Running Head: END POINT SECURITY, SECURING THE FINAL THREE FEET

End Point Security

Securing the final three feet

Charles F. Moore,

East Carolina University

Abstract

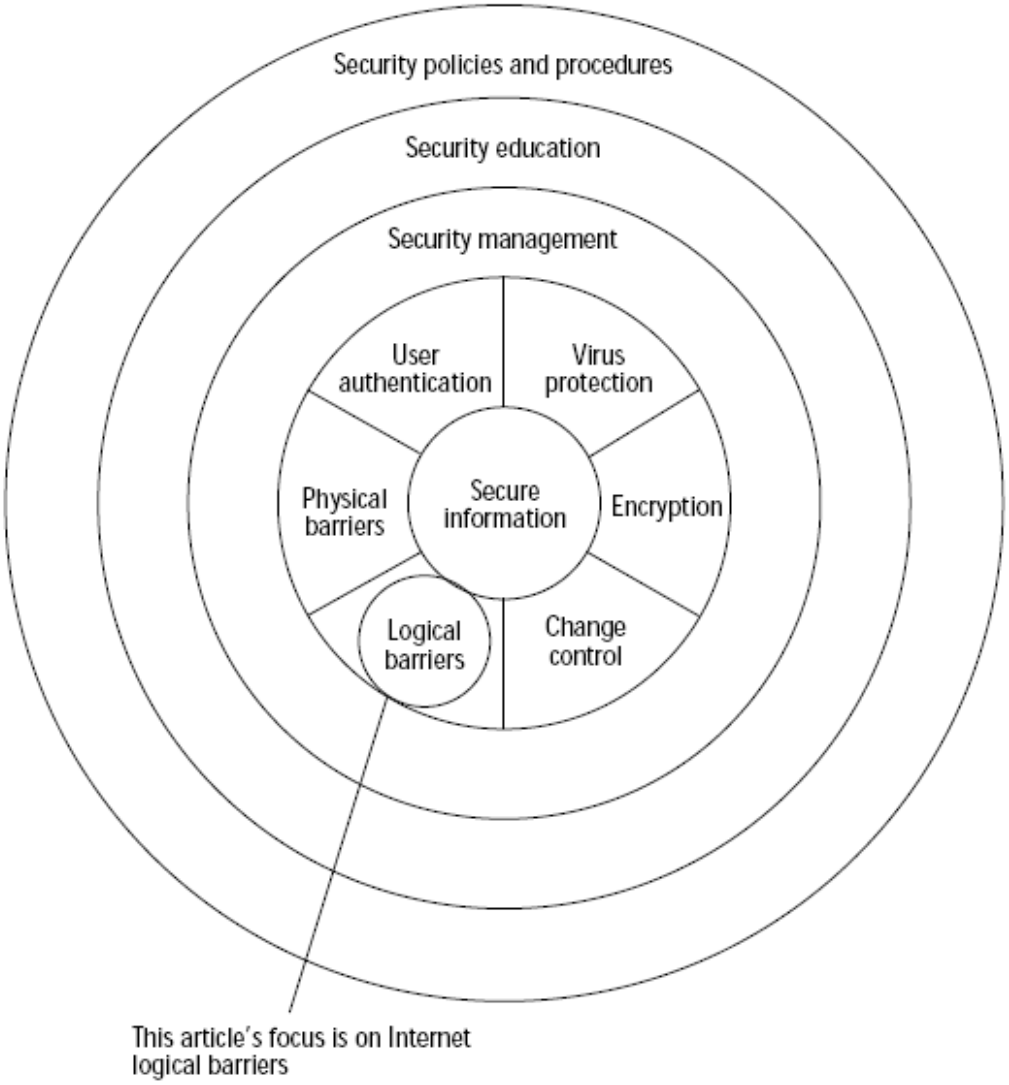
Information security has tended to be reactive over the years. With each new virus, or worm the system administrators struggled to get updates out to the end points. Even if the system administrators were successful, there was always the potential that one device was missed. One device is all it would take to cripple the network. This paper will examine several ways that system administrators can begin contemplating and planning on implementing end point security in their organization. It is time for security to get to the last three feet and protect the organizations assets.

