Global Information Assurance Certification Paper

Edwin L. Armistead
SANS GSEC - Track 1
10 Feb 2003

Patch Management: Can the U.S. Navy Regain the Initiative?

"There is a war out there, old friend - a World War. And it's not about whose got the most bullets; it's about who controls the informa tion. What we see and hear, how we work, what we think. It's all about the information."

Cosmo[1]

Introduction (Abstract)

Five years can be a long time, and if one looks back to where the general public and the computer industry stood at that poin t in history (1999), you can see that indeed much has changed. The initial euphoria associated with the promises of the Information Age, has since evolved to an attitude of cautious pessimism . Waves of virus's and worms have attacked so many different sy stems and computers during this period, that combined with the Y2K scare, our earlier feelings of wonderment and excitem ent about the Internet sim ply no longer exist. Ins tead, today' s consumers and network operators are beginning to feel overwhelmed by th e sheer numbers and ferocity of these attacks. Calls are beginning to go out for more policing and security of the Internet, and greater punishment for those who violate this system. Just lik e the Wild, Wild West of the United States, which had to be tam ed and settled over a century long period, so too could this be the future for the information technology environment. The days of permissive 'anything goes' attitudes are quickly changing as the general population becomes much more aware of the security concerns affecting today's networking environment.

Into this mix, the Department of Defense (DoD) is attempting to evolve their legacy systems and networks into a more integrated and seamless architecture. But within this broad threat environment, where e very connection to a network must be regarded as a potential avenue of attack, comes the realization that there is no one silver bullet or solution that will make the infrastructure safe. Instead it must be a layered approach, one that attempts to lo ok at all aspects of the security solution including personnel, policy and technology. In this paper, the author specifically examines the eff orts by the United States Navy, to address configuration control and especially patch manageme nt as a tool to maintain the security of it's networks. The Information Assurance Vulnerability Management (IAVM) program will be analyzed to determine how successful this process is at keeping the service's architecture up -to-date with respect to mitigating existing threats. I n addition, the author will offer suggestions to improve the ability of the fleet to protect itself against daily attacks by virus's and worms that exploit known vulnerabilities. For as the entire security community has learned over and over again through out the last few years, a network is

Comment: Wrong usage—need a different word

[1] *Sneakers*, movie, director: Phil Alden Robinson, 1992.

only as good as it's weakest link, and a risk assumed by one, is a risk imposed upon all!

The Problem

While 1999 was only a mere five years ago, the revolution of Inf ormation technology since that time, combined wi th the increased use of the Internet, has drastically changed the way the sea service conducts business. Message traffic via e - mail, chat, collaboration tools, the use of internal fleet networks and portals have all combined to make the Navy very dependent on reliable and dependable communications. Whereas previously, the service relied on a series of high frequency and satellite traffic to conduct operations, today much of the bandwidth has been shifted to Non-Secure Internet Protocol Router Network (NIP RNet) and Secret Internet Protocol Router Network (SIPRNet) systems.

Unfortunately, this shift to a network -based architecture has also expose d a whole host of Navy networks to a wide variety of attacks. As with any innovative technology, there are alwa ys inherent dangers with exposing the computer systems and data to the outside world, and yet this threat has in the past not been understood very well. Combine this with the fact that computers by their very nature are extremely complicated devices, and to use them eff ectively on the Internet of ten requires a se ries of standard interfaces and software programs, and one can see how the problem rapidly gets worse. Since modern operating systems and software applications are so extensive and complicated (th e Windows 2000 software currently used by the Navy, f or example, checked in with ov er 30 *MILLION* lines of code[2]), no one person or team can possibly completely understand them as a whole. Therefore, software applications are often written by a number of d ifferent groups or teams, and then integrated together. This practice, which is accepted throughout the industry, often results in exploitable holes or flaws in the code. And the Navy, as an extensive user of commercially available software, is just as s usceptible to these vulnerabil ities as any other large organization.

