Global Information Assurance Certification Paper

GIAC Security Essentials
Patch Management: Tackling the Remote Laptop and Teleworker
A Case Study

GIAC Security Essentials
GSEC – Practical Assignment
V1.4b August 2002
Option 2

Kay A. Cornwell
SANSFire 2003
Washington, DC
July 2003
Submitted Dec 29, 2003

Abstract

In order to earn the SANS GSEA certification the author presented a case study on patch management as part of Defense in Depth in February of 2003. The case study described how the GIAC Institute applies patch management to protect its desktop resources. One of the major weaknesses of this chosen solution was demonstrated by the release of the Blaster and Nachi worms in August 2003. Remote laptops and telework machines, along with personal PCs are highly vulnerable to internet worms and viruses making the institute vulnerable as staff become "wired" at home. The patch management solution implemented as part of the GSEA case study has worked well for institute desktops. This process successfully limited the impact of the worms to a handful of machines while other organizations suffered significant downtime. The Blaster and Nachi worm was introduced and reintroduced to the agency network almost exclusively via remote dial up and VPN services. Due to the way these enterprise services are implemented the author's patch management solution can not connect to remote laptops and telework machines automatically. The manual process used to patch laptops, while successfully limiting the worm infections to less than 5 machines, have proven to be time consuming and not popular with staff.

Teleworkers are not given administrative access to their machines and cannot patch them themselves. The Institute's IT management does not wish to provide admin access as it presents a host of security issues. Currently, the remote access update process requires staff with laptops and telework assignments to physically bring the equipment into the office to be updated quarterly or when a critical patch is released. After a busy summer of exploits and updates being released almost weekly staff has tired of this exercise. Often there is a window of two weeks or longer for those on travel who cannot physically bring in a laptop before patches can be applied. This makes critical "emergency" patching almost impossible. Since the submission of the author's GSEA practical new agency policy has been issued requiring that all remote access machines using agency VPN and dial-up resources be actively patched and have up-to-date antivirus definitions. In order to protect the institute's resources, locally and remotely, and to comply with this newly implemented policy it has become apparent that a process needs to be devised that will allow the ISSO to remotely patch these resources without the need to have them physically located on the institute's network. Such a process will satisfy a frustrated staff, save time for the helpdesk and will improve the institute's defense in depth by narrowing the window between patch release and patch deployment.

TABLE OF CONTENTS

Case Study Environment

The GIAC Institute is a component of the GIAC Research Agency. The GIAC Institute supports basic biomedical research by funding work that focuses on learning more about the basic cellular functions that lead to advanced understanding of fundamental life processes and increases knowledge of the mechanisms involved in disease. The institute has used personal computing technology along with client server based networking for approximately 14 years. The GIAC Research Agency prides itself on its university and research type atmosphere which has resulted in an open computing environment. Communication and collaboration have been the guiding principles for connectivity. Flexibility for employees has also been important which has lead to the use of remote access computing with very few restrictions. The agency developed an enterprise wide dial-up access system and has had a pilot VPN program in use for the last couple of years which has now gone live. The institute uses these agency resources for its remote access needs instead of investing in its own systems. Since 9/11 security has become the watch word for the agency networks. The challenge has been balancing the need for security against the open, collaborative, academic type atmosphere.

IT Infrastructure

Relationship with the GIAC Research Agency

The institute's IT infrastructure is tied closely with the agency's IT infrastructure. The agency's Information Technology Center (ITC) provides the network infrastructure for the institute including the border routers, switches, firewalls and intrusion detection systems along with the skill set needed to monitor and maintain them. Due to a mandate from the GIAC Research Agency's parent organization the ITC is consolidating and providing more enterprise wide solutions and support for the agency network and security infrastructure. Currently the ITC and other agency components are moving to Active Directory, collapsing 300 LANS supporting more than 20,000 PCs, Macs and UNIX workstations to a single forest. The ITC has successfully closed the perimeter and monthly reports have shown a dramatic decrease in successful attacks. Remote access has been consolidated into a single VPN service and a single dial-up service maintained by the ITC. Policy has been implemented which requires all remote access to enter the agency network through these services which are isolated subnets that are monitored by an intrusion detection system.

GIAC Institute Infrastructure

The institute maintains its LAN in a single location spread over 2 floors. Redundant VPN Firewalls are in place waiting for their first rule sets to be implemented to isolate the institute LAN from other agency components. The institute maintains 40+ Windows NT/2000/2003 servers. Migration to the agency's Active Directory service for user accounts was completed in early January. IT staff are currently planning the migration of hardware resources as a result of required consolidation into the single agency forest. All servers are

running McAfee anti-virus in the background and are monitored from McAfee's E-Policy Orchestrator[1] management console.

The firewall will serve as a component in the institute's defense in depth strategy extending from the agency perimeter and will also serve to protect the institute from attack from within the agency network. The institute's perimeter has been a weak area and many others are starting to address the need for firewalls between agency components. During August 2003, the Blaster and the Nachi worms bypassed the agency perimeter firewalls by sneaking in via dial-up and VPN services. The institute firewall would have reduced secondary infections by preventing exploited PCs from other institutes infecting vulnerable PCs on the GIAC Institute network. Fortunately, the author had patched 98% of the desktops before the worms were released. The most vulnerable institute resources proved to be laptops and staff's personal PCs. In this case, while the firewall would have reduced some of the infections it would not have eliminated them entirely. Other organizations also learned this lesson in August as Kevin Poulsen reported the "first confirmed case of malicious code penetrating cash machines." Two financial institution's ATM machines, which are based on the Microsoft XP Operating system, were hit.

> Though ATMs typically sit on private networks or VPNs, the most serious worms in the last year have demonstrated that supposedly-isolated networks often have undocumented connections to the Internet, or can fall to a piece of malicious code inadvertently carried beyond the firewall on a laptop computer. (Poulsen)

Patching the laptops and desktops, thereby removing the vulnerability, is the best line of defense against these types of exploits.

The remainder of the institute network consists of approximately 170 Dell Optiplex Win2K desktop machines. Desktops are standardized with the Microsoft Office XP suite, a browser, FTP client, and custom applications written by the database group to access grant information and financial systems. The desktop also provides access to enterprise tools providing access to agency-wide grant processing software. All desktops have a centrally managed Antivirus program from McAfee that scans in the background during all web downloads, when opening email and attachments, inserting a floppy disk and on boot up. All machines are virus scanned weekly, upgrades and dat updates are managed from the central management console, E-Policy Orchestrator. Desktop machine patches are currently well managed with St. Bernard's UpdateEXPERT[2] patch management software.

