DESIGN AND IMPLEMENTATION OF A SECURED REMOTLY ADMINISTRATED NETWORK

Dr. Qutaiba I. Ali , Salah A. Jaro Alabady
Faculty Computer Eng. Dept., Mosul University, Iraq
QQQ1@maktoob.com, Salah_alabady@yahoo.com

ABSTRACT

As applications become more distributed, the design and management of security services in networked systems play an increasingly significant role. This paper deals with the plan and design of a typical security system for a large cooperative network. The main aim of the design is to protect the network against internal and external threats as well as various types of attacks. The design includes the ability of the administrator to control and manage the network from different locations inside the network and remotely from outside the network. First of all, the current security state of the network is examined, then, complete network security architecture is proposed. This architecture is based on supplying the network with 11 security methods against internal threats and 6 security methods against external threats. These methods have both software and hardware nature and work in all network layers. The affectivity of the suggested security solutions is tested against different attacks and proves its ability to resist these situations.

Keywords**:** *Network Security, Network Management, Firewall, AAA Server, VP, IDS*

1. INTRODUCTION

Security plays a vital role in the design, development and practical use of the distributed computing environment, for greater availability and access to information in turn imply that distributed systems are more prone to attacks. The need for practical solutions for secure networked system management is becoming increasingly significant. In developing these solutions, several important issues need to be carefully addressed. The design of the required security services forms a major part. Often the issues associated with security management are not adequately addressed. First, it is important to identify clearly the functionalities and interfaces of the trusted security management components. Then it is necessary to consider whether some of these trusted management authorities can be grouped together to simplify the overall management. This depends on several factors such as the relationships between organizations (or units) involved in the networked environment and the types of services offered as well as performance considerations. In practice, it is also necessary to consider the system development and deployment in stages thereby enabling a staged adoption [5, 10].

Traditionally, there are four primary classes of threats to network security [4]:

1. Unstructured threats: Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a network.

2. Structured threats: Structured threats come from hackers that are more highly motivated and technically competent. These people know system vulnerabilities, and can understand and develop exploit-code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

3. External threats: External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.

4. Internal threats: Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. This threats occupies for 60 to 80 percent of reported incidents.

In addition, there are 4 primary classes of attacks [6]:

●**Reconnaissance**: Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, it precedes an actual access or Denial of Service (DoS) attack.

●**Access**: System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems to which one does not have access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

●**Denial of Service (DoS)**: Denial of service (DoS) implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack simply involves running a hack or script. The attacker does not need prior access to the target because a way to access it is all that is usually required. For these reasons, DoS attacks are the most feared.

●**Worms, Viruses, and Trojan Horses**: Malicious software is inserted onto a host in order to damage a system, corrupt a system, replicate itself, or denies services or access to networks, systems, or services.

This paper discovers the possibility to build a typical security model for a cooperative network. The design includes the ability of the administrator to control and manage the network from different locations inside the network and remotely from outside the network. As a case study, Mosul university network is chosen to be the considered network.

2. THE NETWORK TOPOLOGY:

Mosul university network was established in 2004. The purpose of the network is to connect the different locations of the university by a high speed (1 Gigabit Ethernet) links. The network introduces several services to its client (2000 user in 2007), such as internet sharing, Email accounts, web hosting and internal chatting. The future may witness its application to be extended to cover more sophisticated fields such as database sharing and interactive multimedia applications.

The topology of the basic installation of the network is shown in Figure (1). The Description of the different network devices and its current configuration are listed in Table (1) [2].

