논문 99-24-12T-10 한국통신학회논문지 '99-12 Vol.24 No.12T

네트워크 침입차단시스템 서버 보호 기술에 관한 연구

정회원 김 점 구*, 이 영 철**, 이 재 광***

A Study on the Security Technique for Firewall Server

Jeom-Goo Kim*, Young-Chul Lee**, Jae-Gwang Lee*** *Regular Members*

요 약

침입차단시스템은 기관의 내부 네트워크를 외부의 신뢰할 수 없는 네트워크로부터 격리 보호를 목표로 설치하는 정보보호 시스템이다. 그러나 이러한 침입차단 시스템의 기본 목표는 날로 지능화 되어 직접 침입차단시스템의 서버를 공격하는 해커들의 해킹 기술에 무너지는 경향이 최근 들어 많이 발생되고 있다.

따라서 본 논문은 보다 안전한 침입차단시스템의 개발, 구축 그리고 관리를 위해서 해커의 불법적인 공격으로부터 침입차단시스템 서버를 안전하게 보호할 수 있는 침입차단시스템 서버 보호 기술을 제안하였다.

ABSTRACT

Firewall is information system protecting and isolating inner network in organization from outer unreliable network. But, nowadays they go on increasing in destroying tendency by hacker with hacking mechanism intruding into server in firewall.

Therefore, this paper suggest detection mechanism for sever in firewall safely to detect them from illegal intrusion by hacker and to develope, construct and control safer intrusion detection systems

Ⅰ. 서 론

컴퓨터 네트워크에서 일어나는 해커들에 의한 불법적인 침입, 중요 정보에 대한 도용, 오용 등과 같은 보안 사고가 더 이상 확대되지 않도록 막는데 사용되는 시스템을 침입차단시스템이라고 한다. 이러한 침입차단시스템은 기관의 내부 네트워크를 외부의 신뢰할 수 없는 네트워크로부터 격리(isolation), 보호(protection)하기 위해 설치한다. 즉, 허가되지 않은 외부 사용자가 내부 네트워크의 정보 자원에 접근하는 것을 막는데 있으며, 필요에 따라 내부 중요 정보의 불법적인 유출을 막는데 이용되기도 한다.[1][4][18]

침입차단시스템의 기본 목표는 기관의 네트워크와 외부 인터넷간의 트래픽에 대해 기관이 갖는 보안 정책에 따른 비인가 된 트래픽은 철저하게 막고, 단지 인가된 트래픽만을 허용하는 것이다. 일반적으로 기관의 내, 외부 네트워크간의 트래픽은 IP(Internet Protocol) 데이터그램에 의한 트래픽은 네트워크 레벨 트래픽이며, TCP나 UDP 패킷은 특정 응용 프로세스간의 접속(connection)과 상호 트래픽을 의미한다. 이때 정보의 교환을 위한 접속 정보는 상호 호스트간의 네트워크 주소(IP address)와 상호 응용에 관한 포트 번호(port number)로 이루어진다. 그래서 두 네트워크간의 인터페이스를 갖는 침입차단시스템은 이 정보를 이용하여 트래픽을 분류하고, 기관에서 필요한 정보보호 서비스를 제공하는 것이다. 일반적으로 이러한 정보보호 서비스에는 사용자 인증(authentication), 로그(logging), 응용 게이트웨이, 기밀성(confidentiality) 등이 있다.[13][17]

최근에 국내에서는 각 기관들이 인터넷/인트라넷 활

* 남서울대학교 컴퓨터학과(jgoo@nsu.ac.kr) ** 한국정보보호센터(yclee@kisa.or.kr)
*** 한남대학교 컴퓨터공학과(jklee@netwk.hannam.ac.kr)
논문번호 : 99034-0928 접수일자 : 1999년 9월 28일

용이 급격하게 늘어나고 있으며, 이러한 인터넷/인트라넷 구축, 운용시 정보보호를 위한 보안 시스템으로 침입차단시스템을 많이 이용하고 있다. 하지만 날로 지능화 되어 가는 해커에 의한 해킹 기술은 이러한 침입차단시스템을 우회하는 시도보다는 침입차단시스템 기능을 수행하는 서버 시스템을 직접 공격하여 내부 망에 침입하려는 시도가 늘고 있다. 따라서 보다 안전한 침입차단시스템을 개발하기 위해서는 침입차단시스템 서버에 대한 불법적인 공격으로부터 서버를 안전하게 보호할 수 있는 기술이 요구된다.[4]