---

[1] For more information on McAfee E-Policy Orchestrator see http://www.networkassociates.com/us/products/mcafee/antivirus/fileserver/epo.htm

[2] For information on St. Bernard's Update Expert see http://www.stbernard.com/products/updateexpert/products_updateexpert.asp.

Windows 2000 laptops are available for permanent loan for upper management and a loaner laptop pool is available for staff use when they travel; need to temporarily work at home, or for training. The ITC maintains a remote dial-up service for all agency staff for travel and telework. The institute's IT staff configures all laptops to use this service, requiring all those needing remote access to apply for a remote account. The business need for remote access is reviewed yearly. This service provides the teleworker with an agency IP address and places them behind the agency firewall granting access to agency and institute services. This eliminates the need for the institute to support modems on site. The agency has been piloting a VPN solution to secure high speed access to the agency-wide network. When accessing via VPN, staff connects to a remote access DMZ with firewall and intrusion detection. As with the remote dial-up service, management must approve staff's need for an account. A recently implemented remote access policy has made these services the only authorized way to remotely access the agency network. The remote access policy has also mandated that institute laptops, desktops and personal PCs be kept up-to-date with application and system patches and anti-virus dat files. These remote access services means that laptops need to be scanned for vulnerabilities and patched regularly to prevent them from becoming a source of attack.

In 2004 the institute will be replacing all desktop and laptop equipment. A contractor is currently on site planning the install of new desktops to take advantage of active directory, group policies and the Windows XP operating system. New laptops are also being created that will allow for docking stations for a specific division that travels often, permanent loan laptops for upper management and a pool of laptops for the remainder of staff to request on an as needed basis. The remote access patch management solution that the author will discuss here is not an automatic process. It requires the cooperation of the institute ISSO (the author) and the users. The author believes that technical controls that ensure policy are followed rather than depending on the good will of the users is the optimum solution. Depending on the user often leads to a failure in the process, especially when there is a time limit of only days. The contractors will be assisting with the implementation of Microsoft's SMS 2003[3] and SUS[4] services to push out patches automatically. As this research is just starting the author was not in a position to concentrate this case study on the implementation of SUS. The August outbreaks of Blaster and Nachi coming on the heels of each other made it clear that the current laptop patch process was not robust enough to handle the shrinking vulnerability-to-exploit window. The institute needed an interim process that had some hope of success between the current quarterly update schedule and the implementation of new laptops that depend on SUS. This process needed to be more user friendly and easy to manage so that staff would not revolt.

[3] For information on Microsoft Systems Management Server see http://www.microsoft.com/smserver/default.asp.
[4] For information on Microsoft Software Update Services see http://www.microsoft.com/windowsserversystem/sus/default.mspx.

The Remote Patch Management Problem - Before

Over the last year, many organizations with Internet access have suffered from fast moving, non-targeted attacks such as the SQL Slammer Worm and particularly in August of this year Blaster and Nachi. These attacks are devastating because they spread almost instantaneously. One infected machine on an internal network can infect all vulnerable machines in a matter of minutes. Rushing to close the firewall does not prevent mass infection. Peter Gregory in his Computer World advice column sums this up as a lessons learned.

> **Organizations are learning that the network perimeter exists in many places besides the Internet firewall.** Connections to other organizations, and even connections within organizations, also need to have firewalls. Company laptops need to take a little piece of the perimeter with them when they travel outside the corporate firewall. Organizations need to consider installing personal firewall software on laptops to protect them from external threats when they're connected to the Internet via an unfirewalled home network or hot spot. (Gregory)

The institute ISSO is looking into a centralized laptop firewall solution, specifically 3Com's Embedded Firewall[5] Policy server. This service utilizes special network interface cards with hardware firewalls that can be monitored and controlled from a centralized server. The author had attempted to get this up and running for this case study but did not have much luck with the system. Implementing it in this environment will take cooperation from the vendor, the ISSO and the ITC. Perhaps it will be ready in time for the author's next SANS practical.

For the time being, the only real way to combat these worms is to make sure it never breaches the agency perimeter, much harder to prevent when the organization allows remote access, or to ensure that institute machines are not vulnerable to these exploits in the first place. On the surface this seems rather easy to address with the assistance of various vendor's products. Patch management is the simple process of discovering there is the need for a patch and deploying it to all vulnerable machines in the organization. It's a simple concept but in reality it can be time consuming and inconvenient as many organizations found out in August. Computer World ran an article shortly after Blaster hit stating that patching was becoming a major resource drain.

> Last week's W32.Blaster worm, which affected thousands of computers worldwide running Windows operating systems, highlighted the enormous challenge companies face in keeping their systems up to date with patches for vulnerabilities, users said.

[5] For information on 3Com Embedded Firewall Policy see http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=134482&selcat=Security+Products&family=134494.

> Companies that, ahead of Blaster's rampage, had installed Microsoft Corp.'s patch for a flaw identified last month said they felt no effect from the worm. But the seemingly constant work involved in guarding against such worms is becoming a burden that could prove unsustainable over time, users said.
>
> "The thing about patching is that it is so darn reactive. And that can kill you," …..
>
> "You need to literally drop everything else to go take care of [patching]. And the reality is, we only have a finite amount of resources." (Vijayan)

The author feels that failure of timely patch management is currently one of the leading causes of exploits in the Windows environment.

In order to earn the SANS GSEA certification the author presented a case study on patch management, Patch Management as a Necessary Part of Defense in Depth: A Case Study. (Cornwell) The case study described how the GIAC Institute applies patch management to protect its desktop resources. A major weakness of the described solution was demonstrated by the release of the Blaster and Nachi exploits in August 2003. The agency network was inundated due to the vulnerability of remote laptops and telework machines connecting via its VPN and dial-up services. Unfortunately, there are numerous reasons driving the demand for laptops and remote access. The number of official agency telework arrangements has doubled in the last year. A growing number of staff are purchasing PCs and wishing to work from home via remote access. There has been an increase in the number of staff requesting laptops when they travel or take leave for vacation or health reasons. More staff are connecting to the internet via personal ISPs or using the agency's dial-up services as their primary ISP. Also, on October 23, 2000, the Federal Government implemented a telework program with Public Law 106-346 § 359 which states that

> Each executive agency shall establish a policy under which eligible employees of the agency may participate in telecommuting to the maximum extent possible without diminished employee performance. Not later than 6 months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall provide that the requirements of this section are applied to 25 percent of the Federal workforce, and to an additional 25 percent of such workforce each year thereafter. (Federal Government)

In response the GIAC Research Agency has developed its Telework policy with the following goals:

> In addition, the purpose of this policy is to promote the GIAC Research Agency (GRA) as an employer of choice; enhance GRA's efforts to employ and accommodate people with disabilities, including employees who have temporary or continuing health problems, or who might otherwise have to retire on disability; reduce office space, parking facilities, and transportation costs, including costs associated with payment of the transit subsidy; enable organizations to remain functional during emergency shutdown; and improve the recruitment and retention of high-quality employees through enhancements to the employees' quality of life. (GIAC Research Agency Telework Policy.)

