CHAPTER

9

System Security

Lauren Collins
kCura Corporation

1. FOUNDATIONS OF SECURITY

Since the inception of technology, data security has revolved around cryptography. Since cryptography is only as good as the ability of a person or a program, new methods are constantly being implemented as technology becomes more sophisticated.

Differentiating Security Threats

Cipher text and secret keys are transported over the network and can be harvested for analysis, as well as impersonate a source or, worst case, cause a service denial. Thus, aiding encryption and complex distribution methods, a network needs to be secure and elegant. That is, the network should have applicable appliances that monitor and detect attacks, intelligence that discriminates between degradations/failures and attacks, and also a convention for vigorous countermeasure strategies to outmaneuver the attacker. Consequently, network security is a completely separate topic from data security.

Incident levels should be defined as low, medium, high, and catastrophic. Level 1 help-desk professionals should be equipped to handle tasks such as these. Low-severity breach examples are:

- Malware or virus-infected system that is on the local area network (LAN)
- Account credentials compromised with general rights
- Spam e-mail incidents

Medium-severity incidents should be escalated to a system administrator or engineer. These would include:

- Website destruction
- Spam impacting an entire environment's performance

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Cyber Security and IT Infrastructure Protection
DOI: http://dx.doi.org/10.1016/B978-0-12-416681-3.00009-4

© 2014 Elsevier Inc. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

- Sensitive information leak
- Account credentials compromised with administrative rights

High-severity incidents would be handled by a senior engineer, architect, manager, or director. Examples include:

- Hacking of the environment
- International, federal, or state law violations:
  1. HIPAA (Health Insurance Portability and Accountability Act)—medical field
  2. FERPA (Family Education Rights and Privacy Act)—education field
  3. Pornography
  4. Illegal download and sharing of copyright material (music, movies, software)
- Disruption of business due to malicious acts
- Breach to systems where an act is in progress of leaking confidential information and hosts need to be disconnected altogether to halt the process

Modern enterprises and their security teams need to be prepared to work with an onslaught of new, rapidly evolving menaces. From novice script writers to sophisticated hackers working for criminal organizations, if an enterprise does not have policies in place to handle threats, they will pay the price in disconcerting, expensive data breaches. An effective threat management platform is one vibrant component for any security team who deals with evolving threats from the world outside of their control. Resources must be allocated to implement such a platform, and an agenda should be put in place while also testing the program. The following are five best practices to increase effectiveness when implementing a vulnerability management program:

1. **Control notifications and alerts.** The most important thing a company can do is get a handle on threat management and ensure an IT professional is available to review and respond to a notification or alert. In order to accomplish this, one or more individuals need to have responsibility assigned to them so that everyone is aware of which point person(s) will review logs and audits on a daily basis, or in the event of an attack. It is not uncommon to see organizations assign different individuals to review different alerts consoles. Case in point: A firewall expert may review firewall changes and logs, while an applications engineer may review the logs and alerts from the Web application firewalls.
2. **Consider a holistic view.** In the domain of discovery avoidance, attackers are growing more and more cutting edge. A multichannel attack is the superficially innocuous spear where a user clicks on a link that leads to a rogue site that has been designed to look authentic. This user may then be deceived into entering sensitive data or clicking another link affecting the target machine with a bot. Once that user's sensitive information has been collected, the attacker can now attempt to log in to a system and dive deeper into the network for more valuable information. To catch multichannel attackers, alerts need to be organized in a meaningful way from all the systems into a single console where correlation rules filter activities and, when combined, creates a single, organized attack.
3. **Slash false positives.** Have you received so many email alerts that you ignore certain alerts and immediately delete them without further investigation? This author surely

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

has. Excessive alerts and false positives intensify the noise ratio so greatly that it can be challenging (if not impossible) to scrutinize data to find truly malicious occurrences. If an organization's administrators cannot differentiate important alert signals through all the less significant events, the system becomes useless. To reduce the number of false positives fabricated, an enterprise should first analyze the alert output of its threat-warning console and then determine if the rules can be fine-tuned to reduce the false-positive noise. Also, filtering the alerts by level of confidence may be useful so that administrators can see which alerts are more likely to be relevant. One way to lower the alert levels without losing the critical alerts would be to set the threshold levels that match normal activity on the network. For example, if a company forces all users to change the password on the same 30-day cycle, they might find that failed logins increase significantly on the day after the end of the cycle. To account for this occurrence, a rule that normally signals an alert after two failed logins could be increased to four failed logins, only on days following the password change. Those logins could also be linked to other threat indicators, such as attempts to log in using the same username from multiple IP addresses, to increase accuracy.