본 논문에서는 보다 안전한 침입차단시스템을 개발, 구축 및 관리를 위하여 해커의 불법적인 공격으로부터 침입차단시스템 서버를 안전하게 보호할 수 있는 보호 기술과 침입차단시스템과 침입차단시스템, 침입차단시스템과 사용자간의 중요 정보 전송시 효과적으로 보호할 수 있는 암호화 응용 기술과 침입차단시스템 구조 및 프로토콜을 기반으로 한 강력한 사용자 인증, 로그, 액세스 제어(access control), 응용 게이트웨이, 기밀성 기능을 갖는 침입차단시스템 서버 보호 기술을 제안한다.

Ⅱ. 침입차단시스템 보안 취약점

침입차단시스템 보안 취약점은 시스템 구현상의 취약점, 시스템 구성상의 취약점, 그리고 시스템 자체적인 취약점으로 나눌 수 있다. 침입차단시스템 구현상의 취약점은 벤더들에 의해 개발된 프로그램상의 문제점이며, 침입차단시스템 구성상의 취약점은 각 기관의 정책에 따라 구현된 침입차단시스템 구성상에 존재하는 문제점이다.

마지막으로 침입차단시스템을 장착한 시스템 자체적인 보안 취약점은 시스템에 운영중인 운영체제, 네트워크 서비스 프로그램, 기타 운영 프로그램 등의 보안 취약점으로 본 논문에서는 주로 침입차단시스템 구성상의 취약점을 분석한다. 이와 관련하여 구분하면 네트워크 관련 취약성, 서비스 포트의 공격 그리고 서비스 거부공격에 대한 취약성으로 구분할 수 있다.[7]

2.1 네트워크관련 취약성

네트워크관련 취약성은 일부 시스템 자체적인 취약성과 중복이 되는 듯 하나 본 논문에서는 특히 침입차단시스템이 구성될 경우 네트워크 관련 부분에서 보안상의 허점이 될 수 있는 기능으로 IP Source Routing, 순서번호 추측 공격 등을 분석하였다.

(1) IP Source Routing

정보의 전달방법 중 인터네트의 표준인 RFC문서에 의하면 응용프로그램이 source route된 데이터를 받으면 이를 통해 지정된 라우트 주소 리스트를 이용하여 반대순서로 응답을 보내도록 되어있다. 이를 악용하여 해커들은 라우팅 정보를 수정하여 침입차단시스템을 넘어가고자 한다. 이 방법은 strict source routing과 loose source routing 두 가지 경우로 나누어 볼 수 있다.

1) Strict source routing

이 경우, 패킷이 지나갈 경로가 지정되면 반드시 해당 경로를 통과해야 한다. 실패할 경우 ICMP "source route failed" 에러가 되돌아온다.

2) Loose source routing

이 경우, 패킷이 지나갈 경로가 지정되면, 반드시 해당 경로를 거쳐야 하지만, 경로상의 두 주소사이에 다른 라우터를 통과할 수 있다.

(2) 순서번호 추측(Sequence number Prediction) 공격

TCP 프로토콜을 이용한 통신에서는 연결의 신뢰를 이용하여 순서번호를 이용한다. 이 순서번호의 범위는 0 - 4,294,967,295 으로 많은 시스템에서 이 번호의 추측이 가능하다. 그 이유는 4.4 BSD의 경우 시스템 초기화할 때 1로 설정된 번호는 1/2초마다 64,000증가(1초에 128,000증가)하고 매 연결 시마다 64,000만큼 증가한다. 9.5시간에 한 사이클을 돌게된다. 해커는 이를 이용하여 번호를 알아낸 후 다양한 공격을 할 수가 있다.

(3) RIP(Routing Information Protocol) 공격

RIP 공격이란 데이터전송에 필요한 라우팅 정보를 변경하는 것을 말한다. 이는 데몬이 시작되면 각 인터페이스로 RIP request (for a complete routing table)를 브로드캐스팅으로 보내며, 응답을 받으면 자신의 라우팅 테이블을 변경한다. 매 30초마다 라우팅 정보의 수정이 주변 라우터사이에 일어난다. 이때 발생할 수 있는 것은 공격자에 의해 수정된 정보가 올 경우도 이를 믿고 라우팅 정보를 수정하는 것이다.