Before the widespread acceptance of the Internet, many service and fleet computer services were built upon standalone system s or self-contained network architectures. Some were part of small Local Area Networks (LANs) or individual workstations that the average user could not access from their desk, much less from their home. Thus these earlier frameworks were not exposed to as much risk as the networks of today. These legacy systems a nd applications, however are no longer the desired method of conducting modern military operations, and most if not all of these programs are being migrated to a much more accessible (networked) design. Consequently, the current configurations of the DoD, and in particular the sea service, are being integrated into a massive enterprise architecture, the Navy - Marine Corps Intranet (NMCI). With almost 150,000 service personnel already switched over, and another 300,000 projected in the next few years, one can see how the complexity of modern computer systems, which are integrated not only into military but also the

[2] Hamm, Steve; Port, Otis. "*The Mother of All Software Projects*," Businessweek Online : February 22, 1999 Issue. http://www.businessweek.com/datedtoc/1999/9908.htm.

civilian infrastructure as well, may need new and innovative solutions to maintain configuration control.

Patch Management as a Solution

Whether planned or not, the Navy, like most of the rest of the Defense Department, has inadvertently introduced a tremendous number of security vulnerabilities into it's networks through the current software development and architectural development processes. These holes in different programs, applications or systems are often not discovered right away, and in fact may not be discovered until years later, either by the company that wrote the application or a military user trying to execute a particular portion of code. Once a vulnerability has been discovered, there are traditionally several methods to correct the deficiency. Normally the software developer, or in the case of the DoD, will develop a patch to correct the deficiency. A patch is simply more code or a small repair program that can then either be uploaded by the user or "pushed" directly to all computers on a network in an automated fashion. Clunky, unreliable and slow to propagate through the network in today's environment, this way of doing business is undesirable from an information assurance standpoint. This point is illustrated in Figure 1, where the time from discovery of a vulnerability to it's announcement and subsequent release of an exploit has shrunk from months to weeks, and in some cases to mere days. This fact should theoretically prompt many program managers to accelerate their patch management process, but unfortunately that is not the case. In today's decentralized environment, where each and every network is considered a stand-alone system, updates must be simultaneously applied by all system administrators to maintain a secure, standard configuration across the Service enterprise.

Comment: Leigh, you need to do a THUS search, it's one of your most over-used words… and often not needed. Simple trick offered by an editor: Deleted it, and if the sentence still makes sense without it, then it really wasn't necessary.

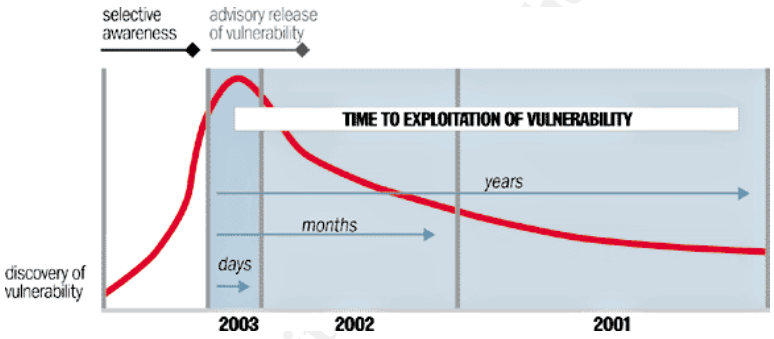

Figure 1 – Decrease in Time from Discovery of Vulnerability to Exploit Release [3]

Yet this isn't always being done. A disturbing trend that has been highlighted over and over in security literature and information assurance conferences around the world is that about 95% of the attacks on computer systems are against known vulnerabilities or previously known exploits. [4] So even though the threat mentioned

Comment: Leigh, "fact is another over-used word.

[3] Eschelbeck, Gerhard. "Do you feel the force? Malware can pull you apart." *SCMagazine*, July 2003.
[4] The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts Consensus

above and shown in the following figures can be rather amorphous and hard to define, the methods by which these hackers conduct their operations are not. Time and time again, successful attacks are made against known vulnerabilities. With that in mind, if a system administrator were to keep up with every patch and service pack, install all hot fixes and monitor their network to ensure that all known vulnerabilities are eliminated, they will prevent the vast majority of attacks which cripple networks everyday. The fact that these worms and viruses do succeed means that there are simply too many systems that are not maintaining good configuration control. Two good examples of this long lead time to fix known vulnerabilities are the SoBig virus, for which the flaw was known for 651 days before an exploit was developed, and the Bugbear worm, where the known vulnerability existed for 550 days. [5] One would think that this is certainly enough time to mitigate these known deficiencies! Yet as mentioned earlier and shown in Figure 2, the vast majority of threats are known and can be defended against if the network owner has the resources and policies in place to make that happen.

