Construction of Computer Network Security Defense System

Deyong Jiang(✉)

Jiangxi University of Applied Science, Nanchang 330041, Jiangxi, China
twd13870937881@126.com

Abstract. With the increase of the number of users all over the world, computer network not only makes people's life more convenient but also brings serious security problems. UCIrusion prevention system is an emerging information security technology in the field of network security to make up for the deficiency of firewall and UCIrusion detection. It UCIegrates the advantages of firewall and UCIrusion detection system and can actively defend the protected network in real time [9]. As the bandwidth of backbone network has generally entered the gigabit era, the research and application of gigabit network UCIrusion prevention system has become one of the hot spots in the field of information security. This article make a detail for today's computer network security, and for the computer network security defense system design and key technology were discussed, to today's problems makes the corresponding solutions and put forward corresponding solutions, aims to speed up the computer network security defense system and the application of key technologies. Thus accelerate the process of computer network security system design, accelerate the design of computer network security system.

Keywords: Computer Technology · Network Security Defense System

1 Introduction

With the gradual increase of network users, computer network not only makes people's life more convenient but also brings serious security problems. UCIrusion prevention system is a new information security technology in the field of network security to make up for the deficiency of firewall and UCIrusion detection. UCIrusion prevention system combines the advantages of firewall and UCIrusion detection system to protect network security in real time [2]. As the network bandwidth has been widely used in millions of households, the research and application of network UCIrusion prevention system has become one of the hot spots in the field of information security [3]. This article make a detail for today's computer network security, and in view of the present computer network security defense system design and key technology were discussed, to today's problems makes the corresponding solutions and put forward corresponding solutions, aims to speed up the computer network security defense system and the application of key technologies, Thus accelerate the process of computer network security system design, accelerate the design of computer network security system [4].

K. Subramanian et al. (Eds.): CTMCD 2022, ACSR 99, pp. 847–854, 2023.
https://doi.org/10.2991/978-94-6463-046-6_96

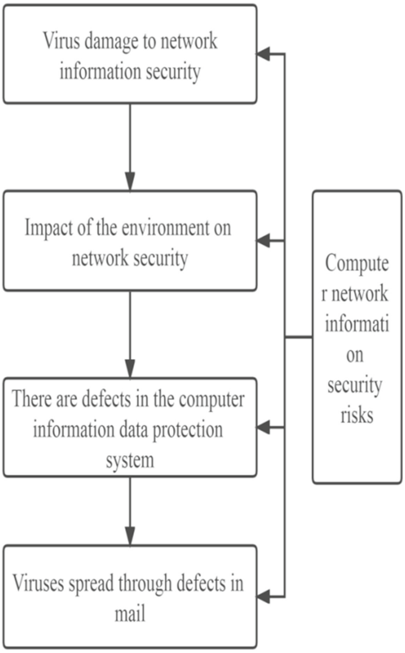

Virus damage to network information security
Impact of the environment on network security
There are defects in the computer information data protection system
Viruses spread through defects in mail
Compute r network informati on security risks

Fig. 1. Computer network information security risks.

2 Computer Network Information Security Risks

2.1 Virus Damage to Network Information Security

The birth of computer network has brought convenience to people's life, but viruses also threaten the security of computer network all the time [5]. Viruses can be spread by sending emails, downloading software, browsing websites and other ways. Users will unconsciously UCIroduce viruses UCIo computers, posing potential threats to users' information security. Virus has certain concealment, when the user's computer is invaded by a virus, the user is difficult to remove the virus in time, when not detected, it may cause great damage to the computer system, when people discover the virus, the virus may have caused serious damage to the user's computer data [7] (Fig. 1).

2.2 Impact of the Environment on Network Security

The network environment can also pose a significant threat to computer information security, but most users do not care about these. The damage caused by the natural environment to the computer operating environment cannot be underestimated, and the computer has high requirements on the temperature and humidity of the working environment [8]. Once out of the range of the computer can withstand, the computer's circuitry will cause major damage, which is called hardware damage. Hardware damage will lead to the loss of data stored in the computer, posing a major threat to user information security [6].