4. **Integrate thresholds and procedures.** As mentioned in #3, aggregating threat information into a single console gives firms threat visibility across the entire infrastructure. You want more visibility? A firm can integrate that single console view with their new, refined thresholds and procedures. That's right: Always keep the mind-set that you want to be a moving target. By treating your monitoring system the same way as your infrastructure, as the infrastructure grows please ensure that your monitoring system accommodates that growth. Rules and log aggregation tools rightfully parse through information and flag legitimate attack activity for further investigation or response. Another key to integrating effectively is to make sure engineers and admins have access to proper escalation paths, communication protocols, and approved response activities.
5. **Corroborate remediation events.** In a heated situation, one can easily overlook validating events in logs upon review. Even when performing routine maintenance such as patch management, many firms fail to close the remediation loop by validating the entries. Did the patch get loaded properly? Did it close the intended vulnerability? Without testing, an organization cannot be certain the remediation was successful and the threat exposure gap was closed. There is a threat management cycle, and it must be completed utilizing steps for validation. This may include rescanning systems to validate patches and also, by performing application and network penetration, testing to confirm that fixes or controls are blocking vulnerabilities as expected.

Hardware and Peripheral Security

Network security deals with the secure transport of data. It requires more awareness and a thorough understanding of the different types of mechanisms and attack scenarios and how they can be differentiated. A topic these days for a controversial discussion is whether to allow employees to bring your own device (BYOD) to the office. Whether it is a mobile device, a desktop or laptop, or a tablet, companies must have policies in place

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

to address security and who owns the data on the device. Several places institute a policy where an application like ActiveSync is used, and upon an employee's termination the device(s) can be wiped of all data. That usually sounds good to the employee upon signing the consent form, but imagine losing all your contacts, music and apps, and all the data on the device. Given the breadth of end users on mobile devices and the diversity of use cases, BYOD is driving not just the need for performance upgrades but also much more fine-grained network access controls.

There is also a method for detecting signatures and how that is used to classify attacks and enhance network security. Computing platforms used in the field are intricate and require interaction between multiple hardware components (processor, chipset, memory) for their normal operation. Maintaining the security of the platforms translates to verifying that no known security exploits are present in the runtime interaction between these hardware units which can be exploited by attackers. However, given the large number of state elements in the hardware units and many control signals influencing their mutual interaction, validating the security of a commercial computing platform thoroughly can be complicated and intractable. By exemplifying challenges to correctly implement security, it is necessary to provide examples of various classes of hardware-oriented security attacks. The following are logic and tools to use:

- For the enthusiastic newbies, there are pre-made, entry-level tool packages as shown in Figure 9.1. You can diagnose your hardware without writing even one line of code. Automatically generate your device driver, and run this nifty tool on any operating system.
- Digital oscilloscopes, logic analyzers, device programmers, and spectrum analyzers are all available on eBay and are no longer out of reach for hardware hackers. Utilizing this equipment, one can take advantage of essentially the same equipment used in production engineering facilities. In Figure 9.2, a logic analyzer displays signals and program variables as they change over time.