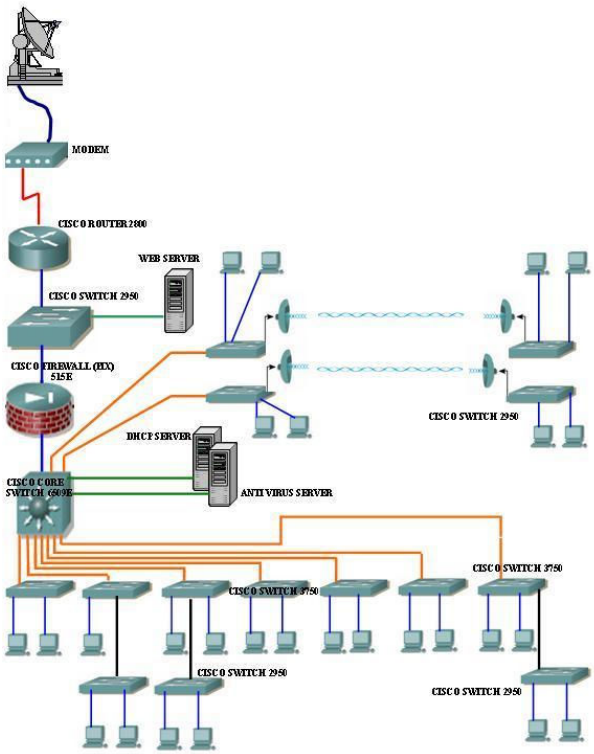

Figure1: Basic Installation of Mosul Univ. Network

The network consists of (41 Cisco 3750 & 2950) switches connected (via 1 Gbps Ethernet) to the Cisco 6051E core switch. These switches represent different university departments. Each switch is connected down to many layer 2 switches and different department's hosts. The connection to the internet is achieved through the Private Internet eXchange (PIX515E) device (which act as a firewall) and the Cisco2800 Network Address Translation (NAT) router. The internet service of the network could also be accessed through several IEEE802.11b WLAN connections.

It is obviously clear that network security concepts have not been considered during the installation of the network. It is important to insert different security levels and methods in a transparent fashion without affecting the performance of the network.

Table 1: Current Configuration of Network Devices

DEVICE NAME	QTY.	DESCRIPTION	CURRENT CONFIG.
Cisco Router 2800	1	●2 Fast Ethernet ports, 2 serial ports ●IOS=12.3 ●Support=Rip1,Rip2,EIGRP,IGRP,OSPF,IS-IS,BGP,VPN,VLAN,VTP	●Dynamic Routing= IGRP ●Static Routing=default state ●Extended access list ●Static NAT ●No Encrypted Password
Cisco Switch 2950	30	●Layer 2 switch ●24 Fast Ethernet ports ● IOS=12.3 ● VLAN, VTP	●1VLAN/Switch ●default configuration ●No Encrypted Password
Cisco firewall(PIX) 515E	1	●3 Fast Ethernet ports,2 serial ports ●IOS=7.21	●Access-list ●Static NAT ●Default configuration
Cisco Core switch 6051E	1	●Layer 3 switch ●3 modules (fiber optic, Gigabit Ethernet, Fast Ethernet,48 port) ●IOS=12.4	●(50)Port Based VLANS ●Inter VLAN Enabled ●Extended access-list ●Default configuration ●Encrypted Password
Cisco switch 3750 layer2 switch	11	●24 Fast Ethernet ports ●2 Gigabit Ethernet Ports ●IOS=12.4	●1VLAN/Switch ●default configuration ●No Encrypted Password
Antivirus Server	1	●DELL POWER EDGE 6600 SERVER	●Password required
Access point	1	● AP 1200	●64 bit WEP ●MAC Address Filtering

3. BUILDING A SECURED NETWORK:

The main goal of the network security is to protect against the mentioned types of threats and attacks. On the other hand, the added security methods should not affect seriously on the network management or its performance. As a suggestion to achieve these goals, the network topology must reorder, new devices should be added and a reconfiguration should be made to the existed devices. Figure (2) shows the topology of the suggested network.

