Global Information Assurance Certification Paper

Critical Overview of System and Information Security

Security Issues vs. Remedies

Nov. 30, 2003

Name: Ming-Yin (Cindy) Huang
GSEC
GIAC Security Essentials Certification Practical Assignment
Version: 1.4b (Option 1)

1. Abstract

The following System and Information Security overview is based on the system of a particular government agency. The purpose of this paper is to show:

(1) The issues that have been put into consideration such as security issues (trouble spot) and remedies (fixing tools) during the system design phases,

(2) The difficulties encountered while tried to deploy the information security plan and enforce the security policy for the entire agency,

(3) The future challenges of protecting the system and information security.

Table of Content

2. Introduction

As the Internet gains its popularity rapidly since the 1990s, more and more universities, companies, enterprises and government agencies have their local area networks (LAN) connected to the Internet. In the recent years, E-Commerce helps enterprises do their business on-line through the Internet, and E-Government also becomes the main stream for most of the government agencies. Information sharing, on-line service and communication through the Internet have been a requirement among government agencies. Nowadays, many federal government agencies such as NIST (National Institute of Standards and Technology), NIH (National Institutes of Health), PSC (Program Support Center), HRS (Human Resources Service), USCIS (U.S. Citizenship and Immigration Services), and most of the local government agencies provide diverse services and information via the Internet to their customers.

Since the Internet is a wide-open network that contents multiple administrative domains with no central authority or management, any one who has access to the Internet can easily penetrate or hack into any private network systems such as a bank to get account numbers and/or transfer money without authorization, a private corporation to steal customer information, a health institution to get confidential medical records, or military systems to grab the national security information, and so forth. In fact, these attacks are on the rise. Fortunately, many of CIOs (Computer Information Officers) and CTOs (Computer Technical Officers) are becoming more and more security conscious and willing to pay more and more attention to the information security than ever. Since the technologies change rapidly, making sure the network and information systems are secured becomes the major challenge for the IT professionals because it does not only require frequent system updates but also constant system review.

3. Network Environment of the Agency

Two major system upgrades - network operating system (NOS) and system backbone security– are scheduled to roll out in a few months period at the agency.

March 2004 – The new NOS upgrade plan is scheduled to roll out starting at the beginning of March 2004. The major NOS will be upgraded from Windows NT 4.0 to Windows 2003 in the native Windows 2003 AD mode. Gradually, more and more servers such as E-mail server, web server, file server, application server, print server and database servers will be set up to join the domain to be the production servers. Like many other government agencies, the network system of our agency also includes other NOSes such as Red Hat Linux/HP-UX that handle DNS (Domain Name Services), Firewall (Gaunlet) and Oracle database systems.

June 2004 – The network backbone security system will be also upgraded. The entire network backbone system will be redesigned, tested run in the computer lab for three months and finally rolled out to production around the end of the second quarter of year 2004. Several new firewall boxes (Sidewinder G2 Firewall) will be integrated into the network system to replace the current firewall that was set up on one of the HP-UX servers. Furthermore, all IOS (Internetworking Operating System) on routers and switches will be updated to the version that supports SSH (Secure Shell) or physically replaced by newer models that are compatible with SSH features. The ACL (Access Control List) which was set up on the routers and switches will be carefully reviewed and reconfigured to make sure only the permitted workstations and users can access the routers and switches.

4. Addressed System and Information Security Issues

When the information security staffs and the system consultants started outlining the System and Information Security Policy and Disaster Recovery Plan, electronic and physical accessibilities were the two major areas we focused on.

4.1. Electronic Accessibility

To make on-line services and shared information available to the government employees and customers, the network system of the agency should not only be accessible from the LAN, but also from the Internet. Therefore, "Who has what permissions to access what" becomes a crucial issue. To make sure only the authorized users with appropriate permissions can get into the network systems, myself, the other IT professionals, and System/Information Security Officers have worked very closely to lay out the information/system security policy and disaster recovery plan.

4.1.1. System and Information Security Policy

The security policy exists to explain what the security goals of the site are, what users can and cannot do, what to do and who to contact when problems occur. In general, the security policy tells the system administrators and end users what the "rules of the game" are.

Firewall, vulnerability scan software, system/software patch management tool, and virus scanning software are the technologies and tools used to ensure the security of the network systems in our agency. As for information security, Kerberos authentication and Encrypting File System (EFS) will be deployed on the server systems to further ensure the data integrity. In addition, there is a system/information disaster recovery plan that includes tape backup, high availability/failover systems such as RAID 5 (Redundant Array of Independent Disks-disk array techniques), Standby Router, and spare switches.