Table 1. Computer network information security risks.

Virus damage to network information security	Impact of the environment on network security	There are defects in the computer information data protection system	Viruses spread through defects in mail
The birth of computer network has brought convenience to people's life, but viruses also threaten the security of computer network all the time. Viruses can be spread by sending emails, downloading software, browsing websites and other ways.	The network environment can also pose a significant threat to computer information security, but most users do not care about these.	All the information of a computer is stored on the hard disk. Once the hard disk fails, it will give criminals an opportunity to attack the hard disk and steal a large number of important information stored on the hard disk, which ultimately leads to the disclosure of user information.	E-mail plays a very helpful role in people's life and work. Everyone receives E-mail more or less. Criminals make full use of E-mail to spread the virus, when the user opens the mail with the virus, the virus will invade the computer system, which is very detrimental to the user's information security.

2.3 There Are Defects in the Computer Information Data Protection System

All the information of a computer is stored on the hard disk. Once the hard disk fails, it will give criminals an opportunity to attack the hard disk and steal a large number of important information stored on the hard disk, which ultimately leads to the disclosure of user information. This is mainly because the computer protection system is not perfect, it is difficult to resist different types of network threats, so it is very important to promote the storage and protection of information data [9].

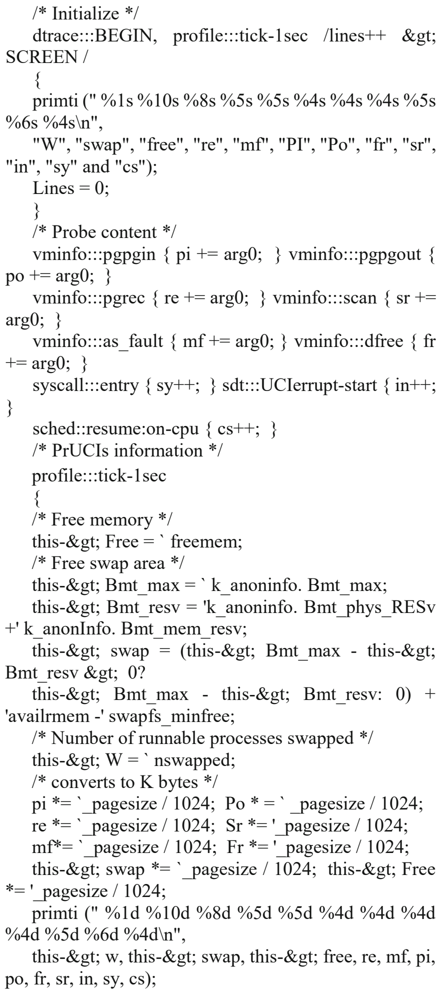
2.4 Viruses Spread Through Defects in Mail

E-mail plays a very helpful role in people's life and work. Everyone receives E-mail more or less [10]. Criminals make full use of E-mail to spread the virus, when the user opens the mail with the virus, the virus will invade the computer system, which is very detrimental to the user's information security. There are some weaknesses in the design of E-mail, which make it impossible for users to reject E-mail and ultimately lead to cyber attacks on users' computers. Cyber crime refers to the criminal activities with stealing passwords as the main means. After stealing users' passwords, criminals may commit fraud, which poses a serious threat to users' property security (Table 1).

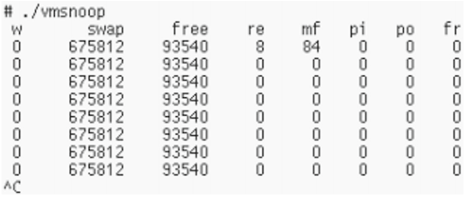
3 Research on Security Application of Dynamic Tracking Technology

The new characteristics of dynamic tracking technology make it play an important role in the field of security. For example, dynamic tracing can be used to monitor reads and writes to specific files, monitor system calls to processes, and so on. Mainly from the system information detection, file reading and writing, process tracking, keystroke capture, network connection and other five aspects to carry on the elaboration [12].

