv4의 주소체계에 따라 주소를 할당받고 서비스를 제공하기에는 많은 한계점에 봉착하게 된다. IPv4는 이론상 43억여개의 인터넷 주소를 지원할 수 있으나 클래스 단위로 주소를 구분하는 비효율적인 주소체계, 초기의 무분별한 클래스 단위의 할당 및 와 매년 급증하는 인터넷 접속호스트 수로 인해 주소고갈의 우려가 대두되고 있으며 QoS나 Security 기능이 없어 특화된 서비스의 제공이 어려운 실정이다. 게다가 최근 컴퓨터와 네트워크의 사용이 보편화되어 사용자의 급격한 증대와 IP를 요구하는 신규서비스의 증가로 인하여 새로운 주소체계의 요구와 보안의 필요성이 강력하게 대두되고 있다.

이러한 새로운 주소체계의 요구사항과 더불어, 인

프라 측면에서의 변화를 살펴보면 국내의 경우 90년대 중반부터 시작한 초고속정보통신망 구축사업이 현재 우리나라가 세계최고수준의 정보통신 인프라 강국으로 자리매김 할 수 있는 기초를 마련하고 있다. 최근 몇 년 동안 정통부에서는 IT389전략(2006년부터는 uIT839전략이라고 함)에 따라 우리나라 IT 산업의 선순환 발전을 위하여 첨단 정보통신 서비스의 도입을 가속화하고 미래핵심기술 확보를 위하여 매진해 오고 있다.

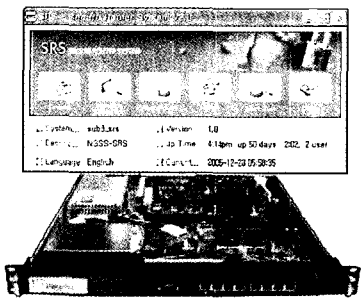
IT839는 3대 인프라를 중심으로 8대 서비스를 제공하고 9대 신성장 동력 산업을 활성화하는 것이다. 이러한 IT839 전략에서 제시하는 3대 인프라는 광대역통합망(BcN : Broadband Convergence Network), u-센서 네트워크와 소프트 인프라웨어이고, BcN은 IPv6 체계를 기반으로 단계적으로 USN(Ubiquitous Sensor Network)이 All-IP 망으로 통합되는 형태로 구축될 것이며 2010완성을 목표로 하고 있다.

향후 유비쿼터스 네트워크 환경은 언제, 어디서나, 어떤 정보나 누구나 통신이 가능한 다양한 정보를 끊김없이 소통시킬 수 있는 첨단 IT 서비스 및 제품을 제공할 것이며, IPv6 네트워크 인프라 환경은 차세대 네트워크 인프라 구축 뿐 아니라 IPv6 네트워크 운용 중에 발생할 수 있는 보안 고려사항들을 해결하는 솔류션을 제공하면서 전개될 것으로 예측된다.

즉, 기존의 IPv4 네트워크에서 문제점으로 부가되었던 주소공간의 유한성, 새로운 인테넷 서비스에서 요구되는 원활한 이동성과 높은 보안성 등을 해결하고자 IPv6라는 새로운 네트워크 환경을 고려하게 되었으며, 이러한 IPv6를 네트워크에 적용하면서 발생하는 여러 가지 문제를 해결하면서 인터넷이 발전될 것이라고 전망하였다. IPv6는 이러한 주소공간의 확대 및 특화된 서비스의 제공을 위하여 IPv4의 문제점을 해결하고자 IPv6 플로우 레이블을 이용한 패킷별 품질제어 및 주소 자동 설정 등의 기능도 추가되어 관리자와 일반 사용자의 편의성도 증가될 것이다.

IPv6는 이렇듯 IPv4에 비해 많은 장점을 지니고 있지만 적용하기 전에 자동으로 이루어지는 주소할당과 설정, IP 패킷의 보호, 스캔과 공격으로부터의 호스트 보호 및 인터넷에서 교환되는 트래픽의 제어 등 고려해야할 추가적인 보안사항이 존재한다.

따라서 본 고에서는 이러한 IPv6 보안사항의 기술동향과 현재 이러한 기술을 기반으로 한국전자통신연구원 보안운영체제연구팀에서 활발히 연구 및 개발되고 있는 IPv6 침입탐지 및 차단 시스템에 대하여 기술하고자한다.



