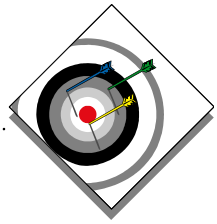


포/커/스

라우터 보안 기술 동향

정보흥* 김정녀** 장종수***

전통적으로 라우터는 패킷의 포워딩을 목적으로 개발된 제품이며, 내부 네트워크와 외부 네트워크를 연결해 주는 중요한 장비이다. 그러나, 최근들어 인터넷 웜 및 침해사고의 유형이 단순 호스트 공격의 특징에서 DoS 및 웜, P2P 등의 다양한 트래픽에 대한 과부하를 발생하는 형태의 공격으로 발전하고 있어 네트워크 보안을 유지하기 위해서는 전통적인 라우터의 접근제어(Access Control: AC)로는 처리하기 힘든 문제점이 있다. 본 고에서는 네트워크 장비로서의 중요성뿐만 아니라 향후 네트워크 보안을 위한 핵심장치 중 하나인 라우터 보안 기술 동향에 대하여 설명한다. ▧

목 차

* ETRI 보안운영체제연구팀/선임연구원
** ETRI 보안운영체제연구팀/팀장
*** ETRI 네트워크보안그룹/그룹장

Ⅰ. 서 론

지금까지의 해킹, 바이러스, 웜과 같은 네트워크 위협의 특징은 버퍼 오버플로, 웹 공격(CGI Attack) 등과 같이 특정 시스템이나 프로토콜의 취약점을 공격하는 형태 또는 서비스 거부 공격(Denial of Service: DoS), 분산서비스 거부 공격(Distributed DoS: DDoS)과 같이 과부하 네트워크 트래픽을 통한 공격의 형태를 가졌다. 그러나, 점차적으로 이러한 위협이 자동화, 분산화, 은닉화, 복잡화, 신속화된 형태로 발전해 가고 있으며 최근에는 웜이 이러한 특징을 수용하여 급속도로 퍼지고 있어 라우터, 방화벽과 같은 단일장비 또는 바이러스 월, 침입탐지 시스템과 같은 단일 보안 솔루션으로 차단하기 힘들어지고 있는 상황이다. 또한, 이러한 웜은 <표 1>에서 보는 바와 같이 E-mail 이나 P2P 와 같이 일반사용자들이 일

상적으로 사용하는 서비스를 대상으로 하고 있어 발생시 그 피해 정도가 심각하다는 특징을 갖는다[1]. 한 예로 '1.25 대란'으로 더욱 잘 알려진 'SQL 슬래머 웜' 같은 경우, 위에서 언급한 특징들을 가지고 있으며, 정통부에 의하면 당시 수 분만에 전세계적으로 7 만 5,000 여 개의 시스템을 감염시켰고 국내의 경우 그 피해의 정도가 더 심한 것으로 알려져 있다. 이 웜은 스위치, 라우터, 방화벽, 침입탐지 시스템, 바이러스 월과 같은 네트워크 장비 및 보안 솔루션을 무력화 시킬수 있도록 자동화된 방법으로 대용량 패킷을 발생시켜 그 피해 정도가 더 심했던 것으로 알려져 있다. 따라서, 최근에는 네트워크 장비와 보안 솔루션의 영역 구분이 모호해져 가고 있으며 네트워크 장비들이 이러한 위협에 대응할 수 있는 보안 기술을 수용하여 발전하고 있는 추세이다. 여기서는 대표적인 네트워크 장비 중의 하나인 라우터를 중심으로 네트워크 보안 기술과 향후 발전방향에 대하여 설명한다.

<표 1> 최근 웜의 동향

Category of Worm	1998	1999	2000	2001	2002	2003*
Traditional	1	1	0	10	3	4
Windows File Sharing	0	7	14	20	28	80
E-mail	1	18	44	93	159	192
IRC	1	16	42	23	45	84
Peer-to-Peer	0	0	1	1	44	128

* 2003 figures are projected form actual lst quarter totals

II. 라우터 보안 기능

라우터는 네트워크와 네트워크간의 데이터 전송을 위해 최적 경로를 설정해 주는 네트워크 장비로 IP 패킷을 입력 링크(네트워크 카드)군으로부터 출력 링크군으로 전달함으로써 인터넷

<표 2> SPR 의 기능별 수익과 점유율 (단위: 백만 달러, %)

	1 사분기	2 사분기	3 사분기	4 사분기	2002
Core	227	196	182	194	798
Edge	353	320	289	272	1,233
Total	579	516	471	466	2,032
Relative Contribution(%)					
Core	39	38	39	42	39
Edge	61	62	61	58	61
Total	100	100	100	100	100

<자료>: Gartner Dataquest, June 2003

네트워크 구성 요소들을 연결해 주는 장치이다[2],[3].