The first is system information detection. Dynamic tracking technology inserts numerous tiny probes in the kernel, which can capture information in a more all-round way. Compared with traditional tracking technology [13], it can obtain system information more conveniently, while eliminating smaller system resources. Take the following code as an example (Fig. 2).



```
    /* Initialize */
    dtrace:::BEGIN,  profile:::tick-1sec  /lines++  &gt;
SCREEN /
    {
    primti (" %1s %10s %8s %5s %5s %4s %4s %4s %5s
%6s %4s\n",
    "W", "swap", "free", "re", "mf", "PI", "Po", "fr", "sr",
"in", "sy" and "cs");
    Lines = 0;
    }
    /* Probe content */
    vminfo:::pgpgin { pi += arg0;  } vminfo:::pgpgout {
po += arg0;  }
    vminfo:::pgrec { re += arg0;  } vminfo:::scan { sr +=
arg0;  }
    vminfo:::as_fault { mf += arg0; } vminfo:::dfree { fr
+= arg0;  }
    syscall:::entry { sy++;  } sdt:::UCIerrupt-start { in++;
}
    sched::resume:on-cpu { cs++;  }
    /* PrUCIs information */
    profile:::tick-1sec
    {
    /* Free memory */
    this-&gt; Free = ` freemem;
    /* Free swap area */
    this-&gt; Bmt_max = ` k_anoninfo. Bmt_max;
    this-&gt; Bmt_resv = 'k_anoninfo. Bmt_phys_RESv
+' k_anonInfo. Bmt_mem_resv;
    this-&gt;  swap  =  (this-&gt;  Bmt_max  -  this-&gt;
Bmt_resv &gt;  0?
    this-&gt;  Bmt_max  -  this-&gt;  Bmt_resv:  0)  +
'availrmem -' swapfs_minfree;
    /* Number of runnable processes swapped */
    this-&gt; W = ` nswapped;
    /* converts to K bytes */
    pi *= `_pagesize / 1024;  Po * = ` _pagesize / 1024;
    re *= `_pagesize / 1024;  Sr *= '_pagesize / 1024;
    mf*= `_pagesize / 1024;  Fr *= '_pagesize / 1024;
    this-&gt; swap *= `_pagesize / 1024;  this-&gt; Free
*= '_pagesize / 1024;
    primti (" %1d %10d %8d %5d %5d %4d %4d %4d
%4d %5d %6d %4d\n",
    this-&gt; w, this-&gt; swap, this-&gt; free, re, mf, pi,
po, fr, sr, in, sy, cs);
```



```
# ./vmsnoop
w        swap      free     re     mf    pi    po    fr
0      675812     93540      8     84     0     0     0
0      675812     93540      0      0     0     0     0
0      675812     93540      0      0     0     0     0
0      675812     93540      0      0     0     0     0
0      675812     93540      0      0     0     0     0
0      675812     93540      0      0     0     0     0
0      675812     93540      0      0     0     0     0
0      675812     93540      0      0     0     0     0
^C
```

Fig. 2. Running results of Vmsnoop.

The second is file monitoring. In active defense technology, file read/write detection is a method of anticipating attacks. A hacker might look at the file information and modify it after becoming the root user. In the traditional approach, it is difficult to monitor the operation of a specified file [14]. However, it is easy to specify a monitor file by writing a D script file using DTrace's Syscall provider [6]. Here is a snippet of source code that monitors the implementation file opening operation. Source file filesnoop, run in Shell environment, core D language code is as follows [11]:

```
   The dtrace: : : BEGIN
   {
   primti("%-20s ", "TIME");  primti (" % 5 s % 6 s ",
"UID", "PID");
   primti("%3s ", "FD");  primti (" % s "3," ERR ");
   primti("%-20s  ",  "PATH");   primti  ("  %  s  ",
"ARGS");
   primti (" \ n ");
   }
   /* Variable attached */
   The syscall: : open: entry, the syscall: : open64: entry
   {
   self-&gt; pathp = arg0;  self-&gt; Ok = 1;
   }
   /* PrUCIs trace information */
   The  syscall:  :  open:  return,  the  syscall:  :  open64:
return
   /PATHNAME == copyinstr(self-&gt; Pathp) /
   {
   primti("%-20Y ", walltimestamp);  primti ("%5d %6d
", uid, pid);
   primti("%3d ", (UCI)arg0);  primti (" % 3 d ", errno);
   primti("%-20s ", copyinstr(self-&gt; Pathp));
   primti("%S", curpsinfo-&gt; Pr_psargs);
   primti (" \ n ");
   self-&gt; Pathp = 0;
   self-&gt; Ok = 0;
   }
```