The evolution of the Internet has seen many twists and turns. For every twist a new opportunity or risk presented itself. Security professionals seem to always be one step behind the bad guys. This point cannot be better illustrated than end point security, e.g. desktop, PDA or laptop security. Over the years little emphasis has been put on end point security, other than the mandatory antivirus package. The early security and network architects tried to deliver a centralized, one size fits all network with security included. This network typically had a router and a firewall. The firewall may or may not have been configured with multiple interfaces. The point is the firewall acted like a choke point restricting all but the permitted traffic. This was a solution that provided management with a level of comfort and security allowing them to sleep at night.

This is a fine solution, one appliance, protecting hundreds or thousands of vulnerable computers. The economies of scale were wonderful. This one device would protect the network from all of those bad people that exist on the Internet. The people trying to infiltrate your network would be kept out. This turned out to be a good solution. Desktops were prevalent and the operating system was the soft under side. However, over time things have changed.

As figure 1 illustrates this is the desired security model one would like to achieve. A layered approach with logical barriers will help to compartmentalize and secure the data.

Figure 1 Information security protection



(Doddrell)

According to the 2005 CSI / FBI Computer Crime and Security Survey the top three threats for companies today are viruses, unauthorized access and the theft of proprietary information. These three activities represent about eighty percent of all dollar damages done. This trend illustrates that securing the perimeter is not a viable option in protecting your infrastructure. It is required, but it will only take a business so far. In "2005 nearly 54 million records containing personal

information – from social security numbers to health care records – were reported compromised" (Kuper). That is "nearly one out of every five Americans facing a potential security issue" (Kuper). This number increases every year. In the not to distant future the number of people who have not had their identity compromised will be easier to count.

The biggest change to this design is portable devices. Portable devices became cheaper and cheaper and faster and faster. Now a user would take one's company laptop home and plug it into one's home network and unknowingly get infected. That hard working user would then bring the infected laptop back to the company network, bypass all of the layers of security, plug it back in and proceed to infect the entire company network. Or a contractor or vendor would bring in an infected device and take down the company's network.

The problem with this network design is that it is like some pieces of candy hard on the outside and soft and squishy on the inside. As the workforce has become more mobile and laptops more common the external perimeter that gave so much comfort in previous years has slowly dissolved and it is now time to take security down to the end point. This paper will explore and contrast different end point security standards focusing on Cisco's network admission control (NAC), Microsoft's network access protection (NAP) and the Trusted Computing Groups hardware based solution. All of these security solutions protect the endpoint however; they all go about it differently.

The Cisco endpoint security solution is called network admission control or NAC. NAC operates at the network layer 1 through 3 (Grimes). It is a proprietary network based solution

that pretty much requires Cisco "NAC" aware routers and switches all along the network. Each endpoint has an agent installed called the Cisco trust agent. Due to the fact that there are agents on the endpoint NAC applies its enforcement policies down to the switch port level (Hultquist). The enforcement is provided through the use of 802.1X using Cisco's Secure Access Control Server (ACS) Radius Server (Strom). The ACS server then communicates with third party vendor servers to insure compliance. The results are then fed back to the switch to allow, deny or remediate the endpoint.

The pros for this solution are it is "available now, a mature product, widespread support, and Linux clients" (Strom). Since it is in the network infrastructure it can also protect against rogue devices. There are over seventy five vendors now supporting the NAC product line (http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html).

The cons for this solution are, as previously stated, that it is Cisco proprietary solution, requires 802.1X, and is agent based (Strom). It may also require IOS upgrades. This could be a challenge for companies with large built out infrastructures. While each end point needs the Cisco trust agent (CTA). The Cisco trust agent requires plug-ins for the specific products that you will be enforcing. The CTA acts as a central repository for other plug ins, e.g. patch management plug in, firewall, or the anti virus plug in. All of these plug ins mean more work and the potential for more compatibility issues. This product is technically challenging working with vendors to complete the integration. To illustrate this point any company looking to install NAC will almost certainly have to rely heavily on Cisco engineers for the duration of the project. This would include the company acting as the mediator between the plug in vendor and Cisco.

