Module 5: Lecture Guide Part II

Overview:

Today's online firms must effectively manage significant security concerns. Most internet businesses develop a written security policy document that lists hazards and the preventative steps that can bring those risks down to a manageable level. Secrecy, integrity, and necessity are components of online security. Each of these three components—client devices, communication channels, and Web server computers—is required for online commercial transactions.

The usage and preservation of intellectual property provide significant difficulties for online firms. These companies must exercise caution to avoid trademark, copyright, or patent infringement as well as defamation, privacy invasion, and publicity rights violations. a global administrative procedure that effectively does away with the necessity for court action to resolve domain name disputes. Online businesses must refrain from indicating relationships that do not exist and giving bad evaluations of entities, even when they are true, given the subjective nature of defamation and product disparagement.

The principal communication route for online commerce, the Internet, is particularly open to threats. When using private keys, public keys, or a combination of methods, encryption can defend against many of these threats by maintaining secrecy and integrity. Digital certificates offer user authentication and integrity, enabling nonrepudiation in online transactions. Secure connections to Web browsers can be provided via specific Internet protocols. A safe type of wireless encryption can lessen the potential of signal eavesdropping that wireless networks are vulnerable to. The usage of mobile devices in online commerce is growing, which exposes communications to new dangers.

Both physical dangers and software attacks from the Internet must be kept at bay on web servers. Access control and authentication, which are supplied via username and password login processes and client certificates, are two server protection techniques. The Internet and other portions of an organization's corporate network system are examples of untrusted outside networks that can be divided using firewalls.

To exchange knowledge about threats to and countermeasures for computer security, several organizations have been established. These groups can help locate and get rid of the threat when large security outbreaks happen. Companies that perform computer attacks on behalf of their clients' machines can be extremely helpful in identifying security flaws.

Computer Security and Risk Management

Protecting assets from unauthorized access, use, change, or destruction is the goal of computer security. Physical security and logical security are the two main categories. Alarms, guards, fireproof doors, security fences, safes or vaults, and bombproof structures are examples of

tangible security measures. Logical security is the safeguarding of assets through means other than physical ones. Threats include any actions or things that endanger computer assets. A countermeasure is a method for identifying, lessening, or getting rid of a threat. Depending on the value of the asset at danger, the scope and cost of countermeasures can change.

When the expense of defending against a threat is greater than the value of the asset being safeguarded, threats that are unlikely to materialize can be ignored. In Miami, for instance, where there is large and frequent hurricane activity, it would make sense to safeguard a computer network from hurricanes. However, since hurricanes cannot occur in Denver, a network of a similar nature there would not need to be protected in the same way.

Protecting Internet and electronic commerce assets from physical and digital dangers requires the same type of risk management methodology. The latter group includes forgers, listeners, and thieves. In this sense, an eavesdropper is a person or object that can listen in on and copy Internet transmissions. Crackers and hackers are individuals who create programs or exploit technologies to gain unauthorized access to computers and networks.

A cracker is an individual with technological prowess who employs that prowess to gain illegal access to computer systems or network systems, typically with the goal of stealing information or causing damage to the data, the system's software, or even the system's hardware. The term "hacker" originally referred to a committed programmer who delighted in creating challenging code that pushed the boundaries of technology. Even though computer experts still distinguish between the term’s "hacker" and "cracker," the term "hacker" is typically used negatively by the media and the public to denote people who misuse their skills. To distinguish between good hackers and evil hackers, some people sometimes use the terms "white hat hacker" and "black hat hacker."

Organizations must evaluate risks, decide how to safeguard threatened assets, and estimate how much it will cost to do so to adopt an effective security plan.

Access to data may be restricted or delayed because of necessity violations. An online attacker could, for instance, delay a transmission conveying a buy order for stock. The sender forfeits the value of any stock price increases that occur during the delay. Other necessary violations include things like flooding a company's website with automated false customer enquiries so that actual customers cannot access the site.

Elements of Computer Security

Secrecy, integrity, and need are the three essential components of computer security (also known as denial of service). When we talk about secrecy, we mean preventing illegal data dissemination and confirming the reliability of the data source. Integrity is the absence of unapproved data alteration. Preventing data delays or denials is referred to as need (removal). Integrity hazards are less commonly reported and less widely understood in society. When an email message is intercepted and its contents are altered before it is forwarded to its intended

recipient, for instance, an integrity violation has taken place. In other words, the message's integrity has been compromised. In this specific attack, also known as a man-in-the-middle attack, the email's contents are frequently changed in a way that alters the message's original meaning.

Establishing a Security Policy

Every firm should have a security policy in place if it is serious about safeguarding its electronic commerce assets. A security policy is a written document that specifies which assets should be safeguarded, why, who oversees that protection, and what behaviors are acceptable and unacceptable. Physical security, network security, access authorizations, virus protection, and disaster recovery should all be included in a security policy. It should also be a live document that is frequently reviewed and updated.