4.1.1.1. System Security

A. Firewall

Firewall is, perhaps, the most common technology widely implemented to protect the network system security nowadays. In other words, the main job of the firewall is to prevent unwanted users from accessing the network while allowing approved users to gain access.

"Firewalls started off as simple packet filters, moved toward more security with application gateways, branched off into stateful inspection, and evolved to today's superior "hybrid" firewall."[1] Today, we can talk of filter-based, proxy-based, and hybrid firewalls, from simple appliances to multipurpose servers.

In recent years, more and more router vendors such as Cisco and Juniper have added the features and functions normally associated with a firewall to their products, so that the router not only can route the network traffics, but also filter any unauthorized inbound/outbound communications. With advanced configurations, any intrusions will be reported to a logging server in the corporate office. Some high-end routers such as Cisco 7000 series also provide VPN (Virtual Private Network), data encryption, and support DMZ (De-Militarized Zone) feature and SSH (Secure Socket Shell) Protocol.

To protect the system at the network level, IT managers at our agency have addressed issues such as (1) how to properly identify users and enforce access control, and (2) how to protect the server from being abused by authorized and unauthorized users. In reality, solving one of these problems generally helps in solving the other. However, since the network isn't segregated, any compromise of one system can potentially be used as a springboard to other systems on the private network. Therefore, the Access Control List (ACL) is carefully designed and deployed on the routers and switches on each floor to ensure the unauthorized users cannot hack into the network systems from any points. Among sites, VPN tunnels are set up to secure the network connections and data transactions. As for DNS server, which provide name resolutions for the entire network systems and need to synchronize with DNS databases with other government agencies, is isolated in the private DMZ.

The access control lists on our Cisco router are useful as a stopgap but unwieldy to manage and prone to letting stray packets through when they should not have. To ensure the system can be easily managed, we eventually decided to deploy a border firewall of our own. After a careful review of our network systems and a number of product testing reports, our IT team finally chose Sidewinder G2 Firewall appliance, the easiest and most sophisticated solution, to guard our system front door. Unlike software package (Gaunlet installed on HP-

UX server), the new preinstalled and pretuned Sidewinder G2 Firewall/VPN appliance provides an out-of-box security solution that does not require complicated configuration or advanced knowledge of HP-UX Operating System. Furthermore, its hybrid, tunable architecture also encompasses the entire range of firewall security mechanisms including stateful inspection, circuit level proxies, application proxies, secured servers, and real-time strike back alerts in one simple, cost-effective package.

B. Vulnerability Scan & System Patch Tools

Both software and hardware companies, in response to the discovery of security vulnerabilities, provide sets of files that have to be installed on the hardware and computer systems. These files "fix" or "patch" the computer - both server and workstation - systems, programs or firmware and remove the security vulnerabilities. However, there is a requirement for constant check, download and installation of the most up-to-date patches/hot fixes, and keeping servers patched with the latest security bug fixes. It may seem like a daunting task. Nevertheless, with some newly developed patch management tools, closing the known security holes, removing security vulnerabilities, and staying current are relatively easy.

a. OS/Software – vulnerability assessment tool vs. Patch management tool

Most successful network security attacks target at known vulnerabilities, which patches already exist. And the reason for that is because network administrators either didn't install/update the patches/hot fixes or users reinstalled the vulnerable systems without awareness of network administrators. It is easy to be smart about the former, but just as important to be vigilant about the latter.

Currently, the agency is using vulnerability assessment tool such as CyberCop, ISS, and MBSA (Microsoft Baseline Security Analyzer) to scan and identify security weaknesses on the servers and workstations. Although these scans provide detailed information on the vulnerabilities found, they don't provide the means to automate the resolution of those vulnerabilities. The remediation process is left to an already understaffed IT department that finds itself overwhelmed by the significant time and effort required to resolve each vulnerability.

The recent W32.Blaster (August 12, 2003), Welchia (August 18, 2003), and Sobig (August 20, 2003) worm attacks, for instance, made IT managers realized that with the increasing frequency of attacks and potential damage, it is

difficult for system administrators to stay on top of the overwhelming remediation task without deploy the automated patch management technologies.

