BUILDING AN UNIVERSAL NETWORK SECURITY MODEL

Zahari Todorov Slavov, Valentin Panchev Hristov

Department of Computer Systems and Technology, South-West University "Neofit Rilski", Blagoevgrad, Bulgaria, e-mail: zack_zs@abv.bg; v_hristov@aix.swu.bg

The paper describes the process of building a universal network security model. Various kinds of network breaches are mentioned and a solution for each kind of intrusion is offered. A spectrum of common and modern network solutions is specified. A basic network topology is analysed and sample configurations of some most common network devices are presented.

The purpose of present paper is to propose a universal comprehensive model of network security. The model helps network administrators and security specialists to implement easily the security policy and protect from most common threads.

Keywords: network security, network threads, universal security model

1. INTRODUCTION

Nowadays computer networks are open structures, which provide high-speed and reliable connectivity. As e-commerce and Internet applications evolved essential become the need to find the right balance between their open character and their isolation of the security threads. The spread use of mobile and wireless communication is the main factor of building more flexible network security model.

Security aims to protect private data, in order to maintain its integrity and availability. It could be done by protecting every network structure from threads and vulnerabilities and thus helping the business evolve to its full potential.

The purpose of present paper is to propose a universal comprehensive model of network security. The model can be used by network administrators and security specialists to implement easily the security policy and protect from most common threads.

2. PROBLEM STATEMENT

As Internet and World Wide Web got bigger and bigger every person and the whole business depends on it and on the services it delivers. The implementation of network applications in every business involves the need of security.

Company information is exposed to great risk. In most cases the need of high-speed access as well as adequate network security must be carried out.

Using software or hardware firewalls, implementing security policy for access and control between the networks, provides the needed balance between reliable security and easy Internet access. Various approaches are involved, like intrusion detection systems (IDS), authentication and authorization.

The security threads are structured, unstructured, external and internal [1].

- Structured threads are an organized attack to break a specific organization network security;
- Unstructured threads are random attacks on unprotected networks;

- Internal threads are realized by the members of an organization, which have access to the network and have a restricted account;
- External threads [1, 2] come from attacker, trying to break in from the outside network.

Knowing how various attacks are accomplished is essential in order build a good protection. They are Reconnaissance, Data Access, Denial of Service (DoS).

Some of the Reconnaissance attacks are Domain Name Service (DNS) queries, Ping sweeps, Vertical scans, Horizontal scans, Block scans, Sniffing.

Illegal Data Access is unauthorized data change, system access and exceeding user rights. It is accomplished by software [2, 3] for decryption, guessing or brute force breaking of passwords, various trojans, viruses, etc.

DoS attacks [6, 7] involve either crashing the system or slowing it down to the point that it is unusable. This kind of breach uses the vulnerabilities in the TCP/IP protocol stack. Some of the attacks [8,9,10] of that kind are Ping of Death, SMURF, Stacheldraht, Flooding, Tribal Flooding, SYN attacks, UDP bombs, Packet fragmentation and reassembly, E-mail bombs, CPU hogging, Malicious applets, chargen attack, Out-of-band attacks, etc.

3. UNIVERSAL SECURITY MODEL

The proposed common model could be used as a template for designing a network structure with a high level of security. For the purpose a sample configuration file should be constructed. It contains example instructions toward the operational system of the network device and applies certain achievements in the security sector.

The fields of implementation of the current solution are intelligent network devices like routers, 3-Layer switches, PIX (Packet Internet Exchange Firewall), IDS (Intrusion Detection System) and Network-based operational systems.

Communication in computer networks is accomplished at several levels. Network security should be considered at each level also.

The basis of a secure network structure is the well-designed network topology, which restricts physical and virtual access to the network media and communication devices. Only network and system administrators should have that kind of access. The configuration model is based on a three zone security topology, in which there are three zones of access- Inside, Outside and Demilitarized networks (fig. 1).

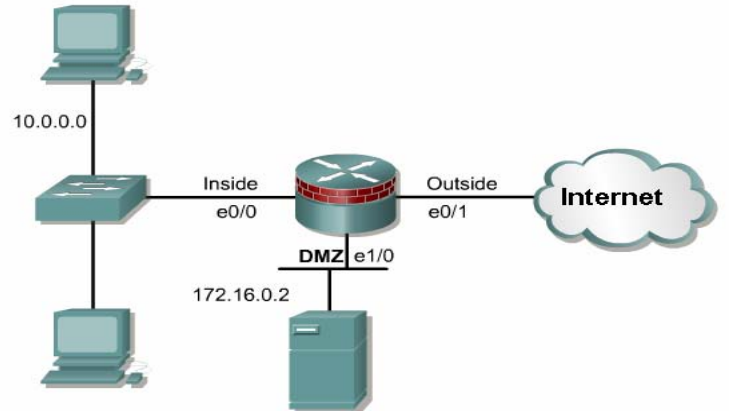

Fig.1 Basic Secure Topology

Network routers and 3-Layer switches are devices, based on a specialized network operation system. It has several access levels. The configuration of the administrative access to these devices is the most important task in securing the network. They can be accessed via console, terminal, AUX, SNMP, HTTP. For example:

```
Router(config)# line console 0
Router(config-line)# password my_pass
Router(config-line)# login
Router(config-line)# end
```