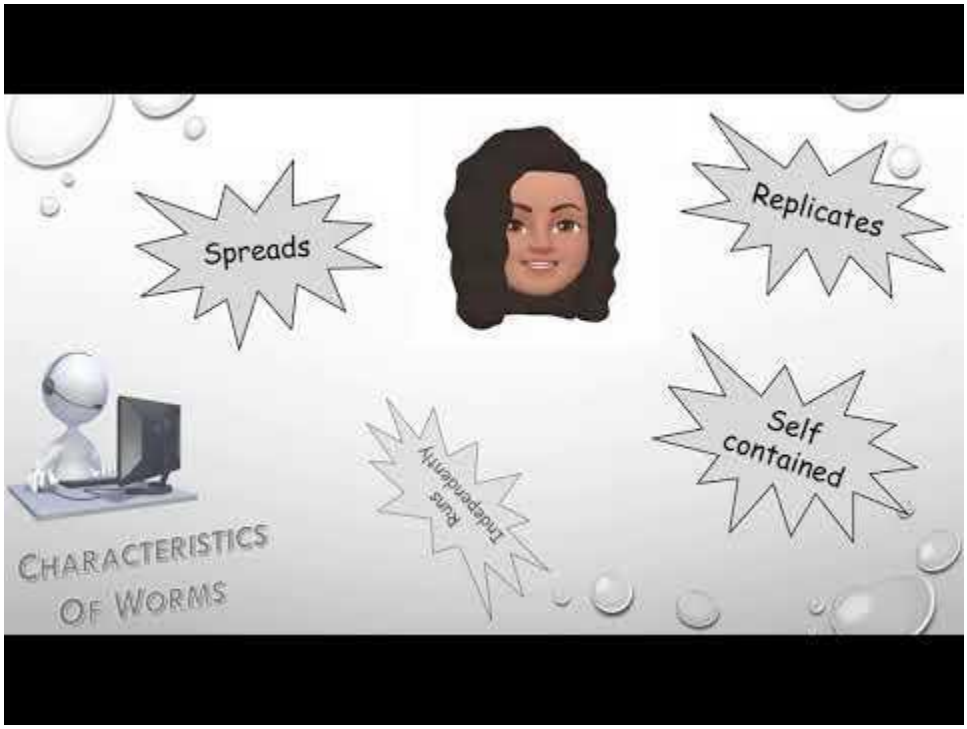
Assets must be safeguarded by organizations against illegal disclosure, modification, or destruction. A corporation's confidentiality policy could be as straightforward as "do not disclose sensitive company information to anyone outside the company." Most firms create security policies using a four-step procedure. These actions comprise: Decide which assets need to be protected and from what dangers. Determine who requires access to certain system components or information assets. It is possible that some of those users are situated outside the company (for example, suppliers, customers, and strategic partners). Determine the resources that are available or required to safeguard information assets while guaranteeing that those who require access may get it. The business creates a written security policy using the data acquired in the first three processes.

The organization commits resources to developing or purchasing the software, hardware, and physical barriers necessary to implement the security policy after it has been created and accepted by management. A thorough security strategy should authenticate users while safeguarding the privacy, integrity, and availability (necessity) of a system. These objectives should be chosen to fulfill the requirements while creating a security policy for an electronic commerce activity.

Security for Client Devices Client

Threats that come from software and data that have been downloaded from the Internet must be kept out of reach for computers, cellphones, and tablet devices. Active content downloaded by clients may be dangerous. Servers that pose as trustworthy websites may pose a threat to

client devices. These dangers are described in the video below.



Client Security for Mobile Devices

Concern over the security of mobile devices, including smartphones and tablets, rises proportionally as more people use them to access the Internet. Simple security concerns pertaining to mobile client devices can include the real possibility of losing a phone or tablet. They can also be more sophisticated, such as a virus, a Trojan horse assault, or an app that distributes your personal data.

Creating an access password for the phone is the first step in safeguarding a mobile device. This can stop a thief from getting access to any confidential information you have stored on your device, or at the very least postpone it.

A remote wipe feature is built into most mobile devices, allowing the owner to initiate it in the event of theft. When you perform a remote wipe, all your emails, texts, contacts, photos, videos, and document files are deleted. If a mobile device does not already have remote wipe software, it can be downloaded as an app. The majority of corporate email servers support remote device wiping via email synchronization software installed on employee mobile devices.

Mobile devices can be infected by malicious websites just as easily as client computers are. Smartphones and tablet computers can be infected by text messages and emails that have viruses and Trojan horses attached. As a result, more users are downloading antivirus software for their mobile devices.

Rogue apps are those that have malware or that gather data from a user's mobile device and transmit it to the perpetrators. Before approving them for sale, the Apple App Store checks

programs to screen out malicious ones. Although the Android Market does not provide as thorough a screening for malicious apps as Apple does, all Android apps must ask the user's permission before they may access any data saved on the device. When a user installs the program, it will ask for these permissions. Mobile device users are advised by experts to study app reviews before installing them and to take their time installing new apps with few reviews to prevent downloading malicious Android apps. Additionally, they advise staying away from app stores other than the Android Market.