라우터는 적용되는 영역에 따라 액세스 라우터, 엔터프라이즈 라우터 및 백본 라우터 등으로 구분되고 있으며, 시스템의 규모와 성능에 따라 소형 라우터, 고속 라우터, 초고속 라우터 등으로 구분되기도 한다. 이 중 ISP(인터넷 서비스 제공업자)를 위한 용도로 사용되는 액세스 라우터는 SPR(Service Provider Router)라고 불리우며 대부분의 보안 기술은 이 라우터에 적용되는 추세이다. 2003 년도 가트너 발표자료에 의하면 <표 2>에서 보는 바와 같이 SPR 의 판매액과 점유율이 Core 라우터에 비해 높으며 향후 더 핵심적인 역할을 수행할 것이라고 예측하고 있다[3].

라우터에 대한 보안 위협은 다양한 형태를 가지며 공격 기술도 패스워드 유추, 라우팅 프로토콜 공격, SNMP 공격, 서비스 거부 공격 등과 같이 다양하다. 이러한 위협에 대응하기 위한 일반적인 라우터 보안 기술로는 사용자 인증 기술, 접근제어 기술, 감사추적 기술 등이 있다[4], [11]. 사용자 인증 기술은 비인가된 접근을 막는 가장 근본적인 방어방법의 하나로 대부분의 라우터 시스템에서 패스워드의 형태로 제공된다. 그러나, ‘adminpass’와 같은 단순 텍스트 형태의 패스워드는 화면에 타이핑되는 경우 또는 네트워크 트래픽을 도청하는 경우 쉽게 유출될 수 있어 안전하다고 할 수 없다. 대부분의 상용 라우터 제품들은 이를 방지하기 위해 MD5 알고리즘 등을 이용하여 암호화하여 제공하고 있다. 감사추적 기술은 로그 시스템 에러, 네트워크와 인터페이스 상태 변환, 접속실패, 접근통제 기록을 비롯해서 많은 종류의 이벤트를 기록하기 위한 기술이다. 이러한 이벤트는 일반적으로 로그 메시지의 형태로 사용자 콘솔, 터미널 라인, 버퍼, syslog, SNMP trap 등의 방법으로 중앙의 서버에 저장하고 이를 모니터링에 사용하는 방법을 사용한다. 접근제어 기술은 라우터에서 통과시켜야 할 트래픽과 차단해야 할 트래픽을 통제하기 위한 것으로 접근 제어 리스트(Access Control List)를 이용한다. 이 리스트에는 IP 헤더의 근원지 주소/포트, 목적지 주소/포트, 프로토콜에 대한 정보가 있어 이를 이용하여 트래픽을 통과(Accept), 차단(Deny) 등의 기능을 수행한다.

최근에는 다양하고 급속도로 발전하는 네트워크 보안 위협과 인터넷 웜 등에 대응하기 위해 점차적으로 방화벽, VPN(Virtual Private Network), IDS(Intrusion Detection System), 바이러스 월(Virus Wall), 네트워크 트래픽 모니터 등과 같은 보안 솔루션의 보안 기능이 라우터에 적용되어지고 있다.

1. IP 스푸핑 방지

라우터 제조업체를 중심으로 연구 및 개발되어 현업에서 사용되고 있는 상용 라우터에 적용된 스푸핑 방지 기술은 크게 3 가지 기술이 있다. 첫 번째는 규칙기반 패킷 필터링, 두 번째는

MAF(Martian Address Filtering) 및 SAV(Source Address Validation), 마지막으로 MAC 주소와 IP 주소간 바인딩 기술이다[9],[10]. 이중 규칙기반 패킷 필터링은 앞서 설명하였기 때문에 여기서는 두 번째와 마지막 방법에 대해서 설명한다.