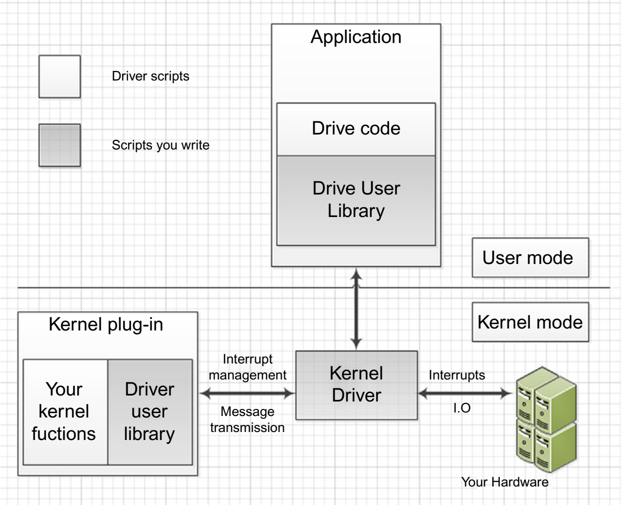
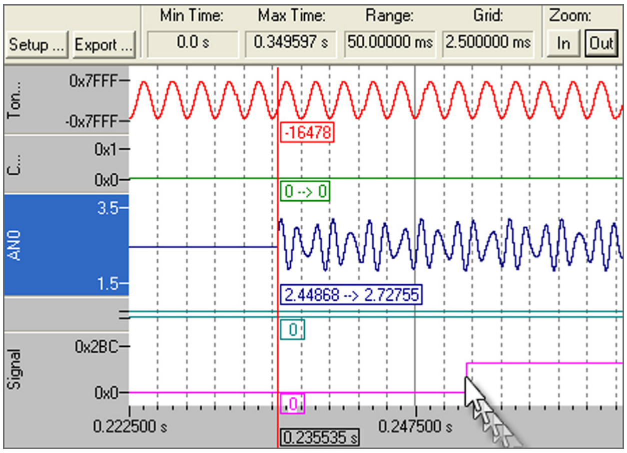


FIGURE 9.1 Architecture to access your hardware directly from the application level.

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.



Min Time: 0.0 s
Max Time: 0.349597 s
Range: 50.00000 ms
Grid: 2.500000 ms

FIGURE 9.2 Signals recorded by the logic analyzer are easily configured to accurately measure signal changes and delta information, and will even allow you to zoom into the area at any point where a signal changed.

- Free tools are available that are open-source Printed Circuit Board (PCB) design tools, which include electronic design automation (EDA). These tools allow hackers to dive deep into the game without bringing a ton of years of electrical engineering to the table. Schematic captures are done interactively with an editor tool and allow one to gain insight on arrays and other miniscule passive components.

The magnificence of hardware hacking, similar to engineering design, is that rarely is there only one correct process or solution. The author's personal hardware hacking methodology consists of the following subsystems:

1. *Gather information:* Hardware hacking, much like any technology, is about gathering pertinent information from an assortment of resources. The answers include product specifications, design documents, marketing data, forums or blogs, and of course, social network sites. Social engineering techniques can be used to manipulate a human victim into divulging applicable information. Many will simply call a vendor's sales or technical engineer directly and invoke interest in a product, and will ask open-ended questions to obtain as much information as the respondent is willing to divulge.
2. *Hardware stripping*: This consists of obtaining the hardware and disassembling it to gather evidence regarding system functionality, design practices, and potential attack areas to target. The primary goal of tearing hardware down is to gain access to the circuit board, which will then allow a hacker to identify high-level subsystems, component types, and values, and in some cases, locate any antitampering mechanisms that would specifically impede physical attack or tampering. Clearly, having direct access to the circuitry allows an attacker to modify, remove, or add components.
3. *Assess external accessibility*: Any product interface that is made accessible to the outside world is an avenue of attack. Programming, debugging, or admin interfaces are of extreme interest, as it allows a hacker direct access to control the device with the same authority as a tech or engineer.
4. *Reverse engineering*: By extracting program code or data and disassembling the contents, a hacker will be able to obtain full insight into the product operation and functionality

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

and potentially modify, recompile, and insert the code back into the product in order to bypass security mechanisms or inject malicious behavior.

The prolific adoption of embedded systems has led to a blurring between hardware and software. Software hackers can now use their skills, tools, and techniques in an embedded environment against firmware without having to grasp hardware-specific paradigms.

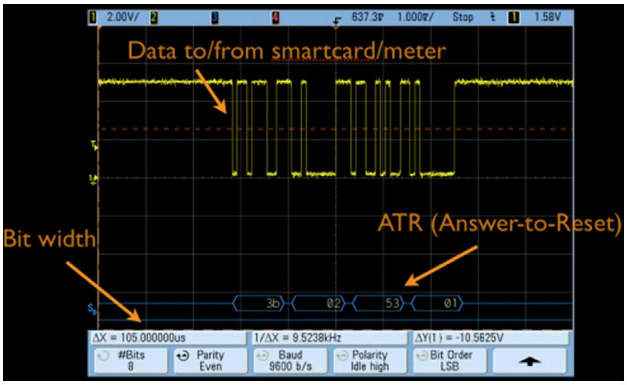
The best way to close the gap between hardware and software hacking is to allow them to work together in order to achieve the desired results. The leading example will enlighten the reader as to why electronic devices used in security or financial applications cannot and should not be fully trusted without thorough analysis and stress testing.