Open the monitor in a Shell environment and read the /etc/passwd file using different users and commands (Table 2).

Next comes process tracking. In an active defense system, a hacker may launch a process after logging in for some time to implement a new attack [15]. The traditional method is to run the ps command to find the process, followed by the truss command to see the details of the process. Here is the code (Fig. 3):

```
dtrace:::BEGIN
{
trace("Strating... \n");
}
proc:::exec-success
/!progenyof($pid) && ring++ < 2/
{
trace("Caution!\nTIME UID PID CMD\n");
primti("%-20Y ", walltimestamp);
primti("%5d %5d %s\n" ,uid,pid,execname);
system("audioplay /usr/share/audio/samples/au/doorbell.au &");
}
profile:::tick-10hz
{
ring = 0;
}
```

Finally, network connection, its core code is as follows:

```
The dtrace: : : BEGIN
{
primti (" % 20 s ", "STRTIME");
primti (" % 5 s % % 6 s to 15 s % 5 s % % 2 s to 15 s % % 5 s 5 s % s \ n ", "UID", "PID",
"LADDR LPORT", ""," DR ", "RADDR", "RPORT", "SIZE", "CMD");
}
/* TCP active external connection probe */
FBT: IP: tcp_connect: entry
{ this-&gt; Arg0 TCPP = (tcp_t *);
self-&gt; commi = (conn_t *)this-&gt; tcpp-&gt; Tcp_commi;
Tname [(UCI) self - & gt; commi] = execname;
Tpid [(UCI) self - & gt; commi] = pid;
Tuid [(UCI) self - & gt; commi] = uid;
}
/*TCP data recognition */
FBT: sockfs: sotpi_accept: return, FBT: IP: tcp_connect: return
/self-&gt; commi /
{
/* Identify the connection direction */
tladdr[(UCI)self-&gt;commi] = self-&gt; Laddr;
tfaddr[(UCI)self-&gt;commi] = self-&gt; Faddr;
tlport[(UCI)self-&gt;commi] = self-&gt; Lport;
tfport[(UCI)self-&gt;commi] = self-&gt; Fport;
Tok [(UCI) self - & gt; commi] = 1;
}
FBT: IP: tcp_get_conn: return
{
this-&gt; Arg1 commi = (conn_t *);
Tok [(UCI) this - & gt; commi] = 0;
Tpid [(UCI) this - & gt; commi] = 0;
Tuid [(UCI) this - & gt; commi] = 0;
Tname [(UCI) this - & gt; commi] = 0;
Tproj [(UCI) this - & gt; commi] = 0;
}
/* PrUCIs TCP external connections */
fbt:ip:tcp_connect:return /self-&gt; commi && self-&gt; Name = = name /
{
primti (" % 20 y, "walltimestamp);
primti("%5d %6d %-15s %5d %2s %-15s %5d %5d %s\n",self-&gt; uid,self-&gt; Pid,
self-&gt; laddr,self-&gt; lport,self-&gt; dir,self-&gt; faddr,self-&gt; fport,self-&gt; size,self-&gt; Name)[1];
}
```

Table 2. The new characteristics of dynamic tracking technology.

The new characteristics of dynamic tracking technology	
system information detection	it can obtain system information more conveniently
file reading and writing	In active defense technology, file read/write detection is a method of anticipating attacks.
process tracking	In an active defense system, a hacker may launch a process after logging in for some time to implement a new attack. The traditional method is to run the ps command to find the process, followed by the truss command to see the details of the process.
keystroke capture	In the traditional approach, it is difficult to monitor the operation of a specified file.