2.2 응용 서비스 포트 취약점

서비스 포트에 대한 취약성은 일반적으로 불필요한 포트를 열어 놓았을 경우 발생하며, 다른 방법은 데이터 전송 시 출발지의 포트번호를 변경하여 전송하는 공격 방법이다.

(1) TCP Port Stealth Scanning

이 방법은 시스템에 불필요하게 제공되거나 열려있는 서비스 포트번호를 점검하는 것이다. 이 점검 방법은 두 가지가 있으며 다음과 같다.

1) Half Open Scan

침입차단시스템에 SYN 패킷을 보낸다. SYN/ACK가 되돌아오면 포트가 열려있음을 나타내고 RST이 돌아오면 포트가 닫혀있음을 나타낸다.

2) Stealth Scan

FIN 패킷을 보내어 되돌아오는 정보를 이용하여 열려있는 포트번호 점검이 가능하며, 다음으로는 ACK 패킷을 보내어 검토한다. 이는 윈도우 크기가 0 이상이거나 돌아온 패킷의 ttl 이 다른 RST 패킷들 보다 더 낮은 경우 포트가 열려있다. 일반적으로 패킷이 인터페이스를 통과할 때마다 ttl이 하나씩 줄어든다. 포트가 열려있는 경우에 패킷을 받아 검사하게되면 ttl이 1 만큼 감소한다.

(2) Source Port Scanning

FTP 연결 시 21번 포트를 이용하지만 데이터 전송은 20번을 사용한다. 따라서 라우터나 침입차단시스템에서 20번 포트를 개방하는 경우가 많다. Source Porting은 이러한 취약점을 이용하여 공격자

```
# ftp             stream  tcp nowait  root        /usr/libexec/tcpd   ftpd -l          -A
# telnet          stream  tcp nowait  root        /usr/libexec/tcpd   telnetd
# shell           stream  tcp nowait  root        /usr/libexec/tcpd   rshd
# login           stream  tcp nowait  root        /usr/libexec/tcpd   rlogind  -a
# exec            stream  tcp nowait  root        /usr/libexec/tcpd   rexecd
# uucpd           stream  tcp nowait  root        /usr/libexec/tcpd   uucpd
# finger          stream  tcp nowait  nobody  /usr/libexec/tcpd fingerd
# tftp            dgram   udp wait    nobody  /usr/libexec/tcpd tftpd
# comsat  dgram   udp     wait  root      /usr/libexec/tcpd comsat
# ntalk           dgram   udp wait    root        /usr/libexec/tcpd   ntalkd
# pop             dgram   udp wait    root        /usr/libexec/tcpd   popper
# ident           dgram   udp wait    root        /usr/libexec/identd identd -l
# #bootp  dgram   udp     wait  root      /usr/libexec/tcpd bootpd -t 1
# echo            stream  tcp nowait  root        internal
# discard stream  tcp     nowait  root      internal
# chargen stream  tcp     nowait  root      internal
# daytime stream  tcp     nowait  root      internal
# tcpmux  stream  tcp     nowait  root      internal
# time            stream  tcp nowait  root        internal
# echo            dgram   udp wait    root        internal
# discard dgram   udp     wait  root      internal
# chargen dgram   udp     wait  root      internal
# daytime dgram   udp     wait  root      internal
# time            dgram   udp wait    root        internal
# kerberos authenticated servies
# klogin          stream  tcp nowait  root        /usr/libexec/rlogind rlgind -k
# eklogin stream  tcp     nowait  root      /usr/libexec/rlogind    rlgind -k -x
# kshell          stream  tcp nowait  root        /usr/libexec/rshd   rshd -k
# Services run ONLY on the Kerberos server
# krbupdatestream tcp     nowait  root      /usr/libexec/registerd  registerd
# kpasswd stream  tc
```

호스트의 20번 포트를 소스포트로 사용하여 침입차단시스템의 취약점을 알아낸다.

