Global Information Assurance Certification Paper

Biometrics for Remote Authentication

John Holbrook
GCFW Practical
Version 4.0

November 1, 2004

Table of Contents

Assignment 1: Biometrics and their use as authentication mechanisms for remote access.3
Abstract....3
What is biometrics?....3
Advantages....4
What's wrong with passwords?....4
Identity Verification....4
Cost....5
Disadvantages:....5
Security Compromises....5
Lack of standards and vendor lock-in....6
User is tied to hardware....6
Further Considerations for biometrics....6
Template Storage....7
User Acceptance....7
Conclusions....8
Assignment 2 – Security Architecture....9
Abstract....9
Network Diagram....9
Note on hardware recommendations....11
Access Requirements....11
Customers....11
Suppliers....11
Partners....11
Branch Locations....11
Internal Employees....11
"Road Warriors" Sales Force....12
The Public....12
Architecture Components....12
Border Router....12
Firewalls....13
Switches....14
Intrusion Detection....14
Stealthed Syslog....15
Additional layers to defense in depth....15
Operating Systems....15
Physical Security....16
Time Synchronization....16
E-mail Traffic....16
Assignment 3: Firewall Policy....18
References....23

Assignment 1: Biometrics and their use as authentication mechanisms for remote access

Abstract

Not too long ago, biometrics was only seen in movies and read about in spy novels. However, biometrics has made, from very humble beginnings, great leaps of reliability and functionality, in a very short period of time. This paper will cover a quick overview of how biometrics works and discuss the advantages and disadvantages of using biometrics for remote employee authentication over more common authentication methods such as passwords and smart cards.

What is biometrics?

Biometrics is "The automated use of physiological or behavioral characteristics to determine or verify identity."[1] In other words, the use of fingerprints, iris, hand geometry, facial geometry, etc to verify the identity of a person.

There are six types of biometric systems:[2]

- Hand Geometry – Mostly used in physical access control due to requirements for a large scanning device
- Fingerprint Recognition - Best known and most common. Low cost. Easy integration.
- Iris Recognition – Uses unique random patterns in the iris (the colored ring of tissue surrounding the pupil) to authenticate a person. Less intrusive then retinal scanning because it does not require close contact to the eye.
- Retinal Scanning – Analyzes blood vessels located at the back of the eye. Inconvenient to use because it requires physical contact with scanner.
- Voice Recognition – Most difficult to use because voices change due to colds, moods, background noise, etc.
- Face Verification – A lot of hype from vendors that it will catch terrorists in airports etc but very little real success to back up these claims

The most prevalent use of biometrics currently is to authorize people for physical access to buildings, offices, etc. However, the market for remote access biometrics is growing extremely fast and there are plenty of companies releasing new products into the marketplace all the time.

How biometrics works

The following was taken from[3] (with additional comments by the author) I will be focusing on fingerprints for biometric authentication, due to its greater prevalence in the biometrics industry.

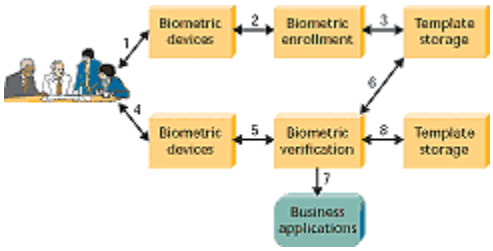


Figure 1. How a biometric system works.
(1) Capture the chosen biometric; (in our case a fingerprint)
(2)process the biometric and extract and enroll the biometric template; Basically a mathematical calculation based on the patterns on the fingerprint which produces a "signature")
(3)store the template in a local repository, a central repository, or a portable token such as a smart card;
(4)live-scan the chosen biometric;
(5)process the biometric and extract the biometric template;
(6)match the scanned biometric against stored templates;
(7)provide a matching score to business applications;
(8)record a secure audit trail with respect to system use.

Advantages

What's wrong with passwords?

All security is based on one or more of the following[4]:
- Something you have (e.g. Picture ID, token, smart card)
- Something you know (e.g. Passwords)
- Something you are (e.g. Biometrics!)