Example

Many large cities have installed digital parking meters throughout the streets, and claim they are secure and tamper proof. While a hacker has many opportunities to attack a metering device, this example focuses on the easily accessible, external smartcard interface. By placing an uninhabited shim between the smartcard and meter, the shim was used to gain the requisite signals and the communication was then captured using an oscilloscope. (It’s good to have friends with cool toys). The serial decoding function of the oscilloscope, displayed in Figure 9.3, points out the actual data bytes that were transmitted from the meter, then to the card, and finally received by the meter from the card.

Patch Management and Policies

Does anyone receive auto-generated email alerts that are excessive, false positives? Not only can it be impossible to examine all of the information, but to assert whether or not the information is truly malicious is another tedious task. Many times this author has ignored countless emails when too many false positives have occurred, which could have been a warning of potential issues. Anytime an environment changes, individuals should be attentive to editing the notifications of the environment. An example would be when


1 2.00V/ 2 3 4 637.3ᴦ 1.000ᴦ/ Stop 1 1.58V
Data to/from smartcard/meter
Bit width
ATR (Answer-to-Reset)
3b
02
53
01

ΔX = 105.000000us
1/ΔX = 9.5238kHz
ΔY(1) = -10.5625V
#Bits 8
Parity Even
Baud 9600 b/s
Polarity Idle high
Bit Order LSB

FIGURE 9.3 Oscillator output displaying the transmission between the smartcard and meter.

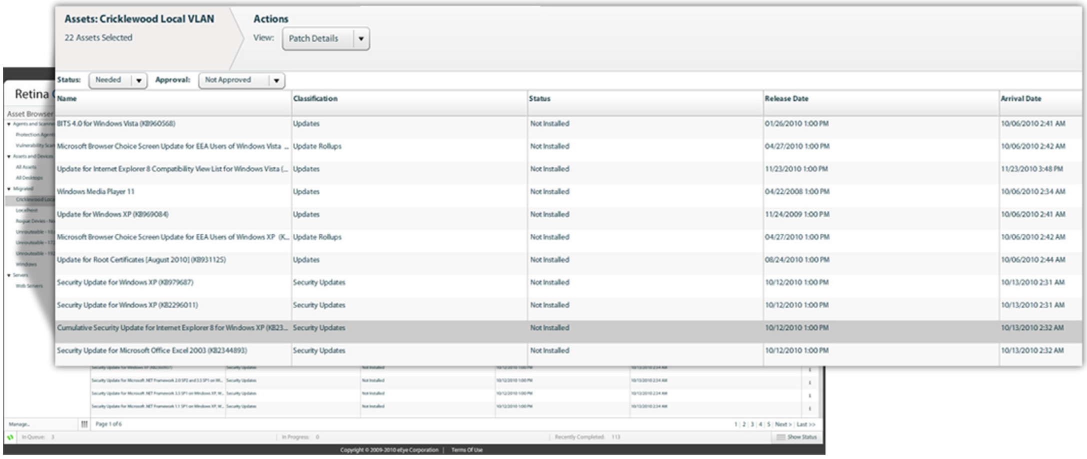
Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

maintenance will be performed where five servers will be restarted multiple times for patches. The alert should be paused for these five servers in an effort to not trigger false alerts where the rest of the team is not aware of the maintenance. If the team is aware of the maintenance, this is a prime example of a false alert that is overlooked, and think through this example happening 10 times a day. Hardly anyone will pay attention to the alerts if 99.99 percent of them are false positives.