Among several patch management tools – Hercules, PatchLink Update, PatchAdvisor, HFNetChkPro, PatchWorks, UpdateEXPERT, and Microsoft SUS (Software Update Services), we recommended Hercules. Hercules, which is developed by Citadel, not only provides central point of management and patch distribution, but also integrates with industry leading vulnerability assessment tools - ISS Internet Scanner and MBSA - which is currently deployed on our system to provide appropriate remedies for all five classes of vulnerabilities: (1) Unsecured Accounts, (2) Backdoors, (3) Software Defects, (4) Unnecessary Services and (5) Mis-configurations.

b. Hardware – firmware and new drivers

Since there is no patch management tool developed to scan and remove the known vulnerabilities of firmware on the network devices such as system network cards, switches, routers, or firewall boxes, the firmware/driver update news are subscripted from the venders' web sites. When new patches or drivers are available, all of them will be downloaded and saved to a central patch & new driver folder on the network-shared drive. Then, the notice of new patches/drivers will be sent out to network maintenance team, so that they can start working on the firmware or driver updates and have the updates completed within a week.

C. Virus Scan & Cleaning

Viruses are certainly unwanted pieces of software that find their way onto a computer. What the virus may do once it has entered its host depends on at least the following two factors: (1) what has the virus been programmed to do (depends on the type of the virus)? (2) what part of the computer system has the virus attacked?

Some viruses are "time bombs" which activate only when given a particular condition such as reaching a certain date. Others remain latent in the system until a particular afflicted program is activated. There are still others that are continually active and exploiting every opportunity to do mischief. A subtle virus may simply modify a system's configuration then hide.

Recently, e-mail has become the favored vector for infections, the rate of infection can hit tens to hundreds of thousands of machines in an hour (witnessed in the Melissa and love letter virus), and the vast majority of users do not have anti-virus software, or if they do, it is not up to date.

In order to standardize e-mail, file/folder, and system viruses scan/clean processes, and centralize the management of virus control, the agency has recently implemented two client/server based anti-virus software: NetShield, which detects file/folder and system viruses, and GroupShield, which detects e-mail viruses, from Network Associates, Inc. With proper configuration and scheduling, both software can automatically detect and clean the viruses, update the virus signatures, send e-mail alerts and report to the system administrators and managers on daily basis.

4.1.1.2. Information Security

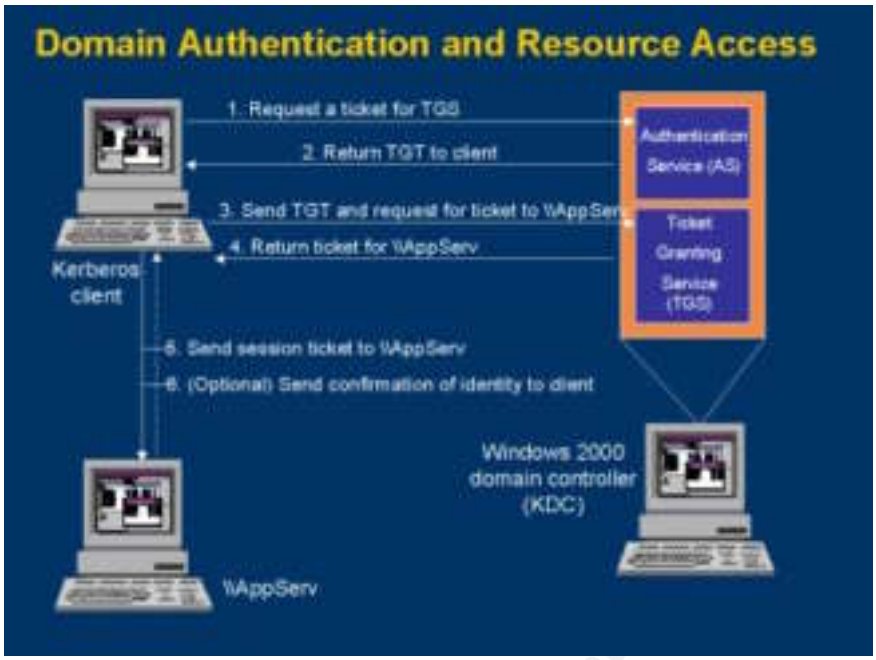
A. Kerberos Authentication

Authentication of the user's identity can be seen as the most frontline of information security. It decides who has the right to get into the system. The default authentication package in Microsoft Windows 2000/2003 is Kerberos. It is based on encrypted tickets with client credentials. "Kerberos is the basis for transitive domain trusts. It is based on RFC 1510 and draft revisions"[1]. It is more efficient (faster and less traffic) and secure than NTLM (New Technology LAN Manager) previously used by Windows NT Server 4.0.