The first two share one common trait – they can be lost, copied, stolen or shared. In fact, in a recent survey more than 70% of people asked would "reveal their computer pasword in exchange for a bar of chocolate".[5]

The International Biometric Industry Association sums up the advantages of biometrics over passwords very well:"Something one possesses, a token, and something one knows, a password, are not sufficient to ensure positive identification of a person. Tokens are routinely mislaid and stolen. Passwords are routinely shared, forgotten, left in plain sight, and stolen. IBIA believes that it is a mistake to regard passwords, tokens, and biometrics as equally sound means of authenticating remote network users. Biometrics can reliably perform that function but passwords and tokens cannot."[6]

Identity Verification

The biggest feature that is missing from passwords which biometrics fulfills is passwords can authenticate a person but cannot verify identity. For example, somebody may remotely log into our network as 'jsmith' with the correct password for 'jsmith' but how do we know that 'jsmith' is REALLY the person logging into the remote PC? We don't. That is why there is so much interest in biometrics.

How does biometrics verify identity? Because users cannot give away, lose, share, forget their fingers, or eyes, etc we can be confident that the user really is who they say they are. Since fingerprints are also unique we can be confident that nobody will be able to 'spoof' the users identity.

The demand for identity verification is growing all over the world. The United Kingdom recently finished a test of various biometric systems to "provide a modern, secure means of confirming identity, helping us to crack down on identity fraud, immigration abuse, illegal working and organised crime."[7]

Cost

To use biometrics for authentication, some sort of biometric device must be purchased. From my research, it appears that the average cost for each biometric fingerprint device is approximately $80-$150US. This cost is dropping as more companies and individuals use biometrics. For our use to authenticate remote users this cost must be justified, compared to the cost of continuing to use passwords, and a ROI must be calculated for management to accept this expenditure.

"Forrester Research estimates the annual cost for password administration per user is between $340 and $800."[8] Because a fingerprint cannot be forgotten your Help Desk staff will not have to spend any more time resetting passwords for users who forget them, you will notice a substantial cost savings in a very short period of time.

Disadvantages:

Security Compromises

There have been several reports of being able to compromise the security of biometric devices using various methods. For example, in 2002 a Japanese researcher was able gain unauthorized access 80% of the time using two different methods against fingerprint based biometric devices with fake gelatin fingers.[9] While most vendors would like you to believe that biometrics is completely secure this obviously isn't the case. As with any security method, if there is a way to bypass it, with enough money and time, somebody will!

If the decision is made to store the biometric templates on a central server and this server is compromised by a cracker what will a company do? You cannot re-enroll your users because their fingerprints are not going to change. Your only apparent option would be to find and purchase another company's product which uses a different calculation method to create the template or talk to the original vendor for a solution. Unfortunately, while you are doing this, your remote users will be unable to authenticate.

Lack of standards and vendor lock-in

Biometrics, like a lot of new and emerging technologies, suffers from a lack of standards and open APIs which has made it difficult to purchase biometrics hardware from one vendor which would work with another vendor's software. This has led to vendor lock-in and challenges when one vendor's software has features which a company would like to use but have already invested heavily in another vendor's products. The wholesale abandoning of an investment in one company's biometrics because of this is not something that any IT Manager is going to want to explain to management.

Several initiatives have been started over the years to solve this problem. The most successful initiatives have been the BioAPI Consortium at http://www.bioapi.org and the Biometrics Consortium at http://www.biometrics.org. The BioAPI Consortium has over 50 members (including Unisys, Compaq and Intel). Microsoft was one of the original members however they abandoned BioAPI several years ago to develop their own "standard". Even though these two organizations released a merged standard several years ago, there is still a very limited number of products which are BioAPI compliant – http://www.bioapi.org/compliantproducts.html.

User is tied to hardware

Currently, your organization may allow remote access to your network through a web browser and simple password authentication. This has the advantage that staff can have network access from anywhere in the world that they can get access to a web browser through. (Of course you would have policies in place on where users can access from and what is required). If you decide to use biometrics, then your users are tied to certain pieces of hardware where the biometric devices are connected to, and have the required software loaded on.

What happens if a user is on the road and his laptop with the built-in biometric device is damaged? This is a consideration that must be taken into account when evaluating biometrics.

Further Considerations for biometrics

Template Storage

When implementing biometrics a consideration is where to store the biometric template. The biometric template may be stored within the biometric reader device, remotely in a central repository or on a portable token (e.g. Smart card).[10]

Each has it's advantages and disadvantages. Storing on the reader device means that there is no external access required to verify the template. This requires that the device works correctly and if there are any technical problems with the device then the user will not be able to authenticate until the problem is fixed.

Storage in a central repository requires reliable network access for authentication to work. If the employee is authenticating over a slow network connection they may find it very frustrating while the template is being verified. Of course if network connectivity is down then the user will be unable to authenticate at all.