(그림 1) ETRI개발 IPv6 침입탐지 및 차단 시스템

(그림 1)은 현재 ETRI에서 공동연구업체와 공동으로 개발하고 있는 IPv6 침입탐지 및 차단시스템의 형상과 그래픽 사용자 인터페이스이며, IPv6 패킷 처리 외에 터널링 패킷도 처리하도록 구현되어 있다.

본고의 나머지는 다음과 같은 구성으로 기술되어 있다. II절에서 IPv6 보안기술 동향에 대하여 정통부가 제시하고 있는 IPv6 보급촉진계획과 실제 적용측면에서 살펴보고, III절에서 IPv6 침입탐지 및 차단 기술에 대하여 요구사항을 정립해보고, 현재 ETRI에서 개발하고 있는 IPv6 침입탐지 및 차단시스템 측면에서 검토해본다. 마지막으로 암호화된 IPv6 트래픽에서 이상상황 감지가 가능한 비정상적인 트래픽

의 모니터링 기술에 대하여 IV절에서 알아본다.

II. IPv6 보안기술 동향

국내에서는 지난 2000년 2월부터 차세대 인터넷 기반구축계획을 발표하고, 2003년 9월 IPv6 보급촉진계획을 수립해 국가 정책으로 채택하고 IPv6 보급촉진을 통해 차세대 인터넷 산업과 신규 서비스를 육성함으로써 인터넷 소비국에서 생산 강국으로 전환을 꾀하고 있다.

IPv6 보급촉진계획에 의하면 IPv6는 2003년~2004년까지 터널링 기술로 백본을 경유하도록 되어있고, 2005~2006년까지 듀얼스택 기술로 IPv6 Native 통신이 이루어지도록 계획되어있으며 마지막 단계인 2007~2010년까지 IPv6 only 통신망으로 전환되도록 계획되어있다. 하지만 현재 IPv6 도입은 몇 개의 Enterprise Network을 제외하고는 1단계의 수준에 머물러 있다고 보여진다.

한편 미국에서는 미국방성이 2008년까지 IPv6 도입을 추진하고 있으며 Cisco나 MS같은 민간기업 중심으로 연구개발이 활발히 진행되고 있다. 최근 Cisco에서 개발되는 거의 모든 제품들은 IPv6를 Dual Stack으로 제공하고 있다.

일본의 경우, IPv6 장비개발 및 채택에 대한 세금 우대정책을 시행하는 등 미국보다 좀더 적극적으로 IPv6 계획이 추진됨을 알 수 있다.

유럽의 경우 98년부터 연간 1,100억원을 투자해 40여개 이상의 연구과제를 수행하고 있으며 에릭슨, 노키아에서 MIPv6 서비스를 개발하고 있다.

마지막으로 최근 IPv6를 가장 적극적으로 개발하고 있는 중국에서는 2000년부터 테스트베드를 구축하고 중국정부 10개부처가 연합해 IPv6 국가 백본망 구축을 추진하고 있다.

여기에서는 우선 IPv6 환경에서의 보안 취약성과 대응방안에 대하여 현재까지 IPv6 관련기관 및 Forum에서 정리한 자료들을 기반으로 살펴보기로 한다. IPv6 제공 환경을 유선환경과 이동환경, 그리고 IPv4/IPv6 전환 환경에서의 보안취약성과 대응으로 분류한다.

첫 번째로 유선환경에서의 보안취약성과 대응방안을 살펴보면 다음과 같다.

- 소스 라우팅을 위한 라우팅 헤더 보안취약성으로 Type 필드값이 0인 라우팅 헤더를 갖는 패킷이 실제 네트워킹에 영향을 주지 않도록 필터링 규칙을 설정
- 사이트 범위(Site-Local scope)를 갖는 멀티캐스트 주소 취약성으로 멀티캐스트 주소를 이용하여 공격할 라우터에 대한 스캔작업 없이 모든 라우터에 대한 서비스 거부 공격이 가능하며 외부에서 멀티캐스트 주소에 접근할 수 없도록 필터링 규칙을 설정
- 통합된 ICMPv6의 보안취약성으로 목적지나 목적포트에 대한 필터링 뿐만 아니라 확장헤더에 대한 필터링이 가능하도록 규칙을 설정
- 최적의 서비스 탐색을 위한 애니캐스트 보안취약성으로 외부에서 애니캐스트 서비스 요청을 제한하기 위해 애키캐스트 주소를 필터링하도록 규칙을 설정하거나 보안통신채널을 설정
- 동적 주소설정을 위한 프라이버시 확장 보안취약성으로 공격자의 인터페이스 식별자 변경이 용이하고 침해사고 시 공격자에 대한 추적 및 호스트의 관리가 어려워져 주소설정을 위한 노드와 DNS 서버 간 SA를 통하여 인증된 노드만이 주소 갱신을 하도록 하며 프라이버시 확장을 사용하는 노드는 주소 업데이트 주기에 대한 적절한 값을 설정
- IPv6 주소 및 포트정보를 이용한 접근제어 취약

성으로 하나의 인터페이스에 여러주소가 허용될때 글로벌 주소와 링크 로컬 주소를 구분하여 접근제어를 제공함

- IPv6 확장헤더 취약성으로 확장헤더 처리시, 확장헤더 체인처리시, Unknown 헤더/목적지 옵션과 보안정책 및 hop-by-hop 옵션헤더 남용과 Router alert option 남용 등을 허용하지 않도록 제어함
- 전송 패킷의 Fragmentation 취약점으로 DHCPv6 서버를 활용하여 보안이 취약한 NDP의 기능을 대체

두 번째로 이동환경에서의 보안취약성과 대응방안을 살펴보면 다음과 같다.

- 바인딩 업데이트 시 취약성으로 임의의 위치, MN(Mobile Node) 및 MN과 CN(Correspondent Node)사이, NM 이전위치에서의 보안 취약성이 있으며 인증된 송신자의 정보가 도청되거나 변조되지 않도록 함.
- 홈어드레스 옵션에 의한 취약성으로 HAO(Home Address Option)를 이용하여 서비스 거부공격을 하지 못하도록 수신된 패킷의 주소를 검증함.
- 라우팅헤더 취약성으로 CN이 MN으로 패킷을 전송할 때 발생하며 MIPv6에 기존의 라우팅 헤더를 사용하지 않고 새로운 목적지 옵션, 새로운 확장헤더 또는 새로운 라우팅 헤더타입을 정의하여 대응함.

세 번째로 IPv6 Network으로 전환하기전 IPv4/IPv6 전환기술의 취약성 및 대응기술에 대하여 살펴본다. IPv4에서 IPv6로의 전환기술은 듀얼스택, 터널링 및 변환기술이 있으며 이들 각각의 보안 취약성은 다음과 같다.

- IPv4/IPv6 듀얼스택의 경우, IPv4/IPv6 듀얼스택 노드는 양쪽 프로토콜을 지원하기 때문에 IPv4주소와 IPv6주소 모두 설정할 수 있어 양쪽 프로토콜의 보안 취약성임.
- IPv4와 IPv6의 호환성 지원시 취약성으로 네트워크를 구성하는 모든 장비가 모두 IPv4, IPv6 두가지 프로토콜을 인식하여 트래픽을 검사하고 차단할 수 있어야함.
- IPv4/IPv6 터널링의 경우, 네트워크를 보호하기 위하여 설치된 침입차단 시스템이나 침입탐지 시스템을 우회할 수 있기 때문에 네트워크상에서 발생하는 보안 위협중의 하나임.
  - 6to4 터널링, ISATAP 터널링, Teredo 터널링 보안취약성이 있으며 터널된 패킷이 비정상적인 패킷인지 검사하여 차단
- IPv4/IPv6 변환기술의 경우, IPv4/IPv6 변환을 통해서 IPv4 호스트와 IPv6 호스트 사이의 통신기술의 보안 취약성임.
  - NAT-PT(Network Address Translation -Protocol Translation)취약성으로 NAT-PT내에서 인그레스 필터링이나 소스 주소 위조 방지, 반사공격 수행방지로 차단.

지금까지 IPv6 보안기술 동향에 대하여 살펴보았다. 최근 몇 개의 시범사업과 서비스의 활성화로 차세대 네트워크인 IPv6 네트워크 인프라 구축이 가시화되면서, IPv6 네트워크 운용뿐만 아니라 IPv6 네트워크 운용 중에 발생할 수 있는 보안 고려사항들이 위와 같이 IPv6 제공환경에 따라 정리되고 있다.

Ⅲ. IPv6 침입탐지 및 차단 기술

IPv6 침입탐지 및 차단기술은 IPv6 환경에서 다

양한 네트워크 공격에 대한 침입탐지를 수행하여 안전한 네트워크 환경을 제공하기 위한 보안 기술이다. 안전한 IPv6 네트워크 구축을 위한 하나의 방안이라고 할 수 있으며, IPv6 네트워크에 적용가능 한 보안 기술들의 정의 및 개발이 중요한 시점이라고 할 수 있다.

여기에서는 이러한 보안기술들에 대하여 현재 개발된 보안시스템 측면에서의 요구사항을 정의하고자 한다.

IPv6 패킷 탐지/차단을 위한 보안 기술은 다음과 같다.

1. 시그니쳐 기반의 탐지/차단

시그니쳐 기반의 침입탐지/차단은 IPv6 프로토콜 스팩을 만족하는 IPv6 패킷 탐지 기능을 제공하며 아래와 같은 항목의 해석이 반드시 제공되어야 한다

- RFC 2460에 정의된 IPv6 기반의 주소를 포함하는 IPv6 기본헤더 탐지
- RFC 2460에 정의된 모든 확장헤더 및 각각 확장 헤더 별 세부 필드
- L4 프로토콜 헤더 및 각 헤더 별 세부 필드 (TCP, UDP, ICMPv6 등)
- 패킷 페이로드에 대한 탐지

2. 기본헤더 탐지/차단

IPv6 패킷을 탐지/차단하기 위해서는 RFC 2460에서 정의한 IPv6 기본 헤더를 해석할 수 있는 기능이 있어야 한다. IPv4와 IPv6의 가장 큰 차이점은 주소길이의 변화에 따른 헤더 구조 변화이다. IPv6에서는 128bit의 주소길이를 가지고 있으므로 IPv6 침입탐지/차단 시스템은 128bit의 주소길이를 해석할 수 있어야 한다.

3. 확장헤더 탐지/차단

IPv6에서는 IPv4에서 가변 길의의 옵션필드를 활용하였던 것과 같은 기능을 확장 헤더를 통해 표현한다. 이들 확장헤더는 RFC2460, RFC4302, RFC4303에 정의되어 있으며, IPv6 프로토콜의 대표적인 특징 중 하나로 설명된다. 즉, IP 패킷 처리에 대한 옵션 사항이 이들 확장헤더를 통해 편리하게 이루어지나, 여러 가지 보안 취약점을 제공하여 공격자에게 공격을 빌미를 제공하는 수단이 되기도 한다.

- 기본적으로 RFC2460, RFC4302, RFC4303에 정의되지 않은 잘 알려지지 않은 확장헤더를 포함하는 패킷을 차단해야 한다.
- 라우팅 헤더는 '0'의 type 값을 가질 경우 라우팅 헤더 내의 주소를 해석할 수 있어야 하며, 이를 통해 접근제어를 회피하려는 행위를 차단해야 한다.
- 단편화 헤더는 전송할 데이터의 크기가 MTU보다 클 경우 단편화하여 전송할 때 사용된다. RFC2460 스팩에 따르면 단편화 및 재조립은 패킷의 출발지와 목적지에서만 수행하도록 하고 있어 중간 노드에서 이를 재조립하는 것은 스팩에 어긋날 수도 있다.하지만 오버래핑된 단편화 패킷은 탐지 및 차단으로 기술된 시그니쳐를 우회하는 수단을 제공할 수 있어서 오버래핑된 모든 단편화 패킷을 차단해야 한다.

4. Pad1과 PadN 옵션 처리

RFC2460은 Hop-by-Hop과 Destination 확장헤더 내에 임의의 크기를 가지는 다수개의 패딩 옵션을 가지도록 한다. 이는 확장헤더 길이를 8옥텟 길이

로 맞추기 위한 수단으로 현재 스펙으로는 몇 번이 반복되어도 상관이 없다. 또한 PadN의 경우 페이로드 부분이 '0'의 값으로 채워져야 하지만, 수신 노드에서는 이를 검사할 의무가 없다. 이는 패딩 옵션이 공격자에 의해 비밀 채널(covert channel)로 사용될 여지를 제공하고 있어 IPv6 기반 침입탐지/차단시스템은 다음과 같은 기능을 제공해야 한다.

- IPv6 기반 침입탐지/차단시스템은 Hop -by- Hop 확장헤더와 Destination 확장 헤더의 옵션 데이터 부분을 해석하는 기능을 제공해야 한다.
- IPv6 기반 침입탐지/차단시스템은 Pad1과 PadN 옵션이 반복적으로 사용되었는지 확인하여 반복 사용이 확인될 경우 차단할 수 있는 기능을 제공해야 한다.
- IPv6 기반 침입탐지/차단시스템은 PadN 옵션의 페이로드 부분에 '0'이 아닌 다른 값을 가지고 있는 경우를 검사하여 다른 값일 경우 차단할 수 있는 기능을 제공해야 한다.

5. ICMP 패킷 탐지/차단

ICMPv4는 많은 보안 취약점을 가지고 있어 IPv4 네트워크에서의 보안장비에서는 대부분 차단하도록 설정되어 있다. 하지만 IPv6에서의 ICMP 기능은 Neighbor Discovery, Stateless Address Auto-configuration, Duplicated Address Detection, Multicast Listener Discovery 등 네트워크 연결관리에 없어서는 안될 중요한 기능을 제공한다. 따라서 아래와 같은 IPv6 기반 침입탐지/차단시스템은 최소한 다음과 같은 ICMPv6 메시지들을 허용해야 하며, 그 방법은 시그너쳐를 기반으로 하든 내부적으로 제공하든 구현에 달려있다.

- Destiantion Unreachable (Type 1) - All codes
- Packet Too Big (Type 2)
- Time Exceed (Type 3) - Code 0 and 1 only
- Parameter Problem (Type 4) - Codes 0 , 1 and 2
- Echo Request (Type 128)
- Echo Response (Type 129)
- Home Agent Address Discovery Request (Type 144)
- Home Agent Address Discovery Reply (Type 145)
- Mobile Prefix Solicitation (Type 146)
- Mobile Prefix Advertisement (Type 147)

6. Tunneling 패킷 탐지/차단

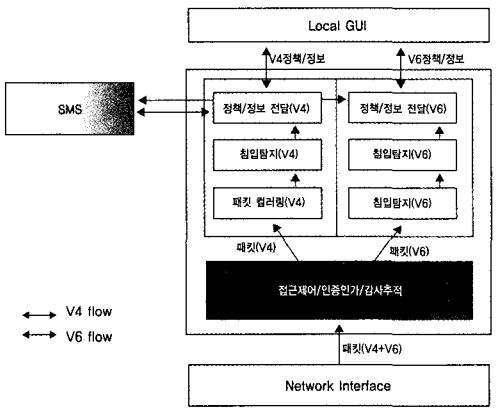
현재 인터넷이 모두 IPv6 네트워크로 운용되기에는 아직 많은 시간이 필요하다. IPv6 네트워크가 보급된다 하더라도 상당 기간 IPv4 네트워크와 혼용될 것이고, IPv4 인터넷을 통한 IPv6 네트워크는 터널링 기법을 통해 운용된다. IPv6 침입탐지/차단시스템으로 인해IPv6 패킷이 탐지 및 차단되는 경우라도 IPv4 헤더를 통해 IPv6 패킷이 캡슐화된다면 IPv6 패킷에 대한 검사가 이루어지지 않아 공격자는 IPv4 터널링 기법을 통해 IPv6 보안시스템을 우회할 여지가 있다. 이를 방지하기 위해 IPv6 기반 침입탐지/차단시스템이 IPv4/IPv6 경계에 적용될 경우 IPv4 헤더로 터널링된 다음과 같은 IPv6 터널링 패킷에 대한 검사 기능을 제공해야 한다.

- Configured Tunnel (RFC 4213), 사용자가 직접 설정한다.
- 6over4 (RFC 2529), IPv4 멀티캐스트로 IPv6 Neighbor Discovery를 수행한다. Host들간의 터널링 제공한다.

- 6to4 (RFC 3056), 6to4 라우터에서 터널링한다. 네트워크 들간의 터널링을 제공한다.
- ISATAP (RFC 4214), Non-broadcast 네트워크에서 사용 가능하다. Host 들간의 터널링 제공한다.
- Tunnel Broker (RFC 3053), 특정 사이트의 터널을 뚫어준다. Configured Tunnel 설정 스크립트를 제공한다.
- Teredo (RFC 4380), NAT 아래에 있는 호스트를 위한 터널링 기법이다. Host 들간의 터널링 제공한다.

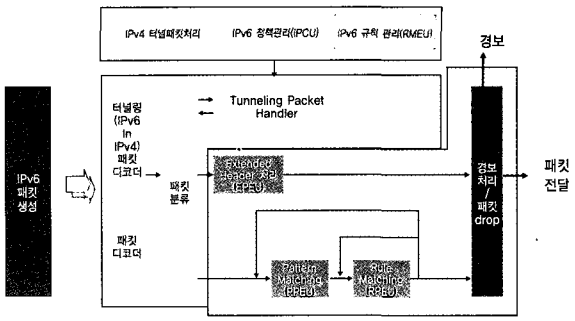
지금까지 기술한 IPv6 보안요구사항들은 IPv6 Network가 전개되기 전 IPv4/IPv6 Dual Network 환경에서 상당기간 제공되어야 할 것이며 보안기능 또한 모두 고려가 가능하여야 한다.