Communication Channel Security

Between buyers (in most cases, clients) and sellers, there is an electronic link made through the Internet (in most cases, servers). The most crucial thing to keep in mind while you study communication channel security is that the Internet was not created with security in mind. Although a military network served as the foundation for the Internet, no significant security measures were included into that network. If one or more communications lines were interrupted, it was made to offer redundancy. To put it another way, the packet-switching architecture of the Internet was intended to offer a variety of different routes for the transmission of vital military information. To ensure that the contents of messages going over any network, even if they are intercepted, remain secret, the military always sends sensitive information in an encrypted form. Software that worked independently of the network to encrypt messages provided the security of messages traveling via the military forerunners to the Internet. The Internet did not have any substantial security mechanisms that were included into the network as it grew.

The Internet as it exists today is unaltered from its unsecure beginnings. Internet message packets take an unforeseen route from a source node to a destination node. Before getting to its destination, a packet travels via a few intermediate computers on the network. Every time a packet is sent between the same source and destination sites, the path may change. Any message going on the Internet is exposed to risks to confidentiality, integrity, and necessity because users cannot control the path and are unaware of the location of their packets, making it possible for an intermediate to read, edit, or even delete them. This section goes into further detail about these issues and offers numerous remedies.

Secrecy Threats Secrecy

Is the security risk that is referenced the most frequently in articles and the mainstream media. Privacy is closely related to secrecy and is also given a lot of attention. Despite similarities, privacy and secrecy are two distinct problems. The goal of secrecy is to stop unlawful information dissemination. Privacy is the defense of each person's right to confidentiality. A comprehensive Web site dedicated to privacy has been developed by the Privacy Council, which assists organizations in implementing sensible privacy and data practices. This site covers both business and legal concerns. While privacy protection is a legal problem, secrecy is a technical challenge needing complex physical and logical procedures. E-mail is a prime illustration of the distinction between secrecy and privacy.

Integrity Threats

When an unauthorized entity can change a message stream of data, this is characterized as an integrity threat, also referred to as active eavesdropping. Integrity violations can occur in unprotected banking transactions, such as deposit amounts sent via the Internet. Naturally, when information is altered, it can be viewed and interpreted by an outsider, resulting in an integrity violation. Integrity risks, in contrast to secrecy threats, can result in a change in the activities a person or organization does because a transmission that is crucial to the purpose has been altered.

Necessity Threats

The goal of a necessity threat, which typically manifests as a delay, denial, or denial-of-service (DoS) attack, is to obstruct or completely prevent normal computer processing. For instance, if a website's response time is slowed down, customers may visit rival sites instead and may never go back. The first known instance of a DoS attack was the Internet Worm attack in 1998, which rendered thousands of Internet-connected computer systems inoperable.

Threats to the Physical Security of Internet Communications Channels

From the beginning, the Internet was built to survive intrusions on its physical communication cables.

The packet-based network architecture of the Internet prevents it from being brought down by an attack on a single communications link. Despite this security measure, as few individual users have numerous connections to an ISP, an individual user's Internet access could be disrupted by the loss of that user's connection to the Internet. Larger businesses and organizations, as well as ISPs, frequently have several connections to the Internet backbone, each one going through a different access provider. To keep the firm, organization, or ISP (and its clients) connected to the Internet, the service provider might switch traffic to another network access provider's link if one link becomes overcrowded or unavailable.

Threats to Wireless Networks

If left unprotected, a wireless network enables access to any resources connected to it by allowing anyone nearby to log in and use them. Any information saved on any networked computer, networked printers, communications sent over the network, and, if the network is connected to the Internet, unrestricted access to the Internet are examples of such resources. The Wireless Encryption Protocol (WEP), which is a set of guidelines for encrypting signals from the wireless devices to the WAPs, is what determines the security of the connection. Large wireless network operators are typically careful to turn on WEP in devices, but smaller operators and homeowners who have built wireless networks in their homes frequently forget to do so.

Many WAPs are delivered to customers with a pre-configured default login and password. Sometimes the businesses who deploy these WAPs forget to update the login and password. This has created a fresh way to access networks. Attackers use their Wi-Fi-equipped laptop computers to drive around in some cities with high concentrations of wireless networks looking for accessible networks. Wardrivers are the name for these attackers. Wardrivers occasionally leave a chalk mark on the structure when they locate an open network (or a WAP with a widely used default login and password) to let other attackers know that an accessible wireless network is nearby. Warchalking is the term for this technique. A few warchalkers have built websites with maps of wireless access points in significant cities around the globe. By simply turning on WEP in their access points and altering the logins and passwords from the manufacturers' default values, businesses may avoid becoming targets.

What better spokesperson to discuss how to lessen the concerns described above than Mayim Bialik, a.k.a. Blossom, the new Jeopardy host? Mayim outlines 5 tips for cyber security safety in this video.