Storage on a token (smart card) is a viable option because it allows the employees to carry their template with them wherever they may be. They will still require access to a biometric device which will be compatible with the smart card, etc.

If storage on a token or the biometric device is selected then what happens if the token or biometric device is lost or damaged? The user will have to re-enroll and go through the entire process of having his or her template recreated. This could be an issue with remote users who travel a lot. If this situation occurs, then the user could be without access for an extended period until they can get to a location to be re-enrolled.

User Acceptance

Just like any other method of authentication, if the users will not accept biometrics then it will not work and you will meet with nothing but frustration.

As an example, my employer installed a small fingerprint biometric device for some software we use. Out of a department of approximately 10 people 9 had no problem with using the device. However, one users absolutely refused to use the device because he honestly believed that the device was taking his complete fingerprint and somehow sharing it with the government, police, “Big Brother”, etc. Even after explaining that that there is no actual copy of your fingerprint and that the template was stored on the local PC, he still refused to use the biometric device.

Because users see their fingerprint as part of their personal identity, privacy concerns can be raised by staff. One solution to this is to put the user in charge

of their template by storing it on a smart card which the user will be in charge of.

Conclusions

Since 9/11, governments around the world have been demanding more secure ways to positively identify people which has increased the demand for biometrics. Companies are also realizing the major weaknesses in depending on passwords as their only form of authentication.

Using biometrics for remote authentication of users makes a lot of sense because it is convenient, lowers costs, and verifies the identity of the user logging in. However, as mentioned there are several shortcomings including standards, user acceptance, etc.

Assignment 2 – Security Architecture

Abstract

GIAC Enterprises was a wholly owned subsidiary of a much larger worldwide conglomerate which has recently gone through some major restructuring. During the restructuring, the decision was made to sell off GIAC Enterprises as a cost saving measure. The existing management team decided to purchase GIAC Enterprises and run it themselves. The existing IT Manager decided to pursue other career options at another company.

GIAC Enterprises markets fortune cookie sayings to customers worldwide. There are currently approximately 50 staff employed at GIAC Enterprises – 15 in the Head Office in Vancouver BC Canada, 5-10 in each of the 4 branch offices (Toronto, San Francisco, New York and Hong Kong), 5 “Road Warriors” (Sales staff who travel the world doing all business from their laptops)

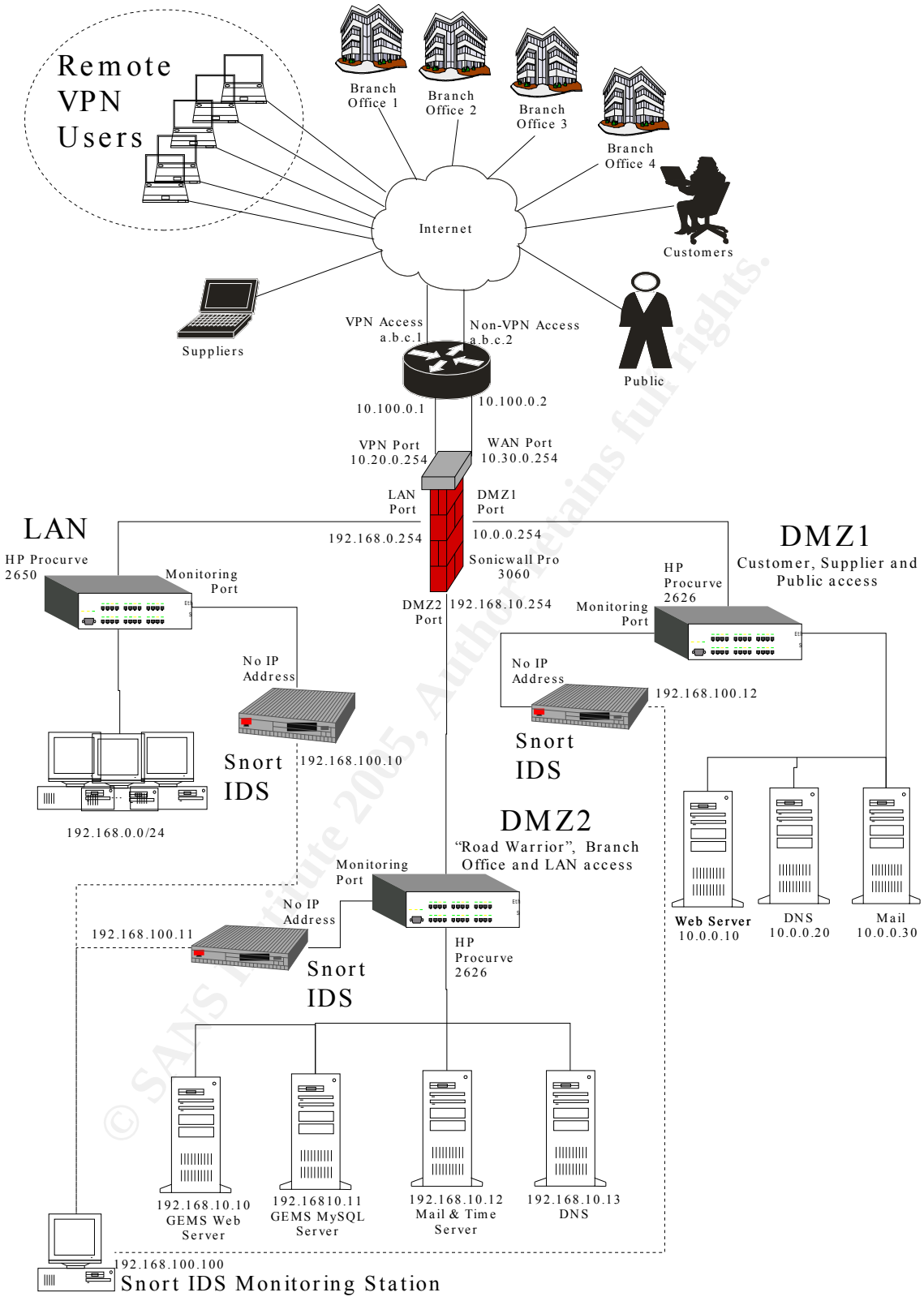
I have been hired as the new IT Manager to reorganize the IT Dept infrastructure and network access. After several meetings with Management, several concerns were raised which had to be resolved in my design:

- Security of paramount importance due to the amount of industrial espionage which occurs in the highly competitive world of fortune cookie sayings.
- The company has some very aggressive expansion plans for the next 2-5 years, therefore they do not want to invest heavily in infrastructure which is purchased without consideration for future growth. This means that several of my decisions may be considered 'overkill' for the present but should fulfill future expansion requirements.
- Remote staff must be have secure access to the network 24/7

Management has also been frustrated in the past with the large amount of time spent by the Network Administrators dealing with the constant threat of worms, viruses, trojans, spyware, etc so the decision was made to go with as much Open Source software for all servers, workstations, etc a few years ago. This decision has paid off in substantial cost savings to the company and an increased level of security.

For managing all sales, accounting, orders, products, etc the company has an in-house developed software system called GEMS (GIAC Enterprises Management System) which is a web-enabled package using all Open Source software including Apache (front end), MySQL (back end), PHP, Qmail (communication), OpenSSL (encryption).

Network Diagram



Note on hardware recommendations

For this paper, I have done as much research as possible into the various hardware and software choices. However, I do not have actual access to actual SonicWALL firewall boxes or a Cisco router therefore my design may have some issues which would be discovered when actually testing and implementing my design. However, I do feel that this design is quite realistic and should work as shown.

If this design was to be actually implemented, I would work with a Value Added Resaler who specializes in network design to verify that everything would work as planned.

Access Requirements

Customers

Customers will access ordering and product information from the Web Servers located in DMZ1. All access that is considered confidential (orders, payment info, etc) will be done over SSL encrypted, password protected, web pages. Access will be over HTTP (Port 80), HTTPS (Port 443) and SMTP (Port 25)

Suppliers

Companies which supply GIAC Enterprises with fortune cookie says use the GEMS Front end Web Server in the DMZ to enter sayings, etc. Access will be over HTTP (Port 80), HTTPS (Port 443) and SMTP (Port 25)

Partners

GIAC Enterprises has several dozen world-wide partners who translate sayings to different languages and sell them in other countries. Partner Access is to the GEMS Front end Server located in the DMZ. Partner access will be over HTTP (Port 80), HTTPS (Port 443) and SMTP (Port 25)

Branch Locations

All four branch locations will be connected to the Head Office using a point to point VPN setup between the SonicWALL Pro 2040 at each location and the SonicWALL Pro 3060 at the Head Office. The Border Router at the Head Office will automatically forward all VPN traffic to the VPN Port on the 3060.

Internal Employees

Internal employees work at individual PCs running Mandrake Linux 10.0. Since

most administrative tasks are done through GEMS, the most critical application for employees is a web browser.