다음 (그림 2)는 이러한 Dual Network환경에서 IPv4/IPv6 보안이 모두 제공가능 한 보안시스템의 개념적인 구조를 나타낸다.



(그림 2) IPv4/IPv6 보안 시스템 개념구조

다음 (그림 3)는 ETRI에서 개발 중인 침입 탐지 및 차단모듈의 구조이다.

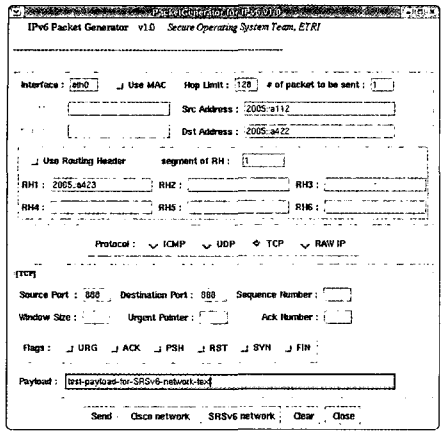


(그림 3) IPv6 침입탐지 및 차단 모듈 구조

(그림 3)에서와 같이 IPv6 침입 탐지 및 차단모듈은 실제 패킷의 인입점에서부터 안전한 패킷을 전달하기까지 여러 단계의 과정으로 이루어져 있으며, 기존의 IPv6 보안장비에서 제시하고 있는 OS수준에서의 단순 IPv6 패킷 처리수준이 아닌 실제 IPv6 공격패킷을 차단하기 위한 침해차단 엔진을 제공한다. RFC 2460과 RFC 3515에 따른 패킷 및 확장헤더 분류가 가능하며 성능향상을 위한 H/W 페이로드 패턴매칭 가속기능도 활용가능한 구조를 제공한다.

아울러 IPv6 정책 및 규칙을 관리하기 위한 별도의 모듈이 제공되며, IPv6 침입탐지규칙은 기존의 공격 시스니쳐를 기반으로 ETRI 독자적으로 개발한 IPv6 침입탐지 규칙을 제공하고 있다. IPv6 침입탐지 규칙은 RFC 3515 에 따른 IPv6 Address Scheme을 지원하고, RFC 2460에 따른 IP 패킷 변경 필드 및 확장헤더 스팩을 지원하도록 정의되어 있다.

다음 (그림 4)는 IPv6 침입탐지 및 차단기술 개발 시 부수적으로 개발된 IPv6 공격패킷 생성기의 초기 화면이다. 아직 IPv6 네트워크가 완전히 활성화 되지 않은 시점에서 다양한 시험환경을 제공하기 위하여 반드시 제공되어야할 S/W이다. 여러 가지 공격 패턴의 시험이 가능하도록 구성되어 있다.



(그림 4) IPv6 공격패킷 생성 S/W

지금까지 기술한 침입탐지 및 차단기술은 IXIA 시험기 및 자체개발한 IPv6 공격패킷 생성기 등을 이용하여 자체적으로 시험하였으며 향후 상용수준의 개발요구사항 수렴을 위하여 2006년 3월부터 IPv6 시범 서비스에 적용하고 있다.

