What is e-Commerce?

e-Commerce refers to the exchange of goods and services over the Internet. All major retail brands have an online presence, and many brands have no associated bricks and mortar presence. However, e-Commerce also applies to business to business transactions, for example, between manufacturers and suppliers or distributors.

In the online retail space, there are a number of models that retailers can adopt. Traditionally, the Web presence has been kept distinct from the bricks and mortar presence, so transactions were limited to buying online and delivering the goods or services. The online presence is also important for researching a product that a customer can purchase later in the store. Recently, there has been a trend towards multi-channel retail, allowing new models such as purchasing online and picking up in store.

e-Commerce systems are also relevant for the services industry. For example, online banking and brokerage services allow customers to retrieve bank statements online, transfer funds, pay credit card bills, apply for and receive approval for a new mortgage, buy and sell securities, and get financial guidance and information.

Back to top

Security overview

A secure system accomplishes its task with no unintended side effects. Using the analogy of a house to represent the system, you decide to carve out a piece of your front door to give your pets' easy access to the outdoors. However, the hole is too large, giving access to burglars. You have created an unintended implication and therefore, an insecure system.

In the software industry, security has two different perspectives. In the software development community, it describes the security features of a system. Common security features are ensuring passwords that are at least six characters long and encryption of sensitive data. For software consumers, it is protection against attacks rather than specific features of the system. Your house may have the latest alarm system and windows with bars, but if you leave your doors unlocked, despite the number of security features your system has, it is still insecure. Hence, security is not a number of features, but a system process. The weakest link in the chain determines the security of the system. In this article, we focus on possible attack scenarios in an e-Commerce system and provide preventive strategies, including security features, that you can implement.

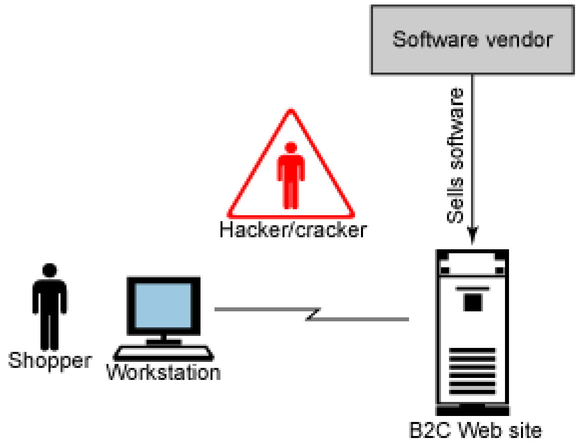
Security has three main concepts: confidentiality, integrity, and availability. Confidentiality allows only authorized parties to read protected information. For example, if the postman reads your mail, this is a breach of your privacy. Integrity ensures data remains as is from the sender to the receiver. If someone added an extra bill to the envelope, which contained your credit card bill, he has violated the integrity of the mail. Availability ensures you have access and are authorized to resources. If the post office destroys your mail or the postman takes one year to deliver your mail, he has impacted the availability of your mail.

Back to top

The players

In a typical e-Commerce experience, a shopper proceeds to a Web site to browse a catalog and make a purchase. This simple activity illustrates the four major players in e-Commerce security. One player is the shopper who uses his browser to locate the site. The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit. As the merchant business is selling goods and services, not building software, he usually purchases most of the software to run his site from third-party software vendors. The software vendor is the last of the three legitimate players. The attacker is the player whose goal is to exploit the other three players for illegitimate gains. Figure 2 illustrates the players in a shopping experience.

Figure 2. The players



The attacker can besiege the players and their resources with various damaging or benign schemes that result in system exploitation. Threats and vulnerabilities are classified under confidentiality, integrity, and availability. A threat is a possible attack against a system. It does not necessarily mean that the system is vulnerable to the attack. An attacker can threaten to throw eggs against your brick house, but it is harmless. A vulnerability is a weakness in the system, but it is not necessarily known by the attacker. For example, only you know that you have left your front door unlocked. Vulnerabilities exist at entry and exit points in the system. In a house, the vulnerable points are the doors and windows. When the burglar threatens to break into your house and finds the vulnerability of the unlocked door, he is exploiting the assets in the house.

Back to top

Security features

While security features do not guarantee a secure system, they are necessary to build a secure system. Security features have four categories:

- Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.
- Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.

Back to top

The criminal incentive

Attacks against e-Commerce Web sites are so alarming, they follow right after violent crimes in the news. Practically every month, there is an announcement of an attack on a major Web site where sensitive information is obtained. Why is e-Commerce vulnerable? Is e-Commerce software more insecure compared to other software? Did the number of criminals in the world increase? The developers producing e-Commerce software are pulled from the same pool of developers as those who work on other software. In fact, this relatively new field is an attraction for top talent. Therefore, the quality of software being produced is relatively the same compared to other products. The criminal population did not undergo a sudden explosion, but the incentives of an e-Commerce exploit are a bargain compared to other illegal opportunities.

Compared to robbing a bank, the tools necessary to perform an attack on the Internet is fairly cheap. The criminal only needs access to a computer and an Internet connection. On the other hand, a bank robbery may require firearms, a getaway car, and tools to crack a safe, but these may still not be enough. Hence, the low cost of entry to an e-Commerce site attracts the broader criminal population.

The payoff of a successful attack is unimaginable. If you were to take a penny from every account at any one of the major banks, it easily amounts to several million dollars. The local bank robber optimistically expects a windfall in the tens of thousands of dollars. Bank branches do not keep a lot of cash on hand. The majority is represented in bits and bytes sitting on a hard disk or zipping through a network.

While the local bank robber is restricted to the several branches in his region, his online counterpart can choose from the thousands of banks with an online operation. The online bank robber can rob a bank in another country, taking advantage of non-existent extradition rules between the country where the attack originated, and the country where the attack is destined.

An attack on a bank branch requires careful planning and precautions to ensure that the criminal does not leave a trail. He ensures the getaway car is not easily identifiable after the robbery. He cannot leave fingerprints or have his face captured on the surveillance cameras. If he performs his actions on the Internet, he can easily make himself anonymous and the source of the attack untraceable.

The local bank robber obtains detailed building maps and city maps of his target. His online counterpart easily and freely finds information on hacking and cracking. He uses different sets of tools and techniques everyday to target an online bank.

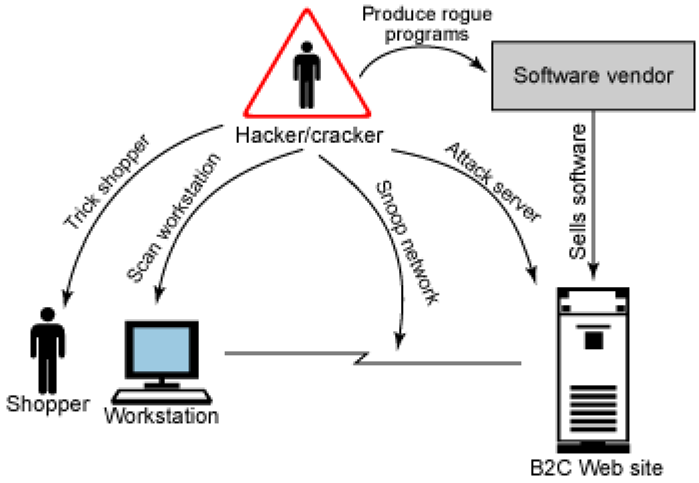
Back to top

Points the attacker can target

As mentioned, the vulnerability of a system exists at the entry and exit points within the system. Figure 3 shows an e-Commerce system with several points that the attacker can target:

- Shopper
- Shopper' computer
- Network connection between shopper and Web site's server
- Web site's server
- Software vendor

Figure 3. Points the attacker can target



These target points and their exploits are explored later in this article.

Back to top

Attacks

This section describes potential security attack methods from an attacker or hacker.

Tricking the shopper

Some of the easiest and most profitable attacks are based on tricking the shopper, also known as social engineering techniques. These attacks involve surveillance of the shopper's behavior, gathering information to use against the shopper. For example, a mother's maiden name is a common challenge question used by numerous sites. If one of these sites is tricked into giving away a password once the challenge question is provided, then not only has this site been compromised, but it is also likely that the shopper used the same logon ID and password on other sites.

A common scenario is that the attacker calls the shopper, pretending to be a representative from a site visited, and extracts information. The attacker then calls a customer service representative at the site, posing as the shopper and providing personal information. The attacker then asks for the password to be reset to a specific value.

Another common form of social engineering attacks are phishing schemes. Typo pirates play on the names of famous sites to collect authentication and registration information. For example, http://www.ibm.com/shop is registered by the attacker as www.ibn.com/shop. A shopper mistypes and enters the illegitimate site and provides confidential information. Alternatively, the attacker sends emails spoofed to look like they came from legitimate sites. The link inside the email maps to a rogue site that collects the information.

Snooping the shopper's computer

Millions of computers are added to the Internet every month. Most users' knowledge of security vulnerabilities of their systems is vague at best. Additionally, software and hardware vendors, in their quest to ensure that their products are easy to install, will ship products with security features disabled. In most cases, enabling security features requires a non-technical user to read manuals written for the technologist. The confused user does not attempt to enable the security features. This creates a treasure trove for attackers.

A popular technique for gaining entry into the shopper's system is to use a tool, such as SATAN, to perform port scans on a computer that detect entry points into the machine. Based on the opened ports found, the attacker can use various techniques to gain entry into the user's system. Upon entry, they scan your file system for personal information, such as passwords.

While software and hardware security solutions available protect the public's systems, they are not silver bullets. A user that purchases firewall software to protect his computer may find there are conflicts with other software on his system. To resolve the conflict, the user disables enough capabilities to render the firewall software useless.

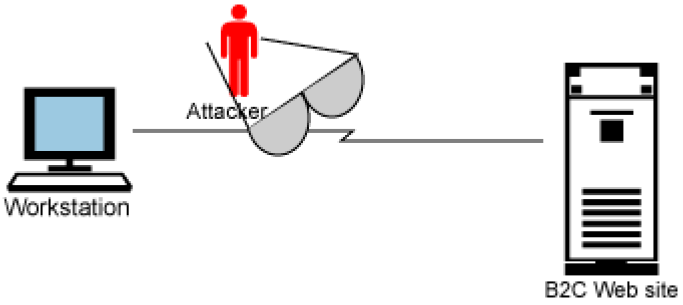
Sniffing the network

In this scheme, the attacker monitors the data between the shopper's computer and the server. He collects data about the shopper or steals personal information, such as credit card numbers.

There are points in the network where this attack is more practical than others. If the attacker sits in the middle of the network, then within the scope of the Internet, this attack becomes impractical. A request from the client to the server computer is broken up into small pieces known as packets as it leaves the client's computer and is reconstructed at the server. The packets of a request is sent through different routes. The attacker cannot access all the packets of a request and cannot decipher what message was sent.

Take the example of a shopper in Toronto purchasing goods from a store in Los Angeles. Some packets for a request are routed through New York, where others are routed through Chicago. A more practical location for this attack is near the shopper's computer or the server. Wireless hubs make attacks on the shopper's computer network the better choice because most wireless hubs are shipped with security features disabled. This allows an attacker to easily scan unencrypted traffic from the user's computer.

Figure 4. Attacker sniffing the network between client and server



Guessing passwords

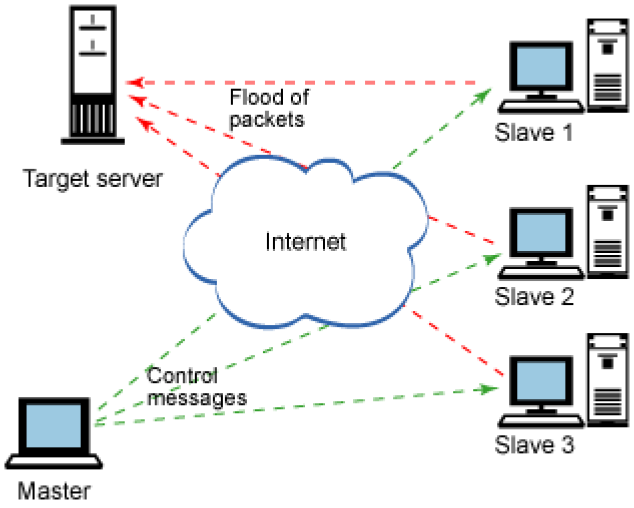
Another common attack is to guess a user's password. This style of attack is manual or automated. Manual attacks are laborious, and only successful if the attacker knows something about the shopper. For example, if the shopper uses their child's name as the password. Automated attacks have a higher likelihood of success, because the probability of guessing a user ID/password becomes more significant as the number of tries increases. Tools exist that use all the words in the dictionary to test user ID/password combinations, or that attack popular user ID/password combinations. The attacker can automate to go against multiple sites at one time.

Using denial of service attacks

The denial of service attack is one of the best examples of impacting site availability. It involves getting the server to perform a large number of mundane tasks, exceeding the capacity of the server to cope with any other task. For example, if everyone in a large meeting asks you your name all at once, and every time you answer, they ask you again. You have experienced a personal denial of service attack. To ask a computer its name, you use ping. You can use ping to build an effective DoS attack. The smart hacker gets the server to use more computational resources in processing the request than the adversary does in generating the request.

Distributed DoS is a type of attack used on popular sites, such as Yahoo!®. In this type of attack, the hacker infects computers on the Internet via a virus or other means. The infected computer becomes slaves to the hacker. The hacker controls them at a predetermined time to bombard the target server with useless, but intensive resource consuming requests. This attack not only causes the target site to experience problems, but also the entire Internet as the number of packets is routed via many different paths to the target.

Figure 5. Denial of service attacks



Using known server bugs

The attacker analyzes the site to find what types of software are used on the site. He then proceeds to find what patches were issued for the software. Additionally, he searches on how to exploit a system without the patch. He proceeds to try each of the exploits. The sophisticated attacker finds a weakness in a similar type of software, and tries to use that to exploit the system. This is a simple, but effective attack. With millions of servers online, what is the probability that a system administrator forgot to apply a patch?

Using server root exploits

Root exploits refer to techniques that gain super user access to the server. This is the most coveted type of exploit because the possibilities are limitless. When you attack a shopper or his computer, you can only affect one individual. With a root exploit, you gain control of the merchants and all the shoppers' information on the site. There are two main types of root exploits: buffer overflow attacks and executing scripts against a server.

In a buffer overflow attack, the hacker takes advantage of specific type of computer program bug that involves the allocation of storage during program execution. The technique involves tricking the server into execute code written by the attacker.

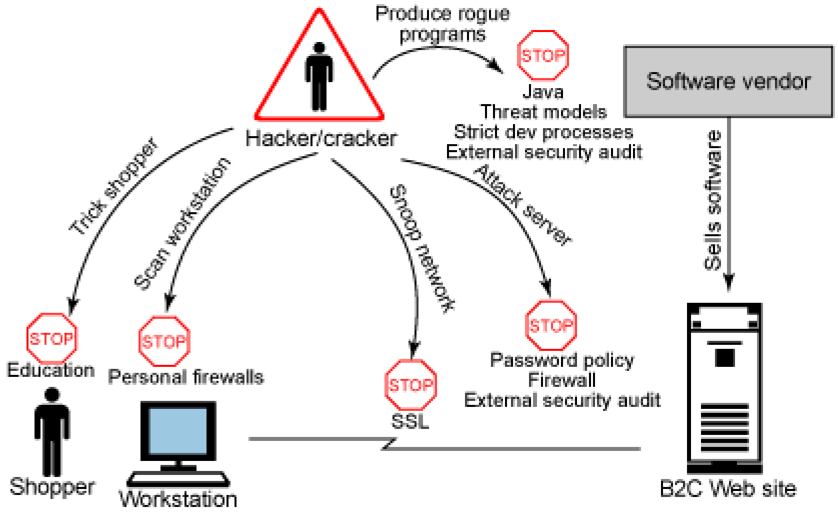
The other technique uses knowledge of scripts that are executed by the server. This is easily and freely found in the programming guides for the server. The attacker tries to construct scripts in the URL of his browser to retrieve information from his server. This technique is frequently used when the attacker is trying to retrieve data from the server's database.

Back to top

Defenses

Despite the existence of hackers and crackers, e-Commerce remains a safe and secure activity. The resources available to large companies involved in e-Commerce are enormous. These companies will pursue every legal route to protect their customers. Figure 6 shows a high-level illustration of defenses available against attacks.

Figure 6. Attacks and their defenses



At the end of the day, your system is only as secure as the people who use it. Education is the best way to ensure that your customers take appropriate precautions:

- Install personal firewalls for the client machines.
- Store confidential information in encrypted form.
- Encrypt the stream using the Secure Socket Layer (SSL) protocol to protect information flowing between the client and the e-Commerce Web site.
- Use appropriate password policies, firewalls, and routine external security audits.
- Use threat model analysis, strict development policies, and external security audits to protect ISV software running the Web site.

Education

Your system is only as secure as the people who use it. If a shopper chooses a weak password, or does not keep their password confidential, then an attacker can pose as that user. This is significant if the compromised password belongs to an administrator of the system. In this case, there is likely physical security involved because the administrator client may not be exposed outside the firewall. Users need to use good judgement when giving out information, and be educated about possible phishing schemes and other social engineering attacks.

Personal firewalls

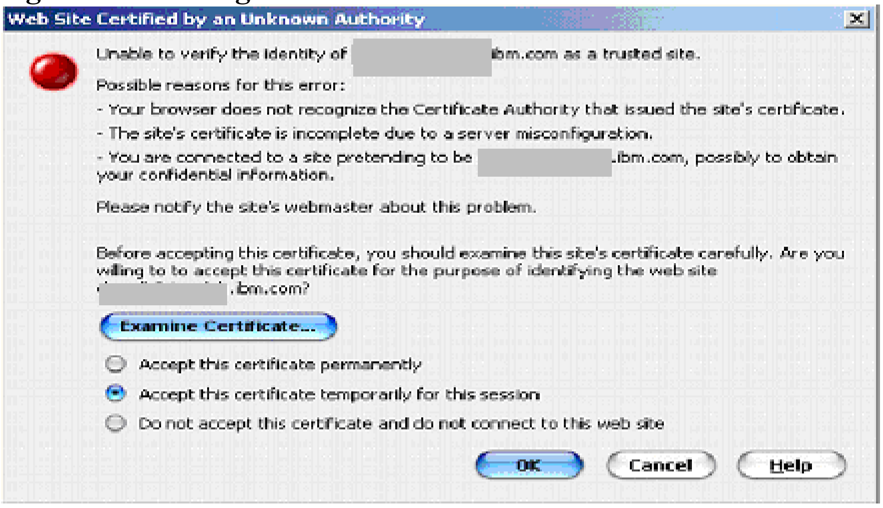
When connecting your computer to a network, it becomes vulnerable to attack. A personal firewall helps protect your computer by limiting the types of traffic initiated by and directed to your computer. The intruder can also scan the hard drive to detect any stored passwords.

Secure Socket Layer (SSL)

Secure Socket Layer (SSL) is a protocol that encrypts data between the shopper's computer and the site's server. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted so that a hacker sniffing the network cannot read the contents.

The SSL certificate is issued to the server by a certificate authority authorized by the government. When a request is made from the shopper's browser to the site's server using https://..., the shopper's browser checks if this site has a certificate it can recognize. If the site is not recognized by a trusted certificate authority, then the browser issues a warning as shown in Figure 7.

Figure 7. Warning to user



Web Site Certified by an Unknown Authority

Unable to verify the identity of [redacted]ibm.com as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be [redacted].ibm.com, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the web site '[redacted].ibm.com?

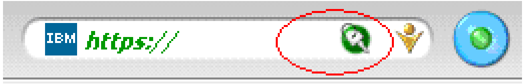
○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this web site

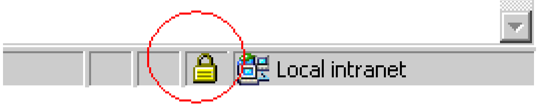
As an end-user, you can determine if you are in SSL by checking your browser. For example, in Mozilla® Firefox, the secure icon is at the top in the URL entry field as shown in Figure 8.

Figure 8. Secure icon in Mozilla Firefox



In Microsoft® Internet Explorer, the secure icon is at the bottom right of the browser as shown in Figure 9.

Figure 9. Secure icon in Microsoft Internet



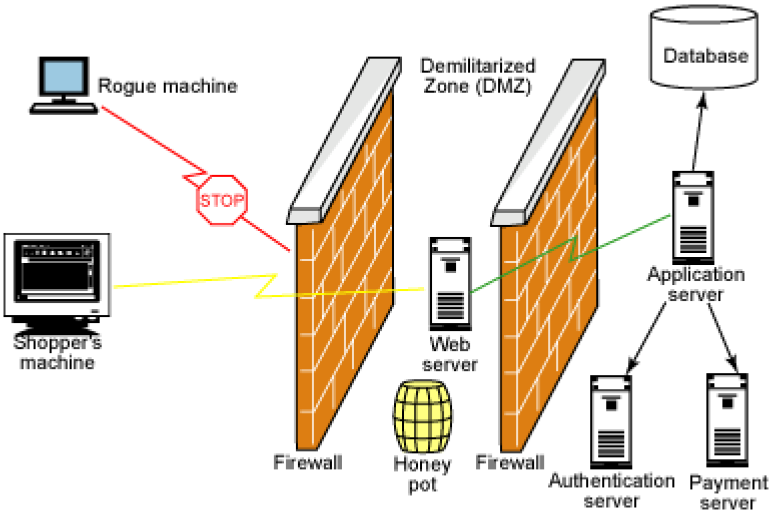
Server firewalls

A firewall is like the moat surrounding a castle. It ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines.

A common technique is to setup a demilitarized zone (DMZ) using two firewalls. The outer firewall has ports open that allow ingoing and outgoing HTTP requests. This allows the client browser to communicate with the server. A second firewall sits behind the e-Commerce servers. This firewall is heavily fortified, and only requests from trusted servers on specific ports are allowed through. Both firewalls use intrusion detection software to detect any unauthorized access attempts.

Another common technique used in conjunction with a DMZ is a honey pot server. A honey pot is a resource (for example, a fake payment server) placed in the DMZ to fool the hacker into thinking he has penetrated the inner wall. These servers are closely monitored, and any access by an attacker is detected.

Figure 10. Firewalls and honey pots



Password policies

Ensure that password policies are enforced for shoppers and internal users. A sample password policy, defined as part of the Federal Information Processing Standard (FIPS), is shown in the table below.

Policy	**Value**
Account lockout threshold	6 attempts
Consecutive unsuccessful login delay	10 seconds
Matching user ID and password	N (no, they cannot match)
Maximum occurrence of consecutive characters	3 characters
Maximum instances of any character	4 instances

Maximum lifetime of passwords	180 days
Minimum number of alphabetic characters	1 alphabetic character
Minimum number of numeric characters	1 numeric character
Minimum length of password	6 characters
Reuse user's previous password	N (no, cannot be reused)

You may choose to have different policies for shoppers versus your internal users. For example, you may choose to lockout an administrator after 3 failed login attempts instead of 6. These password policies protect against attacks that attempt to guess the user's password. They ensure that passwords are sufficiently strong enough so that they cannot be easily guessed. The account lockout capability ensures that an automated scheme cannot make more than a few guesses before the account is locked.

Intrusion detection and audits of security logs

One of the cornerstones of an effective security strategy is to prevent attacks and to detect potential attackers. This helps understand the nature of the system's traffic, or as a starting point for litigation against the attackers.

Suppose that you have implemented a password policy, such as the FIPS policy described in the section above. If a shopper makes 6 failed logon attempts, then his account is locked out. In this scenario, the company sends an email to the customer, informing them that his account is locked. This event should also be logged in the system, either by sending an email to the administrator, writing the event to a security log, or both.

You should also log any attempted unauthorized access to the system. If a user logs on, and attempts to access resources that he is not entitled to see, or performs actions that he is not entitled to perform, then this indicates the account has been co-opted and should be locked out. Analysis of the security logs can detect patterns of suspicious behavior, allowing the administrator to take action.

In addition to security logs, use business auditing to monitor activities such as payment processing. You can monitor and review these logs to detect patterns of inappropriate interaction at the business process level.

The infrastructure for business auditing and security logging is complex, and most likely will come as part of any middleware platform selected to host your site. WebSphere Commerce, for example, has extensive capabilities in this area.

Back to top

Site development best practices

This section describes best practices you can implement to help secure your site.

Security policies and standards

There are many established policies and standards for avoiding security issues. However, they are not required by law. Some basic rules include:

- Never store a user's password in plain text or encrypted text on the system. Instead, use a one-way hashing algorithm to prevent password extraction.
- Employ external security consultants (ethical hackers) to analyze your system.
- Standards, such as the Federal Information Processing Standard (FIPS), describe guidelines for implementing features. For example, FIPS makes recommendations on password policies.
- Ensure that a sufficiently robust encryption algorithm, such as triple DES or AES, is used to encrypt all confidential information stored on the system.
- When developing third-party software for e-Commerce applications, use external auditors to verify that appropriate processes and techniques are being followed.
- Recently, there has been an effort to consolidate these best practices as the Common Criteria for IT Security Evaluation (CC). CC seems to be gaining attraction. It is directly applicable to the development of specific e-Commerce sites and to the development of third party software used as an infrastructure in e-Commerce sites.

Security best practices remain largely an art rather than a science, but there are some good guidelines and standards that all developers of e-Commerce software should follow.

Using cookies

One of the issues faced by Web site designers is maintaining a secure session with a client over subsequent requests. Because HTTP is stateless, unless some kind of session token is passed back and forth on every request, the server has no way to link together requests made by the same person. Cookies are a popular mechanism for this. An identifier for the user or session is stored in a cookie and read on every request. You can use cookies to store user preference information, such as language and currency. This simplifies Web page development because you do not have to be concerned about passing this information back to the server.

The primary use of cookies is to store authentication and session information, your information, and your preferences. A secondary and controversial usage of cookies is to track the activities of users.

Different types of cookies are:

- Temporary cookies: These cookies are valid only for the lifetime of your current session, and are deleted when you close your browser. These are usually the good type. They are mostly used to keep your session information.
- Permanent cookies: These are for a time period, specified by the site, on the shopper's computer. They recall your previous session information.
- Server-only cookies: These cookies are usually harmless, and are only used by the server that issued them.
- Third-party cookies: These are usually used for tracking purposes by a site other than the one you are visiting. Your browser or a P3P policy can filter these cookies.

If you do not want to store cookies, here are other alternatives:

- Send user ID/password on every request: This was popular 5-10 years ago, but now recognized as an insecure technique. The user ID/password flowing under non-SSL is susceptible to attacks. This alternative is not practical for a high volume site. Pages that run under SSL would slow down site performance.
- SSL client side authentication: This is the most secure, but it is cumbersome for shoppers to install on their browsers. You have to pay for a company to verify who you are and to issue a certificate. The popularity of this technique for client-side authentication has decreased in recent years. It remains very popular on server sites.
- URL rewriting: This is a popular alternative to cookies. Each HTTP link on the page is specially encoded, but it is expensive for the site to implement. It interferes with the performance of the site because the pages cannot be cached and reused for different users. This alternative is susceptible to attack if it is not used under SSL.

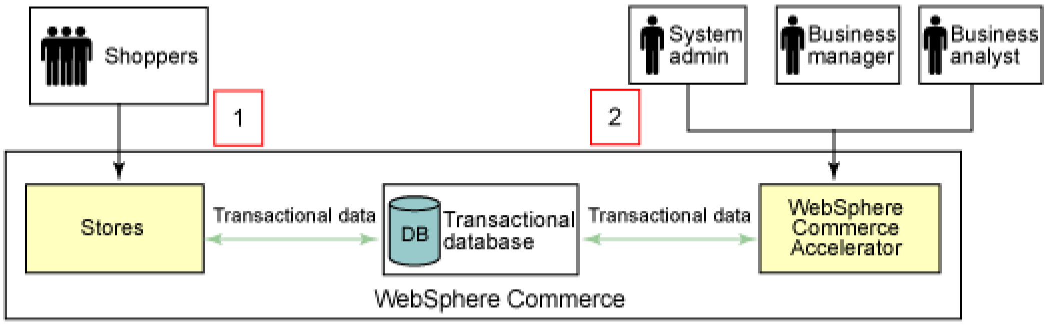
Cookies marked as secure (storing encrypted data and passing to the user only under SSL) remain the most popular method of providing a secure online experience.

Using threat models to prevent exploits

When architecting and developing a system, it is important to use threat models to identify all possible security threats on the server. Think of the server like your house. It has doors and windows to allow for entry and exit. These are the points that a burglar will attack. A threat model seeks to identify these points in the server and to develop possible attacks.

Threat models are particularly important when relying on a third party vendor for all or part of the site's infrastructure. This ensures that the suite of threat models is complete and up-to-date.

Figure 11. Threat models



Responding to security issues

An effective overall security strategy is to be prepared when vulnerabilities are detected. This also means ensuring that software vendors selected for all or part of the site's infrastructure have proactive and reactive policies for handling security issues.

In the case of WebSphere Commerce, we can quickly form a SWAT team with key developers, testers, and support personnel. This becomes the highest priority for all involved parties. An assessment is made immediately, usually within the first few hours, to determine the vulnerability of the merchant's sites. A workaround or permanent solution is developed for the affected sites within a day. Then a "flash" issued to all customers to notify them of the problem, the solution, and how to check if they have been exploited. For critical issues, no one leaves until there is a solution.

Using an online security checklist

Use this security checklist to protect yourself as a shopper:

- Whenever you logon, register, or enter private information, such as credit card data, ensure your browser is communicating with the server using SSL.
- Do not shop at a site when the browser does not recognize the server's SSL certificate. This check is done by your browser the first time your URL becomes HTTPS for the site. If the certificate is not recognized, then your browser presents a pop-up message to inform you.
- Use a password of at least 6 characters, and ensure that it contains some numeric and special characters (for example, c0113g3).
- Avoid reusing the same user ID and password at multiple Web sites.
- If you are authenticated (logged on) to a site, always logoff after you finish.
- Use a credit card for online purchases. Most credit card companies will help you with non-existent or damaged products.
- A bricks and mortar store with an online brand is most likely a legitimate site. However, the site may still have vulnerabilities.

Back to top

Conclusion

This article outlined the key players and security attacks and defenses in an e-Commerce system. Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the shopper to be vigilant when shopping online.

Security Threats to Ecommerce

SECURITY THREATS TO ELECTRONIC COMMERCE

Most businesses that have made the move towards an online presence have experienced some kind of security threat to their business. Since the Internet is a public system in which every transaction can be tracked, logged, monitored and stored in many locations, it is important for businesses to understand possible security threats to their business.

There are many threats to e-commerce that may come from sources within an organization or through some external channel. The following are the top corporate security threats categorized by internal and external threats.

o Unauthorized internal users who accesses confidential information by using a stolen passwords for the purpose of committing fraud or theft.

o Former employees of an organization that maintain access to information resources directly by creating alternative passwords, “back doors” into the computer system, or indirectly through former co-workers.

o Weak access points in information infrastructure and security that can expose company information and trade secrets.

o Management that undermines security is maybe the greatest risk to e-commerce as there

o Contractors, partners, consultants, and temps who take advantage of even limited access to important systems.

o Peoples mentality on Internet security is changing this is evident through the increase in sales of antivirus software and subscriptions to email virus protection.

o Businesses may take Visa’s lead of requiring its service providers and merchants to have firewalls, encryption, as well as testing and access policies as a condition of doing business with them. They feel that the security of their B2B partner is as important as their creditworthiness.

The term *virtual organization* is used to describe a network of independent firms that join together, often temporarily, to produce a service or product. Virtual organization is often associated with such terms as virtual office, virtual teams, and virtual leadership. The ultimate goal of the virtual organization is to provide innovative, high-quality products or services instantaneously in response to customer demands.

The term *virtual* in this sense has its roots in the computer industry. When a computer appears to have more storage capacity than it really possesses it is referred to as virtual memory. Likewise, when an organization assembles resources from a variety of firms, a virtual organization seems to have more capabilities than it actually possesses.

BACKGROUND

Traditional organizations integrated work vertically; that is, they delegated authority in a pyramidal, hierarchical structure. As the pyramid shape suggests, power was concentrated primarily among the handful of individuals at the top. This organizational form, shown in Figure 1, was first developed in the United States in the late 19th century with the advent of mass production.

The prominent theorist of traditional hierarchical organizations was the renowned industrial engineer, Frederick Winslow Taylor. His book, *Principles of Scientific Management,* introduced the principles for designing and managing mass-production facilities such as Ford's automobile factory in Michigan and Carnegie's steel works in Pittsburgh.

The hierarchical structure was designed to manage highly complex processes like automobile assembly where production could be broken down into a series of simple steps. Hierarchical corporations often controlled and managed all activities of a business from, the raw materials to their allocation to consumers. A centralized managerial hierarchy controlled the entire production process, with white-collar workers establishing rules and procedures to manage a blue-collar workforce.

From World War II until the early 1980s, the trend was to build increasing layers of management with more staff specialists. This centralized hierarchical structure

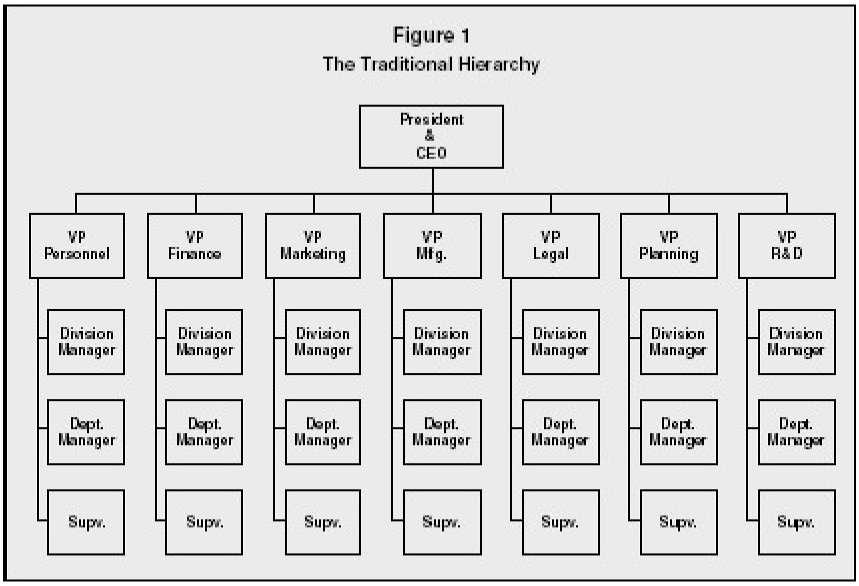


Figure 1

The Traditional Hierarchy

was seen as effective for managing large number of workers, but lacked agility and was unable to process information rapidly throughout the organization.

NEW DEMANDS ALTER ORGANIZATIONAL FORMS

Since the 1980s, many organizations have flattened their structures by shifting authority downward, giving employees increased autonomy and decision-making power. Advantages of flatter organization forms include a decreased need for supervisors and middle management, faster decision making, and the ability to process information faster because of the reduced number of layers in the organization.

A consequence of flatter organizations, though, is that employees tend to be more dispersed both geographically and organizationally. Responding to this problem of dispersion, many organizations have eliminated superfluous processes and begun focusing on their core, value-added business. Flat organizations using joint ventures and strategic alliances are providing increased flexibility and innovation, and are replacing many traditional hierarchies.

THE NEW BUSINESS FORM

Ray Grenier and George Metes discuss the shift to this new organizational structure as a response to unprecedented customer expectations and alternatives, global competition, time compression, complexity, rapid change, and increased use of technology. They describe the virtual model as a lead organization that creates alliances with groups and individuals from different organizations who possess the highest competencies to build a specific product or service in a short period of time (see Figure 2).

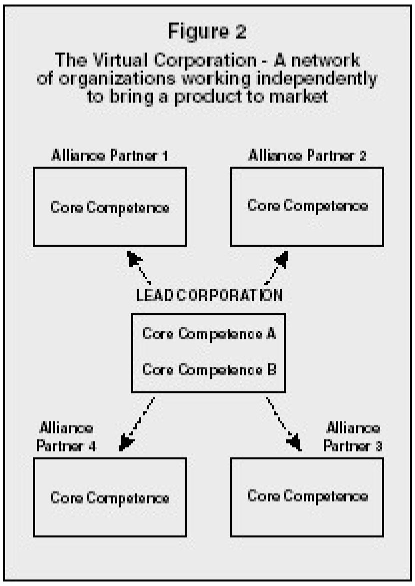


Figure 2
The Virtual Corporation - A network
of organizations working independently
to bring a product to market

Grenier and Meters further explain that these alliances are virtual because products and services are not produced in a single corporation whose purpose is longevity. Rather, these new virtual organizations consist of a hybrid of groups and individuals from different companies that might include customers, competitors, and suppliers who have a focused purpose of bringing a high-quality product or service to market as rapidly as possible. These alliances may be temporary with short concept-to-delivery cycles.

William Davidow and Michael Malone, authors of *The Virtual Corporation,* claim that virtual corporations will be central to the new business revolution. Their concept of the virtual corporation brings diverse innovations together such as just-in-time supply, work teams, flexible manufacturing, reusable engineering, worker empowerment, organizational streamlining, computer-aided design, total quality, and mass customization into a coherent vision for the twentieth century corporation.

The virtual corporation is more permeable than traditional organizational forms. Interfaces in a virtual organization between company, supplier, and customers continuously change, resulting in a blurring of traditional functions. Inside the office, work groups and job responsibilities may shift regularly. The virtual organization may not have a central office or an organizational chart. Suppliers, customers, and even competitors may spend time alongside one another in the virtual organization.

CHARACTERISTICS OF A VIRTUAL ORGANIZATION

Partners in virtual organizations share risks, costs, and rewards in pursuit of a global market. The common characteristics of these organizations include a purpose that is motivated by specific market opportunities, world-class core competence, information networks, interdependent relationships, and permeable boundaries.

Virtual organizations represent structures that are motivated by specific market opportunities. Once the alliance has been formed and the opportunity has been exploited, partners may move on to new partnerships and alliances.

Each partner in a virtual corporation contributes a world-class core competence, such as design, manufacturing, or marketing. This ability of multiple firms to create synergies among world-class functions and processes creates untold possibilities.

As organizations create these new linkages, advanced information technology becomes an important element, and key to the success of a virtual organization. Computerized information systems allow employees from geographically dispersed locations to link up with one another. The virtual office may use desktop videoconferencing, collaborative software, and intranet systems to enhance the flow of information among team members. Besides the need for instantaneous communication with one another, members of these autonomous virtual teams have increasing requirements regarding the amount and quality of information they need to do their work.

Members of the virtual organization, in turn, create a network of interdependent relationships. These relationships require firms to be much more dependent on one another than they have been in the past, demanding unprecedented levels of trust. Strong interdependencies cause organizations' boundaries to be blurred as competitors, suppliers, and customers enter into cooperative agreements. These new relationships among firms obligate organizations to use innovative management practices.

VIRTUAL TEAMS

Virtual teams are often the group structure used in virtual organizations. Jessica Lipnack and Jeffrey Stamps define virtual teams as "a group of people who interact through interdependent tasks guided by a common purpose." Unlike conventional teams, a virtual team performs work across space, time, and organizational boundaries connected by interactive communication technologies. Virtual teams may include employees, management, customers, suppliers, and government working together to achieve common goals. These teams often stay together only to perform its episodic task. They may work jointly on a new project, but when the product is designed and goes into production, the project is finished and the virtual team dissolves.

Lipnack and Stamps offer three key features for a successful virtual team. One is the choice of team members with the appropriate skills and knowledge for the task; second is the definition of a purpose to steer the group; and third is the effective linking of team members, including communication channels, interactions, and relationships.

Virtual team members are required to learn a new set of skills. One skill is the ability to interact with one another effectively despite infrequent or total lack of face-to-face contact. Another is the ability to assimilate quickly and effectively into new teams. Virtual team members should be technically adept to deal with the variety of required computer-based technologies. Additionally, virtual team members may need intercultural skills to work effectively in multi-national organizations.

VIRTUAL LEADERS

Greiner and Metes discuss the new leadership skills required to lead in the virtual environment, including the ability to manage a network of interdependent firms, to design virtual operations, to create and sustain virtual relationships with internal as well as external constituents, to support virtual teams, and to keep virtual teams focused. The leader of a virtual organization demands a new set of skills unlike the skills required in a traditional hierarchy.

VIRTUAL LEARNING

Another critical element to the success of the virtual organization is the ability of the organization to create world-class learning systems. These learning systems help leaders sustain or create world-class competencies. Effective learning systems can create pathways throughout the organization, in network fashion, enhancing the innovative capabilities of the organizational members. An organization's ability to sustain a leadership position in the world economy demands that organizations be on the cutting edge to develop rapid and elegant solutions to emerging consumer demands.

EXAMPLES OF VIRTUAL ORGANIZATIONS

An industry that is known for its use of partners and alliances is the entertainment industry, which has partnered with the computing, communications, consumer electronics, and publishing industries to convert movies, textbooks, and other software into digital formats.

Increasing numbers of firms are moving to these new organizational forms. Corning, the glass and ceramics maker, is one such firm known for making partnerships work to their advantage. Corning has partnered with such firms as Siemens, Germany's electronics conglomeration, and Vitro, Mexico's largest glassmaker. Alliances are so important to Corning's business strategy that the corporation has defined itself as a network of organizations.

Computer organizations that have successfully implemented forms of this new structure include Apple Computer and Sun Microsystems. When Apple Computer linked its easy-to-use software with Sony's manufacturing skills in miniaturization, Apple was able to get its product to market quickly and gain a market share in the notebook segment of the PC industry.

Sun Microsystems has been considered another highly decentralized organization comprised of independently operating companies. Sun positions information systems as a top priority, trying to achieve faster and better communication. With numerous "SunTeams," members operate across time, space, and organizations to address critical business issues. Sun managers identify key customer issues and then form teams with the critical skills and knowledge needed to address the issue. This team might include sales people, marketing personnel, finance, and operations from various places around the globe; customers and suppliers may become episodic members as necessary. Weekly meetings may take place via conference calls. Critical to the team's success is the selection of talent from the organization, defining a clear purpose for the team's efforts, and establishing communication links among the team members.

Sun has been working on further development of technologies such as EDI (Electronic Data Interchange) and RFID (Radio Frequency Identification technology). Both EDI and RFID will impact information exchange globally and across numerous industries.

CHALLENGES

Virtual organizations can be very complex and problematic; they fail as often as they succeed. Among the many challenges of the virtual organization are strategic planning dilemmas, boundary blurring, a loss of control, and a need for new managerial skills.

Strategic planning poses new challenges as virtual firms determine effective combinations of core competencies. Common vision among partners is quintessential to cooperating firms. Focused on a common goal, firms develop close interdependencies that may make it difficult to determine where one company ends and another begins. The boundary-blurring demands that these boundaries be managed effectively. Coordinating mechanisms are critical elements for supporting these loose collections of firms.

Virtual structures create a loss of control over some operations. This loss of control requires communication, coordination, and trust among the various partners, as well as a new set of managerial skills. Employees are exposed to increased ambiguity about organizational membership, job roles and responsibilities, career paths, and superior-subordinate relationships. This ambiguity requires management to rethink rewards, benefits, employee development, staffing and other employee-related issues. Developing leaders who are able to create and sustain these organizational forms is critical.

Les Pang offers a list of best practices, based on a review of successful implementations of virtual organizations.

- Foster cooperation, trust and empowerment.
- Ensure each partner contributes and identifiable strength or asset.
- Ensure skills and competencies are complementary, not overlapping.
- Ensure partners are adaptable.
- Ensure contractual agreements are clear and specific on roles and deliverables.
- If possible, do not replace face-to-face interaction entirely.
- Provide training that is critical to team success.
- Recognize that it takes time to develop the team.
- Ensure that technology is compatible and reliable.
- Provide technical assistance that is competent and available.