Because of the planned future expansions, the company is also in the process of testing the Linux Terminal Server Project (www.ltsp.org) to eventually replace all the standalone PCs with thin clients. This will increase our defense-in-depth because thin clients will not require hard drives or any sort of local storage.

One of the most critical layers of security that is often ignored is the employees. Disgruntled employees and other insiders with legitimate access to critical business networks accounted for more than 80% of the cyberattacks against companies last year, according to a survey conducted by the FBI and the San Francisco-based Computer Security Institute.[11] Staff will receive training to understand security threats, what is acceptable use, etc. Staff also have to sign off on an Accepted Use Policy before they will be given access to the network. All logins will have a warning message about the Accepted use Policy and will have to be acknowledged before login will be allowed.

The use of wireless and installation of any unauthorized equipment, such as modems, will be strictly enforced and will be part of the Accepted Use Policy.

"Road Warriors" Sales Force

The Sales Staff, affectionately known as "Road Warriors" will access the Head Office Servers through a Free/SWAN VPN client installed on their laptops. SonicWALL does not currently offer a VPN Client for Linux. Luckily, the FreeS/SWAN IPSec client will work with SonicWALLS VPN Servers (http://www.sonicwall.com/srevices/VPN_documentation.html).

The Road Warriors do all their work on the GEMS Server installed in the DMZ2 via VPN only.

The Public

The public access product information through the web server in the DMZ over HTTP and HTTPS if required. Public access will be over HTTP (Port 80), HTTPS (Port 443) and SMTP (Port 25) to the servers in DMZ1 only.

Architecture Components

Border Router

One common error that can be seen at many businesses is they will connect a new high speed internet line, order a firewall, set it up and figure "Hey we have a firewall. We're secure." Unfortunately, that means that they have only one layer

of defense and if an intruder gets by it there's nothing else blocking their access to the rest of the internal network. Not a good security posture to take. Therefore, we will install a border router at each location as an added layer of defense in depth.

The perimeter of each location's network will have a Cisco 2620XM router as the first line of our defense in depth. The Border Router will be used to block known bad IP addresses, non-routable IP addresses, known attack signatures based on the The Twenty Most Critical Internet Security Vulnerabilities at http://www.sans.org/top20/, etc.

The Border Router will be configured with ACLs for both egress and ingress network traffic. Many networks are configured to block incoming attacks while ignoring attacks coming from within the network outbound. In some ways we could consider the border router as the last line of defense going outward from our internal networks.

At the Head Office, two ethernet connections will be configured with separate IP addresses facing the internet. One connection will forward all VPN traffic from our Branch locations and “Road Warriors” to the VPN port on the SonicWALL Pro 3060. The second will be used for all internet traffic destined for DMZ1 from Customers, Suppliers and the Public.

The border router will help keep the load off the main firewall so it can deal with more fine control over access to and from the network.

To ensure the security of the border router we will use the Benchmark and Audit Tool for Cisco IOS Routers available at http://www.cisecurity.org/bench_cisco.html. We will also ensure that the latest firmware is installed on all of the routers.

Firewalls

The company has had very good success with SonicWALL in the past so the decision was made to purchase a new SonicWALL Pro 3060 for the Head Office plus a SonicWALL Pro 2040 for each branch location. The firewalls will be purchased with Enhanced OS and Intrusion Prevention Service. The Intrusion Prevention Service has the following security features which will add to our defense in depth: Integrated Deep Packet Inspection Technology, Inter-zone Intrusion Prevention, Extensive Signature List, Dynamically Updated Signature Database, Scalability, Application Control. [12]

The SonicWALL Pro 3060 features 6 fully configurable ports (the additional three ports are only enabled with the “Enhanced OS”). The firewall at Head Office we will be using 5 of the 6 ports. (LAN, WAN, DMZ1, DMZ2 and VPN) The

additional port may be used in the future for redundancy of the firewalls.

To increase our defense in depth and ease administration of the branch firewalls we will use SonicWALL's Global Management System (GMS) – http://www.sonicwal.com/products/gm_standard.html from our Head Office. SonicWALL's Global Management System increases our Defense in Depth by allowing us to centrally manage and monitor all of our SonicWALL firewalls securely from one location.

Switches

The Branch locations plus DMZ1 and DMZ2 subnets will be using HP Procurve 2626 switches with the latest firmware installed (H.07.50). The Head Office LAN will be using a larger switch, the HP Procurve 2650, with the latest firmware (H.07.50). The 2650 was chosen to meet the needs of planned further expansion.