Fig.2 Password applying on console port

```
Router(config)# line vty 0 4
Router(config-line)# password VtyLines123
Router(config-line)# login
Router(config-line)# end
```

Fig.3 Password applying on terminal port(s)

```
Router(config)# line aux 0
Router(config-line)# password ProtectAux0
Router(config-line)# login
Router(config-line)# end
```

Fig.4 Password applying on AUX port

In order a secure encryption algorithm to be used for securing all the passwords configured in a network device the following command is used:

```
Router(config)# service password-encryption
```

Fig.5 Encryption service

If some of the access ports are not used, then it should be forbidden. For example, if the AUX port is not used:

```
Router(config)# line aux 0
Router(config-line)# no exec
```

Fig.6 Closing a port

Other way of protecting the access ports is times of termination of idle sessions to be set:

```
Router(config)# line console 0
Router(config)#  exec-timeout 5 0
Router(config)#  end
```

Fig.7 Termination time

The network devices have 16 privilege access levels which can be configured with the command:

```
Router(config)# privilege exec level 3 ping
```

Fig.8 Access levels

Another way of improving security is to stop or ban some active on default services that are not used:

```
>no service tcp-small-servers
>no service udp-small-servers
>no ip bootp server
>no service finger
>no ip http server
>no snmp-server
```

Fig.9 Stopped services

It is very important to forbid packets, used for remote administration and monitoring, to trespass the devices:

```
>no cdp run
>no service config
>no ip source-route
>no ip classless
```

Fig.10 Blocked packets

The most common attacks are the Denial of Service. They could be evaded using access-lists configured to apply some security rules. For example, the packets with source address, matching the address of an internal host or network but coming from Internet, should be forbidden (See fig.1):

```
Router(config)# access-list 170 deny ip 10.0.0.0 0.0.0.255 any log
Router(config)# access-list 170 deny ip 172.16.0.0 0.0.0.255 any log
Router(config)# access-list 170 deny ip 10.0.0.0 0.255.255.255 any log
Router(config)# access-list 170 deny ip 0.0.0.0 0.255.255.255 any log
Router(config)# access-list 170 deny ip host 255.255.255.255 any log
Router(config)# access-list 170 permit ip any 10.0.0.0 0.0.0.255
```

Fig.11 Rule 1

Packets coming from internal network with source address different from the addresses of the hosts in the internal network must be banned:

```
Router(config)#access-list 107 permit ip 10.0.0.0 0.0.0.255 any
Router(config)#access-list 107 deny ip any any log
```

Fig.12 Rule2

The SYN DoS attacks send a huge amount of packets filling the buffer of their receiver. A way of avoiding this is to forbid answers to requests not coming from the internal network:

```
Router(config)#access-list 108 permit tcp any 10.0.0.0 0.0.0.255 established
Router(config)#access-list 108 deny ip any any log
```

Fig.13 Rule3

Access list should allow only packets from existing hosts.

```
Router(config)#ip tcp intercept list 111
Router(config)#ip tcp intercept connection-timeout 60
Router(config)#ip tcp intercept watch-timeout 10
Router(config)#ip tcp intercept one-minute low 1800
Router(config)#ip tcp intercept one-minute high 5000
Router(config)#access-list 111 permit tcp any 10.0.0.0 0.0.0.255
```

Fig.14 Rule4

Kind of DoS attack is to send packets with destination and source addresses similar to the address of the router. All ingoing packets with destination address the address of the network or the broadcast address should be forbidden:

```
Router(config)#access-list 166 deny ip host 10.0.0.1 host 10.0.0.1 log
Router(config)#access-list 123 deny ip any host 10.0.0.255 log
Router(config)#access-list 123 deny ip any host 10.0.0.0 log
```

Fig.15 Rule5

Nowadays the count of bulk or spam mail attacks is very popular. They could be filtered by monitoring the maximum recipients of an e-mail.

```
Router(config) # ip audit smtp spam number-of-recipients
```