Implementing consistent, updated patches may be cost prohibitive for a company, especially for a mission-critical environment. It is necessary to maintain the integrity of an environment and the data by applying both operating system and application security patches and updates. The security team or IT manager needs to ascertain a criterion for procedures as well as an established time frame to apply patches. Windows patches may alter program functionality and capability so severely that users are unable to effectively perform their job function. For instance, some Web applications were not compatible with Internet Explorer version 9, and if updates are set to automatic, troubleshooting this issue could be quite time consuming. Unless patches have been tested in a testing environment, and were successful, there should not be any patches released to the user community. There are patch management packages that offer automation, of course, after testing has proved to be successful. Figure 9.4 depicts an example of a patch management program. Patch names are shown in the left-hand column, the next column classifies the patch, then displays whether or not the patch was installed, and shows the release date along with the arrival date.

Package management systems are charged with the task of organizing all of the packages installed on a particular system. The characteristics of architectural tasks are shown in the following checklist: An Agenda for Action for Implementing Package Architectural Tasks.



Assets: Cricklewood Local VLAN

22 Assets Selected

Actions

View: Patch Details

Status: Needed

Approval: Not Approved

Name	Classification	Status	Release Date	Arrival Date
BITS 4.0 for Windows Vista (KB960568)	Updates	Not Installed	01/26/2010 1:00 PM	10/06/2010 2:41 AM
Microsoft Browser Choice Screen Update for EEA Users of Windows Vista ...	Update Rollups	Not Installed	04/27/2010 1:00 PM	10/06/2010 2:42 AM
Update for Internet Explorer 8 Compatibility View List for Windows Vista (...	Updates	Not Installed	11/23/2010 1:00 PM	11/23/2010 3:48 PM
Windows Media Player 11	Updates	Not Installed	04/22/2008 1:00 PM	10/06/2010 2:34 AM
Update for Windows XP (KB969084)	Updates	Not Installed	11/24/2009 1:00 PM	10/06/2010 2:41 AM
Microsoft Browser Choice Screen Update for EEA Users of Windows XP (K...	Update Rollups	Not Installed	04/27/2010 1:00 PM	10/06/2010 2:42 AM
Update for Root Certificates [August 2010] (KB931125)	Updates	Not Installed	08/24/2010 1:00 PM	10/06/2010 2:44 AM
Security Update for Windows XP (KB979687)	Security Updates	Not Installed	10/12/2010 1:00 PM	10/13/2010 2:31 AM
Security Update for Windows XP (KB2296011)	Security Updates	Not Installed	10/12/2010 1:00 PM	10/13/2010 2:31 AM
Cumulative Security Update for Internet Explorer 8 for Windows XP (KB23...	Security Updates	Not Installed	10/12/2010 1:00 PM	10/13/2010 2:32 AM
Security Update for Microsoft Office Excel 2003 (KB2344893)	Security Updates	Not Installed	10/12/2010 1:00 PM	10/13/2010 2:32 AM

FIGURE 9.4 Patch management software is a helpful tool to track patches and whether or not the patch has been applied to a client.

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

AN AGENDA FOR ACTION FOR IMPLEMENTING PACKAGE ARCHITECTURAL TASKS

Please see the following package architectural characteristics tasks (check all tasks completed):

_____**1.** Manage dependencies to ensure a package is installed with all packages required.
_____**2.** Group packages related to utility.
_____**3.** Upgrade software to latest (tested) versions from a file repository.
_____**4.** Apply file records to manage encapsulated files.
_____**5.** Verify digital signatures upon substantiation of the source packages.
_____**6.** Corroborate file checksums to confirm authentic, comprehensive packages.

IT admins may install and maintain software-utilizing instruments other than package management software. Dependencies will need to be managed, and additional changes may have to be assimilated into the package manager. This does not seem like a very efficient way to some, although having control of source code and the ability to manipulate code may be an attractive advantage. In addition to the manual process of installing patches, license codes may need to be manually activated. When dealing with large environments, can you fathom typing in an activation code thousands of times? Not only is this counterproductive, but it is severely inefficient as noted in Figure 9.5.