GIAC Enterprises prefers HP switches for their excellent warranty and support. The Procurve switches also include some very good security features which will be enabled on each switch[13].

For administration of the switches we will use Secure Shell (SSHv2) encryption with Public-Key Authentication for an additional layer of security. Public-Key encryption will thus require both a password and the correct private key to administer the switches. Telnet and web based administrative access will be disabled. All unused ports will be disabled by default. MAC address lockdown will also be enabled.

One port on each switch is configured as a monitoring port. A monitoring port allows a packet sniffer/IDS System to log all the packets that cross the switch.

The sniffer/IDS System will be configured with no IP address to add stealth. Please see the “Intrusion Detection” section for more information on this configuration.

Some may consider the use of a 24 port switch “overkill”, especially for the branch locations, however management wants to ability to expand the network easily in the future.

Intrusion Detection

On each segment of the network, there is a Snort Intrusion Detection (http://www.snort.org) PC. Each Snort box will have two network cards. One will be configured with no IP address and connected to the monitor port on each switch. The second network card will have an IP on the 192.168.100.x subnet.

The 192.168.100.x subnet will be used only for administration of the IDS system. This will allow us to stealth the Intrusion Detection PCs. The reason for stealthing the IDS boxes is that in case of an intrusion we want to be alerted to it but also we need to be able to assess what has happened after a break-in (or attempt). Crackers will try to shut down any IDS System and logging system hide their tracks (see the next section on Syslog).

Please note: Instructions for stealthing our IDS and our Logging Servers was written by Eric Lubow at http://www.linuxjournal.com/article.php?sid=6222. However, when I was finishing up my paper I discovered that the original article has been moved due to some restructuring of the Linux Journal website. Hopefully, the article will be available again soon.

"Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more."[14]

An IDS monitoring station will be used to centrally log all Snort alerts etc to a MySQL Database using the setup instructions found in[15]. This station will not be connected to any other network accept for the Snort IDS PCs.

Stealthed Syslog

All Linux PCs and Servers will be configured to log all of their entries to a false remote Syslog server. For example, in DMZ1 all servers will have Syslog configured to send its logs to an IP Address of 10.0.0.100 which doesn't actually exist on the network. The Snort IDS box will be set to log all these packets which will be sent to the Snort IDS Monitoring Station for alerting, etc.

Information for setting this up was found at
http://www.linuxjournal.com/article.php?sid=6222

Please see my note about this source above.

Stealthed Syslog adds to our defense in depth because crackers will, upon successfully breaking into a network, try to remove all traces of what they have done. Because all systems will be broadcasting their logs to a non-existent IP it will be nearly impossible for the cracker to do this.

Additional layers to defense in depth

Operating Systems

All PCs and Road Warrior systems will use Mandrake Linux 10.0. How does this increase our Defense-In-Depth? I do not want to try debating the security differences between Open Source and Proprietary Operating Systems. Any operating system can be considered insecure if it is not properly administered and locked down by a knowledgeable technician. However, I do believe some of the statistics speak for themselves. Even with Microsoft's well publicized 'security is a priority' emphasis over the last few years there has been a growing number of viruses and attacks against Windows systems.

A recent study by Symantec, for the first six months of 2004, showed 4,496 new viruses for Windows (an increase of more than 4.5 times over the same period in 2003) and an increase in bot networks from 2,000 a day to over 30,000 in the same period.[16]

I feel that the decision to use Linux on all PCs and servers will add another layer of our Defense-In-Depth.

Physical Security

All the network security in the world is not going to help if somebody can simply walk into an office and take the servers with them. Therefore, all servers and network equipment located at the Head Office and will be locked in a secured server facility with tightly controlled secure access to only authorized employees. Each branch location will have the firewall, router, and other equipment also locked in a secured area with limited access to authorized employees only.

Time Synchronization

All PCs and servers on the LAN and DMZ2 subnets will synchronize their time from the time server which will be setup on the Mail and Time Server in the DMZ2. The Servers in DMZ1 will synchronize their time from different time servers on the internet.

E-mail Traffic

All e-mail traffic will be split between two different paths. External mail destined for our internal users will be received by the Mail Server in DMZ1 running Qmail (http://www.qmail.org), qmail-scanner (http://qmail-scanner.sourceforge.net) with Clam AntiVirus (http://www.clamav.net) an Open Source Antivirus software package. While we are not running Windows and therefore are not vulnerable to the many viruses and trojans that plague Windows users we still want to be on the safe side.

E-mail going outbound from the LAN will be relayed from the Mail Server in DMZ2 to the E-mail server in DMZ1 which will then send it out to the internet.

