Global Information Assurance Certification Paper

Network Air Gaps – Drawbridge to the Backend Office

Michael Hurley, CCSA

April 4, 2001

Introduction

Administrators who work in Banking, Government and Health industries are required to protect sensitive data by following Government's Rainbow Series, British Standard 7799 or HIPAA. Air Gap technology can give Administrators the flexibility they need to ensure the confidentiality, integrity and availability of sensitive data as it is presented/received over the Internet. This technology is not a replacement of your current security system (i.e. Firewalls, IDS and Anti-Virus systems). But it is another building block in your 'Defense in Depth' strategy.

TCP/IP Vulnerability

Transmission Control Protocol is the most widely used protocol in the movement of data over the Internet and, in many cases, your own Intranet. It is used because of 'guarantee of delivery'. What I mean is it is connection oriented and the protocol is written to resend data when the receiver doesn't acknowledge the complete transmission of data. It was written in the Cold War era and the objective was to ensure delivery regardless of what path was taken. For instance, if a major routing path were destroyed, the data would take a different path.

Unfortunately, the perspective at the time was to ensure that data made it to its destination. There were no controls built in to verify the authenticity of the source IP address and where it came from. This is the crux of the TCP/IP vulnerability. This is where 'crackers' take advantage of the protocol. Crackers utilizing sniffers to capture data can take the time to examine and predict TCP sequence numbers and modify the routing and authentication process to insert their own data streams. The Morris Worm used this approach and Mitnick utilized this technique quite successfully.

Security Systems

Firewalls, Network/Host Intrusion Detection and Anti-Virus systems have weaknesses too. Administrators enable service ports on Firewalls such as http, telnet and ftp to allow traffic through. All other traffic is blocked by a drop rule. The Firewall doesn't perform content checking on the data load coming through the enabled service ports. Thus attacks on web servers through enabled service ports are not preventable.

Network Intrusion Detection Systems (NIDS) can not read the encrypted data portion of an https packet. Therefore the content cannot be compared against the common vulnerabilities database. Host Intrusion Detection systems are reliant upon some known vulnerability, amount of auditing turned on, and event numbers in the logging facility. If there were a new vulnerability it would take some time to update the IDS software. This

would be your period of exposure.

Anti-Virus systems have the same reactive weakness. It has to wait for a patch release to help identify the next new virus. Also you have the same issue with applications and operating system patches/upgrades/revisions. You will always be playing catch up.

In no way does this infer to get rid of these systems. The more layers you can protect your site with the better (Defense in Depth). Either the cracker will move onto an easier site or, as they penetrate your system, tripwires in place will alert you to take action. Also these security systems provide the legal system with evidence and demonstrate your due diligence to protect sensitive data.

Business on the Internet

> "Be prepared for bastion hosts to be compromised" [1]
>
> "A DMZ (Demilitarized Zone) is a separate network where you put systems you do not trust. Since anyone on the Internet will be accessing both our web and mail server, we cannot trust them. Also, systems in the DMZ can never initiate connections to the internal network, since they are not trusted. " [2]

In order for a business to succeed on the Internet it needs a presence to advertise and process transactions from prospective clients and business partners. A business will put bastions host servers in a DMZ (behind a firewall and not connected to their internal network) to receive and store transactions. The next step is getting the transactions out of the DMZ and into their backend office in a real-time mode.

Many security policies are written to disallow untrusted connections from the Internet and DMZ to the backend office Intranet. So how does a business perform transactions with these types of roadblocks? Business can:

- Accept the risk and let the data through. This is obviously dangerous.
- Replicate and store all the data into the DMZ and then have an internal process to go out and pick up new data (difficult for real-time). This would be like a bank putting all its safety deposit boxes out on the street and saying the boxes are protected by a key an surveillance camera.
- Utilize service switching by allowing a service such as https into a DMZ to push/pull data from a client over the Internet. Then the DMZ server would use a different service port into/from the internal network. Keep in mind that any service can run over any service port and you are still vulnerable to weaknesses in TCP.

Network Air Gap Technology

Vulnerabilities in TCP, operating systems and application software is what crackers take

advantage of to break into systems. A finer layer of "Defense in Depth" is accomplished by implementing an air gap. It is an intermediary hardware device that allows for the shuttling of data ONLY that you are sending/receiving to another network. With an air gap device, information such as TCP headers and system operating software commands are not shuttled. By eliminating this information we deny crackers the ability to perform reconnaissance of network topologies and extraction of entire databases.

I'd like to explore two promising air gap technology products on the market today: Whale Communications e-Gap and Spearhead's AirGAP. Both of these products utilize gap technologies called *real-time switch* and *one-way link*. (Note: there is another gap technology known as *network switcher*. Network switcher is a PC with two virtual machines built inside it. Data is written to one virtual machine and then the switch transports the data machine to the other virtual machine. It is slower than the real-time switch and one-way link technologies and isn't the focus of this paper).