Current construction on the agency campus has greatly reduced parking and management has started a renewed push to offer telework as a solution to relieve the parking stress.

The agency as a research organization has chosen to be open with remote access to allow researchers flexibility and to allow staff to become familiar with the Internet as it plays a large role in how it collaborates and disseminates information to the public. Outside influences such as the Telework law and reduced parking has clearly shown that remote access is here to stay and will become even more important in the future. The ITC has implemented wireless access across the agency driving up the demand for laptops. The Blaster and Nachi worms revealed a gaping hole in agency defenses and even though the author had worked to patch the bulk of the institute's equipment before the worm's release the author sees were the current policy and process is not enough to stand up to continued onslaughts of similar fast moving exploits. It is difficult to anticipate when an exploit might happen; therefore an effort to patch as closely as possible to vulnerability notification must be made. The ISSO must determine how to protect the network by protecting remote and staff's personal PCs. This has proven to be difficult when management will not dictate that all access must be done via agency resources, though the author has heard rumors that this issue may be revisited in the near future. The institute will never be able to control personal PC's, nor does it wish to. The newly implemented remote access policy does state that all remote access users agree to keep their personal PC's up to date with patches and anti-virus as the Blaster and Nachi worms clearly demonstrated that many remote access machines were vulnerable.

Refresher on the Vulnerability Assessment and Patch Life Cycle

The author wishes to quickly refresh our memory on the Vulnerability Assessment and Patch Life Cycle as discussed in her GSEA practical in order to point out the current patch management problem. The life cycle is a five step process (Klaren 2).

1. Define your corporate policy on Vulnerability Assessment and Patch Management. This policy should include what the policy is, why you need it, the scope, and how and by whom it will be completed.
2. Inventory your systems. Know exactly what you're running so you know exactly what to worry about.
3. Manage the flow of information. Determine which information resources help you focus exclusively on the vulnerabilities that affect your systems.
4. Assess the information. Evaluate the actual risk to your organization's systems security.
5. Plan for response. Develop standard procedures to translate information into action.

Step 1 – Define/Refine Policy

An institute policy was defined using the SANS basic outline for policy development that laid the ground rules for the patch management process. It's important to remember that policy is not static; it needs to change as business needs change, laws change or in response to outside forces. This case study is one such example. The author will point out the specific policy sections dealing with remote access laptops that have been proven inadequate in order to update them to be able to protect the institute from future worm attacks.

Vulnerability and Patch Management Policy

(Cornwell 12) Only applicable sections excerpted.

5.0 Policy

5.1 Ownership and Responsibilities

All internal servers, desktops and laptops deployed at the GIAC Institute are owned by the IT Operations Section (ITOS) of the institute's Information Resource Management Branch. The network administration group is responsible for all server, desktop and laptop installation, administration and compliance. The ISSO is responsible for development of security guidelines, auditing, scanning and patching of servers, desktops and laptops and compliance testing.

5.2 Action

A Chief of ITOS approved vulnerability scanning and patch management procedure must be established and maintained by the Information Systems Security Officer (ISSO). A mitigation procedure and timeline based on the institute's business needs will be approved by the Chief of ITOS and the CIO. The network administration group will assist the ISSO in implementing patches and monitoring configuration compliance. There should be no exceptions to vulnerability scanning and patch management. Exceptions in mitigation procedures and timelines must be approved by the Chief of ITOS. The ISSO will establish a process for changing and updating the patch management and mitigation procedure. The process will include reviews and approval by the Chief of ITOS.

- All Laptops must be registered in the institute's asset management system. Help desk staff are responsible for the loan paperwork for all permanent and temporary loans of institute laptops. Help Desk Staff will assist the ISSO in a quarterly vulnerability scanning process for all laptops. The help desk staff is also responsible for following the Laptop Checkout Guide (see Laptop Checkout Procedures) which requires the updating of patches before any laptop is let out on property pass.

5.2.1 Vulnerability Scanning Guidelines

- Laptops will be updated by hand during the laptop checkout procedure. Otherwise all laptops will be scanned quarterly with vulnerability scanning software.
- Vulnerability scanning will be performed at a level that does not harm the institute network or its systems. Scanning will occur during business hours unless it is determined that scanning interferes with business processes. Scanning will be performed at the office location. Remote access scanning will only be allowed via agency provided VPN and terminal services and only if determined that scanning will not interfere with systems performance.
- The ISSO and staff responsible for maintaining applications and equipment are responsible for monitoring the various patch mailing lists. Patch notices should be emailed to the ISSO so that vulnerability scanning software can be checked to ensure inclusion of vulnerability. If the vulnerability is not recognized the ISSO will check other patch sources for alternative means of deployment.

5.2.2 Monitoring and Compliance

- The ISSO will use institute purchased patch management software to run as a compliance check for patches. It is expected that the vulnerability scanning software will identify and mitigate most patch needs. This will be done weekly for servers and at least monthly for desktops. Laptops will be checked on a quarterly basis.

To rework the policy the author suggests removing all references to a specific time schedule for updating the laptops and leave "as necessary to fit the current security stance and vulnerability situation." The author suggests changing the bullet point under section 5.2 Action to

- All Laptops must be registered in the institute asset management system. Help desk staff are responsible for the loan paperwork for all permanent and temporary loans of institute laptops. Help Desk Staff will assist the ISSO in the vulnerability scanning process for all laptops. The help desk staff is also responsible for following the Laptop Checkout Guide (see Laptop Checkout Procedures) which requires the updating of patches before any laptop is let out on property pass.

The Laptop Checkout Procedures have been updated to strengthen the process and to correct some deficiencies that were discovered. The author also suggests editing the first bullet point under section 5.2.1 Vulnerability Scanning Guidelines to read:

- Laptops will be updated by hand during the laptop checkout procedure. Otherwise all laptops will be scanned with vulnerability scanning software as required by agency policy or as prescribed by the ISSO.

The last policy section that needs to be revised is section 5.2.2.

