인터네트 환경에서의 다단계 원격지 로그인 최초 사용자 확인 기법

o
윤기송
시스템공학연구소

Initial User Identification Scheme Using Multiple Internet Remote Login

Kisong Yoon
System Engineering Research Institute

요 약

인터네트에서는 Port Number를 이용하여 다양한 응용 서비스를 제공하고있다. 본논문에서는 인터네트 기본 서비스중 하나인 원격지 로그인기능을 이용하여 여러시스템을 경유한 사용자의 위치를 Port Number를 이용하여 파악하는 기법을 제시하고 효율성있는 추적기법 연구를 위한 문제점을 분석하고자 한다.

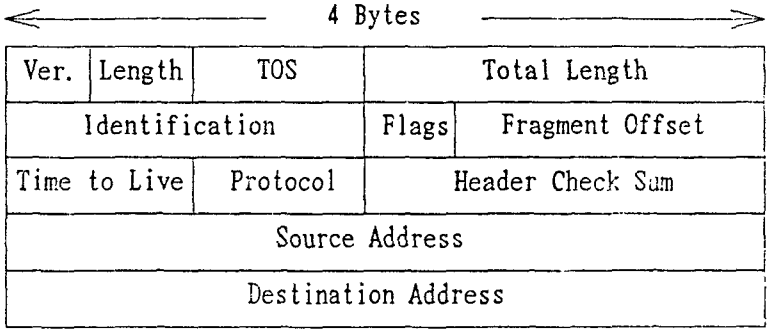
1. 서론

국제 인터네트의 빠른 성장에 따라 국내 인터네트사용도 점차 활성화 되어가고있으며 그 중요성 또한 인정받고 있다. 이제까지의 국내 인터네트는 주로 연구기관, 대학교, 국가기관등 비영리 단체에 국한되어 사용되어 왔으나 최근 한국통신, Dacom, Inet 기술등 국내 상용 인터네트 Provider의 출현에 따라 불특정 다수의 인터네트 사용자가 증가함에 따라 인터네트 보안의 중요성에 대한 인식이 커지고있다. 특히 인터네트는 미국의 대학을 기점으로 시작되었고 또한 BSD UNIX를 통하여 확산 되어 온 바 인터네트의 보안의 취약성은 이미 알려진사실이다. IETF (internet Engineering Task Force) Security Area에서는 인터네트의 보안을 위하여 여러 형태의 보안

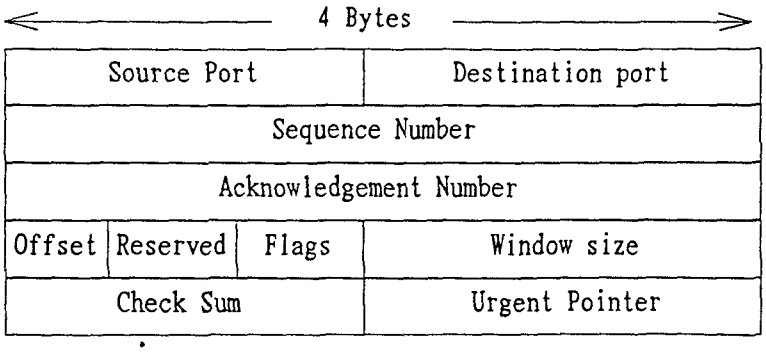
대책을 마련해 오고 있다. 그러나 현재 까지의 인터네트 보안 관련 RFC (Request For Comments) 또는 IETF Working Group에서 논의 되고 있는 대부분의 보안 기술은 주로 암호화 기법을 이용한 전송 데이타 보호 및 사용자 인증등에 중점을 두고 있다. 그러나 실제로 타사용자의 비밀번호를 이용하여 주요 시스템에 로그인 하여 주요전산자원 사용하는 사례가 발생하고 있으며 특히 알려지지 않은 시스템의 보안 취약성을 이용하여 관리자 특권을 가짐으로서 허가되지않은 주요한 정보의 삭제, 변조, 열람등을 행할수있다. 특히 최근의 전용회선 속도의 증가로 여러곳을 경유하더라도 전체 데이타 전달속도에는 큰 변화를 주지 않는다. 이경우 그사용자의 위치를 일반적인 시스템에서 제공하는 로그만으로 파악하기는 어려울뿐 아니라 시스템 로그 자체의 신뢰성에도 문제는 있다. 또한 시스템의 로그는 쉽게 삭제될수도있다. 따라서 본연구에서는 불법 사용자를 발견하였을 경우 전산망상의 최초 사용자의 위치를 확인하는 기법을 제안 하고 문제점을 동시에 제기함으로서 보다 이후 효율적인 전산망 사용자 추적기법의 도출방향을 제시하고자한다.