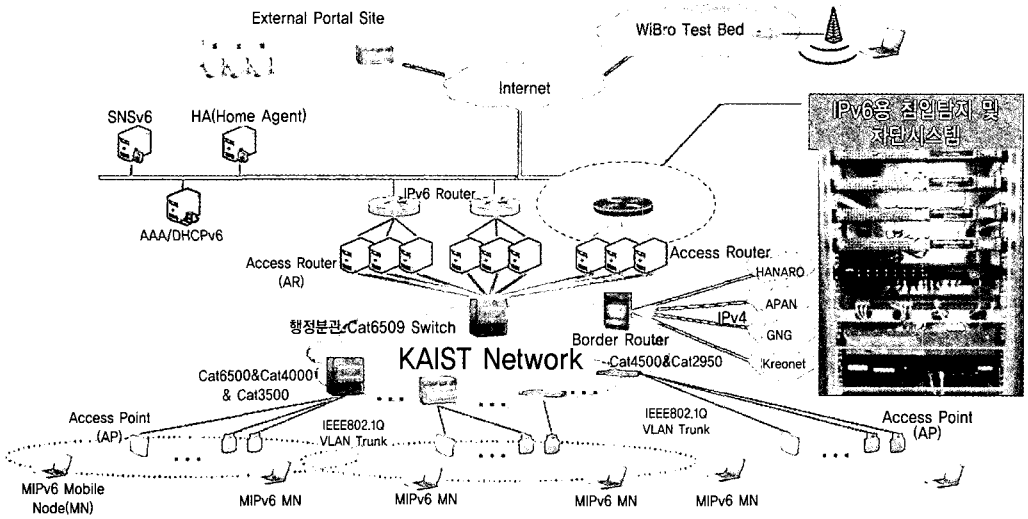
IPv6 시범서비스에 적용된 IPv6 침입탐지 및 차단시스템은 IPv6 트래픽이 빈번하게 발생하는 지점에서 트래픽을 미러링하여 탐지하고 있다. 지금까지 수집된 트래픽의 대부분이 MIPv6 이었으며 아직 특이할만한 IPv6 네트워크 공격패킷을 탐지되지는 않았지만 향후 IPv6의 적극적인 전개에 따라 많은 공격패턴들이 탐지될 것으로 예측된다.

다음 (그림 5)는 IPv6 침입탐지 및 차단 시스템을 개발단계에서 KAIST, IPv6 시범 서비스에 적용한 네트워크 구성도이다.

Ⅳ. IPv6 이상 트래픽 탐지

IPv6 이상 트래픽은 IPv6 네트워크에서 비정상적인 트래픽 흐름을 제공하는 트래픽이다.

IPv6 네트워크에서 이상 트래픽 탐지를 위해서는 IPv4/IPv6 트래픽 모니터링을 동시에 수행할 수 있어야 한다. 현재 IPv6 트래픽을 모니터링 하는 방법은 전용 트래픽 측정 시스템을 활용하여 IP 패킷 단위로 하거나 라우터의 도움을 받아 플로우 단위로 측정



(그림 5) IPv5 침입탐지 및 차단 시스템 적용

하는 방식으로 나눌 수 있다.

패킷 단위의 전용 트래픽 측정 시스템은 아주 정확한 트래픽 모니터링 기능을 수행할 수 있지만, 모든 트래픽 측정 지점마다 설치해야하기 때문에 비용이나 운용면에서 대규모 네트워크에서는 적합하지 않다. 한편 라우터의 도움을 받아 플로우 단위로 모니터링 하는 방식은 비용면이나 관리면에서 효과적이다. 대표적으로 Cisco NetFlow를 이용하면 라우터에서 트래픽 모니터링을 쉽게 수행할 수 있다.

라우터에서 IPv6 트래픽 모니터링을 위해서 IETF IPFIX 표준을 만족하는 기술들은 현재 Cisco, Juniper 등의 라우터 제조업체에서는 라우터기반의 트래픽 모니터링 모듈을 자체적으로 개발하고 있다. 국내에서는 Netflow 5기반의 트래픽 모니터링 제품들이 ifeelnet과 같은 벤처회사에서 개발하여 국내의 ISP에 이용되고 있다.

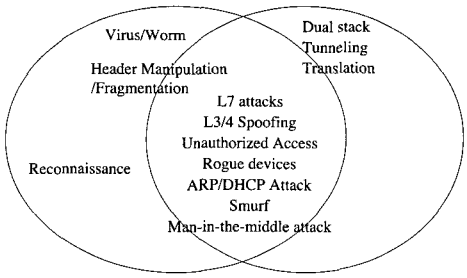
IPv6 네트워크에서의 모니터링을 위한 IETF IPFIX 표준을 지원하는 제품은 현재 많지 않으며, 특히 이상트래픽 모니터링에 대하여는 거의 연구가 진행되어 있지 않다. 향후 IPv6 Network으로 진화하기 위하여는 IPv6 네트워크에서 이상트래픽 모니터링 기술이 필수적이라고 할 수 있다.

현재 IETF에서는 IPFIX(IP Flow Information eXport) WG에서 차세대 라우터에서 트래픽 모니터링 표준화를 진행 중에 있다.

IPv6 네트워크에서 이상 트래픽 탐지를 위해서 IPv6 트래픽 모니터링 기술이 필수적이지만 현재 라우터와 스위치에서 IPFIX 표준을 제공하는 제품들은 현재 거의 개발되어있지 않다.

아래의 그림은 IPv4/IPv6에서의 이상트래픽을 정의한 다이어그램이다.