두 번째 방법은 RFC1812 에 명시된 IP 스푸핑 방지 기술로서 각각에 대하여 명시된 내용을 살펴보면 다음과 같다. Martian Address Filtering 은 출발지 IP 주소가 유효하지 않은 주소 혹은 네트워크 주소로 설정되어 있는 어떠한 패킷에 대해서도 포워딩하지 말아야 할 것을 규정하고 있다. 또한, 출발지 IP 주소로 127 번 네트워크 주소를 가진 패킷 중에서 루프백 인터페이스를 제외한 어떠한 패킷도 포워딩하지 말아야 할 것을 규정하고 있다. Source Address Validation 은 라우터에 수신한 패킷의 출발지 IP 주소와 라우팅 테이블에 명시되어 있는 네트워크 인터페이스를 비교한 결과를 기준으로 필터링할 수 있는 기능을 구현해야 한다고 규정하고 있다. 이 필터링 기능이 활성화되어 있을 때 출발지 IP 주소에 도달할 수 있는 인터페이스와 상이한 인터페이스로 패킷이 수신되었을 경우 라우터는 해당 패킷을 폐기해야 한다. 즉, 만일 라우터가 수신한 패킷의 출발지 IP 주소로 특정 인터페이스를 이용하여 전달할 수 없다면 라우터는 해당 주소를 믿지 말아야 한다는 의미이다. 예를 들어 설명하면, 라우터의 네트워크 인터페이스 1 번으로 올 수 있는 IP 주소의 범위가 129.20.10.xx 인 경우 들어온 패킷이 129.20.20.xx 의 IP 주소 범위를 가지게 된다면 이 패킷은 스푸핑 되었을 가능성이 높기 때문에 라우터에서 그 패킷을 폐기해야 한다는 것이다.

마지막 방법인 MAC 주소와 IP 주소간 바인딩 기술은 ISP 가 제공하는 인터넷 서비스 가입자의 NIC(Network Interface Card)가 갖는 MAC 주소와 가입자에게 할당된 IP 주소간 바인딩 내역을 라우터에서 관리하면서, 가입자가 보낸 패킷의 MAC 주소와 출발지 IP 주소간 바인딩 내역이 라우터에서 관리하는 바인딩 내역과 일치하지 않을 경우, 위장된 패킷으로 판단하여 차단하는 기술로 ISP 의 POP(Point of Presence) 영역에 설치되는 라우터에 주로 적용된다. 상용 라우터 제품들을 예로 들면 시스코 시스템즈의 라우터인 경우 Unicast RPF 기능으로 구현되어 있으며, 쥬니퍼 네트워크의 라우터인 경우 MAC Address Validation 기능으로 구현되어 있다.

2. 가상 사설망

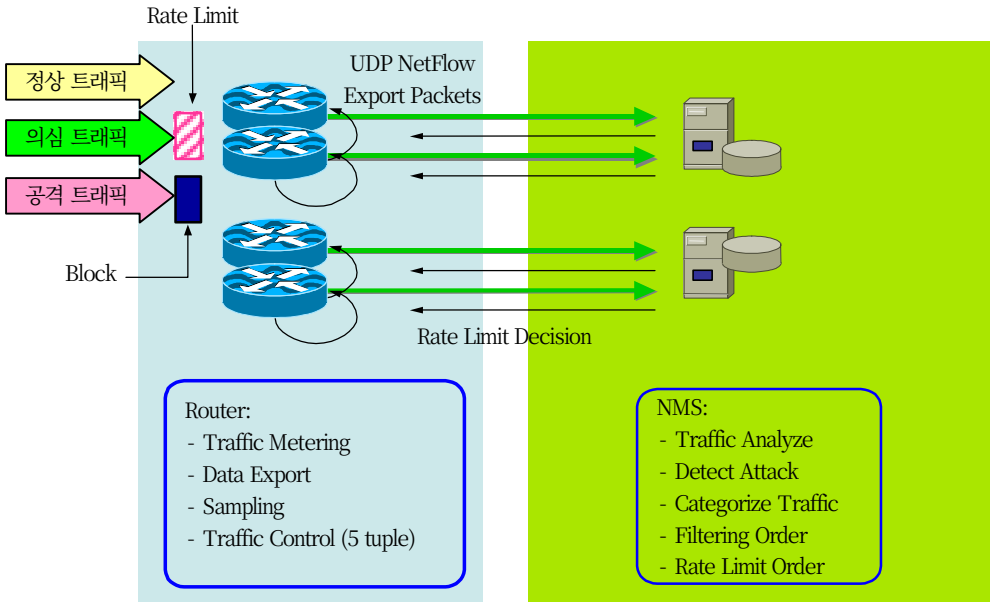
가상 사설망(VPN)을 간략하게 설명하면 인터넷망과 같은 공중망을 사설망처럼 이용해 회선 비용을 절감할 수 있는 기업통신 서비스이다. 특징으로는 전세계가 공유하고 있는 인터넷망을 전용선처럼 사용할 수 있도록 특수통신체계와 암호화기법을 제공하는 차세대 서비스로 기업 본사와 지사 또는 지사간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 전용선에 비해 20