Fig.16 Spam filters

To insure the security and reliability of Internet access a URL, Java and ActiveX filters should be applied.

```
Router(config) # url-server (dmz) host 172.16.0.2 timeout 10 protocol TCP version 4
Router(config) # filter url http 0 0 0 0 allow
Router(config) # filter activex 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Router(config) # filter java 80 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

Fig.17 URL, Java and ActiveX filters

Routers can not block all the attacks coming from Internet but they could ban the ports that most common attacks use. They are TRIN00 (27665, 31335, 27444), Stacheldraht (16660, 65000), TrinityV3 (33270, 39168), Subseven (2222, 6711 – 6712, 6776, 6669, 7000).

In order to improve network security all the new and contemporary security measures should be implemented. Such a solution is the use of Context-based Access Control. It monitors and filters certain protocols at routers interfaces. A session is monitored only if it corresponds to the prior set conditions for filtering.

When constructing a secure and reliable network structure the load of the network device, the number of hosts and services that run on the network should be considered. Specialized hardware devices like Packet Internet Exchange (PIX) firewalls and Intrusion Detection systems should be implemented. They are constructed to meet the huge load of more aggressive attacks. PIX are vital for networks where connectivity is at first place, because they can build failover links. These links are spare routes which are used for routing traffic if the main device crashes [3, 4, and 5].

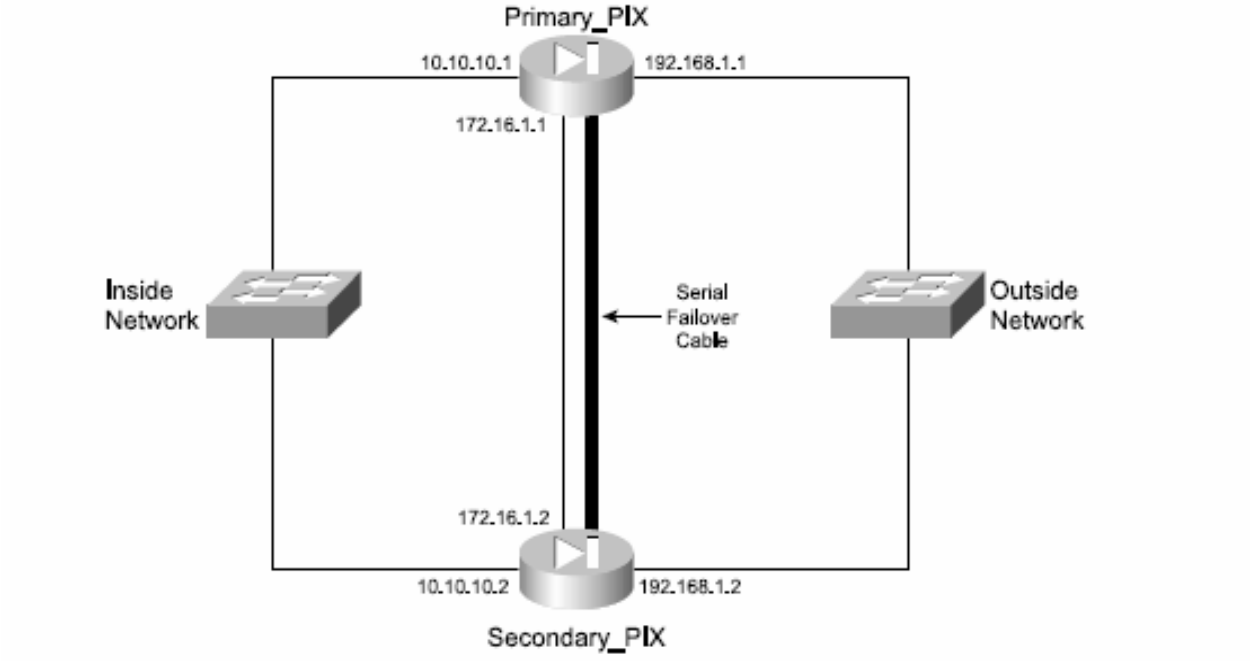

Fig.18 Failover topology

```
Primary-pix (config)# failover
Primary-pix (config)# nameif ethernet2 failover
Primary-pix (config)# interface ethernet2 100full
Primary-pix (config)# ip address failover 172.16.1.1 255.255.255.240
Primary-pix (config)# failover ip address outside 192.168.1.2
Primary-pix (config)# failover ip address inside 10.10.10.2
Primary-pix (config)# failover ip address failover 172.16.1.2
Primary-pix (config)# write memory
Primary-pix (config)# failover link failover
```

Fig.19 Failover configuration

PIX firewalls have various build in guards which protect [3] from some networks attacks like Fragmentation, DNS attack, SMTP attack, SYN flooding, Authentication and authorization attacks.

4. CONCLUSION

In present paper a universal comprehensive model of network security has been proposed. The realization of the network security model may be various according to the used network equipment. Appropriate access lists could be configured at routers. At PIX firewalls some of the protections are build in. Still at systems with UNIX or other network operation system the model could be implemented at various protections like bash scripts which configure the operation system filters and/or application software which is preliminarily installed and configured.

The implementation of network security is constant process at which newer vulnerabilities and threads in software and hardware are discovered. Patching and updating of the systems is necessity because it is as secure as its weakest link.

5. REFERENCES

[1] Cisco Systems, *Fundamentals of Network Security1.1,* CiscoPress 2003.

[2] Swartz, John, Todd Lammele, *Cisco Certified Internetwork Expert Study Guide*, Sybex 2001.

[3] Bastien, Greg, Christian Degu, *CCSP Cisco PIX Firewall Advanced Exam Certification guide*, Cisco Press 2003

[4] Dubrawsky, Ido, *CCSP Self-Study CCSP Exam Certification Guide,* Cisco Press USA 2004

[5] Shimonski, Robert, Debra Shinder, *The Best Damn Firewall Book Period,* Syngress Publishing 2003

[6] netsecurity.about.com

[7] www.windowssecurity.com

[8] www.sans.org

[9] netsec.iseca.org

[10] www.nlcv.bas.bg/bulgarian/vidove.htm