2. 인터네트 데이타 전달방식

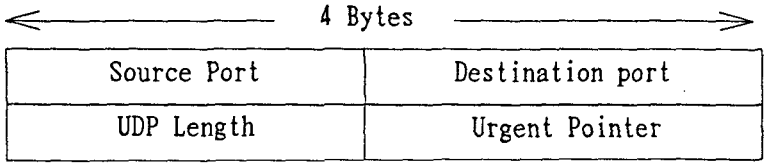
2.1 IP, TCP, UDP Header



IP Header



TCP Header

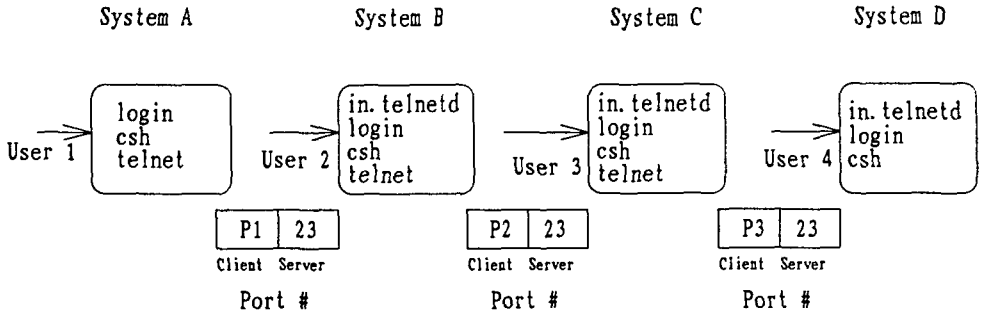


UDP Header

위그림에서 보는바와같이 인터네트상의 모든 데이타는 IP Header에 Source와 Destination의 주소와 TCP, UDP Header에 Source와 Destination의 Port Number를 가지고 Client/Server Model에 의하여 데이타를 전송하고있다. 서비스의 특성에 따라 TCP 또는 UDP가 결정되고 서비스의 종류에따라 Port Number가 결정된다. 예를들면 ftp 서비스는 TCP Port 21, telnet 서비스는 TCP Port 23, mail 서비스는 TCP Port 25, SNMP 서비스는 UDP Port 161를 사용한다. 이와같이 서비스종류에 따라 정해지는 Port를 Well-Known Port라 하고 모든 Client 프로그램은 Server의 특정한 Well-Known Port에 접속함으로서 원하는 서비스의 종류를 구분한다. 본연구에서는 인터네트에서 제공하는 원격지 로그인 기능 즉 telnet에 대하여 살펴본다.

앞서 언급한 바와같이 인터네트의 telnet기능은 Client/Server 모델에 따라 이루어진다. 이경우 Server에서는 Port # 23에서 서비스를 제공하며 Client에서는 임의의 Port Number를 통하여 서비스를 제공받는다. 이러한 기본적인 형태는 다단계원격지 로그인의 경우 다음과 같은 그림으로 나타날수있다.

2.2 telnet을 이용한 다단계 원격지 로그인



다단계 원격지 로그인 형태

위 그림에서는 User 1 이 System A 에 최초로 로그인한후 telnet 기능을 이용하여 User 2,3 의 계정으로 System B, C 를 각각 경유하여 최종적으로 System D 에 User 4 로 로그인 한경우 각 시스템에서 필요한 Process 들과 Port Number 를 보여주고있다(위에 나타난 Process 이름은 SUN OS 4.1.3의 예임). 위그림에서 P1, P2, P3 는 임의의 Port Number 를 나타낸다. 즉 Client 측에서는 임의의 Port Number가 사용된다. 본연구에서는 System D 에서 최초의 사용자 User 1 을 추적하는 기법을 제안하고자한다.