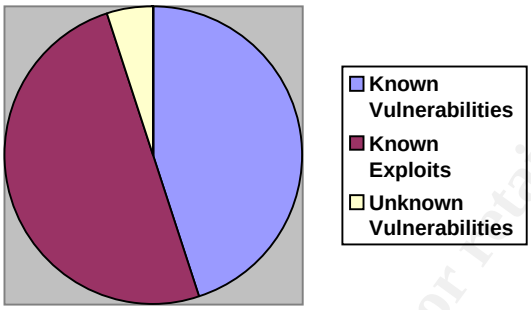

Figure 2 – Percentage of Known Vulnerabilities and Exploits [6]

Eligible Receiver and Solar Sunrise

Even before the above-mentioned exploits, other earlier events prompted the DoD to devise the Information Assurance Vulnerability Management (IAVM) program. This initiative was designed to ensure that known vulnerabilities affecting the various computer networks within DoD were corrected through a series of patches centrally mandated throughout the services. [7] This change came mainly from the deficiencies highlighted by a Joint Chiefs of Staff exercise named *Eligible Receiver* conducted in June 1997, and a real-world attack named *Solar Sunrise* that occurred in the spring of 1998. The purpose of *Eligible Receiver* was to demonstrate that hostile forces could penetrate national infrastructures and DoD networks using Computer Network Attack (CNA) and other techniques to adversely affect the government's ability to conduct

---

Version 4.0 October 8, 2003 Copyright (C) 2001-2003, SANS Institute Questions.

[5] Symantec Internet Security Threat Report, Malicious Code Trends, 1 January – 30 June 2003 (p, 5).

[6] Eschelbeck, Gerhard. "Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats?" Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census House Government Reform Committee, 10 September 2003.

[7] The Information Assurance Vulnerability Management (IAVM) program is defined in Appendix A to Enclosure B of Commander Joint Chiefs of Staff Memorandum 6510.1.

military operations.[8] A number of non-DoD agencies were also involved, including the Federal Bureau of Investigation (FBI), the Department of Justice, the Department of Transportation, the State Department, the Central Intelligence Agency, the National Reconnaissance Office and the National Security Council. The "attackers" consisted of a National Security Agency Red Team replicating the threat from a domestically situated but state-sponsored team operating on behalf of a nation that had refused direct military confrontation with the United States. This 'nation' concluded that the United States had become so militarily and economically dependent on vulnerable information systems that a non-attributable CNA operation offered a viable option. The objective of these attacks was to alter United States policy and delay or deny our ability to respond militarily while avoiding detection and arrest.

The Red Team, using only open source intelligence and hacker tools available on the Internet, was able to fully demonstrate the vulnerability of DoD and national-level systems and networks. The rules of engagement allowed the team to conduct actual attacks on DoD systems and conduct simulated attacks on National Information Infrastructure systems.[9] Lessons learned from *Eligible Receiver* emphasized the need for effective vulnerability assessments, network indications and warning, appropriate command and control, a designated cyber-defense command, consequence management, interdepartmental/interagency planning, procedures, and processes. Probably the most important lesson learned from *Eligible Receiver* was the need for a central DoD agency to be in charge of network defense. The Defense Information Systems Agency (DISA) is normally responsible for protecting the National Information Infrastructure; however, in reality they are a combat support agency and cannot order a DoD or government agency to change any policies. It eventually took over 18 months to solve this problem, and was only complete with the formation of the Joint Task Force-Computer Network Defense (JTF-CND).

In the meantime, during February and March of 1998, the United States military, government and research and development sites experienced a large number of systematic intrusions, which were determined to be related to one another.[10] Code-named *Solar Sunrise*, the timing of these activities was very suspicious since it coincided with another build-up of United States military personnel in the Middle East in response to tensions with Iraq over United Nations weapons inspections.[11] The intruders penetrated many unclassified U.S. military computer systems, including Air Force bases and Navy installations, Department of Energy national laboratories, the National Aeronautic and Space Administration, and a number of university sites. The timing of the intrusions and apparent origination of some activity from the Middle East led many government officials to suspect that this could be an instance of Iraqi CNA aimed at disrupting the U.S. military build up in the region. Subsequent investigation and detailed research by the National Infrastructure Protection Center and the FBI,

[8] "Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack." *SANS Paper*, 24/606.