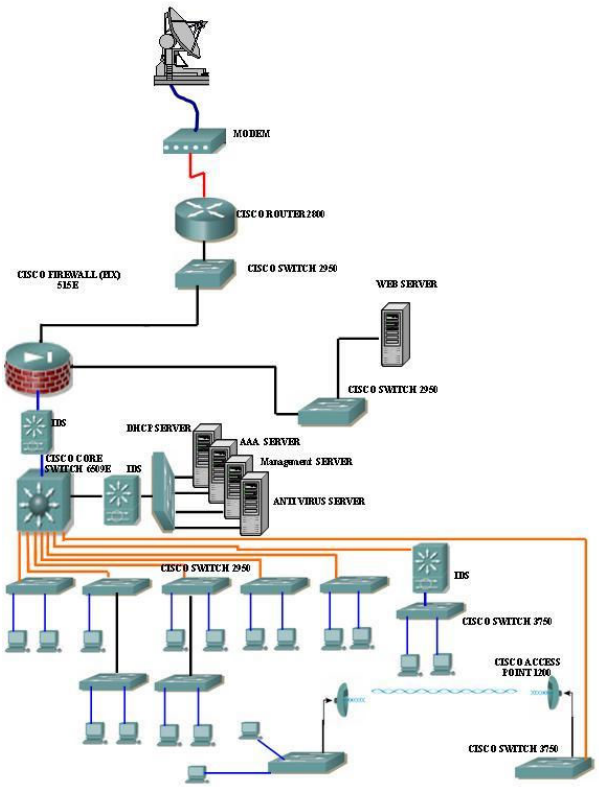

Figure 2: The Structure of the Suggested Network

The heart of the proposed security system is the AAA server. AAA is the acronym for authentication, authorization, and accounting Authentication controls access by requiring valid user credentials, which are typically a username and password. Authorization controls access *per user* after users authenticate. Accounting tracks traffic that passes through the security appliance, gives the ability to have a record of user activity. The security appliance supports a variety of AAA server types and a local database that is stored on the security appliance. Examples of these types are: RADIUS Server, TACACS+ Server, SDI Server, NT Server, Kerberos Server, LDAP Server Support and Local Database Support. Depending on the size of the network and available resources, AAA can be implemented on a device locally or can be managed from a central server running RADIUS or TACACS+ protocols. The AAA server first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the session is allowed and no further intervention is required by the authentication proxy. If no entry exists, the authentication proxy responds to the connection request by prompting the user for a username and password. If the authentication fails, the AAA server reports the failure to the user and prompts the user for a configurable number of retries. The most functionally server type is the TACACS+ Server and it is chosen here for that purpose. Terminal Access Controller Access Control System Plus (TACACS+) is an industry standard protocol specification, RFC 1492, that forwards username and password information to a centralized server. Another AAA server is used as a backup in the case of the fail of the first one and they may cooperate to retrieve against network congestion problem [1, 2].

The other change in the network topology is connecting the web server to the *demilitarized zone* (DMZ) portion of the PIX device. The firewall allows limited access to the DMZ, but because the DMZ only includes the public servers, an attack there only affects the servers and does not affect the other inside networks [1, 2].

In order to manage the network efficiently, a management server is added. This server contains the necessary tools the administrator needs to manage the network, such as traffic analyzer, devices debuggers and remote access software. The server has an HTML Page which acts as a Graphical User Interface (GUI) for the administrator and includes all the accessed network resources. The server could also be accessed using command line interface. It is worth to mention that management server has its own *'User Name & Password'* and can accessed only by the administrator [11].

The other addition to the network is the insertion of Intrusion Detection System (IDS) devices. It is known that IDS monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager. Other legitimate connections continue to operate independently without interruption [3].

The main aim of the proposed solutions is to securely allow the administrator to reconfigure any network device either locally (through console ports), via wired network (switched network), using the WLAN link or remotely using the internet connection.