Kerberos authenticate user's identity by user's principle name such as someone@ctst2004.org. Kerberos securely delivers user credentials in a ticket. That ticket contents a PAC (Privilege Attribute Certificate). It is the attached ticket for a KDC (Key Distribution Center on Windows 2000/2003 Domain Controller) to effectively deliver the users credentials to the network resource. Kerberos also has privacy through encryption and uses keys for encryption.

Kerberos authenticator prevents packet anti-replay. By time stamping each packet, authenticator prevents the packet from being captured off from the wire and resubmitted onto the wire at the later time, so the receiving server will not utilize the payload of the data that had been tempered with. In other words, if the authenticator is not valid, the packet will be discarded.

The following figure demonstrates how Kerberos authentication works.



http://www.wilsonmar.com/kerberos.htm[2]

B. Encrypting File System (EFS) and mobile users

The Encrypting File System (EFS) is a feature of the Windows 2000/2003 operating system that lets any file or folder to be stored in encrypted form and can be decrypted only by an authorized individual user or recovery agents. EFS is especially useful for mobile computer users whose computers (and files) contain highly sensitive data and are subject to physical theft.

However, since Encrypting File System is only supported by NTFS file system on Windows 2000 and later version of Windows (such as Windows XP and 2003) Operating Systems, the Manager of IT department has to make sure the standard of the file system (NTFS) is clear to each helpdesk staff, especially for those who are responsible for setting up the laptops for mobile users (such as department managers or directors) who frequently travel around the country with sensitive data on their hard drives.

C. VPN – IPSec

A VPN (Virtual Private Network) is a way to use a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their organization's private network. Through a tunnel, VPN connections not only allow users to work from home or on the road to connect in a secure fashion to a remote corporate server using the Internet, but also allow a corporation or government agency to connect to other companies or branch offices over the Internet while maintaining secure communications.

In the early days, a virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost. There are three VPN protocols that provide encryption, authentication and data integrity for clients/hardware devices to communicate with the VPN concentrator. The definitions of these three VPN protocols are as the followings:

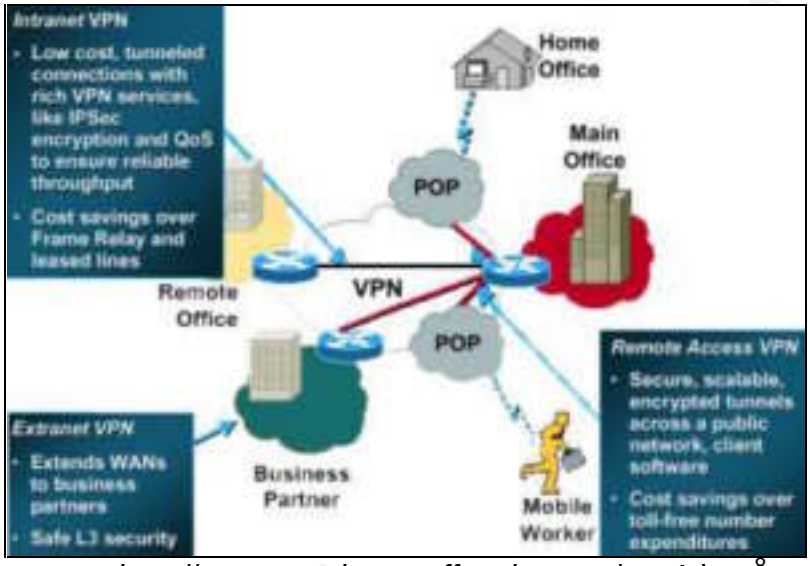
> (1). **IPSec** - "short for IP Security, is a set of protocol developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement VPN. IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the playload. On the receiving side, an IPSec-compliant device decrypts each packet. To IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates."[3]
>
> (2). **L2TP** - "short for Layer 2 Tunneling Protocol is an extension to the PPP protocol that enables ISPs to operate VPNs. L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. Like PPTP, L2TP requires that the ISP's routers support the protocol."[4]
>
> (3). **PPTP** - "short for Point-to-Point Tunneling Protocol, a new technology for creating VPNs. It is developed jointly by Microsoft, US Robotics, and several remote access vendor companies, known collectively as the PPTP Forum. PPTP is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet."[5]

The first and widely distributed remote user VPN protocol is the Point-to-Point Tunneling Protocol (PPTP) from Microsoft. "The Point-to-Point Tunneling Protocol (PPTP) is a de facto industry standard tunneling protocol first supported in Windows NT 4.0."[6] "Today, the IP Security (IPSec) protocol has emerged as an industry standard protocol. While the IPSec protocol provides strong security, we will also see it used with the Layer 2 Tunneling Protocol (L2TP) to help out with IP addressing management on the VPN clients."[7] Because IPSec is relatively simple, easy to setup and integrated with Windows server 2003, and widely supported by the firewall, and client systems, our system upgrade team

had decided to implement it as our VPN solution during the first phase of the system upgrades (Windows Server upgrade).