[9] Lawson, Shannon M. "Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure." *SANS GSEC Paper*, http://www.sans.org/rr/papers/29/821.pdf.

[10] "What is Solar Sunrise? *SANS Intrusion Detection FAQ.*

[11] Glave, Jason. "Getting to the Bottom of 'Cyber Attacks'" 26 February 1998. *Wired News*. http://www.wired.com/news/technology/0,1282,10557,00.html.

working closely with Israeli law enforcement authorities, determined that the perpetrators were two juveniles in Cloverdale , California, and an individual with several accomplices in Israel. Once again, a central governm ent agency to coordinate an appropriate response was needed but not yet available. *Solar Sunrise* validated the need for DoD to closely coordinate with law en forcement agencies, especia lly the FBI, when dealing with unidentified computer intruders. [12] In addition, this incident also reaffirmed the use of military computer emergency response team s as appropriate to not only respond to these types of attacks, but also to develop preventive measures to help prevent or mitigate their eff ects. And once again, as will be shown later in this paper, patch management and configuration control are the most important tools in this constant struggle to protect the service n etworks. Because the level of intruder knowledge and sophisticati on has risen at a constant rate over the last 15 years, as shown below in Figure 3, what was once considered a capability beyond the reach of many individuals is now considered by many in th e hacker community to be common knowledge.

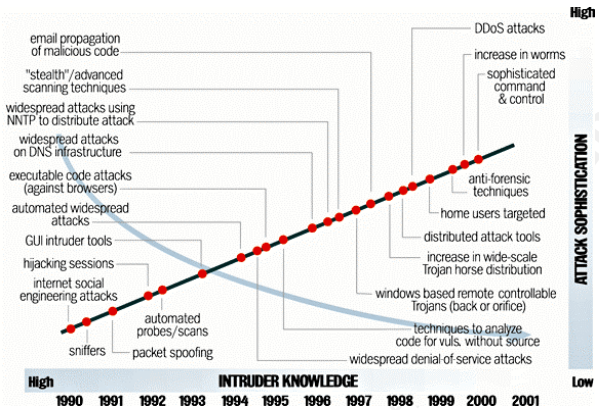

Figure 3 – Changes in Intruder Knowledge vs Attack Sophistication [13]

The Navy and the IAVM Process

From these two seminal events, the Information Assurance Vulnerability Management (I AVM) program was dev eloped. Under this concept, a central DoD organization, in this case the JTF -CND would notify the services and commands of an identified vulnerabilit y and give each unit a certain amount of tim e to take corrective action and report comp liance up the chain of command. In the Navy, the Naval Component Task Force – Computer Network Defense (NCTF -CND) was originally established as the subordinate servi ce component. In 2003, it was aligned under the Naval Computer Incident Response Team (NA VCIRT).[14] These comm ands (NCTF-CND and NAVCIRT) would conduct a risk analysis once a vulnerability was announced

[12] "How To Eliminate The Ten Most Critical Internet Security Threats, The Experts' Consensus." Version 1.32 January 18, 2001, Copyright, 2000, *The SANS Institute*, http://www.sans.org/top20/10threats.rtf.

[13] Eschelbeck, Testimony, September 2003.

[14] U.S. Navy Message, DTG 051953Z May 03. *Navy IAVM Process.*

and would promulgate an Information Assurance Vulnerability Alert (IAVA). After this message was released throughout the service, all units in the service normally had five days to acknowledge receipt and 30 days to correct the vulnerability. However, many commands would routinely ask for and receive blanket waivers for implementing the mandated mitigation action. With all of these caveats, exceptions, waivers and extensions to these deadlines, more often than not the timelines for actual installation of a patch were exceedingly long. In effect, these units were putting their networks at risk by not mitigating a known vulnerability, and in the meantime, hackers were working on an exploit. Clearly, while the IAVM process was a great step in the right direction for the Navy, especially when compared to other parts of the federal government and civilian sector, this process still left a lot to be desired.