2.3 서비스거부공격 취약점

(1) echo, chargen etc. 공격

echo 및 chargen 서버는 받은 데이터를 그대로 되돌려 보내는 특성을 가진 프로그램으로 UDP 프로토콜을 사용한다. 이의 특성을 이용하여 공격자는 침입차단시스템에 공격하고자 하는 시스템의 IP주소와 포트번호를 속여 상대방에게 보내면 두 호스트는 끊임없이 데이터를 주고받게 되므로 제3자의 서비스 요청에 응하지 못하게 된다.

(2) Syslog Flood 공격

Syslog는 514번 포트를 이용하여 다른 시스템의 Syslog를 기록할 수 있는데 통신수단으로 UDP를 사용하여 쉽게 그 정보를 속일 수 있는 취약성이 있다. sysflood프로그램은 다량의 가짜 Syslog 데이터를 상대방 호스트로 보내는 공격이다.

Ⅲ. 침입차단시스템 서버 보호 기술 제안

3.1 불필요한 서비스 데몬과 포트 삭제

침입차단시스템 서버를 보호하기 위해서는 침입차단시스템을 구동하기 위한 데몬(demon)을 제외한 모든 불필요한 서비스 데몬을 제거한다. /etc/inetd.conf 파일을 편집해서, 아래와 같은 출력을 만든다. 이것은 시스템상의 로드를 줄이기 위한 것이다.

이러한 모든 서비스를 중단시키는 이유는 시스템에 침입차단시스템을 설치하여 구성할 때 보안 위협에 노출되는 가능성을 줄이기 위한 것이다. 또한 불필요한 포트로의 TCP 접속을 받아들이지 않아야 한다. 관리지원도구인 portscan을 이용하여 침입차단시스템으로 사용되는 호스트의 필요치 않은 포트를 모두 삭제하여 시스템 자체의 보안 수준을 높여야 한다.

3.2 라우팅 테이블 보안 정책

스크리닝 라우터의 라우팅 테이블은 외부 트래픽이 베스천 호스트에 전달되도록 구성해야 한다. 스크리닝 라우터의 라우팅 테이블은 침입이나 불법적인 변경으로부터 보호되어야 한다. 만약 라우팅 테이블의 기록이 변경되어서 트래픽이 베스천 호스트로 전달되지 않고 곧바로 접속된 내부 네트워크로 보내지면, 베스천 호스트는 우회되어 버린다.[11][19]

그림 1. 은 스크리닝 라우터의 라우팅 테이블이 베스천 호스트를 가리키는 상황을 나타내고 있다. 내부 네트워크 번호는 199.245.180.0이고, 베스천 호스트 IP 주소는 199.245.180.10 이다. 스크리닝 라우팅 테이블에 다음과 같은 기록을 가지고 있다.

Destination = 199.245.180.0

Forward to = 199.245.180.10

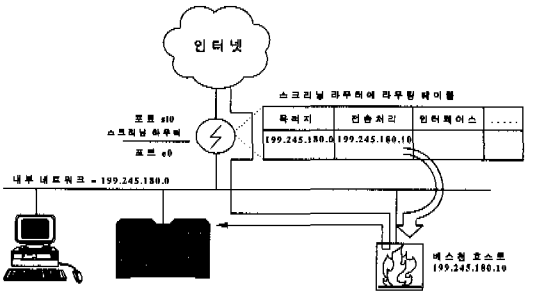


그림 1. 스크리닝 라우터의 라우팅 테이블의 정상적인 설정

네트워크 199.245.180.0에 대한 모든 네트워크 트래픽은 베스천 호스트의 IP 주소 199.245.180.10으로 전달된다.

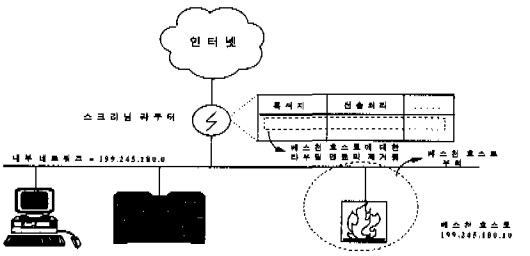


그림 2. 스크리닝 라우터의 라우팅 테이블이 깨졌음

그림 2. 는 스크리닝 라우터의 라우팅 테이블이 깨져서, 목적지 네트워크 199.245.180.0에 대한 기록이 삭제되었다. 네트워크 199.245.180.0에 대해 스크리닝 라우터가 받은 외부 트래픽은 베스천 호스트로 보내지지 않고 내부 네트워크의 로컬 인터페이스를 통하여 직접 보내진다.