- The ISSO will use institute purchased patch management software to run as a compliance check for patches. It is expected that the vulnerability scanning software will identify and mitigate most patch needs. This will be done weekly for servers and at least monthly for desktops. Laptops will be checked before being released on temporary or permanent loan. Flexiplace machines and laptops on long term permanent loans will be patched when notification of applicable vulnerabilities are released. Target is 95% compliance within one week.

This gives the ISSO flexibility to determine the need for scanning based on the current security stance of the institute, technological advances and in reaction to security requirements as they appear. These proposed changes will have to be reviewed by the Chief of ITOS and the CIO before being implemented as revised policy.

Step 2 – Inventory Systems

The second step in the Vulnerability Assessment and Patch Life Cycle is to inventory systems. There are three steps necessary to correctly inventory the network. (Klaren 4)

1. Classify your network assets by platform. Conduct and maintain a complete inventory of the hardware and software, including the versions of software and firmware and any patches or upgrades that have been installed.
2. Determine risk potential. Identify the business exposure of each technology on your network. Which systems and software make up the critical core of your network?
3. Know what defensive tools you have in place. There are many kinds of defenses you can deploy, such as router filters, system logging and intrusion detection systems.

The author discussed these steps and how they were implemented in her GSEA practical. In relation to this case study, the results of the Blaster and Nachi worms have caused the author to rethink the risk potential for institute remote access machines. The defensive tools put in place by the agency and by the

institute; filtering routers, firewalls, virus protection, and intrusion detection did not prevent infection. Vulnerability scanning and patch management on a quarterly time table may not catch new vulnerabilities which are being exploited in a much shorter time frame. There was only a month between the time the DCOM vulnerability was announced and the Blaster exploit was released. It was a challenge to get all the institute's resources patched before the Blaster worm hit. In fact, the author failed; roughly 5 machines were infected because they were either overlooked or users had not brought in a laptop for patching. It has become more and more difficult to get staff to respond to bring in laptops for critical patches. The current laptop and flexiplace procedure must be revisited as there needs to be a more proactive stance that will allow the ISSO to respond quickly to newly announced vulnerabilities.

Step 3 – Manage Information

The third step in patch management is to mange information to assist in the identification of vulnerabilities. In her GSEA practical the author discussed various resources for security notices and that the institute uses St. Bernard's UpdateEXPERT, which provides information on needed patches. UpdateEXPERT identifies Microsoft operating system and application vulnerabilities and allows patches to be managed from a central location. The program enumerates the network and indicates missing patches by machine, making it easy to combine the identification step with the mitigation step. UpdateEXPERT did not require an agent on target machines and that was a main reason for its purchase. As the institute desktops and laptops run the same software it's very easy to determine that most of the patches available for the desktop will also be needed on the laptops. The major problem is that due to the system used for dial-up and VPN, UpdateEXPERT can not see the laptops and remote flexiplace computers when they are on-line. The only way to see the state of a remote machine is to bring it in and physically connect it to the institute network.

Step 4 – Assess the Information

Step four is the point where the information gathered in previous steps is used to evaluate the risk to the Institute's systems. For laptops and remote desktops, once it has been determined that they are susceptible the time factor really determines the risk. The ISSO has little control over the environment in which the laptops and flexiplace computers are placed. The assumption is that all remote access machines are suspect. The author must assume that in the case of worms like Blaster and Nachi that it's impossible to prevent its entry into the network. So the only real defense is to ensure that the laptops and desktops are not vulnerable by being patched. When a patch is released it's a race against the clock; how long does the institute have before an exploit is released? A process that gets the patches deployed quickly is the goal. The vulnerability tools mentioned in the author's GSEA paper have not been able to collect information from laptops because when they connect remotely to the agency network they are cordoned off in a separate subnet which has firewall rules that prevent

communication on the standard ports used by UpdateEXPERT. The remote access facilities are managed by the ITC and for security purposes they have not made available the exact configuration. Since none of the vulnerability scanning tools mentioned can hold the scanning process until a machine becomes available these tools are impractical for use against remote machines. The author needs a patch tool that can push or pull patches down to the machine no matter where it's located.

Step 5 – Plan the Response

The last step is making the decision as to what to do with the identified vulnerabilities. The Blaster and Nachi worms showed that there was a gap in the planned response as dictated by the Vulnerability and Patch Management policy discussed earlier. Quarterly patching is inadequate. The author needs a more proactive way to patch remote machines other than asking users to bring them into the office.

Fixing the Problem – During

Technical Solutions

The author needed to find a solution that would shorten the time between vulnerability notifications and exploits. All the tools at the ISSO's disposal could not connect to remote resources requiring updates to occur by hand. The author could have researched the patch management tools currently available on the market but there was a constraint. In early 2004 the institute will be replacing all its desktops and laptops. Due to a lack of resources this effort will be contracted out. In the contract it was stipulated that the contractor would come up with an automatic patching solution that would include remote laptops. It didn't seem a wise use of the author's resources to tackle this research when contractors would in the near future. On the other hand, the author didn't want to leave the institute at risk using a manual process that could not respond to emergencies. The author needed an interim solution that did not require much in the way of resources to implement. Luckily, St. Bernard's UpdateEXPERT version 6.0 upgrade was a pleasant surprise. It included a new feature that would extend the current investment in UpdateEXPERT and provide a simple, interim solution to the remote access patch problem.

In April 2003, St. Bernard's new version of UpdateEXPERT introduced Leaf Agents. According to a St. Bernard white paper, The Power of Optional Agent Architecture, "A client agent is software installed on managed workstations and servers designed to do the work locally (with proper credentials) that one cannot perform remotely without the agent." (St. Bernard Software, Inc. 4) Previous versions used Window's RPC services to communicate between machines. This required having ports 139, 135 and 445 open. As mentioned before, ITC considers firewall information sensitive and the author does not know exactly what the remote access firewall passes but it would seem it has NetBIOS

and RPC, ports 139 and 135 blocked as UpdateEXPERT could not contact laptops while they were connected via the agency-wide remote access services.

The Leaf Agent performs all the management tasks on the client machine and communicates via a single administrator selectable port. A bonus with the Leaf Agent is that UpdateEXPERT 6.0 encrypts this communication. This is not a requirement in the GIAC Institute's environment, as updates will only occur via the agency remote access services, VPN or dial-up, but it does provide a secure layer to prevent a hacker from trying to hi-jack the update process. The Leaf Agent runs as part of the local system account, meaning that it has administrative rights on the remote machine. This works around the problem of users not having admin rights. Since it handles all the installations locally it also means that if multiple patches require reboots the agent handles the reboots and installation until all patches have been installed.