In addition, since most of the shore infrastructure of the Navy in the United States is migrating to the NMCI architecture, the established method of operating the IAVM program within the service has drastically changed. Because NMCI is an enterprise-wide system that is contract-driven, it is very different than the other Services' operations. As a general rule, patch upgrades or service packs in a non-NMCI environment tend to be pushed out to the military users by their program managers or system administrators. However, within NMCI, the system centrally manages IAVA compliance and distributes patches and updates to the user via the network. Normally accomplished when a service member logs onto their systems, there are however problems in this method of distribution. For instance, it is very difficult to ascertain exactly what percentage of the Navy has actually received the upgrade. Secondly, there is also the possibility that some users never actually receive the needed patch because they infrequently or never fully log into the network, or only log on via slow dial-up links that precludes large file transfers. And finally, the actual time frame scheduled to "push" some of these updates to all users is exceedingly long, often over a 100 days in length. As will be discussed later in this paper, with the decreasing period between discovery of a vulnerability and development of an exploit, the Navy does not have the luxury today of continually putting off the installation of these patches. In fact, the author argues that in the current climate, with the new threats and reduced timelines for exploitation of vulnerabilities, status quo is actually no longer adequate for the Service, and the IAVM program must be updated for not only the Navy but the entire Defense Department as well.

Comment: What are you referring to? NMCI?

The New Threats

Much of the problem facing the information technology industry and the United States government today stems from the fact that the threats to the Internet are growing more sophisticated everyday. Not only are the worms and viruses used to exploit the systems more sophisticated than their predecessors, but the speed in which these attacks are occurring is putting pressure on the system administrators as well. Historically, there has often been a significant time lag between the announcement of a vulnerability and the development of an exploitive code by a hacker (often months). But new evidence suggests that the window is shrinking dramatically. The diagram in Figure 4 depicts the results from study data completed on a large enterprise network, showing how long it took for a vulnerability message to be released in green and then how long it took for the system to be patched in red. The black line is the average

number of days between vulnerabilit y discovery and exploit attack. As you can see from this data, two years ago, it was taking about 200 days from vulnerability discovery to exploit attack; however, today that is no longer the case. The average time from vulnerability to exploit attack is down to less than 20 days, a 90% reduction in the amount of time available to fix and update a system. This is truly dramatic, and drastically affects how a network administrator needs to respond to these threats.

Comment: Do you mean Exploit Attack? Which month?

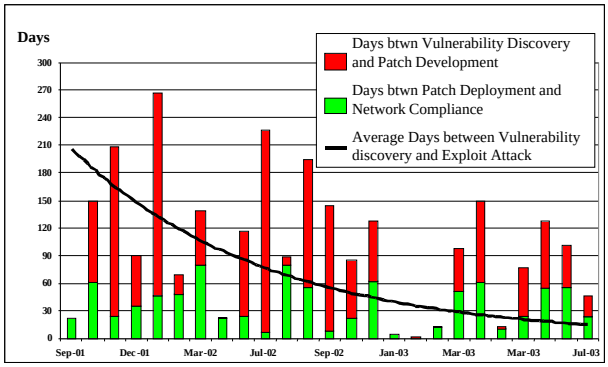

Figure 4 – Decreasing time available between Vulnerability and Exploits

Based on that trend, IA program managers can no longer treat deploying patches and configuration management as "nice to do" or administrative functions. Instead, the release of an IAVA should be treated as an immediate task, an operation that should take precedence over all other issues until it is completed. Yet this was often not done because the leadership or chain of command did not fully understand the inherent dangers these virus's and worms posed to their networks. But that is finally changing. No longer can a system administrator put off applying a patch for a vulnerability alert until they have nothing else to do. Similarly, requests for extension, which in the past were granted routinely, should instead now be considered with great reluctance, since each day a system is not patched is another day in which it can be attacked by a variety of worms or viruses.

The Solution

What Figure 4 and other references illustrate is that patch management (or lack of it) has a definite operational impact, and must become a high priority function within the organization. It can no longer be passed off to the security personnel alone, but instead must become a command function. However, as anyone involved with computer network management understands, the problem has never been a technical one, but instead one that deals with policy, people and enforcement. Unfortunately, this task is also extremely difficult, for so many security vulnerabilities are discovered on a near daily basis that it becomes almost impossible for the system administrator of a large network to keep track of which ones affect his systems and which patches have been deployed. So how does a command or organization increase the visibility of network security and configuration control? It has to come from the top to truly succeed. For if the emphasis is really placed on rapid patch management and IAVM

Comment: Figure 4

compliance, then as mentioned earlier, a system would be protected from 95% of the known threats. Yet to date, that guidance has not come down from the senior management, and much of the real work still tends to reside on the shoulders of security personnel.