This adds another layer of defense because the e-mail servers which the users access for e-mail cannot directly receive e-mails from the internet.

For the internal users to read their e-mail the e-mail server in DMZ2 runs a simple web based e-mail server product. However, there has been more demand for sharing e-mail, calendars, etc between staff so the company is currently evaluating an Open Source based groupware product called Open-Xchange (http://www.open-xchange.org).

Assignment 3: Firewall Policy

As mentioned in Assignment 2, the SonicWALL Pro 3060 at the Head Office will be configured with 5 of its 6 ports in use. The five ports are:

- LAN Internal network port – 192.168.0.254
- DMZ1 – Demilitarized Zone #1 – 10.0.0.254 Customer, Supplier and Public Access
- DMZ2 – Demilitarized Zone #2 – 192.168.10.254 Accessible via VPN for Remote Users and Branch Office Access. Local Access from the LAN.
- WAN – Internet Access – 10.30.0.254
- VPN – Access from Internet via VPN – 10.20.0.254 – All traffic over the VPN port will be encrypted through the "Road Warriors" VPN client or via the Point to Point VPN Access from each Branch Location

The default policy between each of the zones on the SonicWALL is to deny ALL. Therefore I will only list those services and protocols that I specifically want to allow. Anything that is not listed will be denied.

SERVICES
NTP – Port 80 UDP
HTTP – Port 80 TCP
HTTPS – Port 443 TCP
VPN – IPSec
DNS – Port 53 TCP & UDP

LAN -> WAN

SOURCE	DESTINATION	SERVICE	COMMENT
192.168.0.0/24	Any	HTTP	Web Access
192.168.0.0/24	Any	HTTPS	Web Access SSL

LAN to WAN traffic will be limited to HTTP and HTTPS. If other protocols are requested in the future, this will be handled on an individual basis.

LAN -> DMZ1

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

All traffic from the LAN to the DMZ will be disabled. If a user on the LAN requires access to DMZ1 they will go out through the internet via HTTP or HTTPS.

LAN -> DMZ2

SOURCE	DESTINATION	SERVICE	COMMENT
192.168.0.0/24	192.168.10.10 & 192.168.10.12	HTTP	Web Access

SOURCE	DESTINATION	SERVICE	COMMENT
192.168.0.0/24	192.168.10.10 & 192.168.10.12	HTTPS	Web Access SSL
192.168.0.0/24	192.168.10.12	SMTP	E-mail Routing
192.168.0.0/24	192.168.10.13	DNS	DNS
192.168.0.0/24	192.168.10.12	NTP	Time Synchronization

The most important access here will be HTTP and HTTPS to access the GEMS Systems therefore those two rules will be put first. The second most critical would be sending e-mail with DNS and Time synchronization following.

LAN-> VPN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

All access from the LAN to the VPN will be disabled by default.

WAN -> LAN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

All access from the WAN to the LAN will be disabled by default.

WAN -> DMZ1

SOURCE	DESTINATION	SERVICE	COMMENT
ANY	10.0.0.10	HTTP	Web Access
ANY	10.0.0.10	HTTPS	Web Access SSL
ANY	10.0.0.30	SMTP	Incoming Mail
ANY	10.0.0.20	DNS	

The servers in DMZ1 are all publically Accessible. The most important access will be for the Web Server so HTTP and HTTPS access rules will be put first.

WAN->DMZ2

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

All access from the WAN to the DMZ2 will be disabled by default.

WAN->VPN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

Disabled by default.

DMZ1 -> LAN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

Disabled by default.

DMZ1 -> WAN

SOURCE	DESTINATION	SERVICE	COMMENT
10.0.0.20	ANY	DNS	DNS Queries
10.0.0.30	ANY	SMTP	Outbound email

As stated in Assignment 2 GIAC Enterprises will be running a split DNS Server. The DNS Server in DMZ1 will only contain public accessable IP addresses in its Zone files. Any servers in DMZ1 will query the DNS server at 10.0.0.20 for all DNS queries.

DMZ1 -> DMZ2

SOURCE	DESTINATION	SERVICE	COMMENT
10.0.0.30	192.168.10.12	SMTP	Forwarding of e-mail

All mail from the internet destined for our internal users will be received by the mail server in DMZ1 and forwarded to the mail server in DMZ2.

DMZ1 -> VPN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

All access will be disabled by default.

DMZ2 -> LAN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

All access will be disabled by default.