This is not a trivial task to get the plug ins working with the NAC. There may be limited interoperability with other vendor solutions.

Microsoft's endpoint security solution is called network access protection or NAP. NAP like NAC requires an agent. The NAC agent is called the Quarantine agent (Strom). It works prior to the endpoint getting on the network by sending a designated server a list of the hosts programs and configurations on the local endpoint. This list is then forwarded to the designated server, called the Network Policy Server (Strom), where a comparison of products and updates is conducted. The information exchanged would typically include host operating system, patches installed, version and signature file for the anti virus program. If all are up to date then the endpoint is allowed to proceed to log on. If any of the programs are out of date then the endpoint is sent to some kind of restricted area (Xia et al). Enforcement can be handled through DHCP, IPsec VPN, 802.1X using RADIUS (Strom). NAP uses VLANS for enforcement. (Hultquist)

The pros of NAP are that over 60 vendors have announced support for it. Microsoft is building this technology into the operating system. It is possible by dealing with Microsoft this will limit the number of agents and vendors the company is forced to deal with.

The cons to NAP is that it is still in Beta and unproven. It will come native to Vista and Longhorn and it will be a service pack for Windows XP. The latest estimate for delivery of Longhorn and Vista is some time in 2007. NAP will need a RADIUS server. The result is that companies will have to come up to this minimum level of the operating system prior to implementation. This, like updating the Cisco IOS, may be a challenge and costly exercise in

some large organizations. It would also appear that initially NAP will use DHCP as its enforcement mechanism (Langston). The use of DHCP as the enforcement agent will be unacceptable in most organizations in that endpoints with static ip addresses and devices that are not NAP compliant and do not receive valid DHCP leases will not participate in NAP. Thus the policy manager will never be allowed to enforce the policies so malicious code could still be injected into your network. It is expected that Microsoft will use other authentication mechanisms. Since it is looking for authentication as a means to control entry, devices may be added without notice. Also since this is a Microsoft solution support for other operating systems and end points, e.g cell phones and PDAs, will be almost non existent leaving security holes in this solution. There also may be limited interoperability with other vendor solutions.

Finally a third solution exists. This solution has been put forth by the Trusted Computing Group's Trusted Network Connect or TNC (https://www.trustedcomputinggroup.org/home). The Trusted Computing Group is comprised of dozens of hardware vendors and this solution supports open standards. It uses 802.1X and RADIUS for authentication, hardware based chip, and software at each of the endpoints. The chip is rather inexpensive, about $4.00 per chip (Xia). Interestingly enough is that Cisco is not a member of the group. Microsoft is a member, but is waiting on the sidelines. Speculation is that Microsoft will eventually participate in the group (Schacter). The trusted computing effort offers the ability to identify a device by a unique cryptographic identity (Sandhu *et al*). This is the chip that is built on the motherboard.

The pros of the TNC are that it has wide support from over 80 hardware vendors (Langston). The technology is here, by the beginning of 2006, it is estimated that over 50 million computers

had been shipped with the trusted platform module (TPM) (Oltsik). The technology offers advantages over software based solutions in that the machine is identified and verifies the user. It would also apply to any device with the TPM chip, e.g. PDAs and cell phones.

The cons of the TNC are that there is not much industry support to date, it requires trusted platform module, and the standard is incomplete (Strom). It would appear that Juniper Network is the company pushing for implementation of this product. 802.1X is used as an enforcement point. Another drawback of the TNC is that the assumption is made that the devices are not shared (Sandhu *et al).* In some organizations this is not the case so this limits the value of this solution.