Each hardware and software vendor may have differing frequencies for their approach to patch releases. Microsoft has "Patch Tuesday" which occurs the second Tuesday of a month. When Windows updates are set to Automatic, a computer will apply patches as

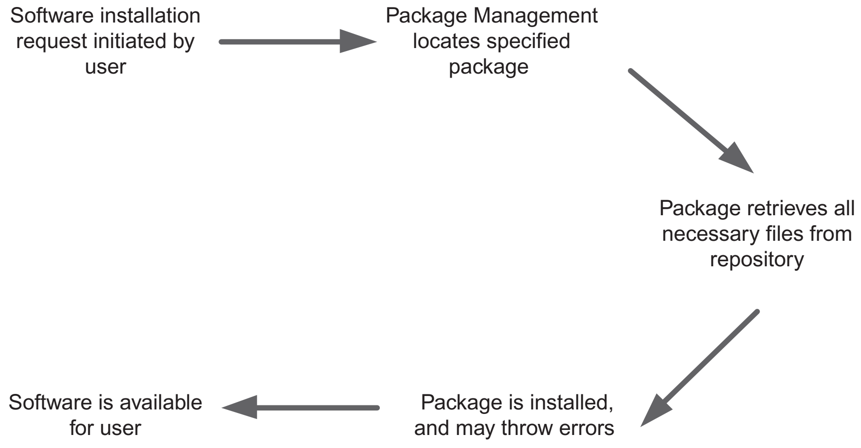

Software installation request initiated by user
Package Management locates specified package
Package retrieves all necessary files from repository
Package is installed, and may throw errors
Software is available for user

FIGURE 9.5 Cycle of a patch management software installation.

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

they're released. These patches may not be tested in an environment, hence the importance of setting updates to manual and having a patch management system. A good practice is to release patches once a month, and to release them roughly a week after the vendor has published the patch. Network hardware patches may not need to be applied, depending on the environment and whether or not the patch will compromise the function of the equipment. Additionally, patches may alter the command set or configuration, so be sure to back up your configuration prior to applying any patch or firmware update.

2. BASIC COUNTERMEASURES

With only 30 to 40 percent of firewall rules in use, security vulnerabilities arise due to misconfigurations. An organization may expose its network to access for which there is no business purpose.

Security Controls and Firewalls

At times, it is not an issue of data sneaking past network controls, but misconfiguration and reluctance to fix issues fearing that the business may be interrupted as changes are implemented. When a team identifies all users' network access, they are able to shape and control access based off rights and proper use. Risk is reduced by blocking unnecessary access paths prior to a security incident occurring. When a consultant is brought into a firm and shows the IT director all the paths, there are holes in the network that could be used for unauthorized access; heads roll, and a plan is soon in place to rectify the holes. Other firms are relatively weak when it comes to monitoring the data right in front of them. While many firms have the appropriate technologies, policies and awareness programs need to be in place for users and their resources. The level of awareness also needs to be known in unmanaged IP devices due to the number of vulnerabilities only increasing over time.

There are many options out there when considering a firewall for your environment. A great deal of firewalls also include other security features: unified threat management (UTM), data loss prevention (DLP), content filtering, intrusion detection and prevention services (IPS), and vulnerability management. A firewall is such a critical component of your infrastructure, and fault tolerance should not be considered optional. A network should be designed so that it is resilient enough to handle the failure of a single firewall. Most concerns with UTM are the amount of processors eaten up by the jobs being performed. With large organizations, you may find you're better off with specialty devices fulfilling each of the security functions covered by UTM. Conversely, UTMs are a great benefit for smaller companies with lower network traffic, especially where costs are concerned when selecting a bundled option.

There is a huge amount of virtual networks out there, both at company office sites and at data center facilities. Virtual firewalls are a way to maximize your security budget by consolidating multiple logical firewalls onto a single platform. Each virtual firewall has its own rules, interfaces, and configuration options that are completely independent from

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

other virtual firewalls running in other infrastructure platforms, but in the same environment. Having this feature also adds the element that a configuration mistake will not only affect performance, but may block all traffic getting to and from the affected segment.

Whether the firewall is hardware or software based, the objective is to control whether or not traffic should be allowed in or out based on a predetermined set of rules. Imagine a security analyst parsing through hundreds pages of logs, where this would only account for 10 to 30 minutes of traffic and determining whether or not rule sets need to be altered.

Case in point: Also envision an issue arising where a complaint comes in from your company's Internet provider stating that your IP address raised a red flag and downloads of copyrighted material were performed. This Internet provider can even state the name of the movie that was downloaded. Other than the Internet provider expecting a response back describing the steps that will be taken to prevent subscriptions from downloading illegal content, internal management at this company expects actions to be taken as well. This is when a security admin will go in and parse through logs searching for the type of file that was downloaded, and if this was not already blocked it will need to be. Bit torrents may need to be blocked. However, depending on the type of work a company performs, there are many legal and necessary uses of bit torrents.