3. 원격지 로그인 사용자 확인 기법

3.1 확인 단계

Si : 확인을 시작한 최초 시스템
Sc : 현재 시스템
Sr : 원격지 시스템

Step 0 Sc := Si
Step 1 Detect a process, P, for user identification on Sc.
Step 2 Provide Si with the host address and user name of P.
Step 3 Check if process P is created by a remote system Sr.
Step 4 If (process P is local) then stop.
Step 5 Get the remote port number, n, of process P on Sc.
Step 6 Sc := Sr
Step 7 Detect a process which owns port number n on Sc.
Step 8 Goto Step 2.

3.2 구현

아래는 SUN OS 4.1.3 에서의 원격지로그인 관련 데이타를 보여주는 구현 프로그램 일부 및 결과이다.

```
int getbuf(addr, buf, len, what)
   long addr; char *buf; int len; char *what;
{
        kvm_read (kd, addr, buf, len);
        return -1;
}

int user_identification()
{
                  . . . .

getbuf (nl[N_NFILE].n_value, &nfile, sizeof(nfile), NULL);
getbuf (nl[N_NPROC].n_value, &nproc, sizeof (nproc), NULL);
getbuf (nl[N_PROC].n_value, &nextaddr, sizeof(nextaddr), NULL);

for (k = 0; k < nproc; k++)
{
                  . . . .
   getbuf (nextaddr, &process, sizeof(process), NULL);
   if (process.p_pid > 0 && process.p_stat != SZOMB &&
       process.p_stat != SIDL)
   {
      getbuf (process.p_uarea, &user_info, sizeof(user_info), NULL);
      proc_files = (struct **) malloc((user_info.u_lastfile + 1) *
                                                sizeof (struct file *))
      getbuf (user_info.u_ofile, proc_files, (user_info.u_lastfile + 1)
                * sizeof ( struct file *), NULL);
      getbuf (proc_files[i], &this_file, sizeof (this_file), NULL);
      if (this_file.f_type == DTYPE_SOCKET)
      {
            getbuf (this_file.f_data, &sockinfo, sizeof(sockinfo),NULL);
            if (sockinfo.so_type != SOCK_STREAM) continue;
            if (!(sockinfo.so_state & SS_ISCONNECTED)) continue;
            getbuf (sockinfo.so_pcb,&protoinfo,sizeof(protoinfo), NULL);
            getbuf (protoinfo.pr_domain,&domaininfo,
                                                sizeof(domaininfo), NULL);
            if (domaininfo.do_family != AF_INET) continue;
            getbuf (sockinfo.so_pcb, &tsinfo, sizeof(tsinfo), NULL);
            strcpy(remotehost, get_fullhost
                                          (gethost(tsinfo.inp_faddr)),15);
            pe = getpwuid ((int) process.p_uid);

                  . . . .
```

결과

User #	Proc #	Local Host	Local Port	Remote Host	Remote Port
27	26007	134.75.30.11	23	166.104.36.64	3757
27	26009	134.75.30.11	23	166.104.36.64	1819
102	5948	134.75.30.11	1325	134.75.30.2	23
34	13557	134.75.30.11	23	198.92.30.32	20494
57	4534	134.75.30.11	2215	134.75.30.2	23
145	87742	134.75.30.11	23	155.230.9.2	267

.
.
.
.

3.3 특성 ·

본 장에서 제안하는기법은 다음과 같은 요구사항을 만족하여야한다. 우선 Recursive Query를 통하여 최초의 원격지 시스템까지 확인할수있어야 하며 경유하는 시스템의 주소와 Port Number 및 사용자정보를 TCP 또는 UDP 방식으로 확인을 시작한 최초 시스템까지 송신하는 기능이 필요하다. 또한 본장에서 제안한 방식으로 경유하는 시스템에서의 사용자와 최초의 사용자를 확인하기위하여는 모든 시스템에서 같은 방식으로 이러한 서비스를 제공하여야한다. 즉 인터네트의 다른 서비스와같이 하나의 Well-Know Port에서 서비스를 제공하여야하며 또한 Client 와 Server의 프로그램도 그이름이 모두 공개되어야한다. 마지막으로 모든 시스템에서는 항상 Server Process는 서비스를 제공할 준비를 갖추고있어야한다.