An interesting side note to the NAP solution is called "policy based networking" (Baltatu). Policy based networking works by modifying the packets as they traverse the network. One way to accomplish is to turn on IPSec. IPsec can provide

- **"Packet confidentiality:** Packets are encrypted before being sent over the network so that only authorized entities can read them.
- **Packet integrity:** Packets are protected so that any alterations during transmission over the network can be detected.
- **Packet origin authentication:** Packets are protected to ensure that they are indeed from the claimed sender whose IP address is contained in the source address of the IP header.
- **Protection against replay:** Packets are protected from being captured and resent at some later time. " (Li)

The use of IPsec is no stranger in most organizations as this is a manner in which virtual private networks (VPN) are created between devices or hosts. IPSec has typically been thought of as it applies to encryption traffic from end to end. Based on a paper called “Performance analysis of IPSec protocol: encryption and authentication” by Elkeelany, O, *et al* the use of IPSec in a VPN using 3DES encryption was almost 50 times slower than using just a hash. While this study is dated and technology has increased the load to run a VPN tunnel is still great.

It is often forgotten that IPSec is actual a suite of standards. The standard typically operates in one of two modes. These two modes are called tunnel and transport modes. “In transport mode an IPsec header is inserted between the IP header and the upper-layer protocol header. As a result, transport mode protects upper-layer protocols only. In contrast, in tunnel mode the entire IP packet is encapsulated into another IP datagram, and an IPsec header is inserted between the outer and inner IP headers. Consequently, tunnel mode protects the entire IP datagram.” (Li)

While tunnel mode is resource intensive transport mode does not suffer from that shortcoming. The beauty of transport mode is that the simple insertion of the IPSec header in each packet turns the network dark based on your policies. This mode will protect the traffic between all trusted computers, and it authenticates every packet. In simplest form in a Windows active directory environment active directory can force the IPSec requirement at the group policy level while the user is authenticating. In this way, only authenticated machines will be allowed on the network. This means that no rogue devices will be allowed on one’s network. By using group policy the company is then able to leverage other pieces and enforce more required policies.

While this may seem like a novel approach to end point security there is plenty of pain along the way and this approach should not be attempted without a thorough understanding of the implications and administrative efforts required to make this successful in your organization. However, if you are a Windows shop this may give a company end point security with little additional capital outlay and it is available now. More information can be found at **http://www.microsoft.com/ipsec/**.

Finally, there is no question that information security needs to be extended down to the end point. The definition of an endpoint should be anything that touches one's network. The direction to go is based on the current state of one's network. Since all of the solutions require interactivity with other vendors the one common theme is that a company should be investigating and begin installing an 802.1X authentication implementation (More information on 802.1X can be found at http://grouper.ieee.org/groups/802/1/pages/802.1x.html). No matter what you will need some kind of authentication strategy. Start working on it now so that it will be mature in one's environment prior to proceeding to the next step. The move to 802.1X is not trivial in any environment. This should be a well thought out and researched implementation that will take time.

The next step is more of a leap than a step. This can be explained that with NAC and NAP one's company is aligning itself with a particular vendor, either Microsoft or Cisco. The company is also deciding whether it is better to enforce at the endpoint (Microsoft's solution) or at the endpoint through the network switch (Cisco's solution). It is up to senior management to map

out the information technology direction of the company as well as evaluate the costs, impact and benefit to the company of each of these particular solutions.

If the company is heavily committed to Cisco equipment and can afford the time and expense to upgrade all of the network equipment and there is an immediate need for end point security then NAC may be the right choice for that organization. However, it is necessary to remember that Cisco acts as the gate keeper it will still be necessary to involve system engineers from a variety of companies. This solution will also force one to work with numerous other vendors, e.g. antivirus, anti spyware, patch management, personal firewall, etc. There is a huge potential for finger pointing when dealing with all of these vendors at installation. The company also needs to recognize the relationship between the Cisco NAC agent and all of the vendor plug ins that will need to be managed indefinitely.

