

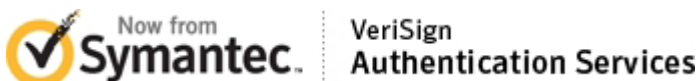
Realtime
publishers

The Shortcut Guide[™] To



**Business
Security Measures
Using SSL**

sponsored by



Dan Sullivan

Chapter 3: Developing a High-Impact Security Management Strategy.....	31
Review of Business Processes and Workflows.....	32
Data in Motion: Identifying Unencrypted Communications	34
Movement Within Secured Network Segments.....	34
Movement Across Enterprise Networks.....	35
Movement Outside of the Enterprise Network.....	35
Data at Rest: Identify Servers Hosting Critical Applications.....	37
Access to Information: Managing Identities and Authorizations	37
Review of Technical Infrastructure	38
Network Security Measures.....	38
Perimeter Device Configuration.....	39
Network Monitoring.....	39
Reporting and Alert Systems	39
Server and Workstation Security Measures	40
Hardening OSs.....	40
Patching	41
Application Security Measures	42
Access Controls.....	42
Security Testing.....	44
Hardening Application Components	45
Security Policies and Governing Procedures.....	45
Summary	47

Copyright Statement

© 2009 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers or its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

This sponsored eBook is valid until July 12, 2012.

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. VeriSign, VeriSign Trust and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. Other names may be trademarks of their respective owners.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library for IT Professionals. All leading technology eBooks and guides from Realtime Publishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 3: Developing a High-Impact Security Management Strategy

Effective information security requires a combination of technical and organizational controls; however, running down a generic checklist is rarely sufficient. Instead, a high-impact security management strategy is driven by the particular needs of a business, and these needs span the breadth of business and technical operations within an organization. For example, consider some of the questions one should pose when developing a security strategy:

- What business processes and workflows are vulnerable to attack?
- If a particular server were compromised, what would be the impact on day-to-day operations to users or customers?
- How can we ensure that our networked applications communicate only with trusted, verified partner applications?
- Can exchange of digital documents be as secure, trustworthy, and enforceable as the exchange of paper documents?
- How can we ensure that confidential information can be exchanged over email and online with reasonable assurance that it won't be intercepted and disclosed to an unauthorized party?

The solution to address the answers to these questions will entail a combination of technical measures, such as hardening servers and deploying SSL certificates for secure communications and authentication, as well as organizational measures, such as developing and enforcing security policies, auditing and monitoring network activities, and providing security awareness training. In Chapters 1 and 2, we examined security threats, technical vulnerabilities, and organizational weaknesses that can directly impact the overall security posture of an organization. In this chapter, we build on those discussions and describe a framework for creating a high-impact security strategy. This task entails a number of steps that are divided into three broad categories:

- Review of business processes and workflows
- Review of technical infrastructure
- Definition of security policies and procedures

Each of these steps addresses both technical and organizational aspects of security, which are tightly coupled. We will not have effective security over the long term without appropriate attention to both.

Review of Business Processes and Workflows

Business processes range from the relatively simple, such as processing time cards, to complex multi-organization operations, such as order processing that entails just-in-time delivery. The flow of information is common to virtually all business processes and information security practices have to take into account those workflows.

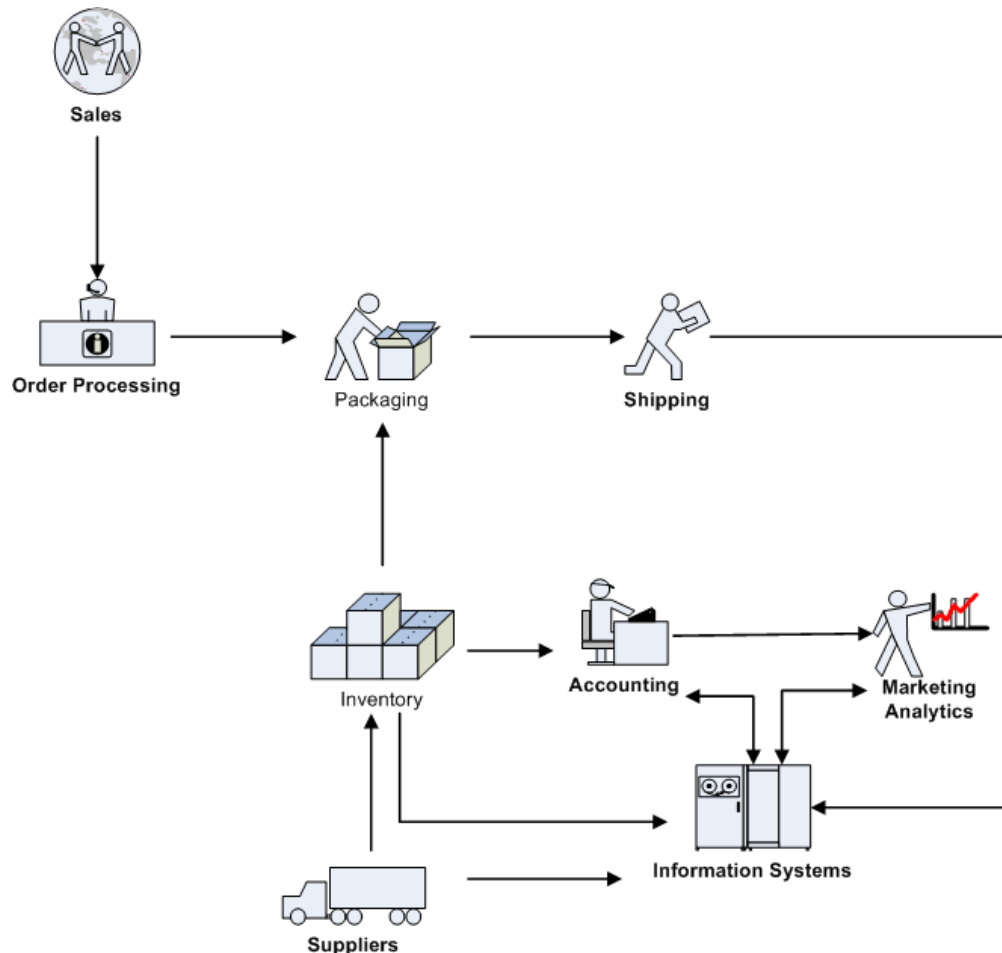


Figure 3.1: Information systems and the flow of information are fundamental aspects of virtually any business process. Securing these information flows begins with understanding the details of the flow and identifying risks to the information.

It is not sufficient to simply protect information at one point in a business flow because, like a chain, a business process is only as secure as its weakest link. For example, a retailer might lock down a database so securely that the time and effort required to break in and steal credit card data is not worth it. However, if credit card data is then sent from a point of sales system to the database using a wireless network encrypted with the weak WEP protocol, attackers will simply target that point in the business process. When we think of protecting information, we need to think in terms of the full life cycle of that information. How and where is it created? How is it transmitted? Where is it stored? How is it backed up and archived? If data is deleted from a production system, how long will it remain in backups? How is data protected when it is moved on physical media, such as backup tapes and disks managed by third-party service providers? These types of questions can be addressed by considering three elements of workflows:

- Data in motion
- Data at rest
- Access to information

When we have a solid understanding of these three elements, we can properly design security measures and implement controls to protect business process and information flows.

Data Classification and Security Measures

When considering information flows, remember that not all information is equally valuable or in need of the same levels of protection. A data classification scheme is a means of defining levels of protection appropriate for different types of information. Public data, such as press releases, do not require special controls because the purpose of this type of data is to share information outside the organization. Prior to release, however, a press release with time-sensitive data may be categorized as sensitive or even confidential if its early release could harm the business. A business' trade secrets or private customer financial data should be treated as confidential and provided with appropriate levels of protection when the data is being transmitted and when it is stored on business systems.

Data in Motion: Identifying Unencrypted Communications

Once we have identified core business processes, we can begin to look into the details of how information moves between servers, workstations, mobile devices, point of sale systems, and other kinds of devices. Key questions to consider are:

- Is the data sensitive, private, or confidential and therefore warrant additional attention to protect the privacy and integrity?
- Does the data move through systems or networks that might be vulnerable to attack?

For the purposes of discussion, we will concentrate on sensitive, private, and confidential information; that is, information, which if disclosed or tampered with, could adversely harm the business, its customers, business partners, or other stakeholders. Sensitive information is information that should not be released for general access, but if were made available, would not have serious impacts on the organization. Private and confidential information, in contrast, is information that if accessed in unauthorized ways would have severe impact on the organization. Private information pertains to individuals, such as customers and employees, while confidential information is related to the business itself, such as trade secrets. With regards to where the information flows, there are so many specific possibilities that it makes sense only to categorize the general range of networks and systems in terms of the level of additional security required.

Movement Within Secured Network Segments

One possibility is that information moves only within a controlled network environment that is already hardened (that is, secured beyond normal default configurations to reduce vulnerabilities). For example, suppose information from a transaction processing database is being copied every night to a data warehouse server on the same network segment. Given the high value of the transaction processing system and the data warehouse, we can assume network security staff has configured servers to run the minimal software needed to complete business operations, keeps the servers patched, and uses network firewalls, intrusion prevention systems (IPS), application firewalls, and database activity monitoring systems. In short, this network segment is made as secure as the risk warrants within the constraints of existing technologies and budgets.

Adding a layer of security with the use of encryption would add another level to a defense-in-depth strategy but at a cost. If the data warehouse required large volumes of data to be transferred within a relatively short window of operation, adding time to encrypt and decrypt data moving over a well-secured network could jeopardize finishing the operation in the time allotted while not significantly reducing the remain risks.

Movement Across Enterprise Networks

Next, consider the case of data moving across an enterprise network. In this case, we can imagine data moving outside of highly secured segments to areas of the network designed for performance and ease of use. There are many ways to use and misuse an enterprise network. Acceptable uses can range: mobile users connecting to the network using virtual private networks (VPNs), contractors and business partners accessing business systems related to their work, developers creating and testing new applications, and systems administrators installing new software and experimenting with different configurations. All of these activities can create risks that do not exist in a highly controlled environment. In addition, there may be activities that violate policy but manage to “fly under the radar.” For example:

- Web application developers may deploy a Web server on an extra workstation in the office without following IT procedures
- An analyst may decide it would take IT too long to develop reports for her, so she creates a database and replicates data as needed from production databases
- A team of consultants set up shop in a conference room for a short-term project and install a wireless access point for their convenience

Security professionals might cringe at these examples while business professionals might be more willing to weigh the pros and cons of bypassing the “IT bureaucracy.” Let us just assume that there are times when reasonable professionals will disagree about the merit of such actions. How should we protect information flowing through parts of the network that could harbor vulnerable systems that could be used for data breaches?

Ideally, we could eliminate all unofficial applications, databases, and make-shift servers; but even if we could eliminate all such systems, the same conditions that prompted their introduction in the first place will likely remain. Another tactic, and one that fits in a defense-in-depth strategy, is to encrypt communications on the enterprise network, at least when dealing with confidential and private data. By using SSL-encrypted communications for the most valuable data, we make it much more difficult for unauthorized persons or programs to capture that data in transit.

Movement Outside of the Enterprise Network

Once data leaves the controlled boundaries of the enterprise network, we cannot safely make any assumptions about the security of such external systems or the applications or servers for which the data is destined. In this situation, SSL technologies provide two types of protection: confidential communication and reliable authentication.

Suppose you would like to send confidential information to a business partner over the Internet. If it is a small amount of data, you might use email; for larger amounts, FTP may be the tool of choice. In either case, there is no way to ensure that the message or transfer could not be intercepted and read unless the message is encrypted. SSL is the standard method for doing so. Another concern is ensuring that the message actually reaches the intended party.

Authentication is the process of verifying a party's identity. Usernames and passwords are frequently used when someone wants to employ an application or service, but these authentication mechanisms are of little use when trying to negotiate a transfer between two servers. A better option is to use digital certificates. These are electronic forms of identification that are designed to be virtually tamper-proof. If you receive a digital certificate electronically signed by a trusted third party, you have sound evidence that the sender is who it claims to be. Figure 3.2 shows an example of a certificate with information about the domain of the server for which it was issued, the issuer, that is the trusted SSL certificate vendor, valid dates for the certificate, and cryptographic attributes that are used to detect tampering.

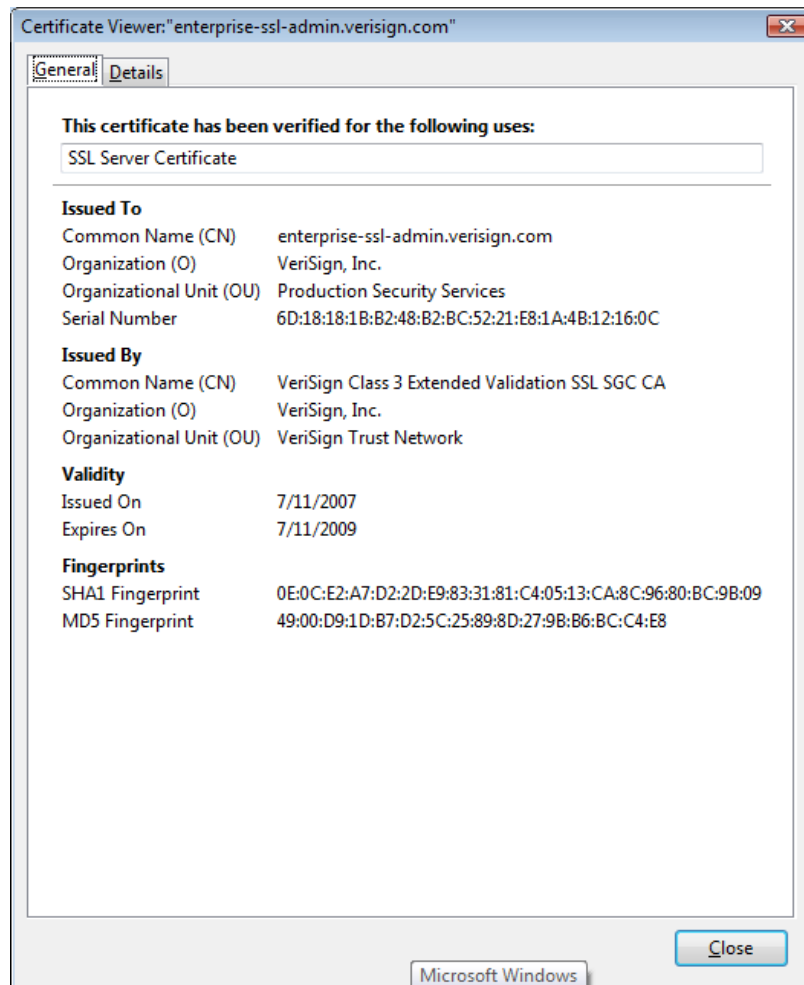


Figure 3.2: An SSL digital certificate is like a digital id card; it is evidence from a trusted third party that the server holding this certificate is actually part of the business it claims to be.

When data moves within highly secured segments of a network and performance considerations outweigh the marginal benefit of another security control, SSL encryption might not be used. However, when data moves outside the enterprise—and for confidential and private data, even within the enterprise network—SSL technologies can provide encryption for confidentiality and digital certificates for authentication purposes.

Data at Rest: Identify Servers Hosting Critical Applications

Another element of a high-impact security strategy is the proper management of servers hosting critical applications. Part of that management process addresses data and part addresses systems issues; here we will focus on data.

Cross-Reference

See the section, *Server and Workstation Security Measures* for more information about systems security.

Business processes and workflows copy, move, and delete data from many parts of the network. During the business process review, it is important to identify servers hosting critical applications and protected data. In the case of highly regulated data, it is important to be able to demonstrate that one knows where private and confidential data is located, how it is stored, and how it is protected. Part of that protection will often include encryption of data when stored persistently and ensuring that servers receiving protected data are properly authenticated, as discussed earlier.

Access to Information: Managing Identities and Authorizations

In addition to reviewing the flow of information and the servers that hold persistent copies of protected data, a high-impact security strategy begins with a review of identities and authorizations. Security technologies, such as SSL encrypted communications and digital certificates, depend on sound business practices that ensure authenticated users are legitimately authorized to view and manipulate information.

The modern workforce is highly dynamic, in both good economic times and during downturns. Employees leave positions to join other firms or move internally, consultants and contractors augment staff during peak demand periods, and businesses form collaborative arrangements with business partners to more efficiently deliver goods and services to their customers. One of the tasks that cannot be fully automated is reviewing user accounts and the privileges they have. This task might sound relatively easy, at least once the responsibility is delegated, but it is often more complicated than it first appears.

There are several ways in which difficulties arise, including:

- Staff may change positions and require some, but not all, of their existing privileges as well as new privileges.
- Companies may use federated identity management, in which each company depends on the other to define the roles of their own employees. This may be difficult to monitor because each business depends on the other.
- Accounts may be shared, sometimes informally, within close working groups.
- Developers and systems administrators may establish common application and database accounts that are shared by pools of users. These accounts may not appear on a standard report of each employee's authorizations.

As these examples demonstrate, tracking identities and authorizations can lead to more complex arrangements than may be apparent at first.

The first step in developing a high-impact security strategy is to understand (1) how data moves through an organization and outside an organization; (2) how data is managed when it is stored; and (3) who has access to that data. As we can follow from this discussion, it sounds easier in theory than it is in practice. Once we have a handle on business process and information flows, it is time to tackle another substantial, but doable, challenge: review the technical infrastructure.

Review of Technical Infrastructure

With a solid understanding of how information flows, we can turn our attention to understanding how the infrastructure that supports those flows can be secured. In particular, we will examine three categories of infrastructure security:

- Network security measures
- Server and workstation security measures
- Application security measures

The goal in examining each of these areas is to identify particular security issues that should be addressed with respect to each of these segments of the IT infrastructure.

Network Security Measures

The overall goal of network security measures is to ensure that the flow of information over the network is authorized and limited to legitimate business purposes. This is a tall order. Some of the technologies that are required include gateways to control traffic in and out of the network, SSL encryption to protect the confidentiality of information flowing through the network, intrusion prevention and monitoring applications to detect unusual patterns in network activity, and vulnerability scanning tools to help identify weaknesses in infrastructure configurations and software. As we drill down deeper into more specific technologies, we can see how various technologies can help protect the network.

Perimeter Device Configuration

Gateways, or firewalls, have improved from relatively simple, stateless packet inspectors to devices that provide deeper and more complex analysis of data flowing over a network. Of course, gateways are still needed to control how data flows in and out of a network, and that starts with controlling which ports are open for use. The emergence of tunneling—the process of using one protocol to carry as its payload traffic in another protocol—is just one example of a data flow that is too complex for simple firewall rules to handle. A perimeter security strategy should consider ways such as these that basic security measures may be circumvented. More advanced gateway devices, such as application firewalls, include software that can analyze data en route to an application and determine whether it is appropriate traffic.

Network Monitoring

IPS may further improve overall network security by analyzing traffic patterns and detecting anomalous activity. When planning on the use of IPS, it helps to understand how they work. IPS can detect anomalous network activity through the use of rules, by comparison to baseline statistical patterns, or both. An advantage of rule-based approaches is that they can be shared across users of an IPS system. For example, an attack using a known vulnerability in an operating system (OS) component may require a particular sequence of actions to initiate, and an IPS could have a rule to detect that pattern. Statistical pattern methods are complementary and can help accommodate the unique activities on a network. For example, it may be perfectly normal for large data transfers to occur between servers during the middle of the night but not in the early morning. If the latter were to occur, it might be an indication of a data breach in progress.

Reporting and Alert Systems

It would be difficult to find a systems administrator or network manager complaining about not enough data or network activity. Security systems, applications, and OSs are profuse generators of logging data. The problem is not lack of data but extracting useful information from that data. Security information management (SIM) systems are tools for collecting, consolidating, and reporting from multiple devices. There are formidable challenges to building SIMs, and we should manage our expectations for these tools.

SIMs are useful today as consolidated reporting tools. Using protocols such as the Simple Network Management Protocol (SNMP), SIMs can collect data from multiple devices and help network administrators review data from across a variety of device types. As the technology advances, more complex analysis may be available, but in some cases, a good solid tool for reporting a diverse set of facts can be still be useful.

Network security at one level entails a combination of perimeter devices, network monitoring, and reporting systems. We have seen how security of data flowing over the network is enhanced with the use of SSL encryption. Next, we will examine the role of server and workstation security measures in strategies for protecting IT infrastructure.

Server and Workstation Security Measures

Servers and workstations are like factories in an industrial society: they are producers of specialized artifacts that depend on each other for inputs and use shared resources for distributing their outputs. Unlike the physical world where it would be difficult to masquerade as a factory, the digital world of servers and workstations do not have the same barriers to fraud. In terms of a high-impact security strategy, a key element is ensuring that servers and workstations can trust each other. For example, when a Web service receives a message requesting a service or piece of data, the server running that Web service needs to be able to trust the requestor if private or confidential information is being requested. SSL digital certificates are the standard means for establishing this trust. In addition to trusting that servers and workstations are what they appear to be, it is important to implement practices that protect the integrity of these devices.

Hardening OSs

A quick scan of a vulnerability database, such as the National Vulnerability Database (<http://nvd.nist.gov/>), will show many different types of vulnerabilities affecting a variety of components, including:

- Web servers
- FTP servers
- Media players
- Network management software
- Process monitoring applications

Some of the problems involve technical issues, such as buffer overflows, and the allowance of remote execution of code and privilege escalation. If systems administrators do not have enough to keep themselves awake at night, a visit to a vulnerability database will solve that problem. Modern OSs are all complex, multi-faceted applications and they have vulnerabilities. One of the best ways to mitigate the risks associated with these vulnerabilities is to harden the OS—that is, minimize the number of services running and the types of applications available on systems—and properly configure the OS.

A general rule of thumb is if a service is not needed, it should not be running. FTP servers, for example, have seen more than their share of vulnerabilities and exploits. If FTP is not required, do not run it. Similarly, production servers should not have compilers installed unless there is some compelling reason. Code should be developed and compiled on development servers and the binaries then ported to a production server. If an attacker were able to compromise a production server and had access to a compiler, the attacker could conceivably download code, compile it locally, and install it on the server. Of course, an attacker could also compile the code remotely and install it, but the attacker would need a compiler for every different type of system targeted; having access to a local compiler just makes an attacker's life easier.

Resource

For more information about hardening OSs, see the Bastille-Linux Project at <http://bastille-linux.sourceforge.net/> and the benchmark tools at Center for Internet Security at <http://cisecurity.org/bench.html>.

Hardening also requires proper configuration, which includes changing default passwords, not re-using passwords across administrator/root accounts, enforcing a strong password policy, and shutting down unnecessary services and daemons. Hardening an OS should be a standardized procedure. Consistency can help improve overall security and ease administrative overhead. However, there are times where some servers should have additional controls put in place. For example, access to database servers may warrant strong authentication, such as multi-factor controls or a challenge-response system.

Patching

A third element of a server and workstation security strategy is patching. We've already described the extent of vulnerabilities and one method for dealing with them (removing the vulnerable applications through hardening). Not all vulnerable applications can be removed, but many of them can be patched. Patching is a sufficiently complex process that it should be carefully considered and procedures formulated for patching in a high-impact security strategy. Some of the key elements of a sound patching strategy are:

- Procedures for monitoring the availability of patches
- Methods for assessing the importance of a patch and the speed with which it should be applied
- Rankings of different instances of systems that should be patched so that IT support staff can prioritize patching operations
- Procedures for testing and then rolling out patches
- Bypass procedures for fast-tracking emergency patches (this should be done judiciously due to the risk of disrupting production operations when sufficient testing is not undertaken)

Servers and workstations require support from several elements of a security strategy, including the use of digital certificates, OS hardening, and patching to reduce vulnerabilities.

Application Security Measures

The third leg of the infrastructure review triad is application security. For our purposes, the term “application” includes software that ranges from monolithic mainframe applications to individual Web services. As part of a security strategy, businesses should assess application-specific security measures, including:

- Access controls
- Security testing
- Hardening application components

As we shall see, these considerations parallel some of the issues in server and workstation security; however, these tend to address security more from a software engineering perspective than from a systems management point of view.

Access Controls

At the very minimum, application security entails specifying who can use an application and what can they do, or in security parlance, authentication and authorization.

Think of authentication and what comes to mind? Probably common scenarios such as a user logging into an email service or verifying the identity of a business running a Web site likely come to mind by checking an SSL certificate (See Figure 3.3, which is actually displaying an Extended Validation—EV—SSL certificate, a form of digital certificate that requires more extensive verification than conventional SSL certificates).

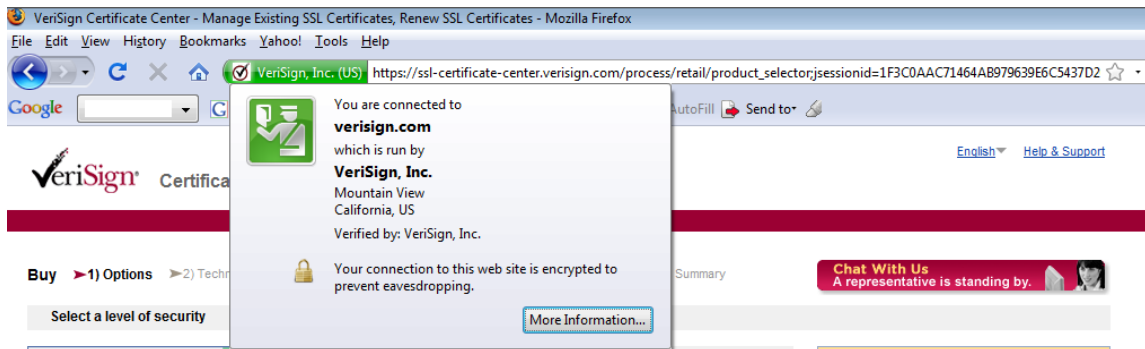


Figure 3.3: When we visit a site, we want to make sure we are dealing with the business we think we are dealing with. In other words, we want to trust the Web site. SSL also supports mutual authentication, which allows the Web site to trust its visitors.

Users trusting a Web site are only half of the authentication process. Business need to verify that business partners, customers, and others who are given access to their applications are who they claim to be. Just as customers want to be sure of the identity of a business behind a Web site before handing over a credit card number, businesses need to be sure of who they are dealing with before handing over data or granting access to services.

This can be done with mutual authentication. For example, a retailer might want suppliers to have access to inventory levels as part of a just-in-time delivery plan. Mutual authentication is in the interest of all parties. The retailer probably does not want competitors poking around its operational databases, and suppliers would not want to lose competitive advantage that access to detailed inventory information can provide.

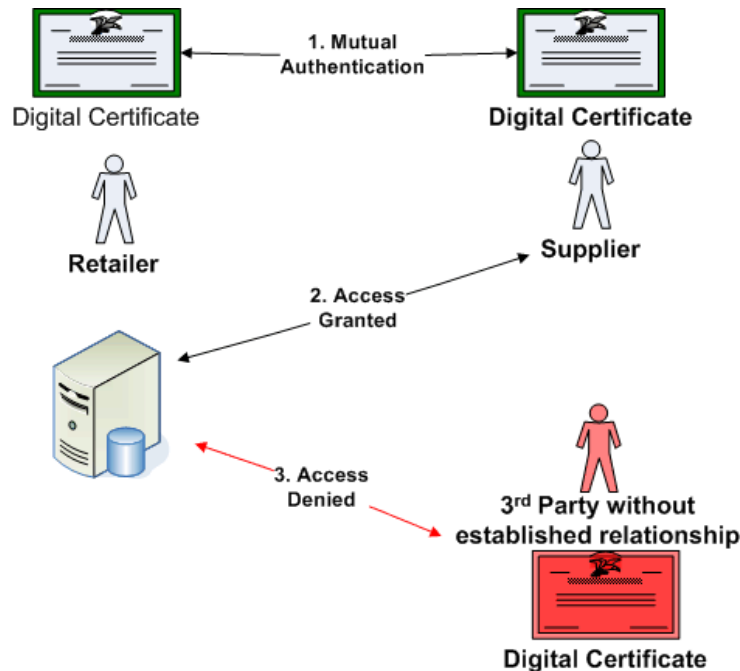


Figure 3.4: Mutual authentication via digital certificates can be used to control access to confidential information and services.

Access controls are based on some level of trust. We trust users not to share their passwords, to change them frequently, and to not reuse them. A business could conceivably just hand out passwords to business partners but that introduces new risks. For example, the business partner might deal with several retailers, each giving out passwords; to keep things manageable, the partner keeps the passwords written down on a sticky note, or worse, recorded in a wiki or other collaboration site. Digital certificates avoid this type of problem. Instead of trusting account users to keep passwords secret, we trust digital certificate providers to use reliable procedures to verify identities and to manage certificate operations, such as revoking certificates when needed.

Security Testing

Security testing is a complex subject but one that can and should be managed in the scope of a broad security strategy. Security testing should be done before a new application is released to production and throughout the life of the application. Initial testing should include tests to ensure:

- Processes run with the least privileges required to function
- Applications fail securely—for example, if an unexpected input is passed to an application, the application should gracefully fail and not suffer a buffer overflow or similar problem that leaves the application in a vulnerable state
- Expose only needed functionality; this reduces the number of ways an attacker can compromise the system and is known as “reducing the attack surface”
- Unusual or unexpected events are logged with sufficient detail to enable administrators and developers to diagnose the problem
- Applications function properly on hardened servers (see the earlier section on Hardening OSs)

Ongoing testing is required for several reasons. First, vulnerabilities in an application or constituent component may be discovered after the application is deployed. Second, during the course of routine patching, a new, unknown vulnerability could be introduced. Third, the configuration states of applications change over time and users may be granted elevated privileges that introduce additional vulnerabilities. Also, applications may be used in new ways, such as providing data to business partners outside the enterprise network, which should prompt thorough testing. Automated testing tools and vulnerability scanners should be used to make this process more efficient than a completely manual operation.

Resource

See the Open Web Application Security Project (OWASP) for more information about best practices in application security testing at http://www.owasp.org/index.php/Main_Page.

Hardening Application Components

The last of the application security measures is hardening applications. As with OS hardening, the goal is to reduce vulnerabilities in an application. Security testing can reveal potential problems with software such as:

- Injection attack vulnerabilities—This can occur if inputs are not properly scrubbed before they are passed to modules or subsystems, such as database query processors; SQL injection attacks are perhaps the most well-known form of such attacks
- Insecure configurations in subsystems such as application servers and database listeners
- Hard-coded username and passwords for database accounts or other service accounts
- Unnecessarily elevated privileges

Many of these vulnerabilities can be corrected by changing code or configuration parameters. In other cases, additional measures, such as the use of application firewalls or database activity monitoring systems, may be warranted.

A review of technical infrastructure can help identify security measures for network security, server and workstation security, and application-specific measures. Not surprisingly, many fundamental security controls, such as the use of SSL for encryption, the use of digital certificates for authentication, and vulnerability scanning play prominent roles in protecting IT infrastructure.

IT environments are highly dynamic. Reviewing business processes, workflows, and IT infrastructure at one point in time is necessary but not sufficient for developing and maintaining adequate security. An ongoing governance process is required as well.

Security Policies and Governing Procedures

Security practices in an organization may begin with best practices established by the security community but will inevitably change to accommodate the particular needs of the organization. Costs and benefits are balanced. Compliance requirements are targeted. Business strategies are accommodated. Even given such dynamic constraints, it is important to formulate policies and governing procedures to avoid *ad hoc* responses to situations and to ensure that lessons learned over time are captured and incorporated into ongoing procedures.

In order to maintain a high-impact security strategy, well-defined policies and procedures should be established covering a number of topics:

- Use of encryption to protect the confidentiality of data at rest and data in motion
- Use of server authentication and mutual authentication for application services; these policies should describe when digital certificates should be used, limits of self-signed digital certificates (that is, digital certificates created by the user of the certificate, not a trusted third party), and the need for mutual authentication in Web services providing private or confidential data
- An overview of patch management procedures, including monitoring the release of patches, testing patches prior to use in production environments, and exceptions for emergency patching
- Processes for hardening OSs and applications to eliminate known vulnerabilities
- Use of vulnerability scanning and reporting tools
- Workstation security practices, including the use of antivirus, anti-spyware, personal firewalls, and disk encryption
- Secure use of mobile devices and limits on the types of data that may be copied to mobile devices
- Security awareness training for staff, contractors, and consultants as well as acceptable use policies clearly describing the types of activities that may be performed on the organization's IT infrastructure
- Auditing and monitoring requirements to maintain compliance with government and industry regulations

Policies addressing these areas and others related to security require maintenance. They have to be modified to accommodate changes in technology, business practices, and business strategy. Governing structures that include both IT and business executives familiar with the breadth of the business environment and current strategy are necessary to ensure that policies and procedures remain useful guides to security practices and not simply documents on a shelf shown to auditors once a year.

Summary

Creating and maintaining a high-impact security strategy begins with understanding business processes and workflow. This process is followed by an analysis of IT infrastructure, particularly networking services, servers and workstations, and applications. The final step is creating policies and governing procedures that shape and maintain a sufficiently secure environment. Throughout this chapter, we have seen recurring reference to fundamental security technologies such as SSL, encryption, and digital certificates as well as core security practices, such as application and OS hardening and vulnerability scanning. This should be no surprise. These technologies and practices are well-established elements of information security best practices that one will see over and over again.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.