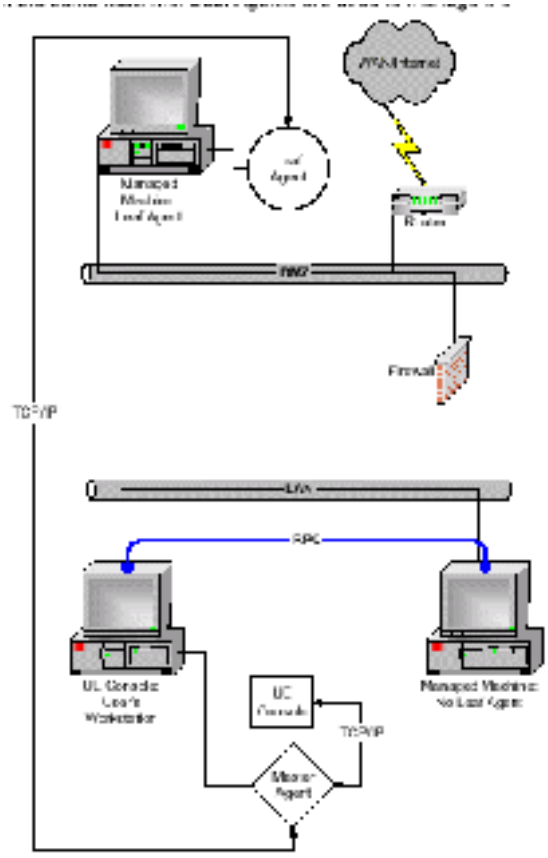

Figure 1. UpdateEXPERT Communication to Leaf Agent in DMZ From http://www.stbernard.com/products/docs/ue_deployguide.pdf p. 16

UpdateEXPERT 6.0 also introduced a console that can be installed on any machine providing access to the Master Agent that resides on a server. The console allows the ISSO to monitor and operate UpdateEXPERT on a remote laptop. The author has been using this feature to assist in updating desktops by monitoring the update process from home as patching must be done during off hours. The console allows flexibility to connect with remote machines at the user's convenience.

The UpdateEXPERT Deployment Manual includes a graphic approximation of the institute's communication setup. (Figure 1) The laptops, when connected to the remote access services are contained in a subnet that acts like a DMZ. The console can be anywhere, on the institute's physical network or connected remotely via VPN. The Master Agent uses an encrypted TCP/IP connection to communicate with the Leaf Agent. Port 9986 is used by default, but this can be changed. In a true DMZ environment, for example the SANS recommended configuration for internet facing servers such as outside DNS, email and web servers this means that this port must be open through the firewall to allow communication. This configuration reduces the risk by allowing the DMZ to keep

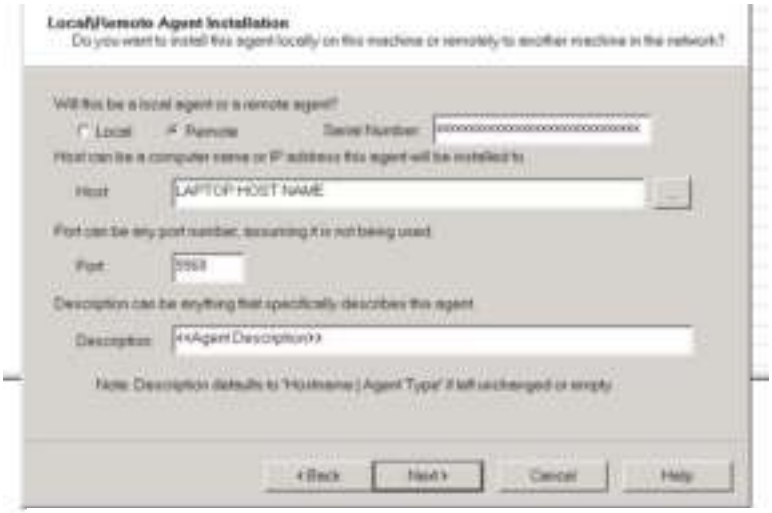

Figure 2. UpdateEXPERT Agent Install Wizard – 1st Screen.

the standard Windows RPC ports closed, 135, 139 and 445 as they are often the target of attacks.

The Leaf Agent is easily installed via the UpdateEXPERT console's agent wizard or it can be installed via the command line. According to St. Bernard it can also be installed remotely. The author tested the Leaf Agent install by taking a regular loaner laptop home and connecting via VPN service with this test laptop along with her normal ISSO laptop running the UpdateEXPERT console. The install took approximately 5 minutes. During the install the administrator provides the Serial Number of UpdateEXPERT, the NetBIOS name or IP address for the Leaf and Master Agents and the port communications will use. (Figure 2.)

UpdateEXPERT suggests that the IP address be used in the name fields. In our case, the host or Leaf Agent machines will change their IP address every time they log into the remote access services. Therefore, the NetBIOS name was placed in the host field and the port and the description was left at its defaults. This description provides a way to "tag" the entry in UpdateEXPERTS' network view. After this information is entered, UpdateEXPERT attempts to connect to the host specified. Once the connection is made a second screen appears. (Figure 3.) The administrator indicates if this is a new Leaf or Master Agent install or a reinstall. The administrator must also indicate the location of the Master agent server. Since the Master Agent is a server with a static IP address the author used the IP address rather than the Netbios name. The communication port is then specified. It should be the same as indicated in the first screen. Once the agent has been successfully installed the icon in UpdateEXPERT for the host

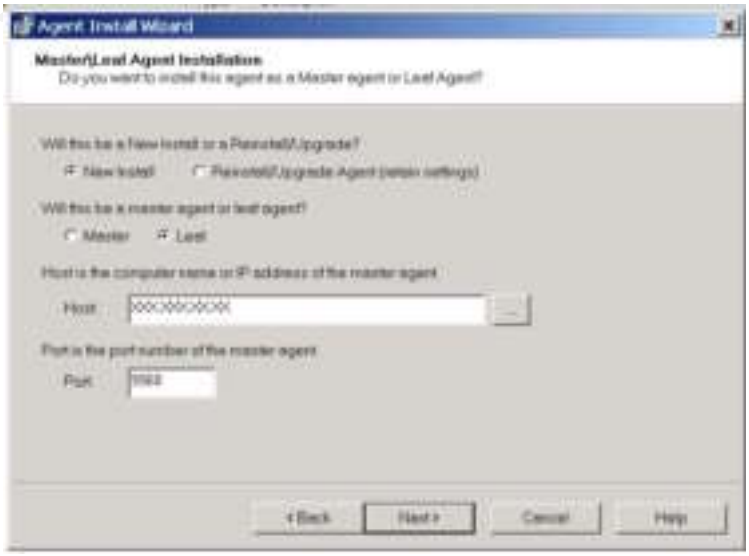

Figure 3. UpdateEXPERT Agent Install Wizard – 2nd Screen.

shows up in the network view. The icon for Leaf Agent clients is distinguishable from the normal icon by the addition of a person's head over the PC icon. (Figure 4.)