The Microsoft solution is untested and unless the company is committed to using all Microsoft products there will be gaps. Microsoft has a personal firewall and anti virus and anti spyware products are already in testing. If the company can wait this may be a better solution in the long run as all software vendors will want to work in the Microsoft environment. It will limit finger pointing and administration. However, this ease may come at a higher cost.

As companies decide on an endpoint strategy they must be aware of the necessity to fully define what an endpoint is. With the exception of the TNC these solutions still pretty much look at the laptop, desktop, server environment. Forward thinking companies would include any type of wireless devices in their quest for a solution. Thumb drives and portable hard drives should also

be factored into the solution. Security has been reacting to security breaches for so long. It is now time to go to the last and most exposed piece of your network the endpoint. Get ahead of the curve and put this on your company's strategic radar. None of these solutions are simple or cheap so do your homework and get it right the first time.

Reference

* Baltatu, Madalina, Lioy, Antonio, Mazzocchi, (2000), Security Policy System: status and perspective. Proceedings of the IEEE International Conference on Networks 2000, *Comuter Journal,* 34, page 881-894

* Doddrell, Gregory, (1996) Information Security and the Internet. Journal: *Internet Research,* volume 6, issue1, page 5-9.

* Elkeelany, O.; Matalgah, M.M.; Sheikh, K.P.; Thaker, M.; Chaudhry, G.; Medhi, D.; Qaddour, J.; (2002) Performance analysis of IPSec protocol: encryption and authentication. Communications, 2002, ICC 2002, IEEE International Conference on, volume 2, 28 April-2 May 2002 Page(s):1164 - 1168 vol.2

Grimes, Roger, (2005) NAC vs. NAP, retrieved from http://www.infoworld.com/article/05/09/05/36FEbattlesecurity_1.html on June 1, 2006

Hultquist, Steve, (2006) Get a Head Start on NAC, retrieved from http://www.infoworld.com/article/06/06/02/78769_23TCnac-sb_1.html on June 5, 2006

* Kuper, P, (2006) A warning to Industry – Fix it or Lose it, *Security & Privacy Magazine, IEEE,* volume 4, issue 2, March – April 2006, pages: 56 – 60, IEEE Journal

Langston, Richard, (2005) Network Access Control Technologies, retrieved from http://searchstorage.bitpipe.com/detail/RES/1144173451_384.html?src=feature_res on June 24, 2006.

* Li, Man (2003), Policy-Based IPsec Management, *Network, IEEE,* volume 17, issue 6, November – December 2003, pages 36 – 43, IEEE Journal

Oltsik, Jon, (2006) Trusted Enterprise Security: How the Trusted Computing Group (TCG) will advance enterprise security, retrieved from https://www.trustedcomputinggroup.org/news/Industry_Data/ESG_White_Paper.pdf on June 18, 2006

* Sandhu, Ravi, Ranganathan, Kumar, Zhang, Xinwen (2006), Secure Information Sharing Enabled by Trusted Computing and PEI Models, Conference on Computer and Communications Security, Proceedings of the 2006 ACM Symposium on Information, computer and communications security, March 21-24, 2006, pages 2 -12

Schacter, Phil, (2004) Enforcing Endpoint Security Policy Compliance: Early Products and Progress Towards a Standard, retrieved from The Burton Group, http://www.burtongroup.com/content/doc.aspx?cid=65&display=full, June 19, 2006

Strom, David, (2006) Which Way? The Roads to Endpoint Security are Confusing. Here is some direction, retrieved from http://informationsecurity.techtarget.com/magLogin/1,291245,sid42_gci1191315,00.htmlon , June 15, 2006, pages 44 to 51.

Unknown, (2005) Tenth Annual CSI / FBI Computer Crime and Security Survey, retrieved from http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf, June 19, 2006, page 16

* Xia, Haidong, Kanchana, Jayashree, Brustoloni, Jose Carlos, (2005), Using Secure Coprocessors to Protect Access to Enterprise Networks. NETWORKING 2005: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communication Systems, 4th International IFIP-TC6 Networking Conference, Waterloo, Canada, May 2-6, 2005, Proceedings. Page 154-165.