With pre-shared keys, the workstations and servers can easily communicate to each other in a more secure and cost-effective fashion through the firewall (Sidewinder G2) and VPN tunnels.

The following figure demonstrates how IPSec works.



http://computer.howstuffworks.com/vpn1.htm[8]

4.1.1.3. System Disaster Recovery Plan

Survivability is probably the most important thing that IT managers focus on. When the servers can not provide services, data is lost, or hardware is damaged, the most common question asked is "How soon can the system be up and provide the services again." At this point, there are three techniques: (1) System Backup, (2) RAID 5, (3) Router/switch clustering will be implemented on the systems to assure the system could be recovered from network disaster within hours.

A. System Backup

Tape backup is a traditional, but probably the best way to assure data, information and system availability and fast system recovery. Without a proper backup solution, any problems with the network systems whether due to accident or malicious attack can be devastating.

While tape backup is a viable solution, it requires additional hardware, software, administration and effective backup strategy. Backup schedules must be created. Tape rotation and off-site storage must be set up as well.

IT managers of our agency take system and information backup very seriously. Based on size of the databases, system files, functions of the server, backup devices used, tape capacity, and importance of the data/information, different types of backups (full backup, differential backup and incremental backup) are implemented on each server. For instance, database servers that contain huge databases of payroll information and are updated frequently will be backed up incrementally on daily basis. Application and print servers that only updated once in a while is backed up fully on weekly or bi-weekly basis.

B. RAID 5

System storage is one of the major parts of the network. RAID, an acronym for Redundant Array of Independent Disks, disk array techniques, allows sets of drives to be grouped for availability purposes, and provides the redundancy necessary for data protection and sometimes performance advantage as well. Depending on RAID levels, 0, 1, 3, 5, 10, 30 and 50 (level 0, 1, 3 and 5 are established as a industry standards), each level provides different degree of data protection and performance advantage.

RAID levels can be implemented with software or hardware. Many, but not all, network operating systems support at least some RAID levels up to level 5. Level 10, 30, 50 are only possible with a Disk Array Controller (DAC). Software-based RAID uses host CPU cycles and system memory, thereby adding overhead that may impact system performance. DACs, on the other hand, move the burden of RAID computations and manipulation from software to specialized hardware and often perform better than software RAID.

Considering data availability, system performance improvement, reasonable costs, and industry standard factors, IT managers eventually choose RAID 5 to be the standard RAID level and widely implement with hardware (DAC) on each server.

C. Standby Routers and spare switches

Hardware such as routers and switches are known as the backbone of the network (LAN, WAN and the Internet). They are also known as very sensitive devices. Power surge or system overheat might easily damage the router/switch interfaces, causes the system crash and cut of the network connection. To prevent this from happening, the Cisco routers are set up to mirror each other (to synchronize the configuration and routing table periodically). One of them is set to be the hot-standby (Cisco term: Hot-Standby 1+1 Redundancy) router. In this case, if one router went down, the hot standby will be able to pick up instantly and continue the routing tasks. Therefore, the chances of experiencing network downtime are reduced.

The agency also purchase extra switches as spare switch so that when floor switch goes down, network engineers can easily replace it with the spare switch to ensure the network downtime is minimum.

4.2. Physical Accessibility

Logical controls can be rendered useless if someone can come in and physically tamper with a machine, change the configuration, cause system outages, or even steal the network devices.

With the increase in the numbers of client-server networks and 3-tier networks, resources are more physically dispersed and, as a result, more vulnerable. Aware of the physical accessibility being a very important part of system/information security, the agency has electronic security guard system such as electronic access card and Kastle systems setup to assure only authorized personnel can get into the building and office (during the office hours or off-hours). And only the IT professionals and system consultants, who have to work on network systems or devices such as cable, hubs, switches, routers or servers, have the permission (access card with access codes) to get into the data center.

5. Critical Overview

Based on the issues that have been addressed in the security policies laid out by our IT team, the network systems, in general, seem to be pretty secure. However, there are still some potential factors that have been ignored and might danger the entire information and network system security.