베스천 호스트는 우회되고 스크리닝 라우터만이 유일한 방어선이 된다. 만약 스크리닝 라우터가 깨지면 위험 영역은 내부 네트워크로 확장된다.

만약 스크리닝 라우터가 ICMP(Internet Control Message Protocol) 재지정(redirect) 메시지에 대해 응답하면, 침입자에 의해 거짓 ICMP 메시지가 보

내질 위험이 있다. 그래서 ICMP 재지정 메시지에 대한 응답은 불가능하도록 해야 한다.

스크리닝 라우터가 정적 라우팅을 사용하도록 구성해야 한다. 정적 라우트는 라우팅 프로토콜에 의해 변하거나 소멸되지 않는다. 이것은 정적 라우트가 잘못된 라우트를 통고하는 것을 방지한다.

라우터에서 ARP, ICMP 재지정, 프럭시 ARP, MOP, ICMP 도착할 수 없는 메시지와 같은 처리를 불가능하게 해야 한다. 예를 들면 아래의 구성 명령문을 Cisco 라우터에서 사용할 수 있다.

```
no ip redirects
no ip route-cache
no ip proxy-arp
no ip unreachables
no mop enabled
no service finger
```

만약 스크리닝 라우터가 TELNET 접속을 지원하면, 이것을 불가능하게 해야 한다. Cisco 라우터에서, TELNET을 통한 원격 접속을 막기 위해 가상 터미널에서 접속 제어 목록을 설치할 수 있다.
정상적인 ARP 동작에서, ARP 표의 기록은 동적으로 만들어지고 설정된 시간이 지나면 없어진다. 수동으로 라우터와 베스천 호스트를 위한 ARP 캐쉬 표를 초기화해야 한다. 수동으로 만들어진 ARP 기록은 절대 지워지지 않고 'static' 기록으로 동작한다. 라우터에서 ARP 처리를 불가능하게 하면, 라우터는 ARP를 위한 하드웨어 주소를 할당하지 않는다.

3.3 침입차단시스템과 침입차단시스템의 암호화

본 논문은 그림 3.과 같이 침입차단시스템과 침입차단시스템간의 암호화를 위하여 비밀 키 암호화 시스템과 공개 키 암호화 시스템을 결합한 하이브리드 암호화 시스템을 이용하여 침입차단시스템 상호간의 사용자 정보 비밀성과 인증을 확립하고자 한다.

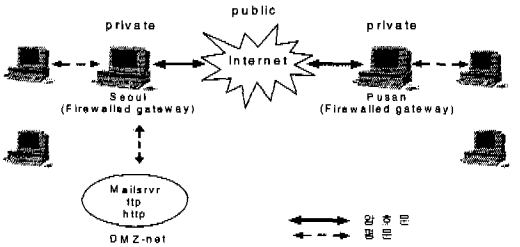


그림 3. 침입차단시스템과 침입차단시스템의 암호화

따라서 침입차단시스템 A와 침입차단시스템 B간의 안전한 통신을 위해서는 먼저 상호간의 키 보증을 확립할 수 있는 키 인증 센터를 두어야 한다. 하이브리드 암호화 방식은 ITU-T와 ISO에서 제안된 디렉토리 인증 골격의 세방향 강한 인증과 매우 유사하다.

(1) 키 등록 절차 : 먼저 그림 4.와 같은 키의 등록 절차가 필요하다.

1) 침입차단시스템 A와 침입차단시스템 B는 자신의 공개 키와 비밀 키를 발생시켜 자신의 공개 키인 Ap와 Bp를 키 인증 센터에 등록한다.

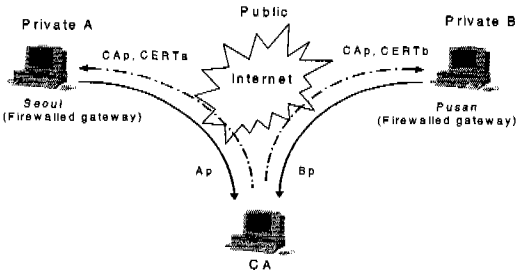


그림 4. 키 인증 센터와의 키 등록 절차

2) 키 인증 센터는 자신의 공개 키와 비밀 키를 발생시켜 자신의 비밀 키로 침입차단시스템 A, 침입차단시스템 A의 비밀 키, 인증서의 타당성 주기를 암호화하여 인증서 CERTa를 만든다. 또 자신의 비밀 키로 침입차단시스템 B, 침입차단시스템 B의 비밀 키, 인증서의 타당성 주기를 암호화하여 인증서 CERTb를 만든다.

3) 키 인증 센터는 공개 키 CAp와 CERTa를 침입차단시스템 A에게 전달하고, 공개 키 CAp와 CERTb는 침입차단시스템 B에게 전달한다.

(2) 침입차단시스템 상호 인증과 통신 절차

: 키 인증 센터에 의해 키 등록절차가 확립되면 침입차단시스템 상호 인증을 위해 그림 5. 와 같은 통신 절차를 따른다.

여기서 키 Ap를 이용한 메시지 M의 암호화는 Ap{M}로 표현한다. 그리고 A : 침입차단시스템 A를, Ap : 침입차단시스템 A의 공개 키를, As : 침입차단시스템 A의 비밀 키를 나타내고, Bp : 침입차단시스템 B의 공개 키를, Bs : 침입차단시스템 B의 비밀 키를, CAp : 인증 센터의 공개 키를 나타내며, CAs : 인증 센터의 비밀 키를, CERTa : 침

입차단시스템 A의 인증서를, TI : 인증서의 타당성 주기를, Ra, Rb, Rc : 카운터에 의한 순서부분을 이용한 난수를 나타낸다. 침입차단시스템 상호간의 인증과 키 비밀성을 위한 통신 프로시져는 다음과 같다.

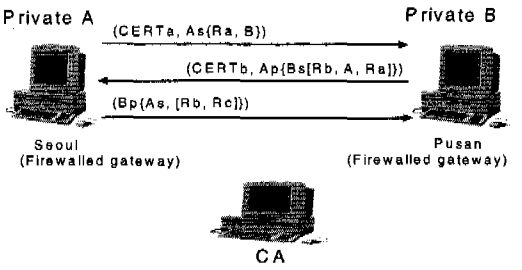


그림 5. 인증과 키 비밀성을 위한 통신절차

1) 침입차단시스템 A는 위조를 예방하고 재생 공격을 알아내기 위해 사용하는 난수 Ra를 만들어낸다. Ra는 카운터 A에 의해 생성된 순서부분에 포함되어있고, 모든 세션에서 매번 유일성에 대해 점검된다. Ra는 토큰의 한 부분이지만 암호화되지 않는 부분이기 때문에 비밀 키 암호에 대한 메시지 키로서만 사용되고 이 암호에 대한 비밀 키로는 사용되지 않는다.

2) 그러면 침입차단시스템 A는 다음 메시지를 침입차단시스템 B에게 보낸다.

CERTa, As { Ra, B }

3) 그러면 침입차단시스템 B는 다음 과정을 실행한다.

① CAp를 이용, 복호화하여 CERTa로부터 Ap를 얻는다. 그리고 침입차단시스템 A의 인 증이 만료되지 않았는지 점검한다.

② 서명을 검증하고 서명된 정보의 무결성을 점검한다.

4) 침입차단시스템 B는 Ra와 같은 목적으로 사용하기 위해 난수 Rb를 생성한다. 순서번호에 없는 이 숫자는 토큰의 서명되고 암호화된 토큰의 한 부분을 형성하기 때문에 비밀 키 부분을 형성하는데 이용될 수 있다.

5) 침입차단시스템 B는 침입차단시스템 A에게 다음 메시지를 보낸다.

CERTb, Ap { Bs (Rb, A, Ra) }

6) 침입차단시스템 A는 다음 과정을 실행한다.

① CAp를 이용하여 복호화하여 CERTb로부터 Bp를 얻는다. 그리고 침입차단시스템 B 의 인증서가 기간이 만료되지 않았는지 점검한다.

② 인증 토큰을 복호화한 다음 서명을 검증한다. 그리고 서명된 정보의 무결성을 점검 한다.

7) 침입차단시스템 A는 수신된 난수 Ra가 보낸 Ra와 동일한 지를 점검한다.