Is Technology A Silver Bullet?

A quick answer is no. For example, in a typical Microsoft installation, one can receive patches, hot fixes and service pack updates all concurrently, with each one needing to be updated in an expedited fashion. This naturally puts a great deal of pressure and corresponding workload on the security professionals and system administrators alike--on top of their normal daily duties. Likewise, trying to keep on top of changes is very difficult, because there is no one source to track these security updates. Microsoft has a tool entitled "Network Security Hotfix Checker" that can run on a system to ensure that the latest patches have been installed. However, other software vendors' updates are not included on this program's database, so even this helpful application is not an end-all solution. Unfortunately, it is still up to the system administrator to track other vendors' software for any new vulnerabilities as well. A variety of 3rd party vendors have developed a series of patch management applications to help the IT team coordinate their hotfixes and patches. The leading companies include Shavlik Technologies, Bindview Corporation, St. Bernard Software, Pedestal Software's Security Expressions and the Polaris Group, to name a few. While these programs can help the system administrator, it is still a tremendous amount of work on the part of this person and their division.

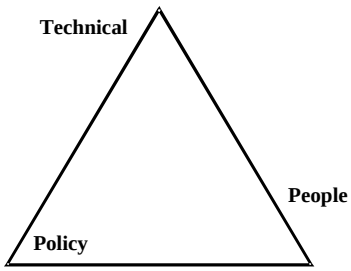

Figure 5 – Standard Information Assurance Structure

Patch management is further complicated by the fact that all changes to the programs' configurations should be tested in a lab prior to introduction onto the architecture. Yet this is a difficult if not impossible task for the average service system administrator, so commands are often forced into the position of accepting the enterprise-wide testing done by the Navy system commands or NMCI. While normally acceptable, there have been instances of patches or service pack upgrades that, when loaded onto the various networks by individual commands, have subsequently crashed the system. So what is worse, having your network taken down by a virus or worm, or by the incompatibility of a series of patches? In this nightmare scenario, which is all too familiar to many a Navy program manager, how does one maintain configuration control over one's network, when compliance is mandatory? In addition, since testing can take

time, will the commands still be able to meet the required deadlines required by the IAVAs?

Command Involvement is Key

Therefore if senior level guidance is not currently present and technology is not an answer, then command involvement within the individual units and activities is key to success for the service. In the Navy, it is at the ship, squadron and station level where key changes are now being made to the DoN IAVM program. The sea service has a process called the Online Compliance Reporting System (OCRS). This web-based program allows all service organizations to report compliance with vulnerability alerts and bulletins, and provides visibility to the chain of command for monitoring subordinate commands. This process has undergone a series of upgrades, with a series of messages released in the spring of 2003. [15] All were designed to significantly limit extensions, yet it is still possible to exceed 100 days if an IAVA is extended twice! Based upon the decreasing period between the discovery of a vulnerability and the exploit attack, has the Navy really done anything to make the infrastructure more secure? All of these instructions have focused on the policy and technical portions of the information assurance (IA) triangle shown above in Figure 5, but to truly succeed, in the author's opinion, more emphasis must be placed on increasing the performance of the IA personnel involved in patch management. Right now, the onus of patch testing, deployment, compliance and reporting is placed entirely on the Information System Security Manager (ISSM). Yet the proper operation of the network is not a concern for just the security personnel, but instead should be a major focus for the entire organization and chain of command.