5.1. IT Budget & Not Me Syndrome

It's not easy getting security funded. Even if the risk is recognized, management may choose a less-expensive alternative solution. Also, the security budgets for government agencies are usually run through a gauntlet of fiscal scrutiny, making it nearly impossible for security officers to submit a proposal based solely on threats. Also, the IT director must change their proposals and look at their mission from a business perspective--justifying expenditures by documenting the extent of business risk reduction. "Believe or not, 'Not Me Syndrome' is one important factor in the decline of efforts toward increased security. The IT/IS professionals understand the need, and provide for security needs in their operating budgets. Upper management slashes the budget, eliminating line items for security in favor of increasing technology. The

result is greater reliance on technology coupled with greater vulnerability to attacks. After all, it won't happen to me." [9]

5.2. No CERT and Lack of Professionally Trained Information/System Security Staffs and Contingency Plan

Base on network environment such as design of the system infrastructure, size of the network, number of the remote sites, and complexity of the interconnectivities of operating system platforms (Windows, Linux/UNIX, Netware or Macintosh), the organization should at least delicate one group of professionally trained information security staffs whose primary job is to make sure the information system is secure and function as a CERT (Computer Emergency Response Team) responding to any network system incidents, and to handle emergency situations.

Regardless of the number of the users (around 400), servers (around 50), server platforms (Windows and Linux/UNIX) and design of the network backbone (routers and switches), the agency assigned only one IT professional to be the information/system security officer who, most of the time, has to function as a help desk, network engineer and cabling technician.

Since the survivability depends not only upon the selective use of traditional computer security solutions, but also upon the development of effective risk-mitigation strategies that are based on scenario-driven "what-if" analyses and contingency (including system recovery), in order to response to system emergencies in a more efficient way, at first, the IT department should form a Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT), and send the team members to the information/network system security training. After all, only the professionally trained staffs know how to respond to various emergency situations.

6. The Challenges

There are three major challenges that we are facing at the network design phase. One is the learning curve. For the infrastructure of Windows 2003 Active Directory is not as simple as Windows NT domain model, every one in the network system design team has to learn the new infrastructure as fast as possible and be able to apply their new-learned knowledge including the new security protocols, issues, and concerns and possible solutions to the real-life situations. While each government agency function as perspective division that requires a unique Active Directory schema, to keep single-forest architecture as Microsoft would recommend is another challenge. The third challenge is that the multiple forests with trust relationships for AD replication and remote accesses require several ports to be opened on the firewall. This also means more network security holes on the system.

7. Conclusion

Getting the right information to the right person, at the right time, anywhere, on any devices is the basic concept behind the information and network system security scene. However, to keep hackers/crackers out of the network systems at our agency, IT managers and professionals need to approach the security issues from different angles. First, all IT staffs need to understand that information system security is a continuous process, not just a "one-time" project. Second, in order to keep the system security to meet a certain acceptable level and consistent, instead of being reactive, Information Security Officers, CERTs/CIRTs, and other IT professionals should all work proactively and be very aware of new security issues that are posted on the public media, e-mail alerts from vendors and as such. The final and most important thing to keep in mind is that precise, firm security and consistent policies and processes are very important. After all, the security doesn't have to be perfect, but risks do have to be manageable.

References

[1] Walla, Mark. "Insider Insights: Kerberos explained," Windows Advantage May, 2000.

[2] Mar, Wilson "Kerberos Authentication Security. "
URL: http://www.wilsonmar.com/kerberos.htm

[3] Author unknown. Webopedia, 29 January 2002
URL:http://www.pcwebopaedia.com/TERM/I/IPsec.html

[4] Author unknown. Webopedia, 9 January 2002
URL: http://www.pcwebopaedia.com/TERM/L/L2TP.html

[5] Author unknown. Webopedia, 27 June 2001
URL: http://www.pcwebopaedia.com/TERM/P/PPTP.html

[6] Author unknown "Point-to-Point Tunneling Protocol." Microsoft Windows 2000 Advanced Server documentation. 28 February 2000
URL:http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/sag_vpn_und07.htm

[7] Author unknown "Virtual Private Networking." 2002.
URL: http://www.securitydogs.com/vpn_overview.html

[8] Tyson, Jeff "How Virtual Private Networks Work." Howstuffworks
URL: http://computer.howstuffworks.com/vpn1.htm

[9] Miora, Michael, "Security Awareness is Rising while Security Protections are Falling, "Carolina Computer News, January 1999