Agent installation revealed that many of the laptops had not been updated correctly after the move to Active Directory in January. Almost all of the laptops did not have the proper administrative accounts in their local administrative group. This caused the agent install to fail. This had to be corrected before the test could continue, requiring everyone to bring in their laptops and flexiplace machines. During the installation process the author found a few more deficiencies in the Laptop Checkout Procedure requiring an update of the process. This need to fix the administrative account deficiencies required that testing of patch rollout be performed in house rather than via live field test. It was a simple manner to duplicate the dial-up configuration in house while VPN testing occurred over the author's DSL line. The author tested the roll out at home with a standard loaner machine. The dial-up process was tested by hooking up laptops with a newly installed Leaf Agent to the dial-up service via an analog line in the office and pushing the latest patches down.

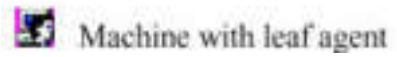

Figure 4. Leaf Agent Icon.

When rolling out patches, the operator can choose to have the machine reboot after each patch. The author forced a reboot after each test patch to see what would happen with multiple patches requiring a reboot to complete the install, thereby causing the laptop to disconnect from the remote access service. The multiple patches worked perfectly. The Master Agent pushed out all patches to the laptop before beginning the installation process. The Leaf Agent, working autonomously, took over and installed all the patches, handling the reboot process without needing further communication with the Master Agent. The entire process using the three latest Microsoft updates took approximately 15 minutes. The time for the patch process to occur on dial-up as compared to DSL was approximately the same. The only difference is in the time required to download the patches. Dial-up will take more time. The time required for the installation process really depends on the speed of the processor. To ensure patching had been successful, the author reconnected to the internet either via dial-up or VPN and had UpdateEXPERT query the machine to see that the patches had been installed. The author then opened a browser on the laptop and ran Windows Update to confirm that there were no outstanding updates. The laptop was then turned over to the help desk to complete the Laptop Checkout Procedure and be returned to the user.

The last feature to investigate was how the Leaf Agent interacts with UpdateEXPERT's ability to delay the time that the update begins. When using the Install Wizard to deploy patches the administrator has the option to push the patches out now or to choose a specific time for the patches to deploy. In order to work correctly upon completing the Install Wizard the author found that the

target machine had to be available on-line to the Master Agent. The patches are downloaded to the Master Agent machine immediately upon completion of the Install Wizard then transferred to the host client "along with a binary file carrying patch installation specs from the Install Wizard" (St. Bernard Software, Inc.) The Leaf Agent contains the patch installer service which manages the install on the time schedule selected by the administrator. The patch installer service runs autonomously, it is "persistent across reboots and shutdowns, meaning that it restarts automatically. If a user shuts the machine down, and boots it after the date/time specified for installation, the installer is smart enough to do the patch installation anyway." (St. Bernard Software, Inc.) This means that "target machines can be rebooted one or more times, or shutdown for an undetermined amount of time, and they will STILL get patched by the UpdateEXPERT installer service upon restart." (St. Bernard Software, Inc.) This facility will be very useful. It will limit the amount of time the ISSO and user needs to be online and it will make it easier for the ISSO to coordinate with the user to ensure that the updates do not interfere with the user's work needs. The ISSO can negotiate a time to "meet" with the remote user online and push out the updates and have them install at a later time when the user is not using the remote access connection to gather email or work.

Procedural Solutions

Personal PC

Since the author, as the ISSO of the institute, does not have the freedom to remotely control a user's personal PC, a process of open communication has been instituted to clearly explain the possible dangers and the need for patching and applying anti-virus to personal machines. An agency policy calls for all staff to take Security Awareness training once a year. In April, all staff was required to go through a web-based training program. As an adjunct to this security awareness training the author has written articles in the institute's IT newsletter and provided links to a Beginner's Guide to Home Computer Security from CERT[6] and a Power User's Guide from the Department of Energy's Computer Incident Advisory Capability (CIAC) office.[7]

When a vulnerability is reported or a new exploit is released an "all-hands" email is sent letting staff know when new critical patches are available. The email informs them of the availability of tools on CD to assist in prevention or clean up such as anti-virus updates, critical patches and tools to detect and fix specific exploits such as Stinger[8], Network Associate's free Blaster/Nachi plus more removal tool. Patches and updates that are available on the internet are provided

[6] See Beginner's Guide to Home Computer Security
http://www.cert.org/homeusers/HomeComputerSecurity/
[7] See Power User's Guide
http://www.ciac.org/ciac/documents/CIAC-2324_Connecting_to_the_Internet_Securely_Protecting_Home_Networks.pdf
[8] For more information on Stinger see
http://vil.nai.com/vil/stinger/

on CD because experience has shown that dial-up users are less likely to install larger patches due to the time involved. The cost of creating and distributing these CDs are miniscule compared to the cost of cleanup.

Since August these "all-hands" emails have been refined to require feedback from users. The author is finding that some users are not sure how to patch their machine or set up their own or institute provided anti-virus program. As a form of compliance check the author has been in discussion with her supervisor, the Chief of ITOS, about having the users provide some proof of updating. The thought is that the users would have to provide a screen shot showing the dat file version for McAfee's AntiVirus program which is freely provided by the institute to anyone who asks, and to run a self Sara[9] Scan, a service provided by the ITC. While the Sara Scan won't necessarily identify all possible vulnerabilities the users won't necessarily know that and will hopefully feel motivated to ensure they are updating when asked. The other option is to have the user send a screen shot of the Microsoft Windows Update[10] history. Of course, this last option requires more of the ISSO's time to check each of the 40 and growing home PC users. This is one reason the author is pushing to have all authorized work at home be done from an institute provided machine. As the institute prepares to replace its current 1GHz desktops, which would normally be surplused, the author feels that these would make great home machines for the currently 60 or so staff that have permission to remotely access the institute. Having institute control over all remote access machines would make the author's job easier. As mentioned earlier, there have been rumors that this might be discussed at future ISSO meetings. The author feels that it probably won't become an agency mandate as larger institutes have expressed issues over cost so the key is convincing institute management that it's worth the extra resources which the author believes would be minimal. Since there is really nothing more the ISSO can do with personal PC's, the extent of protection is limited to awareness training, making it easy for staff to make the necessary updates, holding classes and checking for compliance.