Application Security

An increasing number of organizations are questioning whether they should put a Web application firewall in front of an application, or if the code should just be fixed. Entire teams have committed to securing an application. Consultants travel all over to perform a deep dive of an application environment and suggest measures to correct loopholes. If the strategy shifted toward incorporating applications coupled with Web application firewalls, the company would be more productive integrating this plan as part of its broader application security architectures. Whether Structured Query Language (SQL) attacks or cross-site scripting was the vulnerability, a financial institution would still need about two years to patch 99 percent of the flaws in its applications. By this time, several revisions of the application will have been released, sending teams in downward spirals chasing their tails.

If you ask your customers or colleagues, there is not much collaboration between the security and development teams in an organization. The worst part is that developers are not usually motivated to address secure application development unless they are forced to in the midst of a security incident or to prove compliance initiatives. Developers are sometimes reviewed based on how much software they can build and release on time, and no one holds them accountable for the security portion. The application security challenge has become so difficult to address through development that an alternative plan relies on integrating defensive technologies like Web app firewalls, database audit and protection (DAP), and XML gateways into the infrastructure. Using Web app firewalls in conjunction with coding frameworks fits nicely into filling security functions.

Is it faster, cheaper, and more effective to use a device to shield an application from a security flaw? It may be, but meanwhile hacking strategies are also becoming more accessible, faster, free, and more attractive. Web application firewalls are an appliance, or server, that can monitor and block traffic both to and from the applications. They are

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

common in companies such as credit-card payment firms, which have frequent code reviews. You cannot throw a piece of hardware in front of all applications and expect it to solve all your problems because it is a good idea to build your applications securely from the start.

Hardening and Minimization

The practice of safeguarding systems is to reduce the plane of exposure, also referred to as hardening. An environment where a multitude of cross-functional work is performed can increase the scale of the vulnerability surface since that plane grows larger based on the scope of work. A security engineer can reduce available trajectories of incidents by removing unnecessary software that is not related to business use, deleting usernames or logins for employees or contractors who are no longer at the firm, and also by disabling or removing unnecessary services.

Linux has so many powerful tools where a patch can be applied to the kernel and will close open network ports, integrate intrusion detection, and also assimilate intrusion prevention. While this may work for a smaller firm, the author does not recommend this solution for a robust, large environment. Exec Shield is an undertaking Red Hat began in 2002, with the goal of condensing the probability of worms or other automated remote breaches on Linux systems. After this was released, a patch was necessary that emulated a never execute (NX) bit for a CPU that lacks a native NX implementation in the hardware. This NX bit is a tool used in CPUs to isolate sections of memory that are used by either the storage of processor instructions, or code, or for storage of data. Intel and AMD now also use this architecture; however, Intel identifies this as execute disable (XD), and AMD appointed the name enhanced virus protection. An operating system with the capability to emulate and take advantage of a NX bit may prevent the heap memory and stack from being executable, and may also counteract executable memory from being writable. This facilitates the prevention of particular buffer overflow exploits from prospering, predominantly those that inject and execute code, for example, Sasser and Blaster worms. Such attacks are dependent on some portion of the memory, typically the stack, to be both executable and writable, and if it is not the stack fails.

In the realm of Wi-Fi, companies must implement tight network security controls. Device authentication is another layer of security that would not allow proximity hacking. For example, a car next door is parked in a parking lot and can easily hack onto a firm's network. Guest wireless is a common component to segregate guests off the company's network. With that being said, corporate users might be tempted to switch over to the public, guest network where there are fewer or no controls. This is where leakage may occur. Best practice would be to set up a guest network that issues only temporary credentials to allow connections. This will deter any employees from accessing and utilizing an unsecure connection, and also will not allow former guests or employees' access.

In an ideal world, all traffic would be monitored, but when a company does a cost/benefit analysis, it may seem excessive to do so. Directors make a judgment call based on the threat analysis to ascertain whether it is worth putting these controls into certain segments of the network. It is a terrible practice to have everyone on the same network, but unfortunately that is what most companies do. Whether money is not abundant enough to

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

segment a network, or a security team is not in place to implement policies and maintain them, this is prevalent in most small and medium-sized businesses.