8) 그러면 침입차단시스템 A는 난수 Rc를 생성하고 점검한다. Rc는 비밀 키 암호 시스템에서 비밀 키를 위하여 Rb와 결합할 목적으로 생성하는 또 다른 난수이다. 일단 세션이 끝나면 이 생성된 세 개의 난수는 모두 없어지게 되고 단지 순서부분만 참조를 위해 기억시켜 둔다.

9) 침입차단시스템 A는 다음 인증 토큰을 침입차단시스템 B에게 보낸다.

Bp { As (Rb, Rc) }

10) 침입차단시스템 B는 다음 과정을 실행한다.

① 인증 토큰을 복호화하고 서명을 점검하고 서명된 정보의 무결성을 점검한다.

② 수신된 Rb가 보낸 Rb와 동일한 것인지 점검한다.

상호 인증이 확립된 후 그림 6. 과 같이 침입차단시스템 A는 Rb를 이용하여 메시지를 암호화한 후 침입차단시스템 B에게 전송하면, 침입차단시스템 B는 자신이 알고 있는 Rb를 이용하여 복호화를 한 후 메시지를 받아 볼 수 있다. 반대로 침입차단시스템 B는 Rc를 이용하여 메시지를 암호화한 후 침입차단시스템 A에게 전송하면, 침입차단시스템 A는 자신이 알고 있는 Rc를 이용하여 복호화한 후 메시지를 받아 볼 수 있다.

이 시스템의 장점은 침입차단시스템이 네트워크에서 상대방에 대한 공개 키를 인증할 때에 키 인증센터를 한번만 액세스하면 된다. 그래서 긴 디렉토리를 분배할 필요도 없고, 통신을 원할 때 on-line 키 분배 센터로부터 새로운 세션 키를 얻어야하는 결점(Bottleneck)도 없다. 또 다른 장점은 침입차단시스템 자신들이 직접 비밀 키와 공개 키를 생성할 수 있고, 키 인증센터가 할 수도 있다. 또 이 하이브리드 암호화 시스템을 이용하면 디지털 서명과 인증의 부가적인 장점을 갖는다. 이 하이브리드 암호화 시스템은 점-대-점, 패킷교환 통신, 전자우편

시스템과 같은 여러 가지 통신 시스템의 응용에 맞출 수 있다.

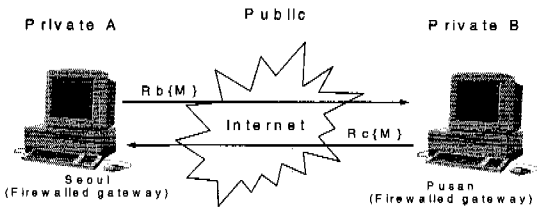


그림 6. 메시지 비밀성을 위한 통신절차

Ⅳ. 결 론

인터넷 응용 기술의 발달로 인터넷의 활용 범위가 점차 늘어나고 있으며, 활용 수요 또한 급격히 증가하고 있다. 반면에 각 기관들의 정보 시스템은 인터넷에 노출되어 해커들의 침입 위협을 받게되고, 침입을 당했을 경우는 신뢰와 막대한 자산이 순식간에 무너지게 될 것이다. 따라서 이러한 해커의 위협과 공격으로부터 각 기관의 정보 시스템의 보호를 위한 보안 시스템으로 침입차단시스템을 많이 이용하고 있다. 침입차단시스템의 기본 목표는 기관의 네트워크와 외부 인터넷간의 트래픽에 대해 기관이 갖는 보안 정책에 따른 비인가 된 트래픽은 철저하게 막고, 단지 인가된 트래픽만을 허용하는 것이다.

그러나 이러한 기능을 가진 침입차단시스템의 서버 자체를 직접 공격하는 해킹 방법에는 아주 취약한 면이 있어 본 논문에서는 해커의 불법적인 공격으로부터 침입차단시스템 서버를 안전하게 보호할 수 있는 기술로 침입차단시스템과 침입차단시스템, 침입차단시스템과 사용자간의 중요 정보 전송시 효과적으로 보호할 수 있는 암호화 응용 기술과 침입차단시스템 시스템 구조 및 프로토콜을 기반으로 한 강력한 사용자 인증, 로그, 액세스 제어, 응용 게이트웨이, 기밀성 기능 등의 정보보호 서비스를 제공하는 침입차단시스템 서버 보호 기술을 제안하였다.