80% 이상의 비용을 줄일 수 있다. 그러나, 공중망을 이용하여 데이터를 송신하여 모든 사람에게 정보가 노출될 수 있기 때문에 데이터를 송신하기 전에 데이터를 암호화하고 수신측에서 이를 복호화하는 보안 기술이 사용된다. 이러한 이유로 가상 사설망 기술은 보안 솔루션에 먼저 적용되어 활발하게 사용되어져 왔다. 그러나, 보안 솔루션을 이용한 가상사설망 서비스 제공에는 이미 설치된 네트워크 장비 이외에 부가적인 장치가 필요하다. 최근에는 라우터에서 이러한 서비스를 제공하여 경제적 부담 및 네트워크 보안성을 강화하기 위한 노력이 진행되고 있다. 그 예로서 대부분의 라우터 장비 업체에서는 VPN 서비스를 기본적으로 제공하거나 하드웨어 가속 보드 형태로 제공하여 좀 더 높은 보안성을 제공하는 라우터 제품들을 출시하고 있다.

VPN 기술은 일반적으로 3DES, MD5 등의 암호화 방법과 안전한 채널 생성 및 관리를 위해 IPSec 을 사용한다. DES 는 1970 년대에 미국 국립 표준 기술 연구소(National Institute of Standards and Technology: NIST)에 의해 신뢰할 수 있고 안전한 데이터 교환에 사용할 수 있는 표준 암호화 방법의 하나로 개발되었다. 초기에는 56 비트 암호화에서 128 비트 암호화 방식으로 그 복잡도가 증가하고 있으며 최근에는 좀 더 안전한 암호화를 위해서 3 중으로 DES 를 수행하는 3DES 가 보편적으로 사용되고 있다[6]. MD5 는 디지털 데이터 전송에 있어서 인증을 위해 사용되고 데이터 무결성을 유지하기 위한 암호학적 체크섬의 기능을 수행한다. 체크섬(checksum)이라는 것은 네트워크상에서 데이터 전송시 네트워크 오류 등과 같은 이유로 바뀌어진 데이터를 알아내기 위해 방법이다. 이러한 방법을 통해 전송되는 데이터의 내용이 고의적으로 수정되었는지 쉽게 알 수 있고 암호화하여 전송하여 안전한 전송채널을 보장할 수 있다는 장점을 가진다. IPSec 은 앞서 설명한 암호화, 인증방법을 이용하는 AH, ESP 와 채널설정을 위한 키교환 방법인 IKE 등을 사용하여 전송되는 데이터의 인증, 기밀성, 무결성, 재전송공격에 대한 보호, 그리고 트래픽 흐름분석을 막는 역할을 제공하기 위한 기술이다.

3. 트래픽 제어

트래픽 제어 기술을 간략히 설명하면 (그림 1)과 같이 라우터를 통과하는 네트워크 패킷을 정상 트래픽과 그 외의 트래픽으로 분류하여 이들 트래픽 중 일부를 차단하거나 그 양을 조절하는 기능을 말한다. 이 기술은 네트워크 관리 및 네트워크 장치와 그들의 동작을 감시, 통제하는 표준 프로토콜인 SNMP(Simple Network Management Protocol)에 근간하여 동작한다. 또한 이들 데이터는 네트워크의 상태를 측정, 분석하여 향후 네트워크 문제점을 예견하기 위한 응용 프로그램인 Netflow, MRTG(Multi Router Traffic Grapher)와 같은 NMS(Network Management System)에 사용되어지며 이를 위한 데이터의 관리 및 프레임워크에 대한 사항은 RFC 1757



(그림 1) 트래픽 제어 기술의 개념도

RMON(Remote network MONitoring)에 표준으로 정의되어 있다. 트래픽 제어 기술은 최근과 같이 불필요한 패킷 또는 악의적인 의도를 가진 공격 패킷이 범람하여 개별호스트의 속도를 느리게 만들거나 라우터에 과부하를 발생시키는 경우에 사용되어진다. 즉, 단위시간 동안 일정량 이상의 패킷이 라우터로 들어올 경우, 일정량 이상의 패킷은 통과시키지 않도록 한다는 것을 의미하며 Rate limiting 이라고도 한다. 이를 위해서는 트래픽 분류 및 측정이 선행되어야 한다. 트래픽 분류라는 것은 트래픽을 TCP, UDP, ICMP, IP 등의 프로토콜 또는 FTP, TELNET 등의 서비스별로 분류할 수 있는 능력을 말한다. 다음으로 이들 트래픽이 단위시간 동안 얼마나 통과하는지를 측정한다. 이러한 기법을 이용하여 라우터에서 트래픽 제어 기술이 활용되고 있으며 시스코의 경우 'CAR(Committed Access Rate)'으로 쥬니퍼의 경우에는 'Rate-limit'의 형태로 제공되고 있다[5],[11].

4. 콘텐츠 필터링

콘텐츠 필터링은 네트워크 패킷의 내용에 따라 다양한 네트워크 트래픽을 분류하여 서비스별로 차등화된 네트워크 품질을 제공하는 QoS(Quality of Service)적인 측면과 최근의 CodeRed, Nimda 등과 같은 웜 형태의 공격을 라우터에서 차단하는 수단으로 제공되는 측면이 있다. 먼저, QoS 적인 측면에 앞서 설명한 트래픽 분류 기술과 유사한 특징을 가진다. 즉, 동적으로 할당된

TCP/UDP 포트번호를 가진 애플리케이션 분류, URL, HOST, MIME 타입에 의한 HTTP 트래픽 분류 등의 다양한 기능을 수행한다. 웜 형태의 공격 차단 측면은 패턴매칭 알고리즘을 이용하여 바이러스 월이나 침입탐지 시스템과 같은 보안 솔루션이 수행하는 기능을 일부 수용한 것이라고 할 수 있다. 이는 최근에 웜 형태의 공격 수단이 파괴적인 전파력과 치명적인 피해를 주는 특징 때문이다. 즉, 호스트 또는 침입탐지 시스템이 이를 탐지한 경우 웜이 이미 네트워크내 대부분의 호스트에 전파된 뒤라고 생각해도 무방하기 때문이다. 따라서, 네트워크의 진입 관문인 라우터에 이들 웜을 차단하는 기능이 더욱 더 요구되어지고 있으며 대부분의 라우터 업체에서 이 기능을 채용하고 있다.