The best approach would be to have anomaly detection that baselines the network traffic and assesses patterns, identifying the anomalies. For the determined attacker, you need to be prepared on the host; so, you need to have it tightly secured where users do not have admin rights. Having a good anti-virus and anti-malware software platform in place is mandatory, too. Depending on the business purpose, classifying data and ultimately segregating that data is also key. The only way to access that data would be through a secured connection through Citrix or some other key/fingerprint mechanism.

In programming, minimization is the method of eradicating all unnecessary character from source code, keeping its functionality. Unnecessary characters may include comments, white space characters, new line characters, comments, and occasionally block delimiters, which are used to enhance comprehension to the code but are not required for that code to execute. In computing machine learning, a generalized model must be selected from a finite data set, with the consequent challenge of overlifting. The model may become too strongly modified to the particularities of the training set and oversimplifying new data. By balancing complexity to institute security against success to seamlessly provide data to groups across the entire firm, one can master risk minimization.

3. SUMMARY

This chapter focused on how the objective of systems security is to improve protection of information system resources. All organizational systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a systems security plan.

The purpose of the systems security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The systems security plan also delineates the responsibilities and expected behavior of all individuals who access the system. The systems security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners and the system owner. Additional information may be included in the basic plan, and the structure and format should be organized according to organizational needs.

In order for the plans to adequately reflect the protection of the resources, a senior management official must authorize a system to operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the systems security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by the assessment report and the plan of actions and milestones. In addition, a periodic review of controls should also contribute to future authorizations. Re-authorization should occur whenever there is a significant change in processing, but at least every three years.

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

Finally, let's move on to the real interactive part of this chapter: review questions/exercises, hands-on projects, case projects, and optional team case project. The answers and/or solutions by chapter can be found in the Online Instructor's Solutions Manual.

CHAPTER REVIEW QUESTIONS/EXERCISES

True/False

1. True or False? Since the inception of technology, data security revolves around cryptography.
2. True or False? Cipher text and secret keys are transported over the network and can be harvested for analysis, and furthermore to impersonate a source or, worst case, cause a service denial.
3. True or False? Network security deals with the insecure transport of data.
4. True or False? Implementing inconsistent, updated patches may be cost prohibitive for a company, especially for a mission-critical environment.
5. True or False? With only 30 to 40% of firewall rules in use, security vulnerabilities arise due to misconfigurations.

Multiple Choice

1. At times, it is not an issue of data sneaking past network controls, but __________ and reluctance to fix issues fearing that the business may be interrupted as changes are implemented.
   - **A.** qualitative analysis
   - **B.** vulnerabilities
   - **C.** data storage
   - **D.** misconfiguration
   - **E.** DHS
2. There are many options out there when considering a ____________for your environment.
   - **A.** firewall
   - **B.** risk assessment
   - **C.** scale
   - **D.** subcomponents
   - **E.** bait
3. There are an increasing number of organizations questioning whether they should put a (n) ______________ in front of an application, or if the code should just be fixed.
   - **A.** organizations
   - **B.** fabric
   - **C.** psychological
   - **D.** Web application firewall
   - **E.** security

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.

4. The practice of safeguarding systems is to reduce the plane of exposure, also referred to as:
  A. cabinet-level state office
  B. nonsubtle
  C. hardening
  D. SAN protocol
  E. taps

5. The purpose of the ______________ is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements?
  A. systems security plan
  B. consumer privacy protection
  C. IP storage access
  D. vulnerability
  E. unusable

EXERCISE

Problem

If continuous monitoring does not replace security authorization, why is it important?

Hands-On Projects

Project

Who should be involved in continuous monitoring activities?

Case Projects

Problem

What role does automation play in continuous monitoring?

Optional Team Case Project

Problem

What security controls should be subject to continuous monitoring?

Copyright © 2013. Elsevier Science & Technology Books. All rights reserved.

Vacca, J. R. (2013). Cyber security and it infrastructure protection. Elsevier Science & Technology Books.
Created from think on 2025-10-11 05:43:47.