Institute PC/Laptop

Since the ISSO does have control over the institute's laptops and flexiplace PCs the technical solution of the deployment of UpdateEXPERT Leaf Agents was the interim solution put into place. This solution is attractive because it's a simple extension of a package that is already in use and has worked well. There is little in the way of extra resources required to implement the Leaf Agents and there is little in the way of learning curve. UpdateEXPERT has proven itself as it was instrumental in limiting the impact of the Blaster and Nachi worms.

[9] For more information on Sara (Security Auditor's Research Assistant) see http://www-arc.com/sara/

[10] For more information on Microsoft Window Update see http://v4.windowsupdate.microsoft.com/en/default.asp

Due to the problem of many of the laptops not having the required Active Directory administrative credentials all laptops and flexiplace equipment had to be brought in and brought up to standards before having the Leaf Agent installed. Unfortunately, the Leaf Agent is not a totally automated solution. The laptop has to be connected via remote access for the initial roll out of patches. Once the Master Agent has pushed down the patches the laptop will work on its own, but a procedural process must be put into place to make that initial connection. This process is going to require more of the ISSO's time, for as patches become available the ISSO must coordinate with the help desk to determine where all the laptops are. A set number is on permanent loan but the remainder may be in the office or out on temporary loan. There will be a different procedure depending on the type of remote access equipment; flexiplace, permanent laptop or loaner laptop.

The ISSO has created a mailing list of remote access users to facilitate the initial email. There are three types of messages that will be created. The first will go to flexiplace employees. They have a desktop machine and work one or more days at home. This means that the ISSO will simply need to make an online appointment on a flexiplace day, connect to the flexiplace machine and load the patches. Because the staff is supposed to be working at home that day the ISSO will have to provide an estimate of how long the process will take. This is determined during the patch testing phase. Testing is a patch management best practice. Federal Computing Week reported testing as a recommendation from the General Accounting Office in its "Patch management best practices" article:

> * Test each patch. Evaluate individual patches in various system configurations in a test environment before installing them agency wide to avoid any negative impact on the network. (Yasin)

The author will change the normal patch testing procedure to include installing patches deployed via the Leaf Agent to a laptop connected to the network to simulate a VPN connection and a laptop connected via dial-in. During testing the author will note the time it takes for patches to be installed. This information will be included in the email to provide an estimate for when the author should attempt to reconnect to determine if the updates were successful. This information will also provide the user an idea on when they can return to work. This has been a rather easy process as most flexiplace employees are very accommodating to any process that saves them from having to bring in their regular desktop machine.

The second type of email will go to staff with a permanent laptop. Currently the author gives those with a permanent laptop two choices; bring in their laptops within 3 days, as some already bring their laptops in daily or make an appointment with the ISSO to connect via remote access and push down the updates. If staff chooses the online route, this will usually have to happen after

hours. The UpdateEXPERT console makes this possible, allowing the ISSO to make these connections from home. The idea, of course, is to try and limit the amount of after hours time put in by the ISSO but right now there is less than 20 staff that has permanent laptops. As of this writing there has not been a chance to effectively try this procedure. The ISSO hopes to sell this as being more convenient for staff, but unless they are on travel, bringing in a laptop is not that difficult.

The third type of email goes to staff with laptops on temporary loan. These people may be on vacation, on travel, taking a class or perhaps on sick leave. The ISSO feels these are probably going to be the most difficult group as they use the laptops temporarily, they tend to be less technically astute and security and safety of the equipment is only a peripheral concern for them. This group also has the most diverse schedule. The ISSO may very well have to asses the risk of each laptop on a case by case basis and only update those that are not coming in within a certain time window. For example, for a person on travel who will return the laptop in two days the author may not attempt to remotely update but for a person on sick leave for four weeks remote updating would be necessary. The window will be determined by the ISSO, depending upon how long the vulnerability has been available, the availability of known exploits, the risk to the institute, etc. The ISSO has discussed the potential problems of getting staff to cooperate with the Chief of ITOS and a decision has been made that the ISSO will be able to inform staff that failure to cooperate will result in the ISSO having their remote access account temporarily disabled. This is the only true leverage the ISSO has. Staff has been informed that IT management reserves the right to disable remote access accounts. We have also discussed creating policy that states IT will pull all remote access if an exploit is released that the institute is not protected against to give the ISSO time to eliminate the vulnerability.

Putting it all Together

This case study described the process of recognizing that there was a hole in the institute's patch and vulnerability policy making remote access machines vulnerable to fast moving exploits such as the Blaster and Nachi Worms. The author needed to find an interim solution that did not require any financial resources and little in the way of time to research and implement as there was a plan for contractors to image new desktops and laptops and to suggest an automated way to protect remote access machines in early 2004. The author needed a stop gap measure to protect the institute's resources until the deployment of new hardware. The author found a workable solution when UpdateEXPERT, the patching program of choice, released its new version in April. New features provided the tool the author needed to connect to remote computers that she had not been able to before. The advantage of this tool was that the author was already familiar with UpdateEXPERT so there was no

learning curve. The installation of the Leaf Agent was simple, requiring less than 5 minutes and there were no extra costs to implement.

Along with implementing a technical solution the author had to revise or create new procedural solutions. The author had to revisit the Patch and Vulnerability policy to remove the quarterly vulnerability/patch mandate as that left institute resources dangerously exposed for too long a period. The laptop checkout process also had to be revised as the process of installing the Leaf Agents proved that most of the laptops were not up to standards. Procedures for contacting staff and providing more security awareness training and for setting up appointments to allow the ISSO to push out patches remotely had to be devised. The author is also working with the Chief of ITOS to find a way to have staff with personal PC's prove compliance to the agency remote access policy that states they will keep their PC's up-to-date with patches and anti-virus definitions.

The author sees UpdateEXPERT Leaf Agents as a temporary solution. As mentioned earlier, the author believes that the best solution for patch management is a technical solution that eliminates depending on people to do the right thing whenever possible. An automated process that will check the laptop and if it needs updates will push them down when the laptop connects via remote access would be the best solution. The contractor chosen to develop images for new desktops and laptops has suggested that the automated tool that would best fit the institute's environment is the SUS service by Microsoft. If we find that the remote machines can pull updates from the SUS server without intervention that would be ideal. The author predicts that remote access use in the institute will only increase and that the Leaf Agent will become difficult to manage. For the time being, the Leaf Agent provides the ISSO a chance to update laptops that are on the road rather than being forced to disable remote access privilege until the laptop can be returned or having to accept the risk of the laptop infecting the network. The Leaf Agent will allow the ISSO to handle emergency critical patches where before there was no practical solution. This will be immensely helpful as during the last few "major" patch releases the agency ISSO's have had to report what they are doing toward reducing the vulnerability and what percentage of resources have been patched. Usually the time frame for these reports has been less than a week with the unwritten requirement being to get to 100% patched as quickly as possible.