DMZ2 -> WAN

SOURCE	DESTINATION	SERVICE	COMMENT
192.168.0.13	ANY	DNS	DNS Queries for LAN and DMZ2
192.168.0.12	Selected Time Servers	NTP	Time Synchronization from internet

All DMZ2 Servers will query the DNS Server at 192.168.0.13 for all name resolution queries.

DMZ2 -> DMZ1

SOURCE	DESTINATION	SERVICE	COMMENT
192.168.10.12	10.0.0.30	SMTP	Outbound e-mail

All outbound destined e-mail will be forwarded from the e-mail server in DMZ2 to the Mail Server in DMZ1.

DMZ2 -> VPN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

VPN -> LAN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

VPN -> WAN

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

VPN -> DMZ1

SOURCE	DESTINATION	SERVICE	COMMENT
			Deny All by Default

If Branch Locations or "Road Warriors" need access to servers in DMZ1 they will use their own internet access.

VPN -> DMZ2

SOURCE	DESTINATION	SERVICE	COMMENT
ANY VPN	192.168.10.10 & 192.168.10.12	HTTP	GEMS and Web based E-mail Access
ANY VPN	192.168.10.10 & 192.168.10.12	HTTPS	GEMS and Web based E-mail Access
ANY VPN	192.168.10.13	DNS	DNS Queries
ANY VPN	192.168.10.12	SMTP	Outbound E-mail
ANY VPN			

All VPN traffic from the Branch Offices and from the "Road Warriors" will only be allowed to access the various servers in DMZ2. Thus all the traffic will be encrypted through the VPN Tunnel and only allowed over VPN.

References

1“International Biometrics Group – How is 'Biometrics Defined?” 2004. URL: http://www.biometricgroup.com/reports/public/reports/biometric_definition.html (03 Oct 2004)
2Palmgren, Keith. “Biometric Authentication, An Introduction.” 14 Oct 2004. URL: http://www.netip.com/articles/keith/biometric_authentication.htm (15 Sep 2004)
3Liu,Simon and Silverman,Mark. “A Practical Guide to Biometric Security Technology.” 2000. URL: http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (21 Oct 2004)
4Page,Max. “Biometrics Explained.” 21 Dec 2000. URL: http://www.pcstats.com/articleview.cfm?articleID=500 (22 Oct 2004)
5“Passwords revealed by sweet deal.” 20 Apr 2004. URL: http://news.bbc.co.uk/1/hi/technology/3639679.stm (23 Oct 2004)
6French,Verrick & Gill,Richard & Dornbusch,Rebecca. “IBIA Biometrics Advocacy Report, March 19, 2004.” 19 Mar 2004. URL: http://www.ibia.org/newslett040319.htm (23 Oct 2004)
7Editor. “Biometrics passports in 2005, as trial for national ID cards.” 04 Dec 2003. URL: http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=304 (23 Sep 2004)
8Mansfield,Steve. “Fingerprint Biometrics Could be a Boon for ASPs.” 09 Mar 2004. URL: http://www.linuxinsider.com/story/33072.html (24 Oct 2004)
9Costello,Sam. “Japanese Researcher Gums Up Biometrics Scanners.” 13 June 2002. URL: http://www.itworld.com/nl/unix_sec/06132002/ (23 Oct 2004)
10Ashbourn,Julian. “A Biometric White Paper.” 1999. URL: http://homepage.ntlworld.com/avanti/whitepaper.html (25 Oct 2004)
11Verton,Dan. “Analysts: Insiders may pose security threat.” 15 Oct 2001. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,64774,00.html (20 Sep 2004)
12URL: “Intrusion Prevention Service.” http://www.sonicwall.com/products/ips.html (30 Sep 2004)
13http://www.hp.com/rnd/products/switches/switch2600series/features.htm
14“What is Snort?” URL: http://www.snort.org/about.html (10 Oct 2004)
15Rehman, Rafeeq Ur. Advanced IDS Techniques Using Snort, Apache, MySQL, PHP and ACID. Upper Saddle River:Prentice Hall PTR,2003.
16“New Release.” Symantec Internet Security Threat Report Identifies More Attacks Now Targeting e-Commerce, Web Applications. 20 Sep 2004. URL: http://www.symantec.ca/region/can/eng/press/2004/n040920b.html (15 Oct 2004)
www.digitalpersona.com
http://www.andrewpatrick.ca/biometrics/templates/template.shtml
http://www.netip.com/articles/keith/biometric_authentication.htm
http://www.linuxsecurity.com
http://www.sonicwall.com