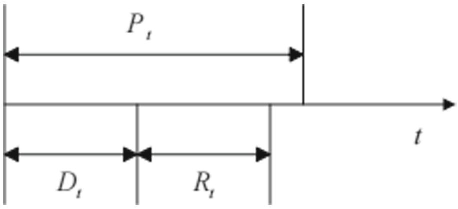


Fig. 3. P2DR time.

4 Conclusion

The security of information system has become a common problem. To this end, many scientists have done a lot of research. It can be seen that the way of network intrusion is changing, the means of attack is becoming more and more diversified, and advanced covert attack technology is becoming more and more common. In view of these complex security problems, the establishment of firewall cannot meet the urgent security needs of information system. Many important achievements have been made in the security of computer network system from hardware model to software system. With the diversification of threats to network security and the concealization of hacker attack means, conventional security defense measures such as firewall and passive identification of vulnerability characteristics cannot meet the new requirements to a certain extent. It is a hotspot and consensus in the field of network security to construct a security system that conforms to the current situation of network development and to develop new key technologies.

References

1. Chencan Wang, Xu Yanbin, Fan Yige, Luo Yuhao. Analysis of Key Technology of Computer Network Security Defense System [J]. Network security Technology and Application, 2021 (05): 20-22.

2. Fengxiu Lv. Design and Implementation Analysis of Computer Network Security Defense System in the Era of Big Data [J]. Electronic World, 2020(21): 177-178. DOI: https://doi.org/10.19353/j.cnki.dzsj.2020.21.075.
3. Haitao Lan. Design, Research and Analysis of Computer Network Security Defense System in the Era of Big Data [J]. Computer Products and Circulation, 2019 (11): 45.
4. Hengni Ren. Design, Research and Analysis of Computer Network Security Defense System in the Era of Big Data [J]. Electronic designer.
5. Hongyu Chen. Design of Computer Network Security Defense System in the Era of Big Data [J]. Digital Technology and Application, 2018, 36(11): 204+236. DOI: https://doi.org/10.19695/j.cnki.cn12-1369.2018.11.111.
6. Juan Qiao. Research on the Implementation and Key Technology of Computer Network Security Defense System [J]. Communication Power Supply Technology, 2021, 38(04): 34-36. DOI: https://doi.org/10.19399/j.cnki.tpt.2021.04.010.
7. Pingli Wang. Design of Computer Network Security Defense System for Chemical Enterprises Based on Artificial UCIelligence Technology [J]. Bond, 2021, 47 (08): 106-109+122.
8. Piya Huang. The Implementation and Key Technology of Computer Network Security Defense System [J]. Electronic Technology and Software Engineering, 2021 (16): 259-260.
9. Ruihua Wang. Design and Key Technology of Computer Network Security Defense System [J]. Network Security Technology and Application, 2021 (12): 7-8.
10. Wenxia He. Design and Research of Computer Network Security Defense System in the Era of Big Data [J]. Network Security Technology and Application, 2021 (02): 58-59.
11. Xiangyu Chai. Design of Computer Network Security defense System Based on Big Data and Artificial UCIelligence Technology [J]. Network security Technology and Application, 2020 (09): 52-53.
12. Xiaoyan Zhou. Construction and Analysis of Computer Network Security Defense System Based on Big Data [J]. Wireless UCIerconnection Technology, 2021, 18 (23): 22-23.
13. Yan Li, Ma Xudong. Implementation and key technology analysis of computer Network Security Defense System [J]. Electronic Technology and Software Engineering, 2021 (10): 249-250.
14. Yao Ma. Design of Computer Network Security defense System Based on Big Data and Artificial UCIelligence Technology [J]. Information and Computer (theoretical edition), 2020, 32 (04): 208-209.
15. Yueying Gong, Qiao Yueying round. Design and Research of Computer Network Security Defense System in the Era of Big Data [J]. Information and Computer (theoretical edition), 2019, 31 (20): 199-201.