The idea of remote updates has been well received by most of the institute's remote access users. The practicality may prove a little difficult until the users see that it is painless and benefits them. The IT section has managed to protect institute users from seeing the results of the latest exploits so the author feels it make take a while for them to understand the small inconvenience can have a much larger payoff in prevented downtime. If it so happens that the Leaf Agents became a longer lasting solution, the author would consider writing a specific policy to ensure that laptop users cooperate completely. Perhaps, through this constant contact, users will begin to understand the hurtles the IT

staff must jump through to keep the institute's resources safe. The author feels that if the users can understand the need for security, and if their approach to laptop, remote access and their own PC's security can be positively influenced then a small victory has been won.

References

Cornwell, Kay A. “Security Essentials: Patch Management as a Necessary Part of Defense in Depth. A Case Study.” Feb 20, 2003. <http://www.giac.org/practical/GSAE/Kay_Cornwell.pdf>. (28 Dec 2003).

Cornwell, Kay A. “Security Essentials: Patch Management as a Necessary Part of Defense in Depth. A Case Study.” Feb 20, 2003. 12. <http://www.giac.org/practical/GSAE/Kay_Cornwell.pdf>. (28 Dec 2003).

Federal Government. Public Law 106-346, § 359. October 23, 2000. <http://www.telework.gov/twlaws.asp>. (28 Dec 2003).

GIAC Research Agency. “GRA Telework Policy (Internal Documentation.)” October 30, 2003.

Gregory, Peter. “Lessons learned from the Blaster worm.” September 24, 2003. <http://www.computerworld.com/securitytopics/security/story/0,10801,85247,00.html>. (28 Dec 2003).

Klaren, Judy. “Managing Vulnerability Assessment and Patch Installations.” January 24, 2003. 2. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (28 Dec 2003).

Klaren, Judy. “Managing Vulnerability Assessment and Patch Installations.” January 24, 2003. 4. <http://www.giac.org/practical/GSEC/Judy_Klaren_GSEC.pdf>. (28 Dec 2003).

Poulsen, Kevin. “Nachi worm infected Diebold ATMs.” November 25, 2003. <http://www.theregister.co.uk/content/55/34175.html>. (28 Dec 2003).

St. Bernard Software, Inc. “The Power of Optional Agent Architecture: Advantages of Managing Patches Remotely with UpdateEXPERT®” July 28, 2003. 4. <http://www.stbernard.com/products/docs/OptionalAgent.pdf>. (28 Dec 2003).

St. Bernard Software, Inc. “How does UpdateEXPERT deploy patches?” <http://www.stbernard.com/products/support/updateexpert/uetechfaqs/UpdateEXPERT6.x/Patch_Deployment/Configuration/UE0146.htm>. (28 Dec 2003).

St. Bernard Software, Inc. “How does UpdateEXPERT deploy patches?” <http://www.stbernard.com/products/support/updateexpert/uetechfaqs/UpdateEXPERT6.x/Patch_Deployment/Configuration/UE0146.htm>. (28 Dec 2003).

St. Bernard Software, Inc. “How does UpdateEXPERT deploy patches?” <http://www.stbernard.com/products/support/updateexpert/uetechfaqs/UpdateEXPERT6.x/Patch_Deployment/Configuration/UE0146.htm>. (28 Dec 2003).

St. Bernard Software, Inc. “How does UpdateEXPERT deploy patches?” <http://www.stbernard.com/products/support/updateexpert/uetechfaqs/UpdateEXPERT6.x/Patch_Deployment/Configuration/UE0146.htm>. (28 Dec 2003).

Vijayan, Jaikumar. “Patching Becoming a Major Resource Drain for Companies.” August 18, 2003. <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,84083,00.html>. (28 Dec 2003).

Yasin, Rutrell. “Patch management best practices.” Dec 1, 2003. <http://www.fcw.com/fcw/articles/2003/1201/cov-patch2-12-01-03.asp>. (28 Dec 2003).

Figure References

Figure 1. UpdateEXPERT Communication to Leaf Agent in DMZ. From UpdateEXPERT v. 6.1 Deployment Guide. <http://www.stbernard.com/products/docs/ue_deployguide.pdf>. 16. (28 Dec 2003)

Figure 2. UpdateEXPERT Agent Install Wizard – 1st Screen. Screenshot from UpdateEXPERT.

Figure 3. UpdateEXPERT Agent Install Wizard – 2nd Screen. Screenshot from UpdateEXPERT.

Figure 4. Leaf Agent Icon. From UpdateEXPERT 6.1 Manual. 17. (28 Dec 2003).

Footnote References (Product Websites)

[1] McAfee E-Policy Orchestrator Website
URL:
http://www.networkassociates.com/us/products/mcafee/antivirus/fileserver/epo.htm. (28 Dec 2003).

[2] St. Bernard's UpdateEXPERT Website
URL:
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp. (28 Dec 2003).

[3] Microsoft Systems Management Server Website
URL: http://www.microsoft.com/smserver/default.asp. (28 Dec 2003).

[4] Microsoft Software Update Services Website
URL:http://www.microsoft.com/windowsserversystem/sus/default.mspx. (28 Dec 2003).

[5] 3Com Embedded Firewall Policy Website
URL:
http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=134482&selcat=Security+Products&family=134494. (28 Dec 2003).

[6] Home Computer Security
URL: http://www.cert.org/homeusers/HomeComputerSecurity/. (28 Dec 2003).

[7] Connecting to the Internet Securely: Protecting Home Networks
URL: http://www.ciac.org/ciac/documents/CIAC-2324_Connecting_to_the_Internet_Securely_Protecting_Home_Networks.pdf. (28 Dec 2003).

[8] McAfee AVERT Stinger
URL: http://vil.nai.com/vil/stinger/. (28 Dec 2003).

[9] Sara (Security Auditor's Research Assistant) Website
URL: http://www-arc.com/sara/ (28 Dec 2003).

[10] Microsoft Windows Update Website
URL: http://v4.windowsupdate.microsoft.com/en/default.asp (28 Dec 2003).