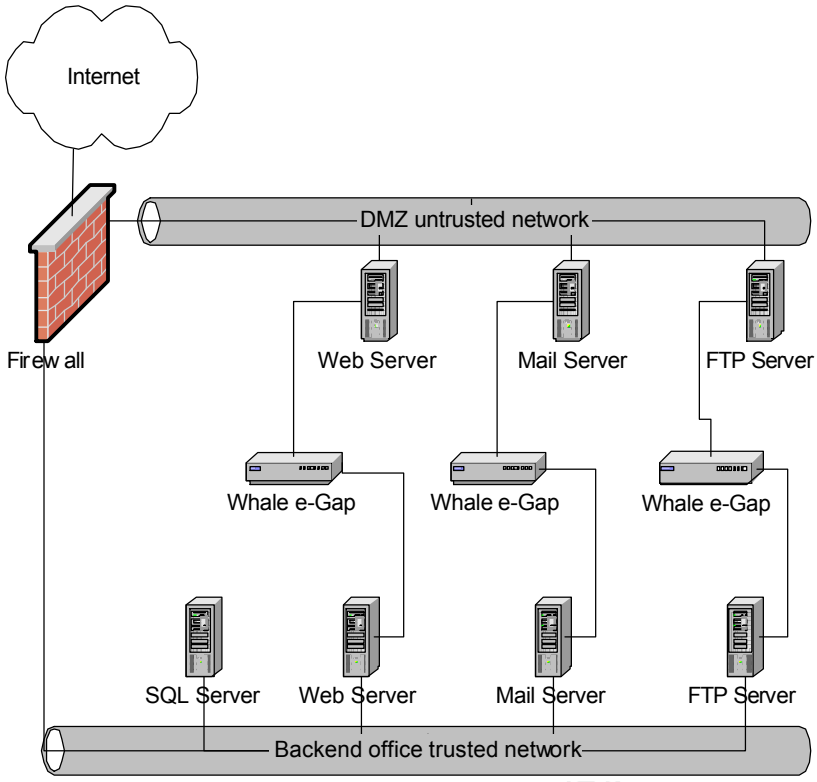
Real-time switch utilizes a hardware device connected to both networks making it capable of only receiving or transmitting data to one network at a time. In essence, the switch connects to Network A, obtains data, switches to Network B and pushes the data onto it. Prior to the push to Network B, the network connection is broken and the TCP information removed. The switch could then transmit a response from Network B to Network A. The movement of data at high speeds gives the appearance of real time processing.

One-Way Link also utilizes a hardware switching device but data can only move in one direction from the source network to the destination network.

Whale Communication's e-Gap

This product is a hardware device that is a real-time switch and capable of being a one-way link. The device sits between a server on the DMZ (untrusted) network and a server on the back end office (trusted) network. Data is written to the device's RAM via SCSI. The device switches the SCSI interface from source to destination servers and vice versa. A short circuit indicator on the front panel of the device would stop all traffic if the internal & external SCSI buses were connected at the same time.

The DMZ server and internal server are configured as each other's gateway with additional Network Interface Card. Each server is loaded with one of three types of application software that communicates via the SCSI protocol. By communicating out-of-band (SCSI) we have effectively eliminated TCP vulnerabilities.



The three types of application software are:

Web Shuttle

This software enables the external and internal servers to transport HTML requests. The external server receives requests, strips TCP headers off and writes it to the RAM on the device. When completed, the device toggles the switch and writes it to the internal server. The internal server performs content checking and directs it to the backend server: SQL, LDAP or SSL. Thus your private data - customer information, authentication credentials and private encryption keys (SSL) - are all stored on the internal network and are not subject to being compromised because it is the external server which the crackers have access to.

File Shuttle

With File Shuttle, virtual folders are set up on the internal and external servers. When the folders are populated the data is transported to the destination folder. When data is written to the internal folder, content inspection and virus checking are performed on the data. Again the controls (content & virus) are not exposed to the crackers who are hammering away on the external server.

Mail Shuttle

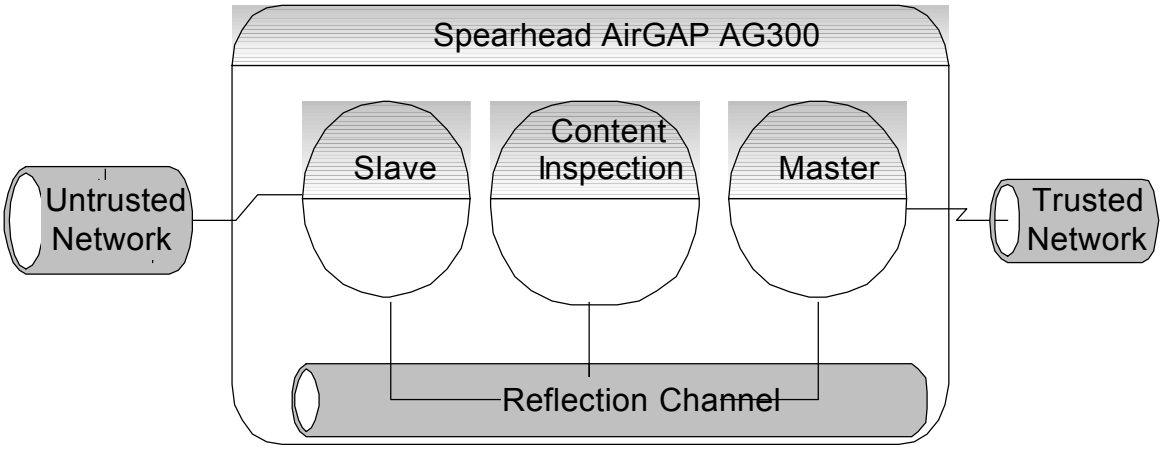
In Mail Shuttle, the external server acts as a mail relay system. When the mail is received on the external server, it is stripped of TCP headers and shuttled across gap to the internal server. Here the data is subjected to both content and virus checking. Mail Shuttle software can be modified by the administrator to look for certain words or it can be hooked into third party content and virus checkers.