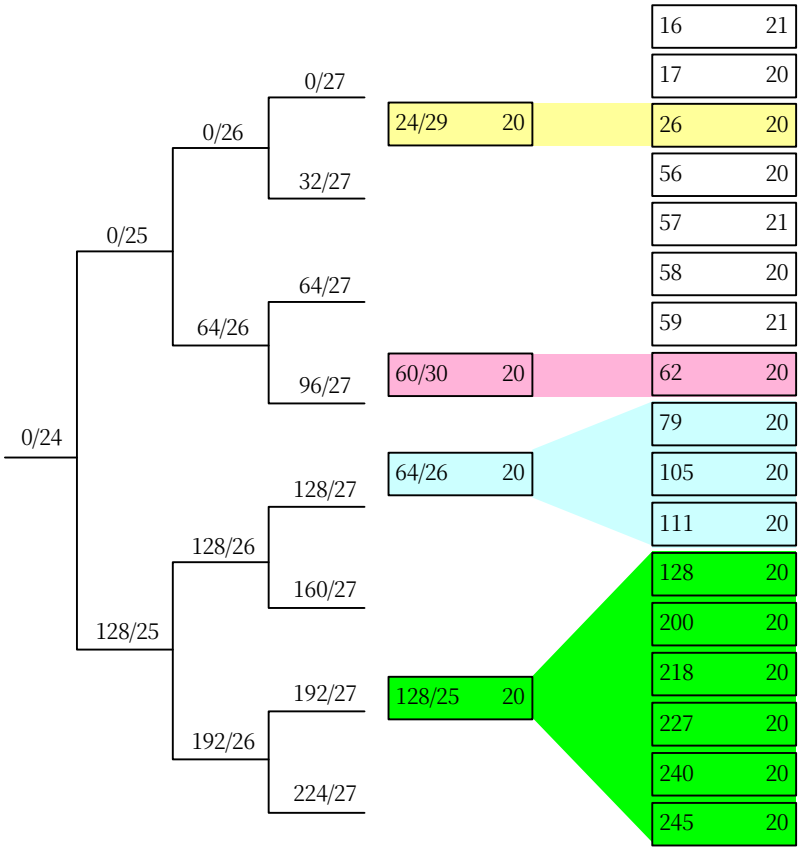
III. 최근 라우터 보안 기술 연구 동향

최근 라우터 보안 기술에 대한 연구 동향은 크게 S/W 측면의 접근과 H/W 측면의 접근으로 구분할 수 있다. S/W 측면에서는 공격 패킷을 역추적하기 위한 확률적 패킷 마킹(Probabilistic Packet Marking: PPM)기법, ICMP(Internet Control Message Protocol) 메시지를 이용하는 역추적 방법, 해시 함수를 이용하여 역추적을 수행하는 Hash-based IP 역추적 방법, 패킷의 TTL 값을 이용하여 IP 스푸핑을 방지하기 위한 TTL based Hop-Count computation 방법 등과 같이 다양한 분야에서 라우터의 보안성을 높이기 위한 연구가 활발히 진행되고 있다[7],[9],[10],[12],[13]. H/W 측면에서는 라우터 보안 기술이 S/W 적인 기술에서 점점 더 H/W 적인 기술로의 변화를 추구하고 있다고 할 수 있다. 즉, VPN 기능과 같은 경우 S/W 적으로 제공하기도 하지만 ASIC 등을 이용한 전용 보드로 제작하여 라우터에 슬롯 형태로 추가하여 사용하는 형태를 취하고 있으며 더욱이 암호화 기능의 경우에는 암호화 칩을 사용하는 경우가 일반화되어져 가고 있는 실정이다.

1 TTL based Hop-Count computation 방법

TTL based Hop-Count computation method 는 패킷 헤더의 각 항목들이 공격자에 의해 위조될 수 있어도 패킷이 목적지에 도착할 때까지 거쳐야 하는 Hop 수는 변경될 수 없다는 사실을 이용한다. 즉, Hop 수는 IP 헤더의 TTL 필드를 참조하여 패킷이 목적지에 도착했을 때의 TTL 값(final TTL)과 출발지에서 설정된 TTL 값(initial TTL)의 차를 구하여 계산될 수 있는데, 이 때 출발지 주소와 initial TTL 필드를 비롯한 IP 헤더의 항목들은 공격자에 의해 위조될 수 있어도 목적지에 도착한 패킷의 final TTL 값은 패킷이 거치는 네트워크 인프라 및 해당 네트워

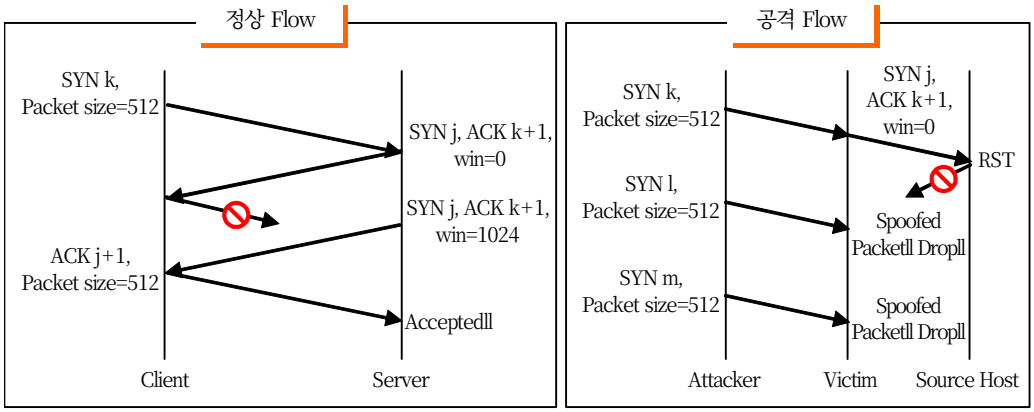
크의 라우팅 프로토콜에 의존하기 때문에 임의적인 변경이 불가능하다. 따라서 정상적인 두 호스트 사이의 네트워크 인프라에 큰 변화가 없다면 전달되는 패킷이 거치는 hop 수는 일정한 값을 가지게 되며 정상적인 hop 수를 거치지 않고 도착한 패킷은 spoofing 되었다고 볼 수 있다. 이 방법은 (그림 2)와 같이 TTL 의 hop 을 clustering 하여 도착한 패킷의 TTL 값과 비교하여 위조된 패킷을 분별한다.



(그림 2) IP spoofing 방지를 위한 Hop count clustering 개념도

2 TCP specific 방법

TCP specific method 는 (그림 3)과 같이 spoofing 된 패킷을 전송하는 공격자가 victim 의 응답패킷을 확인할 수 없다는 사실을 이용하여 공격자에게 TCP 헤더의 window size 필드가 작은 값으로 설정된 응답 패킷을 보냄으로써 IP spoofing 을 방지한다. 즉, victim 은 공격자가 spoofing 한 호스트 주소로 모든 응답 패킷을 전송하기 때문에 공격자는 victim 으로부터 자신이



(그림 3) TCP Specific 방법

보낸 패킷에 대한 어떠한 응답 패킷도 받아 볼 수 없게 된다. 따라서 victim 이 flow control 을 위해서 응답 패킷의 window size 필드를 변경해도 공격자는 이를 알지 못한다는 사실을 이용하면 IP spoofing 방지가 가능하다. 호스트는 자신에게 전송되는 모든 SYN 패킷의 첫 번째 응답 패킷(SYN/ACK)을 보낼 때 window size 를 작은 값으로 설정하여 전송함을 가정하기 때문에, 정상적인 수신자는 다음 패킷부터 window size 를 victim 이 설정한 값 이하로 조절하여 보내게 된다. 이때 정당한 window size 가 설정된 패킷을 보낸 수신자에게는 호스트가 window size 를 정상적인 값으로 증가시킨 패킷을 보내기 시작한다. 그러나 victim 이 설정한 window size 보다 큰 값으로 패킷을 전송하는 송신자는 victim 이 전송하는 SYN/ACK 를 받지 못하고 일방적인 패킷 전송을 한다고 볼 수 있으므로 비정상적인 사용자로 유추할 수 있다. 정상 시나리오와 공격 시나리오는 (그림 3)과 같다.

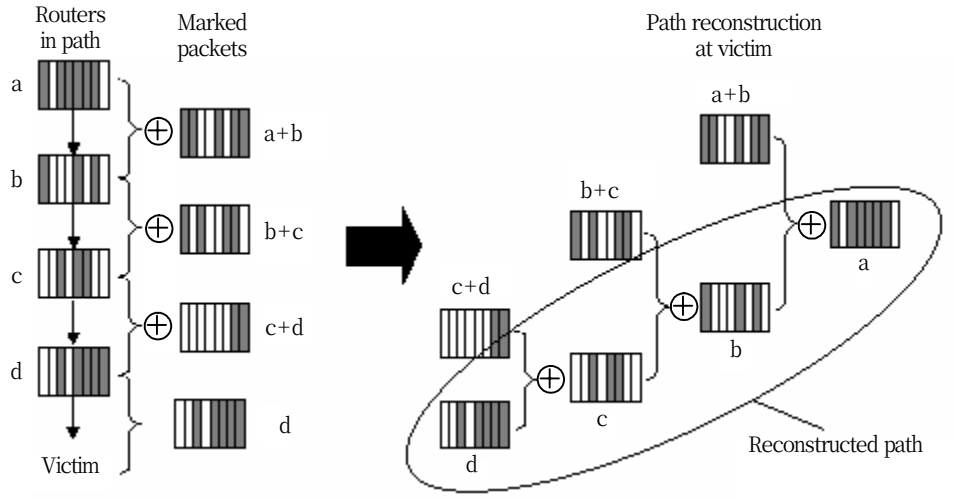
3. Automatic spoof detector

Automatic spoof detector 는 네트워크의 특정 호스트에 IP spoofing 을 방지하기 위해 설치되는 유틸리티의 일정으로 ARP 요청 패킷을 이용하여 같은 랜상에 존재하는 모든 호스트들의 MAC 주소와 IP 주소의 바인딩 목록을 관리함으로써 IP spoofing 을 방지한다[4]. 이 경우 우선 별도의 스캐닝 도구를 이용하여 랜의 IP 주소들을 수집하며, 추후 수집된 IP 주소로 ARP 요청 패킷을 전송함으로써 각 호스트들로부터 수신된 ARP 응답 패킷을 이용하여 MAC 주소와 IP 주소간 바인딩 내역을 생성할 수 있다. Automatic spoof detector 가 설치된 시스템은 랜상의 모든 패킷을 모니터링하여 관리되는 MAC 주소와 IP 주소간 바인딩 내역과 일치하는지 검사한다. 일치하지 않는 패킷이 발생할 경우 spoofing 된 패킷인지 정당하게 갱신된 바인딩 내역을 포함

한 패킷인지 결정하기 위하여 현재의 패킷 정보를 별도로 저장한 후 패킷에 설정되어 있던 출발지 IP 주소로 다시 ARP 요청 패킷을 전송한다. 만약 호스트가 이전에 별도로 저장된 패킷의 정보와 일치하는 ARP 응답 패킷을 전송한다면 이는 정당하게 바인딩 내역이 갱신된 것임을 의미하나, ARP 응답 패킷이 수신되지 않거나 이전에 저장된 패킷의 정보와 일치하지 않는 ARP 응답 패킷이 도착하는 경우에는 IP spoofing 이 발생한 것으로 간주하게 된다.