3.4 문제점

본장에서 제안한 방식은 telnet을 이용한 다단계 원격지 로그인 사용자를 추적확인 하는데 사용할수있으나 다음과 같은 문제점들을 가지고있다. 첫째 Port Number와 Client, Server Program이 반드시 알려져야만 하는 점이다. 이점은 불법으로 침입을 시도하는 해커들에 의하여 쉽게 기능이 정지될수있는 취약성이다. 또한 인터네

트상의 모든 시스템은 다단계 원격지 로그인의 경유지가 될수있으므로 본장에서 제시한 기법을 이용하기위해서는 인터네트상의 300만 이상의 모든 시스템이 이러한 기능을 지원해야한다. 마지막으로 인터네트특성상 개방형 프로토콜이므로 모든 종류의 H/W 및 OS에서 이러한 기능을 지원해야한다.

4. 효율적인 사용자확인을 위한 고려 사항

보다 근본적인 원격지 사용자 확인 기법을 연구하기위하여는 앞서 언급한 원격지 사용자 확인 기법의 문제점들은 반드시 해결되어야한다. 첫째 인터네트의 일반적인 서비스 표준과는 다른 형태의 표준이 필요하다. 즉 원격지 사용자 확인 서비스의 Port Number 와 Client, Server Program은 같지않아도 되는 표준형태여야한다. 둘째 인터네트상의 다양한 모든 시스템이 이러한 기능을 지원하는것은 현실적으로 불가능하므로 다른 방향의 접근이 필요하다. 이러한 문제점외에도 셋째 원격지 사용자가 경유하는 시스템을 직접 추적하지않고 간접적인 방식으로 모니터링하여 불법사용자가 추적을 감지할수없는 방식이 필요하며 넷째 초고속 전산망 환경으로의 변화에 따라 원격지 사용자확인은 DNS(Domain Name System)과 같이 Worldwide 서비스가 되어야한다. 마지막으로 다섯째 인터네트이외의 전산망 사용자가 게이트웨이를 통하여 원격지 로그인하는 경우의 대책 또한 고려 되어야 할사항이다.

5. 결론

본연구에서는 인터네트 환경에서 다단계 원격지 사용자 확인기법을 제시하고 문제점을 분석하여 보다 효율적인 사용자 확인을 위한 고려사항들을 언급하였다. 전산망 보안을 위하여 기본적으로 필요한 암호화 기법, 사용자 인증 기법이외에 전산망의 국제화, 대형화, 서비스의 다양화 및 불특정 다수사용자의 전산망 사용에따라 시스템을 보호하기위한 기법으로 불법사용자 추적확인기법은 반드시 필요하다고하겠다. 이를 통하여 모든 전산망 사용은 모니터되고있고 전산자원을 불법사용할 경우 추적당한다는 인식을 확산시켜 전산망의 안정적 사용을 도모할수있을것이다. 본연구에서 제시한 인터네트환경에서의 원격지 사용자 확인기법내지 문제점 분석을 바탕으로 차세대 고속 및 초고속망환경에서의 효율적인 원격지 사용자 확인기법 연구의 활성화가 필요하겠다.

참고문헌

[1] 안금혁, 장청룡 '개방형 통신 시스템 인증 프레임워크' 한국통신정보보호학회 종합학술발표회 논문집 1993

[2] Daniel C. Lynch, Marshall T. Rose, Internet System Handbook, Addison-Wesley, 1993

[3] Steve Crocker, Overview of Internet Security Development, INET '93

[4] Rober B. Reinhardt, An Architecture Overview of UNIX Network Security, Oct 8, 1992

[5] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1340, USC/Information Science Institue, July 1992.

[6] Simon Garfinkel and Gene Spafford 'Practical UNIX Security' O'Reilly & Associates, Inc., 1991

[7] Deborah R., and G.T. Gangemi Sr. 'Computer Security Basics' O'Reilly & Associates, Inc., 1991

[8] Seberry, J., and Pieprzyk, J. Cryptography - An Introduction to Computer Security, Precice-Hall, 1989

[9] RFC 1244, *Site Security Handbook*

[10] RFC 1281, Guideline for Secure Operation of the Internet

[11] St. Johns, M., "Authentication Server", RFC 931, TPSC, January 1985.