향후 연구방향으로는 침입차단시스템과 침입차단시스템, 침입차단시스템과 사용자간의 정보보호를 위한 보다 강화된 침입차단시스템 보호와 성능 강화를 위한 모델 및 기법을 설계하고자 한다.

참 고 문 헌

[1] 시스템공학센터/ 연구전산망, 관리자를 위한 인터네트 보안 지침서, 1997

[2] 한국전산원, "전산망 보안을 위한 위험관리 지침서", 1994

[3] 한국정보보호센터, "'99 정보보호 심포지움", 1999

[4] 한국정보보호센터, "정보시스템 해킹 현황 및 대응", 1998

[5] 한국정보보호센터, "정보보호 총서", 1996

[6] 한국정보기술원, "Firewall 구축 세미나", 1996

[7] 한국정보보호센터, "정보시스템 침해사고 방지 기술 개발에 관한 연구", 1999

[8] 포항공과대학교, "Security+ for UNIX Ⅳ", 1999

[9] 이재광, 이용준, 박성열, "인터넷 방화벽과 네트워크 보안", 1996

[10] D. Brent chapman & Elizabeth D. Zuicky, "Buliding Internet FIREWALLS", O'Reilly & Associates, Inc, 1997

[11] Karanjit S. Siyan & Chris Hare, "Internet Firewalls and Network Security", NRP , 1997

[12] Robert B. Reinhardt, "An Architectural Overview of UNIX Network Security", Oct.8, 1992

[13] Simson Garfinkel & Gene Spafford, Practical UNIX Security, 1991

[14] William Cheswick & Steven Bellovin, Firewalls and Internet Security, 1994

[15] Rovert B. Reinhardt, "An Architectural Overview of UNIX Network Security, 1994

[16] David A Curry, "UNIX System Security : A Guide for Users and System Administra -tors", Addision-Wesley, 1992

[17] Carfinkel & Spafford, "Practical UNIX Security", O'Reilly & Associate, Inc., 1992

[18] Eugene II. Spafford, "The Internet Worm Program : An Analysis", Purdue Technical Report CSD-TR-823, Nov, 1988

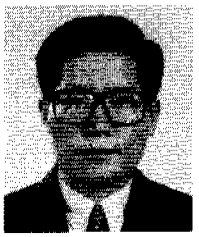
[19] Bill Cheswick, "The Design of a Secure Internet Gateway", AT&T Bell Lab. 1991

[20] Marcus J. Ranum, A Network Firewall, Digital Equipment Corp., 1992

[21] William R. Cheswick, Steven M. Bellovin,

Firewalls and Internet Security, Addison-Wesley, 1994
[22] BraCAstad, D. K., "CoCAsideratioCAs for security in the OSI architecture", IEEE Network Magazine, 1987.
[23] Derek ArkiCAs, Paul Buis, William Steen, "Internet Security", 1996

김 점 구(Jeom-Goo Kim)



1990년 광운대학교 전자계산학과 (이학사)
1994년 광운대학교 전자계산학과 (이학석사)
1999년 한남대학교 컴퓨터공학과 박사수료

1990년~1994년 (주)제성프로젝트 연구원
1995년~1998년 (주)시사컴퓨토피아 연구원
1999년~현재 남서울대학교 컴퓨터학과 전임강사
<주관심 분야> 컴퓨터 네트워크, 정보통신, 정보보호

이 영 철(Young-Chul Lee)

1988년 서울산업대학교 재료공학과(공학사)
1994년 광운대학교 전자계산학과 (이학석사)
1983년 4월~1996년 6월 시스템 공학연구소 연구원

1996년 7월~현재 한국정보보호센터 주임연구원
<주관심 분야> 정보보호, 컴퓨터네트워크

이 재 광(Jae-Gwang Lee)

1984년 광운대학교 전자계산학과 (이학사)
1986년 광운대학교 전자계산학과 (이학석사)
1992년 광운대학교 전자계산학과 (이학박사)

1986년~1993년 8월 군산전문대학 전자계산학과 부교수
1997년 미국 University of Alabama 객원교수
1993년 8월~현재 한남대학교 컴퓨터공학과 부교수
<주관심 분야> 컴퓨터 네트워크, 정보통신, 정보보호