5. 확률적 패킷 마킹 방법

PPM(Probabilistic Packet Marking)은 지나가는 패킷을 확률적으로 마킹함으로써 이전의 역추적 방법에 비해 라우터의 오버헤드를 줄이고, 마킹 사이즈를 최대한 줄임으로 단편화에 의한 역추적 문제를 극복하기 위한 방법이다. PPM 은 패킷이 지나가는 경로에 이웃하는 두 라우터들이 일정한 확률을 가지고 패킷에 마킹을 하여 자신의 정보를 남겨두고, DDoS 공격이 발생하였을 때 victim 쪽에서 패킷에 마킹된 정보를 보고 공격 근원지를 알아내는 방법이다. 이때 라우터들이 모든 패킷에 마킹을 하는 것이 아니기 때문에 마킹을 하기 위한 라우터의 오버헤드를 줄일 수 있다. 그리고, 공격이 진행 중일 때 뿐만 아니라 공격이 끝난 후에도 역추적을 실시하여 공격지를 추적할 수 있기 때문에 역추적에 관한 매우 견고한 알고리즘이라고 할 수 있다. PPM 의 방법은 (그림 4)와 같다. 즉, (그림 4)에서 보는 바와 같이 각 라우터들은 미리 설정된 라우터별 해시값을 이용하여 패킷에 마킹을 한다. 라우터를 통과하면서 이전의 마킹값과 현재 패킷이 통과하는 라우터의 해시값을 XOR 연산을 수행하여 다시 패킷에 마킹을 한다. 따라서, (그림 4)



(그림 4) 확률적 패킷 마킹 방법

에서 보는 바와 같이 패킷이 목적지 라우터에 도착하면 이 과정을 역순으로 수행하게 되면 패킷이 지나온 경로를 알 수 있다. 물론, 각 라우터들은 다른 라우터의 해시값을 미리 알고 있어야 한다.

IV. 결 론

지금까지 살펴본 바와 같이 라우터의 보안 기술은 이전의 사용자 인증, 접근제어, 감사추적 기술에서 심화된 접근제어 기술, IP 스푸핑 방지 기술, VPN 기술, 트래픽 제어 기술, 콘텐츠 필터링 기술 등과 같이 다양한 기술이 적용되어지고 있다. 따라서 방화벽, 침입탐지 시스템, 바이러스 월 등과 같은 기존의 보안 솔루션과의 경계도 점차 모호해져 가고 있다고 할 수 있다. 그러므로, H/W 의 발전과 처리능력의 향상으로 향후에는 라우터와 같은 네트워크 장비가 보안 솔루션의 기능을 모두 수용할 것이라는 예측도 가능할 것으로 보인다. 또한, 라우터 보안 기술이 S/W 적인 기술에서 점점 더 H/W 적인 기술로 변화하고 있고 향후 점점 더 H/W 적인 형태로 발전하게 될 것이다. 즉, 고속 및 고대역화되어 가는 네트워크에 적용하기 위해서는 H/W 형태의 보안 기술이 더 요구되어질 것이다. 그러나, 이와 병행하여 다양한 분야에서 라우터의 보안성을 높이기 위한 연구가 활발히 진행되어야 할 것이다.

<참 고 문 헌>

[1] Darrel M. Kienzle, Matthew C. Elder, “Recent Worms: A Survey and Trends,” ACM WORM’03, 2003

[2] “Service Provider Router Trends and Outlook,” http://www.gartner.co.kr

[3] “Routers: Overview,” http://www.gartner.co.kr

[4] “Cisco Systems’ Intrusion Detection System,” http://www.gartner.co.kr

[5] “라우터를 이용한 네트워크보안,” http://www.kisa.or.kr/sis2003/data/program_9_seminar_6.JHC.pdf

[6] 정재원, 류대걸, 강한 공역, “보안과 암호화 모든 것,” 인포북, 2001.

[7] Cheng Jin, Haining Wang, Kang G. Shin. “Hop-Count Filtering:An Effective Defense Against Spoofed Traffic,” University of Michigan CSE Tech-Report, 2003.

[8] W.Richard Stevens: TCP/IP illustrated., Volume I – The Protocols, Addison-Wesley, 1st Edition, 1994.

[9] Steven J. Templeton, Karl E. Levitt., “Detecting Spoofed Packets,” In Proceedings of the Third DARPA Information Survivability Conference and Exposition(DISCEX III)’ 2003, 2003.

[10] http://www.www.anml.iu.edu/PDF/Automatic_Spoof_Detector.pdf

[11] http://www.cisco.com/kr

[12] Stefan Savage, David Wetherall, “Network Support for IP Traceback,” IEEE/ACM Trans. Net., Vol.9, No.3, June 2001.

[13] Alex.c.Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountie, Stephen T. Kent, and W. Timothy Strayer, “Hash-Based IP Traceback,” IEEE/ACM Trans. Net., Vol.10, No.6, 2002.