The philosophy of the suggested security solutions is based on using multiple dimensions of protection and it could be explained as followed:

1. The first security dimension is to protect the network against the internal threats. This was achieved using the following techniques:

- Any access to the network must pass through the AAA server. The AAA server is configured to have two administrators groups. First group consists of 41 sub administrators and the second consists of 2 main administrators (for the whole network). The sub administrators have limited access and authorities to the network devices in their departments only. The main administrator has unlimited authorities and can access any portion of the network with configurations privileges over the sub administrators. Also, The AAA server has different groups and accounts for the different users.
- The (Wired & Wireless) LAN connections of the main administrator are protected using Virtual Private Network (VPN). It is found that VPN connection decrease the channel throughput by (70%) [7], for that reason it is used for the administrator communications only. The following VPN parameters are chosen: The authentication method is pre shared keys, AES encryption method, MD5

Hashed Message Authentication Codes (HMAC), Diffie-Hellman Group 2 (1024-bit) and 12 hour policy lifetime.

- Installing Intrusion Detection System (Cisco IDS 4215) devices in front of important (sensitive data) locations such as the servers farm and the university presidency switch.
- Splitting the network into 50 port based Virtual Local Area Networks (VLANs). It is known that access is denied for a cretin VLAN except their members. The other benefit of using VALN it to limit the damage caused by viruses or worms to the members of the VLAN. Looking from the management point of view, it is easier to administrate a network consist of several VLANs [3]. The main administrator's VLAN has the access privilege over the other network VLANs.
- Each network device is protected using an '***encrypted User Name & Password'*** assigned by the administrator with two attempts. Also the IP address of the administrator is checked by enabling the access list VTY property.
- For further protection, the TELNET service and PING command is disabled in all the switches ports except one of them. These ports on the different switches represent the backbone of the management network. Additionally, Secure Shell Header (SSH) is used instead of TELNET. SSH is an application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities [8]. SSH is configured to have a key modulus size of (1024bit). This key is used by the RSA ciphering.
- The WLAN security is achieved using: Rotated 64bit WEP keys (for better performance), MAC address filtering in each access point and network access is achieved through the AAA server. Also VPN is used for administrator's WLAN connections as mentioned earlier.
- The core switch, AAA server and VPNs are supplied with an Extended access lists. These lists are made up of one or more Access Control Entries (ACE). An ACE is a single entry in an access list that specifies a permit or deny rule, and is applied to a protocol, a source and destination IP address or network, and the source and destination ports [1]. Each device has its own rules on which the access lists were written in order to control the traffic inside the network.
- Disabling any unnecessary services on the network devices.
- Physical protection through installing the important network devices in immune locations. Also each port of the main switches has been secured using a predefined MAC addresses allowed to be connected.
- Using central viruses' server. Symantec Norton Antivirus corporation edition is installed at the server and each client has its own copy which is updated periodically by the server.

2. In order to simplify the management operation, the administrator must be able to access the network from external locations. However, this remote access must be protected against external threats:

- Using AAA server. Any connection request is checked by the AAA server and only the authorized users can access to the network according to their policies.
- In order to access the network remotely, the administrator must use Remote Access VPN connection. This allows the administrator to connect to the management server through a secure connection over a TCP/IP network such as the Internet. This connection has the same VPN parameters mentioned earlier while setting the dynamic Crypto Map. These dynamic crypto maps let the security appliance receive connections from peers that have unknown IP addresses.
- Enabling Network Address Translation (NAT) control. Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. NAT is comprised of two steps: the process in which a real address is translated into a mapped address, and then the process to undo translation for returning traffic [9]. The security appliance translates an address when a NAT rule matches the traffic. If no NAT rule matches, processing for the packet stops. The benefits of NAT are preventing private addresses from being routable on the Internet and NAT hides the real addresses from other networks, so attackers cannot learn the real address of a host. In order to apply Remote administration through VPN connection, static NAT is used.
- In addition to the Extended access lists mentioned earlier, The PIX device (Firewall) is also supplied with an extended access lists. These lists control the traffic in both directions (inside and outside the network) according to predefined rules.
- The whole network is protected against external attacks using another IDS device connected to the *inside* portion of the firewall.
- SSH is used by the administrator only for remote access to the system. It has the configuration mentioned earlier.