IPv6 이상트래픽도 Native IPv6 이상 트래픽과 Transition IPv6 이상 트래픽으로 분류해 볼 수 있다. Native IPv6 이상 트래픽의 경우 THC 도구를



(그림 6) IPv4/IPv6에서의 이상 트래픽 정의

이용한 이상 트래픽으로 Reconnaissance, ARP/DHCP IPv6, Smurf, Fake RA, Fake MIPv6 BU가 있고, Covert Channel이 있다. Transition IPv6 이상 트래픽으로는 Tunneled IPv6 트래픽이 있다.

지금까지 IPv6 네트워크에서 모니터링 할 수 있는 이상 트래픽에 대하여 살펴보았다. 본격적인 IPv6 도입이 활성화 되고, 국내에서도 이미 국방부 및 주요 정부부처 기관들을 중심으로 IPv6로 전환되는 로드맵이 작성되고 있으며 이미 국내 연구망인 KOREN과 KREONET2에서는 IPv6 연구시험망 서비스를 제공하고 있는 시점에서의 IPv6 보안기술개발의 필요성은 더 이상 언급하지 않아도 충분하다고 생각된다.

기존 시그니쳐 기반의 침입탐지 및 차단시스템의 수준이 아니라 보안성이 강화된 IPv6 네트워크에서 암호화된 트래픽의 흐름에서 이상트래픽의 모니터링의 중요성도 더 이상 강조하지 않아도 충분하다고 생각되며 이를 어떻게 표준화된 인터페이스와 네트워크 장비를 활용하여 효율적으로 운영할 것인가에 대한 고려가 절실히 요구된다.

V. 결 론

지금까지 차세대 인터넷 기반구축계획 및 IPv6 보

급촉진계획에 따른 IPv6 동향 및 국내 보급단계 등에 대하여 살펴보았으며, 향후 안전한 IPv6 Network구축 시 고려해야할 여러 가지 보안요구사항 및 기술, 그리고 ETRI가 개발한 IPv6 침입탐지 및 차단시스템에 대하여도 살펴보았다.

향후 몇 년 이내로 IPv6 표준화가 완성되고, 상용제품이 등장하기 시작하면 본격적으로 IPv6 도입이 가시화 될 것으로 예측된다. 이러한 상황에서 IPv6 네트워크를 안전하게 운용할 수 있는 네트워크 보안 기술 및 독자적인 보안시스템들의 개발은 필수적이며, IPv6 환경에서 발생 가능한 네트워크 공격 방법과 대응 방안에 대한 핵심기술 확보는 인터넷 보안 기술의 수준을 한 단계 향상 시켜줄 것이다.

이제 이러한 기술을 바탕으로 IPv6 기반의 차세대 인터넷 보안 분야에서 선도적인 위치를 점할 수 있는 기틀을 마련할 것이며 안전한 네트워크 인프라 제공에 기여 할 것으로 기대한다.

[참 고 문 헌]

[1] IPv6 보안기술 해설서, 한국정보보호진흥원, 2005.10.

[2] 2005 IPv6 동향, 정보통신부/한국전산원, 2005.12.

[3] BcN 동향 2005, 정보통신부/한국전산원, 2005.12.

[4] 임재덕, 김기영, "리눅스 시스템 기반의 IPv6 네트워크 보안", 한국정보보호학회지, 2005.4.

[5] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC2460, Internet Engineering Task Force, December 1998.

김기영

1988년 전남대학교 전산통계학과 졸업
1993년 전남대학교 전산통계학과 석사
2002년 충북대학교 전자계산학과 박사
1988년 ~ 현재 한국전자통신연구원 보안운영체연구팀 팀장/책임연구원
관심분야 : 네트워크보안, 고성능 네트워크 침해탐지 및 대응기술, IPv6 보안기술

정보흥

1996년 인하대학교 전자계산공학과 졸업
1998년 인하대학교 전자계산공학과 석사
2002년 인하대학교 전자계산공학과 박사
2002년 ~ 현재 한국전자통신연구원 보안운영체제 연구팀 선임연구원
관심분야 : 네트워크보안, IPv6 보안기술

장종수

1984년 경북대학교 전자공학과 졸업
1986년 경북대학교 전자공학과 석사
2000년 충북대학교 컴퓨터공학과 박사
1989년 ~ 현재 한국전자통신연구원 네트워크보안 그룹장/책임연구원
관심분야 : 네트워크보안, 고성능 네트워크 침해탐지 및 대응기술, 정보보호