That is why I propose that the Navy make the DoN IAVM process a more direct responsibility of the senior official of each command or agency. In effect, just as a unit is graded on it's readiness and training posture, it should also be graded on its security posture. The status of patch management and IAVM compliance should be a regular discussion item at every staff meeting, and all departments should be aware of the vulnerabilities and what needs to be done. Just as all divisions in a group contribute to the overall readiness and training grades, the same can be said for security, because in many instances it is the user who is the weakest link, and they must be made aware of the vulnerabilities that they can inadvertently introduce into a system. Some analysts have gone so far as to suggest that an entire patch management team should be created, perhaps as a separate division or fly-away team. The idea is to have a sub-unit or group that has support from the command's leadership and the authority to jump onto a network or system, shut it down for the time needed to bring it under a standard

[15] The oversight of the DoN IAVM program was assumed by Commander Navy Network Warfare Command (CNNWC) per Navy message Date Time Group (DTG) 052021Z Mar 03. In the next update to the Navy IAVM process, the Navy Component Task Force – Computer Network Defense (NCTF-CND) released a message DTG 051953Z May 03, to align with the Command Joint Chiefs of Staff Memorandum (CJCSM) 6510.01 directive. This particular instruction tightened the IAVA extension process, and defined specific information needed for evaluation by these requests. In a follow-on message by NCTF-CND on DTG 022059Z Jun 03, this new IAVA extension process was tied to Online Compliance Reporting System (OCRS) and directed every command in the Navy to set up an account.

configuration control and then move on.[16] While this approach may not be suitable for all staffs and units within the Navy, it is one method to implement patch management that could ensure that commands are compliant with the latest IAVA. The bottom line is this: unless some sort of pressure or accountability is introduced into the process, commands will never be safe from known vulnerabilities and their accompanying worms, viruses and denial of service attacks.

Summary

In conclusion, the real key to maintaining a secure network and information environment is upper-level leadership. The network cannot be seen as an administrative tool or the sole domain of the IT team, but instead should be viewed as a primary resource for mission accomplishment. The process of configuration control must therefore be viewed as an all-hands effort, one that involves the entire organization from the newest recruit to the Chief of Naval Operations. This is the only way that real change will occur. If a risk accepted by one truly is imposed upon all, it is critical that Navy leadership ensures patch and service pack update compliance by everyone. Similarly, if the DoN IAVM process is changed to require command accountability and tighten up the compliance timeline, it will go a long way toward ensuring a more protected environment that can decrease the exploit timeline and prevent the next generation of worms, viruses or multi-payload malware from exploiting known vulnerabilities.

[16] Voldal, Daniel. "A Practical Methodology for Implementing a Patch Management Process." *SANS Institute*, 2003.

References Cited

"Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack." *SANS Paper*, 24/606.

Eschelbeck, Gerhard. "Do you feel the force? Mal ware can pull you apart." *SCMagazine*, July 2003.

Eschelbeck, Gerhard. "W orm and Virus Defense: How Can We Protect the Nation's Computers From These Threats?" Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relatio ns and the Census House Government Reform Committee, 10 September 2003.

Glave, Jason. "Getting to the Bottom of 'Cyber Attacks'." 26 February 1998. *Wired News.* http://www.wir ed.com/news/technology/0,1282,10557,00.html .

Hamm, Steve and Otis Port. " *The Mother of All Software Projects* ," Businessweek Online : Feb 22, 1999 http://www.businessweek.com/datedtoc/199 9/9908.htm .

"How To Eliminate The Ten Most Critical Internet Security Threats, The Experts' Consensus." Version 1.32 January 18, 2001, Copyright, 2000, *The SANS Institute*, http://www.sans.org/top 20/10threats.rtf .

Lawson, Shannon W. "Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infr astructure." *SANS GSEC Paper* . http://www.sans.org/rr/papers/29/821.pdf.

Sneakers, movie, director: Phil Alden Robinson, 1992.

Symantec Internet Security Threat Report, *Malicious Code Trends* , 1 Jan – 30 Jun '03.

"The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts Consensus." Version 4.0 October 8, 2003, *SANS Institute* .

U.S. Department of D efense, Commander Joint Chiefs of Staff Memorandum 6510.1, Appendix A to Enclosure B. *The Information Assurance Vulnerability Management (IAVM) Program* .

U.S. Navy Message, DTG 052021Z Mar 03. *Commander Navy Network Warfare Command (CNNWC).*

U.S. Navy Message, DTG 051953Z May 03. *Navy IAVM Process.*

U.S. Navy Message, DTG 022059Z Jun 03. Update to *Navy IAVM Process.*

Voldal, Daniel. "A Practical Methodology for Im plementing a Patch Management Process." *SANS Institute* , 2003.

"What is Solar Sunrise?" SANS Intrusion Detection FAQ.

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor