BSc CsIt SEM - VI
E-Commerce
Unit 5: Security in E-Commerce (7 Hrs.)

Syllabus:

Unit 5: Security in E-Commerce (7 Hrs.)

E-commerce Security, Dimensions of E-commerce Security: Confidentiality, Integrity, Availability, Authenticity, Nonrepudiation, Privacy, Security Threats in E-commerce: Vulnerabilities in E-commerce, Malicious Code, Adware, Spyware, Social Engineering, 2 Phishing, Hacking, Credit card fraud and Identity theft, Spoofing and Pharming, Client and Server Security, Data Transaction Security, Security Mechanisms: Cryptography, Hash Functions, Digital Signatures, Authentication, Access Controls, Intrusion Detection System, Secured Socket Layer(SSL)

==========

E-commerce Security

From the earliest of days, humans have warred against and stolen from each other, with the tools evolving over time from sticks and stones, to arrows and spears, to guns and bombs. Physical weaponry is familiar and readily recognizable. But today, algorithms and computer code have moved to the forefront. Cyberspace has become a new battlefield, one that often involves targets such as financial systems and communications networks.

Large business and government Web sites are constantly under attack by a variety of potential intruders, ranging from computer-savvy high school students to highly trained espionage workers employed by competing businesses or other governments.

For example, the U.S. Pentagon reports that its computers are scanned by potential attackers thousands of times every hour. These attackers are continually looking for a way to break through computer security defences in the hopes of finding any information that could help their employers embarrass, disable, or hurt competitors or enemies.

In 2009, during the U.S. July 4 holiday and continuing for more than a week after, a series of attacks on U.S. and South Korean Web sites was launched from networks that included more than 200,000 computers located all over the world. These attacks, which targeted both government and business Web sites in both countries, shut down the sites for several hours and included attempts (none reported to be successful) to gather sensitive data. These attacks occurred just a few weeks after U.S. President Barack Obama had announced the creation of a new government agency devoted to defending the country against cyberterrorism, including attacks of exactly this nature. Although investigators believed that the attacks were the work of operatives of the North Korean government, they were not able to identify definitively those responsible for the attack.

Later in 2009, an attack was successful in obtaining an 11-page file that contained a briefing on defensive military operations that would be undertaken by the United States and South Korea if war were to break out with North Korea. A South Korean military officer had left a USB device containing the plans plugged into his computer when he switched the computer from a restricted access military network to the Internet. Within minutes, an attacker accessed the document and stole a copy of the briefing. Investigators traced the attack to an IP address that is owned by the Chinese government, which had leased it to North Korea. Both governments denied any involvement in the theft.

BSc CsIt SEM - VI
E-Commerce

Now, E-commerce has become one of the largest industries in the world to function. The evolution of technology and the internet led to the opening of infinite ways to engage with consumers worldwide. But the larger the business, the greater the risk.

As a brand or an organization, it is organizations responsibility to protect all the consumers and themselves from threats. This is why security concerns over the internet and privacy have gone up in the last few years. Information about the brand and the consumer is out there, making them vulnerable to security issues.

The software that potential attackers use to scan computers is widely available; therefore, government agencies, companies, organizations, and even individuals can expect that their computers are scanned frequently as well.

Ecommerce sites will always be a hot target for cyberattacks. Today, privacy and security are a major concern for the electronic technologies. M-commerce shares security concerns with other technologies in the field. Privacy concerns have been found, to revealing a lack of trust in a variety of contexts, including commerce, electronic health records, the e- recruitment technology and social networking, has directly influenced users. Security is one of the principal and continuing concerns that restrict customers and organization engaging with ecommerce.

Ecommerce security refers to the measures taken to protect your business and your customers against cyber threats that is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

E-commerce Security is a part of Information Security of the framework and is specifically applied to the components that affect e-commerce include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particulars nuances and is one of highest visible security components that affect the end user through their daily payment interactions with their business.

Dimensions of E-commerce Security

As the security issue is the most worrying issue for E-Business, ensuring the security of E-Commerce activities has become the core research field of E-Commerce. The following are some of the security elements involved in E-Commerce.

There are six key dimensions to e-commerce security:

1. Integrity
2. Nonrepudiation
3. Authenticity
4. Confidentiality
5. Privacy And
6. Availability.

BSc CsIt SEM - VI
E-Commerce

Integrity

Integrity refers to the ability to ensure that information being displayed on a Web site, or transmitted or received over the Internet, has not been altered in any way by an unauthorized party.

Integrity can ensure that information on the internet has not been altered in any way by an unauthorized party. It maintains the consistency, accuracy, and trustworthiness of the information over its entire life cycle.

For example, an unauthorized person intercepts and changes the contents of an online communication, such as redirect a bank payment into a different account.

Nonrepudiation

Nonrepudiation refers to the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions.

Non-repudiation confirms whether the information sent between the two parties was received or not. It ensures that the purchase cannot be denied by the person who completed the transaction. In other words, it's an assurance that anyone cannot deny the validity of transaction.

Mostly non-repudiation uses a digital signature for online transactions because no one can deny the authenticity of their signature on a document.

For instance, the availability of free e-mail accounts with alias names makes it easy for a person to post comments or send a message and perhaps later deny doing so. Even when a customer uses a real name and e-mail address, it is easy for that customer to order merchandise online and then later deny doing so.

In most cases, because merchants typically do not obtain a physical copy of a signature, the credit card issuer will side with the customer because the merchant has no legally valid proof that the customer ordered the merchandise. So, when a merchant doesn't have enough proof of customers who have ordered with them during a credit card payment transaction, it will not be processed further to the merchant.

So, good business depends on both buyers and sellers. They must not deny any facts or rules once they accept that there should not be any repudiation.

Authenticity

Authenticity refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet. How does the customer know that the Web site operator is who it claims to be? How can the merchant be assured that the customer is really who she says she is? Someone who claims to be someone he is not is "spoofing" or misrepresenting himself.

So, in ecommerce, since both the customer and seller need to trust each other, they must remain as who they are in real. Both the seller and buyer must provide proof of their original identity so that the ecommerce transaction can happen securely between them.

Confidentiality

Confidentiality refers to the ability to ensure that messages and data are available only to those who are authorized to view them. That is, it refers to protecting information from being accessed by an unauthorized person on the internet or in other words, only the people who are authorized can gain access to view or modify or use the sensitive data of any customer or merchants.

Confidentiality is sometimes confused with privacy, which refers to the ability to control the use of information a customer provides about himself or herself to an e-commerce merchant.

Confidentiality is a concern about the information present during communication, privacy is concerned with personal details. In general, privacy is used to control the usage of information by the customers that they have given to the merchant.

E-commerce merchants have two concerns related to privacy. They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use. For example, if hackers break into an e-commerce site and gain access to credit card or other information, this violates not only the confidentiality of the data, but also the privacy of the individuals who supplied the information.

Availability

Availability refers to the ability to ensure that an e-commerce site continues to function as intended.

The continuous availability of the data is the key to provide a better customer experience in ecommerce. The continuous availability of the ecommerce website increases online visibility, search engine rankings, and site traffic. Data which is present on the website must be secured and available 24x7 for the customer without downtime. If it is not, it will be difficult to gain a competitive edge and survive in the digital world.

Table 4.3 summarizes these dimensions from both the merchants' and customers' perspectives. E-commerce security is designed to protect these six dimensions. When any one of them is compromised, overall security suffers.

TABLE 4.3 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

Security Threats in E-commerce:

Vulnerabilities in E-commerce

- In cybersecurity, a vulnerability is a weakness that can be exploited by cybercriminals to **gain unauthorized access to a computer system**. After exploiting a vulnerability, a cyberattack can run malicious code, install malware and even steal sensitive data.
- Vulnerabilities can be exploited by a variety of methods including SQL injection, buffer overflows, cross-site scripting (XSS) and open-source exploit kits that look for known vulnerabilities and security weaknesses in web applications.
- From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the **client**, the **server**, and the **communications pipeline**.

Figure 4.2 illustrates a typical e-commerce transaction with a consumer using a credit card to purchase a product.

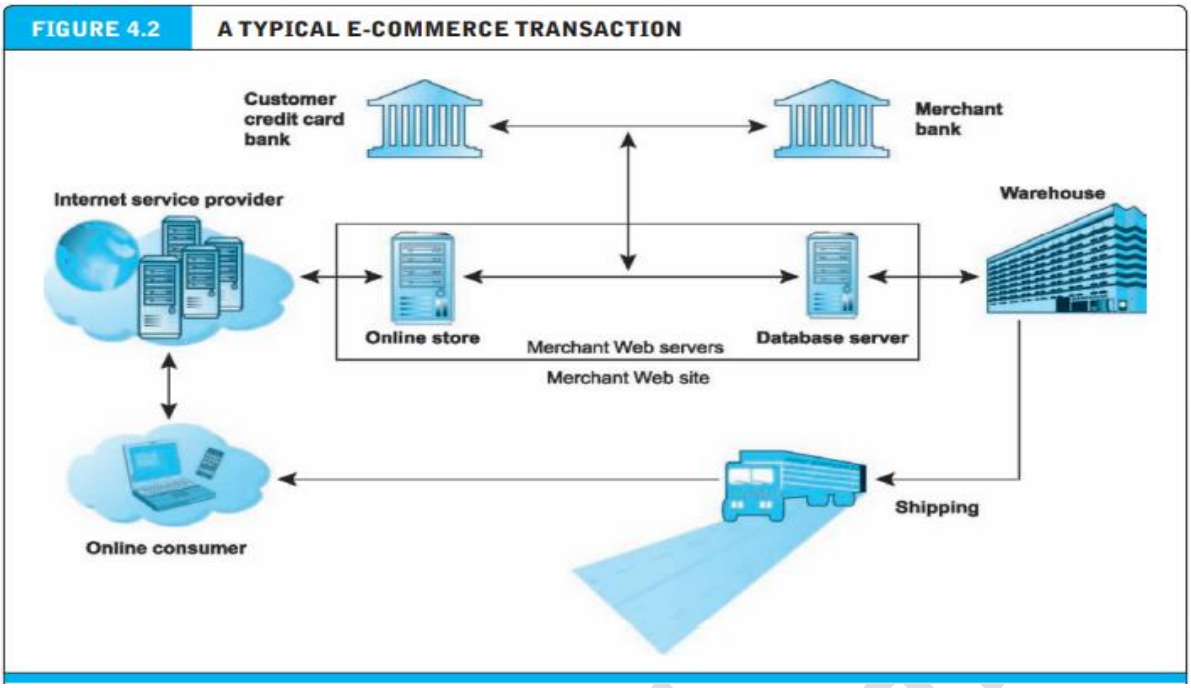
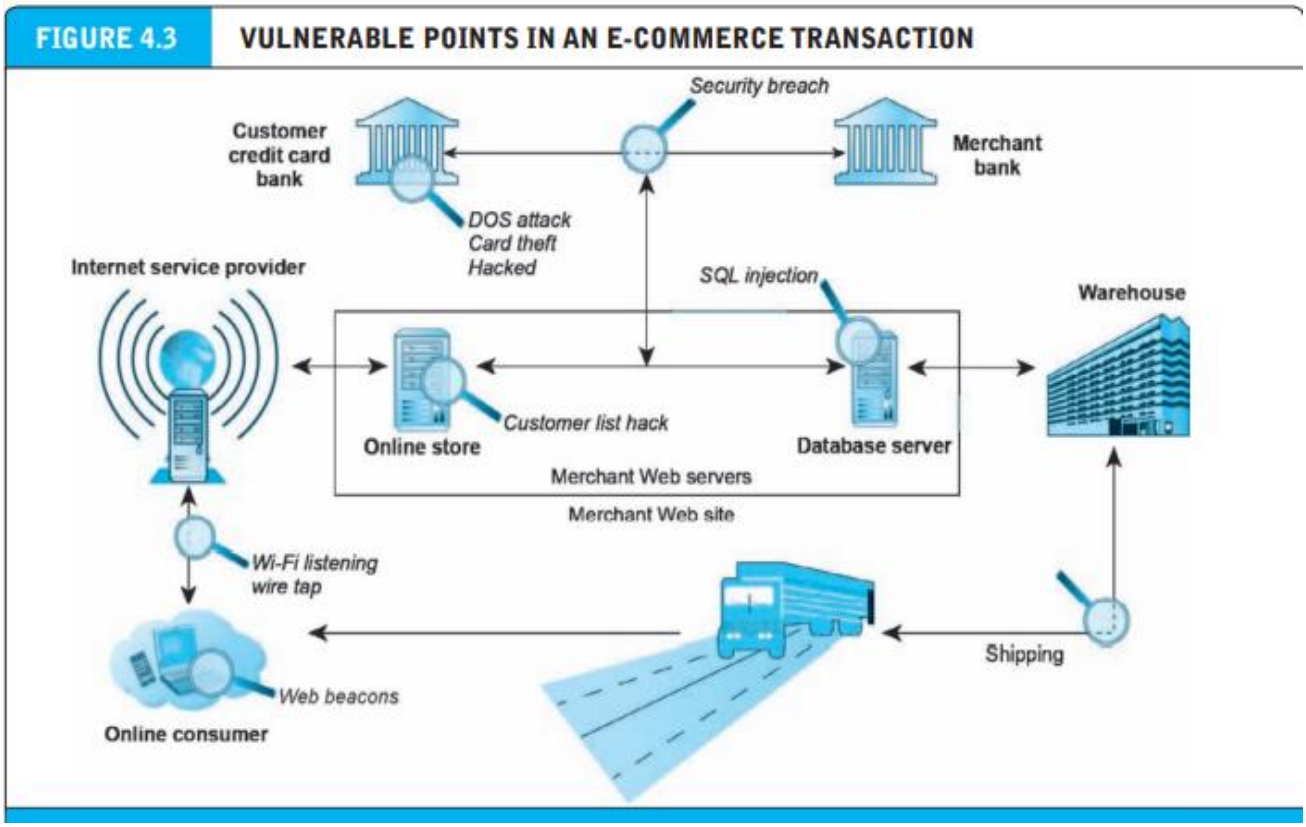


Figure 4.3 illustrates some of the things that can go wrong at each major vulnerability point in the transaction—over Internet communications channels, at the server level, and at the client level.



BSc CsIt SEM - VI
E-Commerce

Malicious Code

Malicious code (sometimes referred to as "malware") includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots. Some malicious code, sometimes referred to as an exploit, is designed to take advantage of software vulnerabilities in a computer's operating system, Web browser, applications, or other software components.

In the past, malicious code was often intended to simply impair computers, and was often authored by a lone hacker, but increasingly the intent is to steal e-mail addresses, logon credentials, personal data, and financial information. Malicious code is also used to develop integrated malware networks that organize the theft of information and money.

In the early days of the Internet, malicious code was often delivered by e-mail, in the form of a malicious attachment such as a Microsoft Word document or Excel spreadsheet and this remains a popular distribution method, with 1 in about every 244 e-mails containing mailware, either in the form of a malicious attachment or a malicious URL. The links lead directly to a malicious code download or Web sites that include malicious code (Symantec, 2015). One of the latest innovations in malicious code distribution is to embed it in the online advertising chain (known as maladvertising), including in Google, AOL, and other ad networks. As the ad network chain becomes more complicated, it becomes more and more difficult for Web sites to vet ads placed on their sites to ensure they are malware-free.

A drive-by download is malware that comes with a downloaded file that a user intentionally or unintentionally requests. Drive-by is now one of the most common methods of infecting computers. For instance, Web sites as disparate as eWeek (a technology site), to MLB (Major League Baseball), and Yahoo have experienced instances where ads placed on their sites either had malicious code embedded or directed clickers to malicious sites (RAND Corporation, 2014).

Malicious code embedded in PDF files also is common. Equally important, there has been a major shift in the writers of malware from amateur hackers and adventurers to organized criminal efforts to defraud companies and individuals. In other words, it's now more about the money than ever before.

Exploit kits

Exploit kits are collections of exploits bundled together and rented or sold as a commercial product, often with slick user interfaces and in-depth analytics functionality. Use of an exploit kit typically does not require much technical skill, enabling novices to become cybercriminals. Exploit kits typically target software that is widely deployed, such as Microsoft Windows, Internet Explorer, Adobe Flash and Reader, and Oracle Java. In 2014, according to Cisco, Angler, an exploit kit that uses Flash, Java, Microsoft Internet Explorer, and Microsoft Silverlight vulnerabilities, was one of the exploit kits most observed "in the wild" (Cisco, 2015).

BSc CsIt SEM - VI
E-Commerce

Adware

Adware is typically used to call for pop-up ads to display when the user visits certain sites. While annoying, adware is not typically used for criminal activities. A browser parasite is a program that can monitor and change the settings of a user's browser, for instance, changing the browser's home page, or sending information about the sites visited to a remote computer. Browser parasites are often a component of adware. In early 2015, Lenovo faced a barrage of criticism when it became known that, since September 2014, it had been shipping its Windows laptops with Superfish adware preinstalled. Superfish injected its own shopping results into the computer's browser when the user searched on Google, Amazon, or other Web sites. In the process, Superfish created a security risk by enabling others on a Wi-Fi network to silently hijack the browser and collect anything typed into it. Lenovo ultimately issued a removal tool to enable customers to delete the adware.

Spyware

Spyware is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission. Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties. In some cases, these may be advertisers or marketing data firms, which is why spyware is sometimes referred to as "adware." It is installed without user consent by methods such as a drive-by download, a trojan included with a legitimate program or a deceptive pop-up window.

Spyware, can be used to obtain information such as a user's keystrokes, copies of e-mail and instant messages, and even take screenshots (and thereby capture passwords or other confidential data).

Spyware uses your internet connection to relay personal information such as your name, address, browsing habits, preferences, interests or downloads. Other forms of spyware hijack your browser to point it to another website, cause your device to place calls or send texts automatically, or serve annoying ads even when you are offline. Spyware that steals your username, password or other credentials is referred to as a "keylogger" – an insidious prerequisite for cyber crime.

Signs of a spyware infection can include unwanted behaviors and degradation of system performance. It can eat up CPU capacity, disk usage and network traffic. Stability issues such as applications freezing, failure to boot, difficulty connecting to the internet and system crashes are also common.

Social engineering

Social engineering is a form of deceit where a person pretends to be someone he or she is not and tries to infiltrate a facility or gain information. Social engineering can be the easiest way to gain access to an account, system or facility and does not require much technical knowledge. "It's a common hacker trick to telephone unsuspecting employees and pretend to be a network system administrator or security manager. If the hacker knows enough about the company's network to sound convincing, he can get passwords, account names, and other

sensitive information. This could also be done in-person or over the phone and a hacker could gain access to and account or a secure area in a facility.

Social engineering is the art of manipulating, influencing, or deceiving you in order to gain control over your computer system. The hacker might use the phone, email, snail mail or direct contact to gain illegal access. Phishing, spear phishing, and CEO Fraud are all examples.

Social engineering relies on human curiosity, greed, and gullibility in order to trick people into taking an action that will result in the downloading of malware. Kevin Mitnick, until his capture and imprisonment in 1999, was one of America's most wanted computer criminals. Mitnick used simple deceptive techniques to obtain passwords, social security, and police records all without the use of any sophisticated technology.

Phishing

Phishing is any deceptive, online attempt by a third party to obtain confidential information for financial gain. Phishing attacks typically do not involve malicious code but instead rely on straightforward misrepresentation and fraud, so-called "social engineering" techniques. One of the most popular phishing attacks is the e-mail scam letter. The scam begins with an e-mail: a rich former oil minister of Nigeria is seeking a bank account to stash millions of dollars for a short period of time, and requests your bank account number where the money can be deposited. In return, you will receive a million dollars. This type of e-mail scam is popularly known as a "Nigerian letter" scam.

Thousands of other phishing attacks use other scams, some pretending to be eBay, PayPal, or Citibank writing to you for account verification (known as spear phishing, or targeting a known customer of a specific bank or other type of business). Click on a link in the e-mail and you will be taken to a Web site controlled by the scammer, and prompted to enter confidential information about your accounts, such as your account number and PIN codes. On any given day, millions of these phishing attack e-mails are sent, and, unfortunately, some people are fooled and disclose their personal account information

Phishers rely on traditional "con man" tactics, but use e-mail to trick recipients into voluntarily giving up financial access codes, bank account numbers, credit card numbers, and other personal information. Often, phishers create (or "spoof") a Web site that purports to be a legitimate financial institution and cons users into entering financial information, or the site downloads malware such as a keylogger to the victim's computer. Phishers use the information they gather to commit fraudulent acts such as charging items to your credit cards or withdrawing funds from your bank account, or in other ways "steal your identity" (identity fraud). Symantec reported that in 2014, about 1 in every 965 e-mails contained a phishing attack. The number of spear-phishing attacks increased by 8%, with the average duration of campaigns reaching 9 days.

Hacking

A hacker is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term cracker is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker tend to be used interchangeably.

Hackers and crackers gain unauthorized access by finding weaknesses in the security procedures of Web sites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use. In the past, hackers and crackers typically were computer expert excited by the challenge of breaking into corporate and government Web sites. Sometimes they were satisfied merely by breaking into the files of an e-commerce site. Today, hackers have malicious intentions to disrupt, deface, or destroy sites (cybervandalism) or to steal personal or corporate information they can use for financial gain (data breach).

Hacktivism adds a political twist. Hacktivists typically attack governments, organizations, and even individuals for political purposes, employing the tactics of cybervandalism, distributed denial of service attacks, data thefts, doxing (gathering and exposing personal information of public figures, originating from the term "documents" or "docx"), and more. LulzSec and Anonymous are two prominent hacktivist groups.

In 2015, another hacktivist group called the Impact Team allegedly hacked the Ashley Madison Web site to call attention to its weak security, and after its owner Avid Life Media refused to shut it down as they demanded, the group released millions of sensitive customer records.

Groups of hackers called tiger teams are sometimes used by corporate security departments to test their own security measures. By hiring hackers to break into the system from the outside, the company can identify weaknesses in the computer system's Armor. These "good hackers" became known as white hats because of their role in helping organizations locate and fix security flaws. White hats do their work under contract, with agreement from clients that they will not be prosecuted for their efforts to break in.

In contrast, black hats are hackers who engage in the same kinds of activities but without pay or any buy-in from the targeted organization, and with the intention of causing harm. They break into Web sites and reveal the confidential or proprietary information they find. These hackers believe strongly that information should be free, so sharing previously secret information is part of their mission.

Somewhere in the middle are the grey hats, hackers who believe they are pursuing some greater good by breaking in and revealing system flaws. Grey hats discover weaknesses in a system's security, and then publish the weakness without disrupting the site or attempting to profit from their finds. Their only reward is the prestige of discovering the weakness. Grey hat actions are suspect, however, especially when the hackers reveal security flaws that make it easier for other criminals to gain access to a system.

Credit card fraud and Identity theft

Theft of credit card data is one of the most feared occurrences on the Internet. Fear that credit card information will be stolen prevents users from making online purchases in many cases. Interestingly, this fear appears to be largely unfounded. Incidences of stolen credit card information are actually much lower than users think, around 0.9% of all online card transactions. Online merchants use a variety of techniques to combat credit card fraud, including using automated fraud detection tools, manually reviewing orders, and rejection of suspect orders.

In addition, U.S. federal law limits the liability of individuals to $50 for a stolen credit card. For amounts more than $50, the credit card company generally pays the amount, although in some cases, the merchant may be held liable if it failed to verify the account or consult published lists of invalid cards. Banks recoup the cost of credit card fraud by charging higher interest rates on unpaid balances, and by merchants who raise prices to cover the losses.

In the past, the most common cause of credit card fraud was a lost or stolen card that was used by someone else, followed by employee theft of customer numbers and stolen identities (criminals applying for credit cards using false identities). Today, the most frequent cause of stolen cards and card information is the systematic hacking and looting of a corporate server where the information on millions of credit card purchases is stored.

Spoofing and Pharming

Spoofing involves attempting to hide a true identity by using someone else's e-mail or IP address. For instance, a spoofed e-mail will have a forged sender e-mail address designed to

mislead the receiver about who sent the e-mail. IP spoofing involves the creation of TCP/IP packets that use someone else's source IP address, indicating that the packets are coming from a trusted host. Most current routers and firewalls can offer protection against IP spoofing.

Spoofing a Web site sometimes involves pharming, automatically redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination. Links that are designed to lead to one site can be reset to send users to a totally unrelated site—one that benefits the hacker.

Pharming

- Pharming is a malicious website that resembles a legitimate website, used to gather usernames and passwords
- pharming is a advance technique to get users credentials by making effort to entering users into the website
- In order words, it misdirects users to a fake website that appears to be official and victims gives their personal information by fault.
- In pharming, fake website is created which appears to be official. Users then access the website and request is popped up regarding username and password and other credentials

Although spoofing and pharming do not directly damage files or network servers, they threaten the integrity of a site. For example, if hackers redirect customers to a fake Web site that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business from the true site. Or, if the intent is to disrupt rather than steal, hackers can alter orders—inflating them or changing products ordered—and then send them on to the true site for processing and delivery. Customers become dissatisfied with the improper order shipment, and the company may have huge inventory fluctuations that impact its operations.

In addition to threatening integrity, spoofing also threatens authenticity by making it difficult to discern the true sender of a message. Clever hackers can make it almost impossible to distinguish between a true and a fake identity or Web address.

Spam (junk) Web sites (also sometimes referred to as link farms) are a little different. These are sites that promise to offer some product or service, but in fact are just a collection of advertisements for other sites, some of which contain malicious code. For instance, you may search for "[name of town] weather," and then click on a link that promises your local weather, but then discover that all the site does is display ads for weather-related products or other Web sites. Junk or spam Web sites typically appear on search results, and do not involve e-mail. These sites cloak their identities by using domain names similar to legitimate firm names, and redirect traffic to known spammer-redirection domains such as topsearch10.com.

Client and Server Security

Client-server architecture consists of multiple user's workstations, PCs, or other devices, connected to a central server via an Internet connection or other network. In another words a client-server network is a network consisting of a central computer, also known as a server, which hosts data and other forms of resources and clients such as laptops and desktop computers contact the server and request to use data or share its other resources with it that is the client sends a request for data, and the server accepts and accommodates the request, sending the data packets back to the user who needs them.

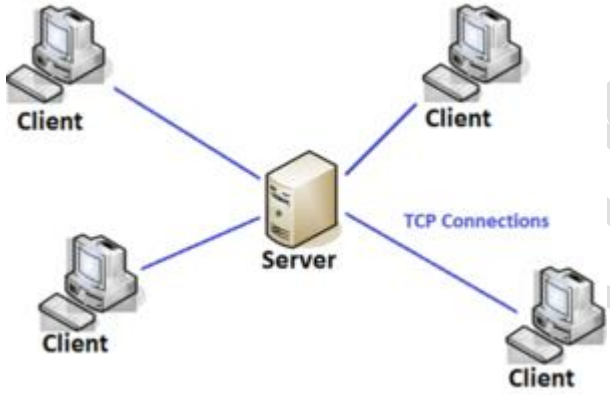


Fig:- Client-server architecture

There are three components to client-server environments: the client, the server, and the network. The network bridges the physical and functional separation between the client and the server. The multiple connections possible between clients and multiple servers really provides the visual of a web or network. Networks provide a flexible environment where clients can mix and match hardware, software, and operating systems.

Client/ Server security mechanism provides authorization methods which ensure that only valid users can access information on client or server machines. The client server security use password, encryption, firewalls etc.

Client-server network uses various authorization methods to make sure that only valid user and programs have access to information resources such as databases.

Access control mechanisms must be set up to ensure that properly authenticated users are allowed access only to those resources that they are entitled to use. Such mechanisms include password protection, encrypted smart cards, biometrics, and firewalls etc.

BSc CsIt SEM - VI
E-Commerce

Client-side security

Client-side security simply refers to the protection of web applications from cyberattacks. One of the most basic examples client-side security is something like an SSL certificate which helps encrypt website communication channels. Unfortunately, SSL certificates don't protect from the dangers of vulnerable or malicious JavaScript, used in all websites. And front-end web applications don't always contain the necessary client-side protection solutions.

Desktops are the front-end system devices, the ones that deal most directly with user input. They are also the least secure environments in client-server models. Clients connect to servers and these connections, if left open or not secured, provide entry points for hackers . Aside from physical client security in the form of disk drive locks or diskless workstations that prohibit the loading of unauthorized software or viruses, accessibility to all files stored on a workstation operating system is the other gaping security hole in clients.

Today's web applications are complex, often made up of a mix of existing software, open-source and third-party code, and custom JavaScript and HTML all integrated via application program interfaces (APIs).

While web applications are hosted and maintained on an organization's server, they actually run on an end user's browser. The scripts that run the applications are referred to as 'client-side scripts.' These scripts create an incredibly dynamic environment that enable a high level of functionality, but also facilitate tremendous risk since the combination of potentially flawed or vulnerable systems, servers, codes, and applications creates the perfect scenario for threat actors to leverage in client-side attacks.

Client-side attack

Client-side attacks occur when a user unintentionally downloads malicious or vulnerable content from a server, often by doing nothing more than simply clicking on a web page and filling out a form. That content could take the form of bad JavaScript code or unsafe third-party code that exists as part of the web application.

The term 'client-side' refers to end-user devices, like desktops, laptops, mobile phones, and tablets, which are considered 'clients.' Conversely, the systems that the devices are connected to are referred to as 'servers.' Client devices send requests to the server and the server responds to the request. Servers usually support multiple client devices at the same time, and client devices usually send requests to multiple different servers while operating on the internet.

Common client-side security risks

1. **Document Object Model (DOM)-based Cross-site Scripting**—Sometimes also called just 'cross-site scripting' or 'XSS', this is a vulnerability that affects websites and enables an attacker to inject their own malicious code onto the HTML pages displayed to users. If the malicious code is executed by the victim's browser, the code performs actions, such as stealing credit card information or sensitive credentials.

2. **JavaScript Injection**—This type of vulnerability is considered a subtype of XSS involving the injection of malicious JavaScript code executed by the end user's browser application. JavaScript injunctions can be used to modify the content seen by the end user, to steal the user's session cookies, or to impersonate the user.
3. **Hypertext Markup Language (HTML) Injection**—Another type of cross-site scripting attack, an HTML injection involves injecting HTML code via vulnerable sections of the website. Usually, the purpose of the HTML injection is to change the website's design or information displayed on the website.
4. **Client-side URL Redirection** or Open Redirection—In this type of attack, an application accepts untrusted input that contains a URL value that causes the web application to redirect the user to another, likely malicious page controlled by the attacker.
5. **Cascading Style Sheets (CSS) Injection**—Attackers inject arbitrary CSS code into a website, which is then rendered in the end user's browser. Depending on the type of CSS payload, the attack could lead to cross-site scripting, user interface (UI) modifications or the exfiltration of sensitive information, like credit card data.
6. **Client-side Resource Manipulation**—This type of vulnerability enables the threat actor to control the URL that links to other resources on the web page, thus enabling cross-site scripting attacks.
7. **Cross-site Flashing—**Because Flash applications are often embedded in browsers, flaws or vulnerabilities in the Flash application could enable cross-site scripting attacks.
8. **Web Messaging**—Also called cross-document messaging, web messaging enables applications running on different domains to communicate securely. If the receiving domain is not configured, problems could arise related to redirection or the website leaking sensitive information to unknown or malicious servers.
9. **Local Storage**—Sometimes called web storage or offline storage, local storage enables JavaScript sites and apps to store and access the data without any expiration date. Thus, data stored in the browser will be available even after closing the browser window. Since the storage can be read using JavaScript, a cross-site scripting attack could extract all the data from the storage. Malicious data could also be loaded via JavaScript.

How to protect from client-side risks and attacks

- Regularly patch and update all software and applications associated with the website.
- Use identification and detection security technology to scan for intrusions, anomalies, and unknown threats.
- Employ ongoing monitoring and inspection with a solution designed specifically to alert to any unauthorized website script activity.
- Be cautious when selecting and implementing third-party scripts.
- Use content security policies to help detect and mitigate some types of attacks.
- Compartmentalize web applications by splitting up front-end applications into smaller components, like public, authenticated, and admin.
- Store sensitive website data appropriately, for example in a unique meta field and keeping API keys hidden from public view.
- Use an SSL certificate for all websites.
- Employ vigilance when it comes to regular inspection, monitoring, and patching.

BSc CsIt SEM - VI
E-Commerce

Server Security

Essentially, server security is the controlling of access to the database server itself. The server must be attached to a stable power supply that provides backup up power if the there's a problem with the supply. This enables the server to shut down in a way that protects data and causes the least amount of damage. They should comply with business standards in password policy to protect database access.

Encryption also protects data through advanced DES (Data Encryption Standard) mechanisms or cryptograms. The degree of encryption depends on government standards. Database servers should not be visible to the world.

To secure the database, the server should be configured to accept only trusted IP addresses. If the database is a backend for a web server, the IP address of the web server should be the only address that can access the database server.

Networks are vulnerable to intruders who 'sniff' or eavesdrop on networks that can contain sensitive company information, passwords, and other potential company weaknesses.
Secure networks should conform to four principles these are:

1) Identification and authorization
2) Discretionary control
3) Audit, and
4) Object re-use.

Identification determines the user's identity.

The user is then authenticated through a password or the completion of a registration form or some other access-controlling barrier. Authentication also ensures the identity stays consistent across time. Authorization defines what the user is allowed to do, what processes users have access to.

Discretionary access control (DAC)

It is a security system that gives users, processes, and devices specified permissions to gain access to system resources in clearly defined ways. Or if an individual user can set an access control mechanism to allow or deny access to an object, that mechanism is known as DAC also known as identity-based access control (IBAC).

Audits

Audits are systematic evaluations of the security of a company's information systems. Audits examine the most secure physical configuration of hardware and software connections, how information is handled, and user practices.

Object reuse

Object reuse takes a storage medium that contains one or more objects. It protects network security by ensuring that all residual data from previous objects is removed before the storage can be re-assigned.

BSc CsIt SEM - VI
E-Commerce

Network Security

Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls etc.

Network Security Protections

Antivirus and Antimalware Software: This software is used for protecting against malware, which includes spyware, ransomware, Trojans, worms, and viruses.This software handles this threat by scanning for malware entry and regularly tracks files afterward to detect anomalies, remove malware, and fix the damage.

Application Security: Any application can comprise vulnerabilities or holes that attackers use to enter your network. Application security thus encompasses the software, hardware, and processes you select for closing those holes.

Behavioral Analytics: To detect abnormal network behavior, you will have to know what normal behavior looks like. Behavioral analytics tools can automatically discern activities that deviate from the norm. Your network security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.
Data Loss Prevention (DLP): Organizations should guarantee that their staff does not send sensitive information outside the network. They should thus use DLP technologies, network security measures that prevent people from uploading, forwarding, or even printing vital information in an unsafe manner.

Email Security: Email gateways are considered the number one threat vector for a security breach. Attackers use social engineering tactics and personal information to build refined phishing campaigns to deceive recipients and then send them to sites serving up malware. An email security application can block incoming attacks and control outbound messages to prevent the loss of sensitive data.

Firewalls: Firewalls place a barrier between your trusted internal network and untrusted outside networks, like the Internet. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and secures all connections when you are online.

Intrusion Prevention System (IPS): An IPS is network security capable of actively scanning network traffic to block attacks. The IPS Setting interface permits the administrator to configure the ruleset updates for Snort. It is possible to schedule the ruleset updates allowing them to run at particular intervals automatically, and these updates can be run manually on demand.

Network Segmentation: Software-defined segmentation places network traffic into varied classifications and makes enforcing security policies a lot easier. The categories are ideally based on endpoint identity, not just IP addresses. Rights can be accessed based on location, role, and more so that the right people get the correct level of access and suspicious devices are thus contained and remediated.

Virtual Private Network (VPN): A VPN is another type of network security capable of encrypting the connection from an endpoint to a network, mainly over the Internet. A Remote VPN Access typically uses IPsec or Secure Sockets Layer to authenticate the communication between web and device.

Web Security: A perfect web security solution will help in controlling your staff's web use, denying access to malicious websites, and blocking

Wireless Security: The mobile office movement is gaining momentum along with wireless networks and access points. However, wireless networks are not as secure as wired ones, which makes way for hackers to enter. It is thus essential for wireless security to be strong. It should be noted that without stringent security measures installing a wireless LAN could be like placing Ethernet ports everywhere. Products specifically designed for protecting a wireless network will have to be used to prevent an exploit from taking place.

Endpoint Security: Endpoint Security, also known as Network Protection or Network Security, is a methodology used for protecting corporate networks when accessed through remote devices such as laptops or several other wireless devices and mobile devices. For instance, Comodo Advanced Endpoint Protection software presents seven defense layers: virus scope, file reputation, auto-sandbox, host intrusion prevention, web URL filtering, firewall, and antivirus software. All this is offered under a single offering to protect them from both unknown and known threats.

Network Access Control (NAC): This network security process helps you control who can access your network. It is essential to recognize each device and user to keep out potential attackers. This, indeed, will help you to enforce your security policies. Noncompliant endpoint devices can be given only limited access or just blocked.

BSc CsIt SEM - VI
E-Commerce

Data Transaction Security

- Many people regularly bank and shop online with ease, confident that the millions of transactions that take place each day are secure.
- Good safeguards are in place, but as the internet is constantly susceptible to new threats, these best practices will help you keep your money and financial information safe
- Online buying presents challenges to keeping your money safe, but if you're smart, they're challenges that aren't too hard to overcome
- Different methods can be used to secure online transactions
    1. Picking a secure password
    2. Two-factor authentication
    1. Use of well-known and secured payment gateway apps.
    3. Use of web browser privacy mode
    4. Keeping the browser up to date
    5. Disable Autocomplete/Password storage in-browser
    6. Passwords - make them complex, change them frequently etc.

Security Mechanisms:

Cryptography

A word cryptography comes from two Greek words meaning "secret writing". The word refers to the science and art of transforming messages to make them secure and immune to attack. **Cryptanalysis** is the breaking of code. The basic component of the cryptography is a **cryptosystem**. Network security is mostly achieved through encryption.

A cryptosystem is a 5-tuple (E, D, M, K, C), where M is the set of plain text, K is the set of keys, C is the set of cipher text, E: M * K = C is a set of enciphering functions and D: C*K = M is the set of deciphering function.

The goal of the cryptography is to keep enciphered information secret. Let us assume that subject wishes to break a cipher text. Standard cryptographic practice is to assume that he knows the algorithm to encipher the plaintext but not the specific cryptographic keys. Three types of attack are possible in cipher text:

- **Cipher text only attack**: here, subject has only the cipher text. His goal is to find corresponding plaintext. If possible, he may try to find the key too.
- **Known plain text attack**: here subject knows the cipher text and the plaintext that was enciphered. His goal is to find the key that was used.
- **Chosen plain text attack**: the subject may ask that specific plain text be enciphered and given the corresponding cipher texts. His goal is to find the key that was used.

Categories of Cryptographic Algorithm:

All the cryptographic algorithm can be classified into two group:

- **Symmetric encryption (secret key or classical cryptosystem or conventional encryption):** here same key is used by sender for encryption and the receiver for decryption. The key is shared.
- **Asymmetric encryption (public key):** here two keys are used private key and public key the private key is given to receiver and used for decryption whereas public key is announced for public and used for encryption. Public key is different from the private key. Here, to send a secret message simply message is enciphered with the recipient and send to the receiver. The receiver deciphers it using his private key.

Hash function:

Hashing is the method of cryptography that convert any form of data into a unique string of text. A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size. A cryptographic hash function is considered practically impossible to invert i.e., to recreate the input data from its hash value alone. In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions

The input data is called message and hash value is often called message digest or simply the digest. Any piece of data can be hashed no matter its size or type. Digital signature, message authentication code (MAC) is application of hash function.

Message digest is the fixed size message generated as a result of hashing of variable length message and key.

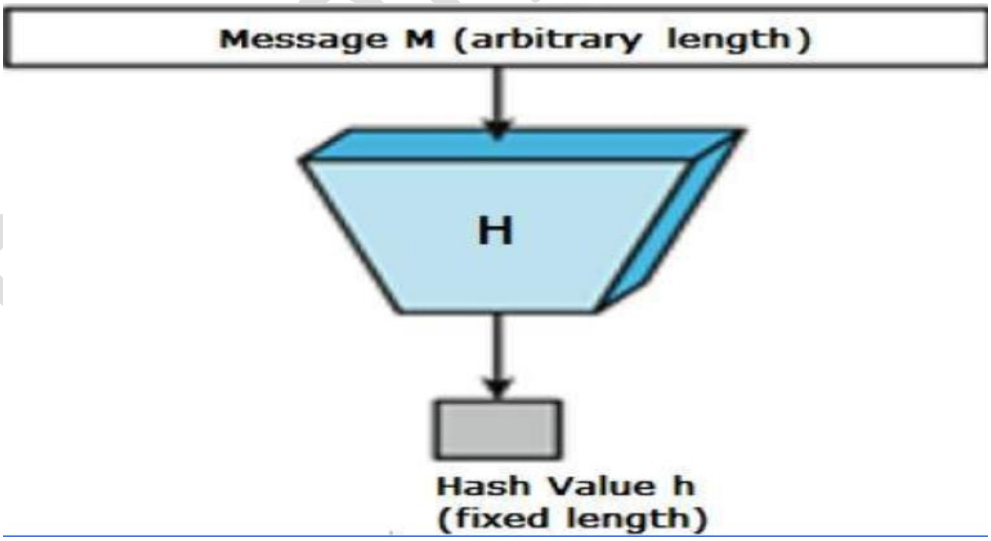


Figure: Hashing

BSc CsIt SEM - VI
E-Commerce

Digital Signature:

A digital signature is a construct that authenticates both the origin and content of a message in a manner that is provable to a disinterested third party. It is an authentication mechanism that enable the creator of a message to attach a code that acts as a signature. The signature is formed by taking hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message. The digital signature standard is an NIST standard (National Institute of Standards and Technology) that uses the secure hash algorithm (SHA).

Following figure 1, shows the working mechanism of digital signature. Here, in order to send the message, first signature is produced my taking the hash of message and private key of sender. Such signature is attached to message and sends to receiver. Receiver receives the message and signature.

In order to verify the message, receiver uses the message, signature and sender's public to compute the hash value using verification algorithm. If signature matches with original signature, then the sender is verifying as original or intended sender.

Figure 2 shows how signature is generated by sender and how it is compared in receiver side. Sender creates the message and in order to generate the signature, the message is converted to hash value using hash function. Such hash value and sender's private key is fed into encryption algorithm. As a result, signature is produced.

At receiver side, receiver receives the message and signature. Hash value of message is computed using has function and signature is decrypt using sender's public key and decryption algorithm. The hash value of message and decrypted signature is compared and if matches signature is valid.

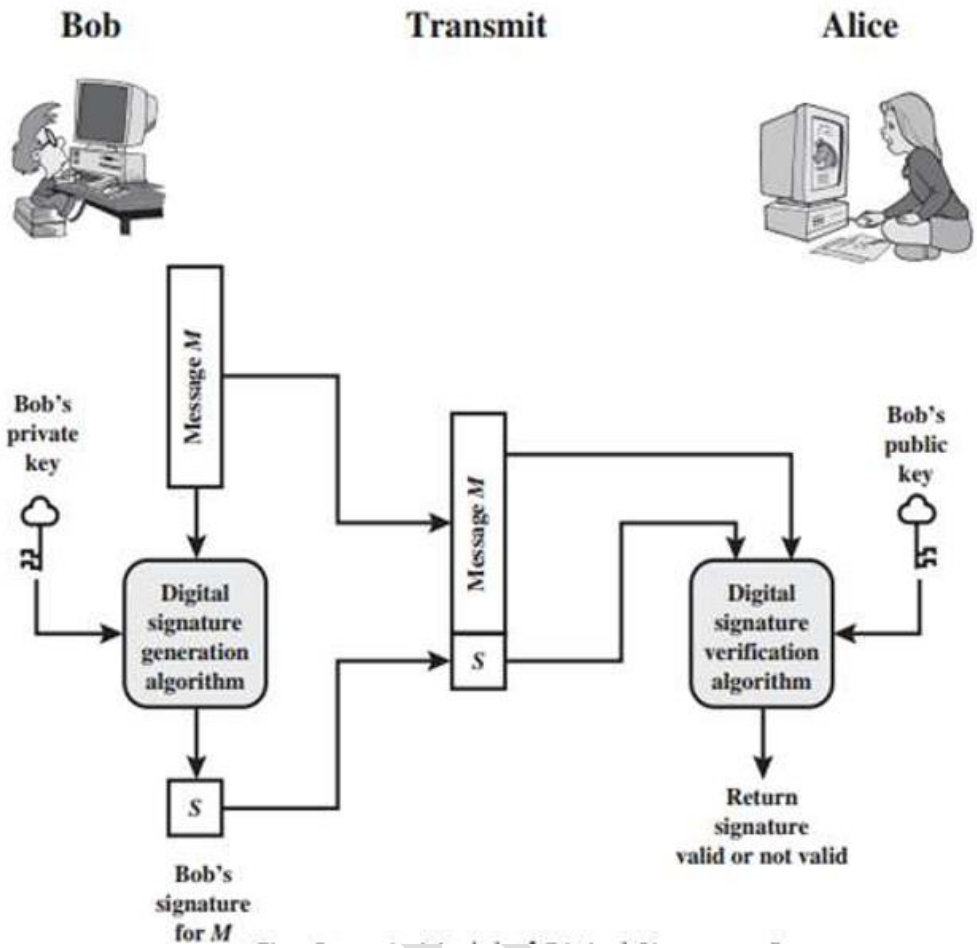


Figure: General process of Digital Signature:

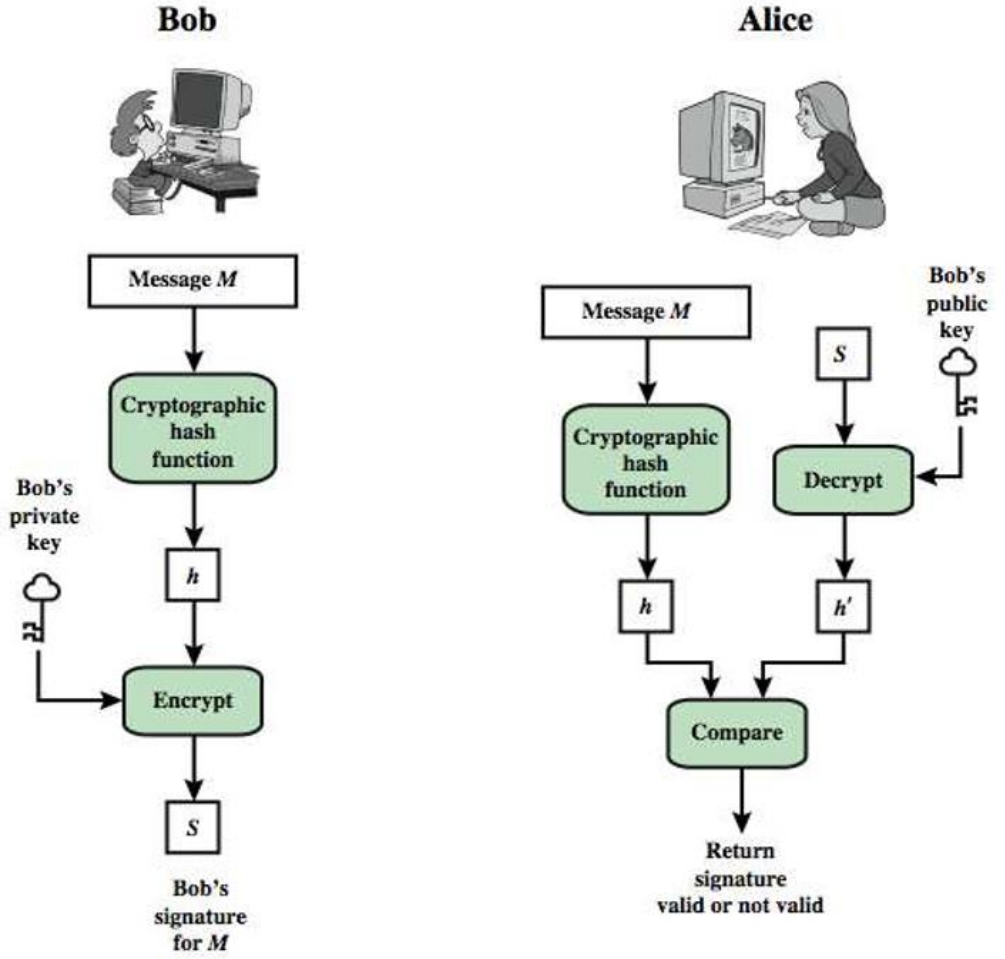


Figure: Essential Elements of Digital Signature Process

Authentication

Authentication is the binding of an identity to a subject. It is the process of determining whether someone or something is, in fact who or what it is declared to be. It is the process of proving or showing something to be true or genuine. Subject act on behalf of some other external entity. The identity of that entity controls the action that its associated subject may take. Therefore, subject must bind to the identity of that external entity.

Basis of authentication:

- What the entity knows (such as password or secret information)
- What the entity has (such as a badge or card)
- What the entity is (such as fingerprint or retinal characteristics)
- Where the entity is (such as in front of a particular terminal)

The authentication process consists of obtaining the authentication information from an entity, analysing the data and determining if it is associate with that entity. That is, computer must store some information about the entity and also suggested that the mechanism for managing the data is also required. These requirement in an authentication system consisting of five components:

i. **Authentication Information**: it is the set of specific information with which entities prove their identity.
ii. **Complementary Information:** it is the set of information that system stores and uses to validate the authentication information.
iii. **Complementary Function:** it generates the complementary information form the authentication information.
iv. **Authentication Function:** use to verify the identity
v. **Selection Function:** enable an entity to create or alter the authentication and complementary information.

Intrusion Detection System

An intrusion is defined as the unauthorized access, misuse or abuse of computer system either by authorized user or by external unauthorized user. That is intrusion detection is unwanted trespass by unauthorized user or software or the action performed by authorized user like reading a file, altering a file etc. for which privilege (access) is not given. If the attacker enters into the system as a non-privileged user, he or she must acquire system privilege to change the file and the technique used to acquire those privilege may involve sequence of command designed to violate the security policy of the system. Software trespass can take a form of virus, worm, Trojan horse etc.

If an attacker modifies a user file, then process executing on behalf of that user now behave in abnormal way such as executing the command that the user did not execute before, executing the files for which he or she don't have access right etc.

Types of Intrusion:

- External attack: attempts break-in, denial of service etc.
- Internal attack: masquerading as some other user, miss use of privilege, malicious attack.
- Clandestine user: exploiting the bugs in privilege program.

Intruder:

An intruder is a person who attempt to gain unauthorized access to a system, to damage the system or to disturb the data in the system. The main goal of this person is to violate the security of the system by interfering with system availability, data integrity or data confidentiality. Intruder are often related to hackers or cracker. Intruder attack range from the benign to serious. At the benign end, the attack may be simply to explore the internet or local system and see what is out there. At the serious end the attack may be attempting to read privileged data, perform unauthorized modification of data or disrupt the system.

Types of Intruder:

- **Masquerader:** an individual who is not unauthorized to use the system but act as authorize user to penetrate a system's access control to exploit a legitimate user's account. A masquerader is likely to be an outsider.

- **Misfeasor**: a legitimate user who accesses data, program or resources for which such access is not authorize or which is authorize for such but misuse privilege. The misfeasor is generally insider.
- **Clandestine User:** an individual who seizes supervisory control of the system and uses this control to evade auditing and access control or to surpass audit collection. The clandestine user can be either outsider or insider.

Some examples of intrusion are:

- Performing a remote root compromise of an email server
- Defacing a web server
- Guessing and cracking password
- Copying a database containing credit cards number.
- Viewing sensitive data, including payroll records and medical information without authorization.
- Running a packet sniffer on a workstation to capture usernames and password
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's email password and learning the new password.
- Using an unattended, logged in workstation without permission

Intrusion Techniques:

The objective of the intruder is to gain access to a system or to increase the range of privilege accessible on a system. Most initial attacks use system or software vulnerabilities that allow a user to execute code that open a back door into the software. The intruder attempts to acquire information that should have been protected and such information can be acquire through the knowledge of some other user's password from which an intruder logs into a system and exercise all the privileges according to the legitimate user.

A system must maintain a file that associates a password with each authorized user. If such file is stored with no any protection, then it will be easy to gain access and learn password. The password file can be protected in one of the two ways:

- **One way function:**

  The system stores only the value of a function based on the user's password. When a user presents a password, the system transforms that password and compare it with the stored value. Generally, system only performs one way transformation (not reversible) in which the password is used to generate a key for the one-way function and in which a fixed length output is produced.

- **Access control:**

  Access to the password file is limited to one or very few accounts.

If one or both of these countermeasures are in place some effort is needed for a potential intruder to learn passwords.

Techniques for learning password based on different survey and interviews with a number of password cracker are:

- Try default password used with standard account that are shipped with the system.
- Exhaustively trying all short password like of two or three characters.
- Try word in the system's online dictionary or a list of likely passwords
- Collect information about users such as their full name, name of spouse and children, pictures in their office and books in their office that are related to hobbies.
- Try users' phone number, social security number and room number.
- Try all legitimate license plate number for particular state.
- Use a Trojan horse to bypass restriction on access
- Tap the line between a remote user and the host system.

Overview of Intrusion Detection System (IDS):

Computer system that are not under attack exhibits several characteristics:

- The action of the users and processes generally conform to a statistically predictable pattern. For example, a user who use only word processing when using a computer is unlikely to perform a system maintenance function.
- The action of the users and processes do not include sequence of command to subvert the security policy of the system. In practice only sequences known to subvert the system can be detected.
- The action of the process conforms to a set of specifications describing actions that the processes are allowed to do.

The system that are under attack fail to meet at least one of these characteristics.

Intrusion Detection System (IDS):

Intrusion detection system is a system use to detect unauthorized intrusion into computer system and network. This system is not new, it has been user for a generation to defend valuable resources. IDS is based on the assumption that the behaviour of the intruder differ from that of a legitimate user in a way that can be quantified.

Goals of intrusion detection:

- Detecting a wide variety of intrusion like intrusion from within the site as well as those from outside the site, both known and previously unknown attacks should be detected. This suggest a mechanism for learning or adapting to new types of attacks or to changes in normal user activity.
- Detecting an intrusion in a timely fashion. It suffices to discover an intrusion within a short period of time so that the damage from any intrusion can be reduced.
- Present the analysis in a simple, easy to understand format.
- Be accurate:
  A false positive occur when an intrusion detection system reports an attack but no attack is underway. This will reduce the confidence in the correctness of the results as well as increase the amount of work involved.
  However, the false negative occurring when an intrusion detection system fails to report an ongoing attack are worse because the purpose of the IDS is to report attacks. The goal of the intrusion detection system is to minimize both type of error.

BSc CsIt SEM - VI
E-Commerce

Intrusion Detection Model:

Intrusion detection system determines if action constitute intrusion or not on the basis of one or more models of intrusion. A model classifies a sequence of action or state or a characterization of state or action as "good" (no intrusion) or "bad" (possible intrusion). Some of the models are:

1. **Anomaly Modeling:**
   This model uses a statistical characterization and action or state that are statistically unusual are classified as bad. Anomaly detection uses the assumption that unexpected behavior is evidence of an intrusion. Anomaly detection analyzes a set of characteristics of the system and compares their behavior with a set of expected value. Expected behavior can be characterize by some set of metrics like threshold metric, statistical moments etc.
2. **Misuse Modeling:**
   This model compares action or states with known sequence to indicate intrusion and classified those sequence as bad. In the context of intrusion detection system, when the attack is done by insider or authorize user it means "rule base detection". Misuse detection determines whether a sequence of instruction being executed is known to violate the site security policy being executed. If so, it reports a potential intrusion.
   Modeling of misuse requires a knowledge of system vulnerabilities or potential vulnerabilities that attacker attempts to exploit. The IDS incorporates this knowledge into rule set.
   Working mechanism:
   - When a data is passed to the IDS, it applies the set of rule on data to determine if any sequence of data match any of the rule.
   - If so it reports that a possible intrusion is underway.

   Misuse based IDS often use expert system to analyze the data and apply the set of rule set. These system cannot detect attacks that are unknown to rule set's developer. Previous unknown attack or variation of known attack are difficult to detect using expert system. Later, IDS used adaptive method involving neural network to improve their detection abilities.
3. **Specification Modeling:**
   Specification based model classify states that violate the specification as bad. Specification based detection determines whether or not a sequence of instruction violated a specification of how a program or system should execute. If so, it reports a potential intrusion. For security purpose only those programs that in some way change the protection state of the system need to be specified and checked.

Architecture of Intrusion Detection System (IDS):

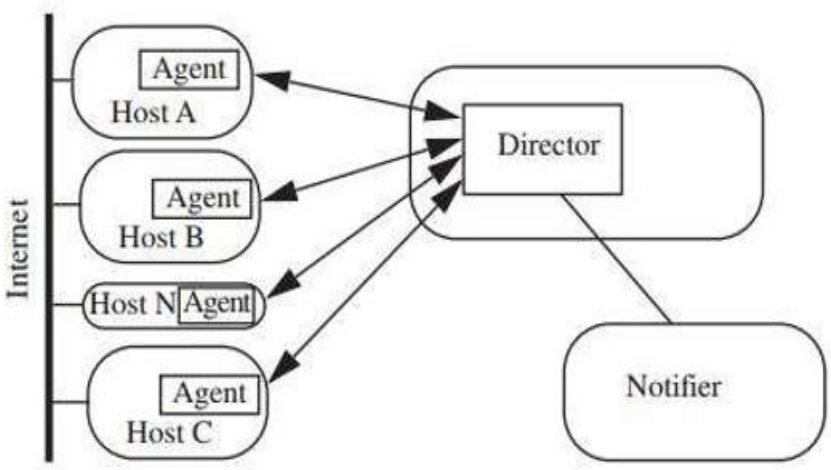


Figure: Architecture of Intrusion Detection System (IDS):

An intrusion detection system is an automated auditing mechanism and consists of three parts:

1) **Agent:**

Agent corresponds to logger and acquires the information from the target such as computer system, network etc. An agent obtain information from a data source or set of data source and source may be a log file, another process, network etc. the agent may also discard information that it deems irrelevant. An agent can obtain information from a single host, from set of hosts or from network. The main goal of the agent is to monitor the overall system and network for any suspicious activity. For example: if the agent is to transmit the time and location of fail login attempt, it will scan the appropriate log file, discard any records of successful logins and send the remainder to the director.

Agent can gather the information from following approach:

- **Host Based Information Gathering:**

  Host based agents usually uses system and application logs to obtain records of events and analyze them to determine what to pass to the director. The logs may be security related logs or other logs such as accounting logs.

  In another variation, agents generates its own information. They analyze the state of the system or some object in the system and treat the result as log.

- **Network Based Information Gathering:**

  Network based agent use a variety of devices and software to monitor network traffic. This technique provides different information than host based. It can detect network oriented attack such as denial of service, flooding etc. it can monitor traffic for a large number of host and can also examine the content of the traffic itself called content monitoring.

  Network based agent may use network sniffing to read the network traffic. In this case, system provide the agent access to all the network traffic passing that host. If the medium is point to point the agent must be distributed to obtain a complete view of the network message. If the medium is broadcast then only one computer needs to have the monitoring agent.

- **Combining Sources:**

  The goal of this agent is to provide the director with information so that the director can report possible violation of the security policy (intrusion). An

aggregate of information is needed and the information can be viewed at several levels.

2) **Director (Analyzer):**
The director itself reduces the incoming log entries to eliminate unnecessary and redundant records. It then uses an analysis engine to determine if an attack is underway. The analysis engine may use any of several techniques to perform its analysis.
The function of the director is critical so it is run on separate system. Due to this attacker lacks the knowledge to evade IDS by conforming to known profiles or using only techniques that the rule do not include. The director must correlated information from multiple logs.

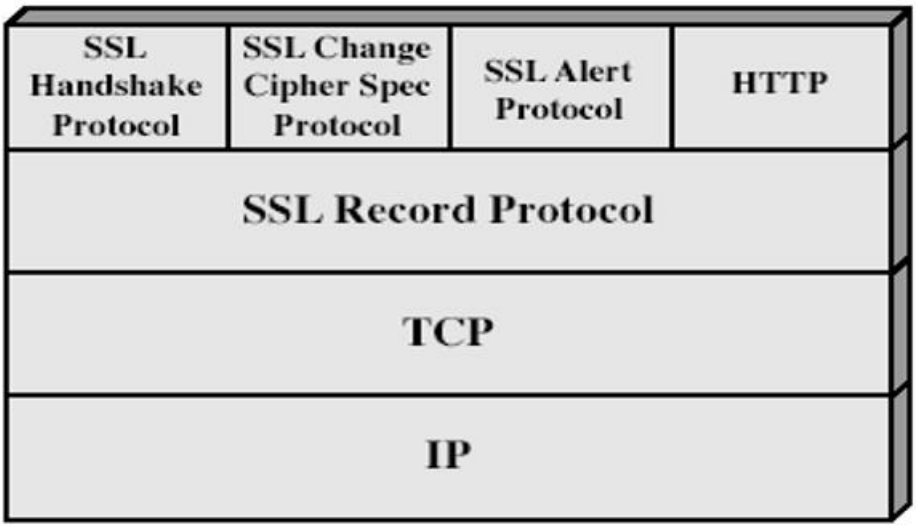
3) **Notifier:**
The notifier accepts information from the director and takes the appropriate action. In some case this is simply a notification to the system security officer that an attack is believed to be underway and in some case the notifier may take some action to responds to the attack. Some IDS may use graphical user interface which allows the intrusion detection system to convey information in an easy to grasp image or set of image.

Secure Socket Layer (SSL):

Secure Socket Layer (SSL) which is developed by Netscape, is a standard protocol used for the secure transmission of document over network. It is a standard security technology for establishing an encrypted link between a web server and a browser i.e. it creates a secure link between a web server and browser to ensure private and integral data transmission. SSL uses cryptographic system that uses two keys to encrypt data: a public key known to everyone and a private key or secrete key known only to the recipient of message.
SSL v3, design with public input became internet standard known as Transport Layer Security. It uses underlying protocol i.e. TCP to provide a reliable end to end service.

SSL Architecture:
SSL is designed to provide security and compression services to data generated from the application. The data received from the application layer is compressed, signed and encrypted and then passed to reliable transport layer protocol i.e. TCP. Some of the services provided by SSL are:

- **Data confidentiality**: to provide confidentiality, original data and the MAC are encrypted using symmetric key cryptography.
- **Data integrity:** to preserve the integrity of the data, SSL uses the key hash function to create a MAC.
- Peer entity authentication
- Compression /decomposition
- **Fragmentation:** SSL divides the data into block of 2^{14} bytes or less.
- **Framing**: a header is added to the encrypted payload. The payload is then passed to a reliable transport layer protocol.
- Generation/ distribution of session keys
- Security parameter negotiation



SSL provides two layer of protocol:

- **SSL Record Protocol**: provide basic security service to various higher layer protocol. HTTP, a higher layer protocol can operate on the top of the protocol.
- **Higher Layer Protocol:** includes handshake protocol, change cipher spec protocol, alert protocol and HTTP. These protocol are used in management of SSL exchange.

SSL Session and Connection:

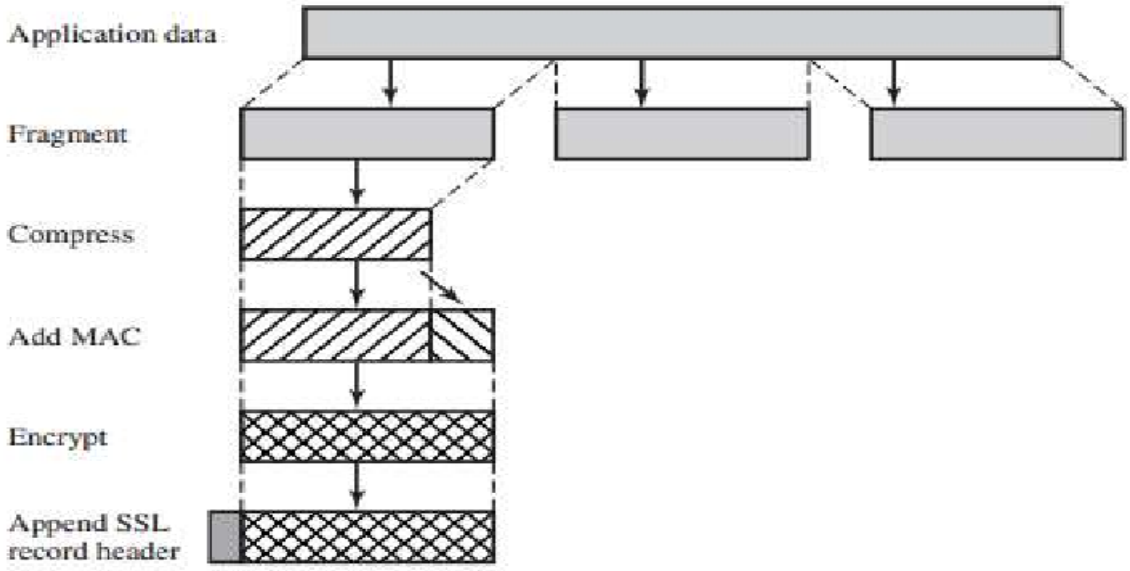
A session is an association between a client and a server. After a session is established two parties have common information such as the session identifier, the certificate authenticating each of them, the compression method, cipher suite and a master secret that is used to create keys for message authentication encryption. It may be shared by multiple connection.

A connection is a transport that provides a suitable types of service. For SSL such type of connection are peer to peer relation. Connection are transient and every SSL connection is associated with one SSL connection.

SSL Record Protocol:

Record protocol is the carrier and carries message from three other protocol as well as the data coming from the application layer. Message from the record protocol are payloads to the transport layer. The message is fragmented and optionally compressed, a MAC is added to the compressed message using negotiated hash algorithm then the compressed fragment and the MAC are encrypted using the negotiated encryption algorithm. Finally, SSL header is added to the encrypted message.

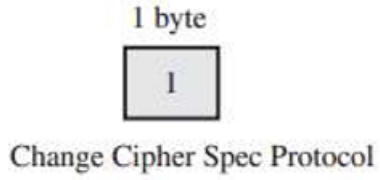
Integrity is provided using MAC and confidentiality using symmetric encryption.



SSL Change Cipher Spec Protocol:

This protocol uses record protocol and used for signaling the readiness of cryptographic secrets. It have two state: one state consists of pending state which keeps track of parameter and secrets. Another state known as active state holds the parameter and secret used by record protocol to sign/verifies or encrypt/decrypt message.

Consist of single value with message 1. It keeps the track of the parameter and secrets and causes the pending state to become current hence updating the cipher suit in use.

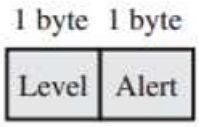


Change Cipher Spec Protocol

SSL Alert Protocol:

This protocol is used for reporting errors and abnormal conditions. It uses only one message that describes the problem and its level i.e. warning or fatal. Each message consist of two byte:

- First byte: takes the value warning or fatal
- Second byte: contains a code that indicates the specific alert.



Alert Protocol

========== End of Unit-5 ==========

BSc CsIt SEM - VI
E-Commerce

Unit 5: Security in E-Commerce (7 Hrs.)

E-commerce Security, Dimensions of E-commerce Security: Confidentiality, Integrity, Availability, Authenticity, Nonrepudiation, Privacy, Security Threats in E-commerce: Vulnerabilities in E-commerce, Malicious Code, Adware, Spyware, Social Engineering, 2 Phishing, Hacking, Credit card fraud and Identity theft, Spoofing and Pharming, Client and Server Security, Data Transaction Security, Security Mechanisms: Cryptography, Hash Functions, Digital Signatures, Authentication, Access Controls, Intrusion Detection System, Secured Socket Layer(SSL)