If the above applications software does not fit your needs, there is an additional product called e-Gap's Software Developers Kit. This kit allows customers to write custom APIs to be loaded onto the system.

Spearhead's AirGAP

Spearhead's hardware device AG300 is a real-time switch and capable of being a one-way link. It is positioned between networks - either the Internet and the DMZ or the DMZ and trusted backend office. This would provide data transfers from multiple servers on both networks.

Three component boards are inside: slave, content inspection and master. The slave board is connected to the untrusted network. The content inspection board uses eSafe's content verification engine to test application data for RFC compliance and to stop binary code. The master board is connected to the trusted backend office. Slave and Master boards have Network-1's Intrusion detection software built in. An additional component from Radware is available for load balancing and failover.



The slave board receives Internet requests from the untrusted network. The TCP headers are stripped off and the slave board maintains state with the Internet host. The slave board moves data to the reflective channel (out of band) where the data is written to both the content inspection board and the master board. The content inspection board checks

for malicious code and informs the master board if the data is clean. The master board compares the data to the security policy, regenerates TCP headers and forwards the data to the backend office server.

Another layer of protection within the system is performed by two random key generations. The first key set is shared amongst the boards and generated when the system is initialized. The second set is only known to the boards and is used to read data off the reflection channel.

Control Room software is installed on a management server. The software enables the administrator to write and install security policies (over the SSL channel), push software updates and monitor heartbeats of multiple AG300 devices. It also generates reports of security events. Another package - Admin GUI - can be installed on an administrator's desktop to communicate with the management server running Control Room.

Conclusion

Vulnerability probing tools and rootkits are free on the Internet. Chat rooms and Newsgroups openly discuss how to break into computer systems. New crackers are an email away from asking for guidance from a professional cracker on how to accomplish a clean break in. Application software and operating system vendors are negligent in rigorously testing their products because of the rush to market.

Increases in credit card theft, corporate espionage and stealing of identities will increase the need for tighter controls on the way data is stored and accessed. Air gap technology will help you to control the traffic through your sensitive networks and add to your "Defense in Depth". Of course, the technology can't stop criminals who have obtained valid credentials from 'other' sources. But….do you want to be the 'other' source?

Footnotes

1.) Zwicky, Elizabeth D., Cooper, Simon., Chapman, D. Brent. "Building Internet Firewalls", Sebastopol: O'Reilly & Associates, June 2000. 242
2.) Spitzner, Lance. "Building your Firewall Rulebase" 26 January 2000 http://www.enteract.com/~lspitz/rules.html (2 April 2001)

References

Bobbitt, Michael. "(Un)Bridging the Gap" Information Security.
July 2000 (2000): 35 – 47
http://www.infosecuritymag.com/articles/july00/cover.shtml (2 April 2001)

Bellovin, S.M.. "Security Problems in the TCP/IP Protocol Suite" April 1989
http://www.ja.net/CERT/Bellovin/TCP-IP_Security_Problems.html (2 April 2001)

Avolio, Frederick M.. "e-Business and the Need for "Air Gap" Technology" October 2000 (PDF format)
http://www.avolio.com/papers.html (2 April 2001)

Ranum, Marcus. "Internet Firewall Protection"
http://www.networkcomputing.com/unixworld/tutorial/09.txt.html (2 April 2001)

McClure, Stuart & Scambray, Joel. "Once-promising intrusion detection systems stumble over switched networks" Infoworld 11 December 2000 (Vol. 22, Issue 50)
http://www.inquiry.com/pubs/infoworld/vol22/issue50/001211opswatch.asp (2 April 2001)

Dickerson, Michael. "Spearhead AirGAP Model 300" SC Info Security News Magazine.
http://www.sphd.com/read_about_us/sc_reprint.html (2 April 2001)

Reuters. "E-Gap Cuts Off Hacker Access" Wired News 8 January 2001
http://www.wired.com/news/print/0,1294,41044,00.html (2 April 2001)

Whale Communications – e-Gap Products
http://www.whalecommunications.com/ (2 April 2001)

Spearhead Technologies Ltd.
http://www.sphd.com/ (2 April 2001)
http://www.spearhead.net/ (2April 2001)

Aladdin Knowledge System's eSafe content verification product
http://www.aks.com/ (2 April 2001)

Network-1's Intrusion Detection software
http://www.network-1.com/ (2 April 2001)

Radware's load balancing & failover products
http://www.radware.com/ (2 April 2001)