Design a High-Level Language for Large Network Security Management

Jangha Kim[1], Byungwook Song[1], Kanghee Lee[1], Sangwook Kim[1],
Daesik Choi[2], and Jungtaek Seo[2]

[1] Department of Computer Science, Kyungpook National University
1370 Sankyuk-dong Buk-gu, Daegu, 702-701, Korea
{jhkim, bwsong, khlee, swkim}@cs.knu.ac.kr
[2] National Security Research Institute
161 Gajeong-dong Yuseong-gu, Daejeon, 305-350, Korea
{dschoi, seojt}@etri.re.kr

Abstract. A common breach of network security is the class of attacks called Worm-virus. This paper proposes a language called Triton whose goal is to efficiently and effectively safeguard large network security for management system. We represent abstract language that supports various functions. This high-level language abstracts the control behavior of the network nodes, which has various setting-up methodology. We shall describe the feature of Triton language and give some example of the preliminary Triton implementation on the test-bed.

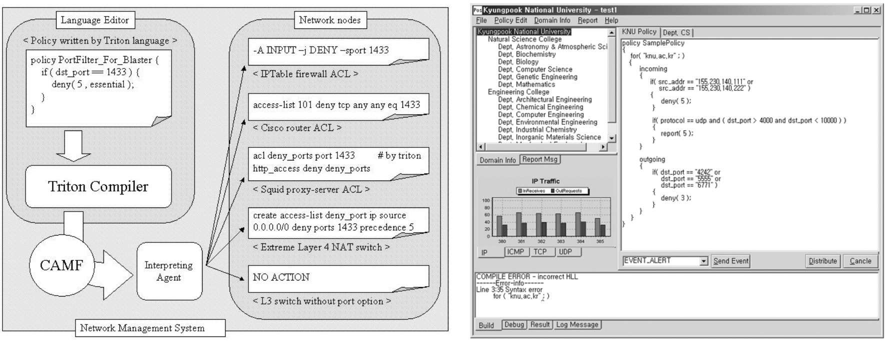
1 Introduction

Malicious codes and worms comprise the largest portion of the loss caused the security problem in the Internet. Small worms such as the "Blaster" spread quickly through the enormous network. It causes the network to lock down within an hour or so[1]. The situation worsens before it can be monitored and notified by the supervisor. Since the network is not available, it becomes hard to serve a node with an order. It is for this reason that the abstract ACL policy language and hierarchy security management system are necessary in delivering security information. The Triton is an abstract high-level language that manages the lower node and the network node through the administrator of the Domain.

2 Triton Language

It is necessary to describe the heterogeneous and configurative information of various network nodes. This approach provides the highest Domain with a methodology to manage the large-scale network. A high-level Triton offers various political functions that manage lower network nodes. This mechanism provides five perspectives of a description:

R. Meersman et al. (Eds.): OTM Workshops 2004, LNCS 3292, pp. 7–8, 2004.


Language Editor
< Policy written by Triton language >
Triton Compiler
CAMF
Interpreting Agent
Network Management System
Network nodes
< IPTable firewall ACL >
< Cisco router ACL >
< Squid proxy-server ACL >
< Extreme Layer 4 NAT switch >
< L3 switch without port option >
Kyungpook National University - test1
File
Policy Edit
Domain Info
Report
Help
Kyungpook National University
Natural Science College
Dept. Astronomy & Atmospheric Sci
Dept. Biochemistry
Dept. Biology
Dept. Computer Science
Dept. Genetic Engineering
Dept. Mathematics
Engineering College
Dept. Architectural Engineering
Dept. Chemical Engineering
Dept. Computer Engineering
Dept. Environmental Engineering
Dept. Industrial Chemistry
Dept. Inorganic Materials Science
Domain Info
Report Msg
IP Traffic
InReceives
OutRequests
100
80
60
40
20
0
380
381
382
383
384
385
IP
ICMP
TCP
UDP
KNU Policy
Dept. CS
EVENT_ALERT
Send Event
Distribute
Cancle
Build
Debug
Result
Log Message

```
policy PortFilter_For_Blaster {
    if ( dst_port == 1433 ) {
        deny( 5 , essential );
    }
}
```

```
-A INPUT –j DENY –sport 1433
```

```
access-list 101 deny tcp any any eq 1433
```

```
acl deny_ports port 1433        # by triton
http_access deny deny_ports
```

```
create access-list deny_port ip source
0.0.0.0/0 deny ports 1433 precedence 5
```

```
NO ACTION
```

```
policy SamplePolicy
{
  for( "knu.ac.kr" ; )
  {
     incoming
     {
        if( src_addr == "155.230.140.111" or
            src_addr == "155.230.140.222" )
        {
            deny( 5 );
        }

        if( protocol == udp and ( dst_port > 4000 and dst_port < 10000 ) )
        {
            report( 5 );
        }
     }

     outgoing
     {
        if( dst_port == "4242" or
            dst_port == "5555" or
            dst_port == "6771" )
        {
            deny( 3 );
        }
     }
  }
}
```

```
COMPILE ERROR - incorrect HLL
------Error-info------
Line 3:35 Syntax error
      for ( "knu.ac.kr" ; )
                        ^
```

Fig. 1. An abstract policy for network ACL and an administrator interface

- Abstract description for the configuration of a lower node
- Mechanism of policy compliance
- Grouping
- Event for a polymorphous policy
- Semi-structured communication form

Figure 1 shows the process of converting the abstract policy into a configuration of the lower node. The editor delivers a semi-structured ACL delivery form, in an intermediate form, to the Interpreter that has information on the lower nodes. The Interpreter agent generates the ACL commands according to the each feature of the lower nodes. We implement the compiler that converts the high-level language to the intermediate form. For code generation, use the win32 versions of the MKS LEX & YACC and the algorithm of tree traversals.

3 Conclusion

The Triton language is independent of specific network devices and is familiar with the existing programming language of the large-scale network manager. This paper proposes a language that is analogous to the C language and describes network security ACL policies. The Triton is able to control the lower nodes using the CAMF in intermediate form. It is different from the other policy languages. The policy manager has summarized and abstracted the information on large-scale networks to set up a coherent ACL policy. Additionally, if the Domain server accommodates a policy delivered from the other trustable Domains, the lower Domain then, is improving in security. This gives a tried manager the important function of managing the security of the large-scale network.

References

1. Mohit Lad, Xiaoliang Zhao, Beichuan Zhang, Dan Massey and Lixia Zhang : “An Analysis of BGP Update Burst during Slammer Attack,” IWDC, Calcutta, 2003