4. TESTING NETWORK CONFIGURATION:

In order to test the correctness of the network configuration after considering the proposed security methods and prior to implementing them practically, an experimental test bed represents the network was built. The purpose was to test the network security robustness against different types of attacks. Figure (3) shows a photo of the experimental network.

In order to consider all the suggested security methods, a configuration was made to the network devices as mentioned earlier. The following procedures were taken to examine the network operation:

1. Monitoring the network traffic: attempts were made to monitor the network traffic (as the hacker does before his attack).It was assumed that packet sniffing procedure is done by an authorized user (internal threat) at different locations (inside and out side the network). This action was detected and prevented by the IDS devices.

2. The illegal log in to the network as well as unauthorized access to some services and resources was prevented by the AAA server.
3. Trying to use the TELNET service or PING command was stopped by the switches access lists. Also, the firewall prevents any suspicious packet from entering the network.
4. Any attempt to discover the real IP addresses of the network was stopped by the NAT policies.
5. VPN technique was very effective in hiding the administration packets from the eyes of the eavesdroppers.

Also, several additional tests were made on the network to check the activity of the other security methods (the authors have the detailed documented lab tests in addition to the configuration files for all devices). It was found that protection of a network could not be achieved by a single technique but with an integrated bundle of solutions.

Figure 3 : The Experimental Network

5. CONCLUSION

The growing demand of the Internet performance has greatly complicating the design of high performance network infrastructure. In spite of the convenience brought by networks, many security problems such as filching computer document, sniffing network data, computer virus, and crack arise. For these reasons, researchers had brought up various mechanisms to solve them. This paper examined the possibility of building a typical security model for Mosul university network. The procedure in which security methods is added guarantees strong resistance against different intrusions and attacks. The proper adoption of different security levels, methods and procedures in a highly integrated fashion safeguard the operation of the network. The design of such a system should provide the balance between creating a highly immune system and good performing, efficiently managed network.

REFERENCES

[1] Cisco Inc., “Cisco Security Appliance Command Line Configuration Guide”, 2006

[2] Cisco Inc., "Cisco Product Catalog", http://cisco.com/univercd/cc/td/doc/pcat

[3] Cole E., Krutz R. and Conley J., ”Network Security Bible”, 1’st Edition, Wiley Publishing Inc., 2005.

[4] Gabrys, E., “The international dimensions of cyber-crime”, Information Systems Security, 2002.

[5] Hyland P. C. and Sandhu. R., “Management of Network Security Applications” In Proceedings of 21st NIST-NCSC National Information Systems Security Conference, 1998.

[6] Ohta K., Mandfield G., Takei Y., Kato N. and Nemoto Y., “Detection, Defense, and Tracking of Internet-Wide Illegal Access in a Distributed Manner”, In Proceedings of INET'2000, July 18-21, 2000.

[7] Riedmüller S., Brecht U., Sikora A., "IPsec for Embedded Systems", in: H. Weghorn (Ed.), "Proceedings of the 2ndAnnual Meeting on Information Technology & Computer Science at the BA-University of Cooperative Education", ITCS 2005.

[8] Stallings W.,”Data & Computer Communications”, Sixth Edition, Prentice Hall Publishing, 2003.

[9] Tanenbaum A.S.,”Computer Networks”, 4’Th Edition, Prentice-Hall Publishing, 2003.

[10] Varadharajan V., “Design of a Secure Network Administration System", Technical Report, UWS Computing, 1995.

[11] Yemini Y., “Emerging Trends in Networks and System Management", Third International Symposium on Integrated Network Management, San Francisco, USA, 1993.