CHAPTER TEN

Electronic Commerce Security

Instructor: Wuman Luo

luowuman@ipm.edu.mo Office: A323

Introduction

- Proper use of password protection is an important element in maintaining security
  - Most people unwilling to remember numerous complex passwords and change them often
- Password management tools are popular solutions for maintaining multiple complex passwords
  - The user simply needs to remember one master password
  - Weak link: when hackers access master passwords, it opens the door to every single password and login stored in the password manager
    - Encryption is an important safeguard to help address attacks

Online Security Issues Overview

- Individuals and businesses have had concerns about security since Internet became a business communications tool
  - Increasing with steady increase in sales and all types of financial transactions
- Chapter topics
  - Key security problems
  - Solutions to those problems

Computer Security and Risk Management

- **Computer security**: asset protection from unauthorized access, use, alteration, and destruction
  - Physical security includes tangible protection devices
    - Alarms, guards, fireproof doors, security fences, safes or vaults, and bombproof buildings
  - Logical security is protection using nonphysical means
    - Threat is anything posing danger to computer assets
  - Countermeasures are procedures (physical or logical) that recognizes, reduces, and eliminates threats
    - Extent and expense depends on importance of asset at risk

Elements of Computer Security

- Secrecy refers to protecting against unauthorized data disclosure and ensuring data source authenticity
- Integrity is preventing unauthorized data modification
  - Integrity violation occurs when an e-mail message is intercepted and changed before reaching destination
    - Man-in-the-middle exploit
- Necessity refers to preventing data delays or denials (removal)

Establishing a Security Policy

- Is a written statement of: assets to protect and why, who is responsible for protection and acceptable and unacceptable behaviors
  - Addresses physical and network security, access authorizations, virus protection, disaster recovery
- Steps to create security policy
  - Determine which assets to protect from which threats
  - Determine access needs to various system parts
  - Identify resources to protect assets
  - Develop written security policy

Establishing a Security Policy (cont'd.)

- Once policy is written and approved resources are committed to implement the policy
- Comprehensive security plan protects system's privacy, integrity, availability and authenticates users
  - Selected to satisfy Figure 10-2 requirements
  - Provides a minimum level of acceptable security
- All security measures must work together to prevent unauthorized disclosure, destruction, or modification of assets

Requirement	Meaning
Secrecy	Prevent unauthorized persons from reading messages and business plans, obtaining credit card numbers, or deriving other confidential information.
Integrity	Enclose information in a digital envelope so that the computer can automatically detect messages that have been altered in transit.
Availability	Provide delivery assurance for each message segment so that messages or message segments cannot be lost undetectably.
Key management	Provide secure distribution and management of keys needed to provide secure communications.
Nonrepudiation	Provide undeniable, end-to-end proof of each message's origin and recipient.
Authentication	Securely identify clients and servers with digital signatures and certificates.

FIGURE 10-2 Requirements for secure electronic commerce

Establishing a Security Policy (cont'd.)

- Security policy points
  - Authentication: Who is trying to access site?
  - Access control: Who is allowed to log on to and access site?
  - Secrecy: Who is permitted to view selected information?
  - Data integrity: Who is allowed to change data?
  - Audit: Who or what causes specific events to occur, and when?

Security for Client Devices

- Threats to computers, smartphones, and tablets
  - Originate in software and downloaded Internet data
  - Malevolent server site masquerades as legitimate Web site

Cookies and Web Bugs

- Internet connection between Web clients and servers accomplished by multiple independent transmissions
  - No continuous connection (open session) maintained between any client and server
- **Cookies** are small text files Web servers place on Web client to identify returning visitors
  - Allow shopping cart and payment processing functions without creating an open session
  - Session cookies exist until client connection ends
  - Persistent cookies remain indefinitely
  - Electronic commerce sites use both

Cookies and Web Bugs (cont'd.)

- Cookies may be categorized by their source
  - First-party cookies are placed on client computer by the Web server site
  - Third-party cookies originate on a Web site other than the site being visited
- Disable cookies entirely for complete protection
  - Useful cookies blocked (along with others) so that information is not stored
  - Full site resources not available if cookies are not allowed

Cookies and Web Bugs (cont'd.)

- Most Web browsers have settings that allow the user to refuse only third-party cookies or review each cookie before allowing
- Web bug or Web beacon is a tiny graphic that third-party Web site places on another site's Web page
  - Provides method for third-party site to place cookie on visitor's computer
  - Also called "clear GIFs" or "1-by-1 GIFs" because graphics created in GIF format with a color value of "transparent" and as small as 1 pixel by 1 pixel

Active Content

- Active content programs run when client device loads Web page
  - Example actions: play audio, display moving graphics, place items into shopping cart
  - Moves processing work from server to client device but can pose a threat to client device
- Methods to deliver active content
  - Cookies, Java applets, JavaScript, VBScript, ActiveX controls, graphics, Web browser plug-ins, e-mail attachments

Active Content (cont'd.)

- Scripting languages provide executable script
  - Examples: JavaScript and VBScript
- Applets are small application programs that typically runs within Web browser
- Most browsers include tools limiting applets' and scripting language actions by running in a sandbox
- ActiveX controls are objects containing programs or properties placed on Web pages to perform tasks
  - Run only on Windows operating systems
  - Give full access to client system resources

Active Content (cont'd.)

- Crackers can embed malicious active content
  - Trojan horse is a program hidden inside another program or Web page that masks its true purpose
  - May result in secrecy and integrity violations
  - Zombie secretly takes over another computer to launch attacks on other computers
    - Botnet (robotic network, zombie farm) is all controlled computers act as an attacking unit

Graphics and Plug-Ins

- Graphics, browser plug-ins, and e-mail attachments can harbor executable content
  - Embedded code can harm client computer
- Browser plug-ins (programs) enhance browser capabilities bit can pose security threats
  - Plug-ins executing commands buried within media

Viruses, Worms, and Antivirus Software

- Programs automatically execute associated programs to display e-mail attachments
  - Macro viruses in attached files can cause damage
- Virus is software that attaches itself to host program and causes damage when program is activated
  - Worm is a virus that replicates itself on computers it infects and spreads quickly through the Internet
  - Macro virus is a small program embedded in file
- First major virus was I LOVE YOU in 2000
  - Spread to 40 million computers in 20 countries and caused estimated $9 billion in damages

FIGURE 10-4
Early computer viruses, worms, and Trojan horses

Year	Name	Type	Description
1986	Brain	Virus	Written in Pakistan, this virus infected floppy disks used in personal computers at that time. It consumed empty space on the disks, preventing it from being used to store data or programs.
1988	Internet Worm	Worm	Robert Morris, Jr., a graduate student at Cornell University, wrote this experimental, self-replicating, self-propagating program and released it onto the Internet. It replicated faster than he had anticipated and crashed computers at universities, military sites, and medical research facilities throughout the world.
1991	Tequila	Virus	Tequila writes itself to a computer's hard disk and runs any time the computer is started. It also infects programs when they are executed. Tequila originated in Switzerland and was mostly transmitted via Internet downloads.
1992	Michaelangelo	Trojan Horse	Set to activate on March 6 (Michaelangelo's birthday), this Trojan Horse would overwrite large portions of the infected computer's hard disk.
1993	SatanBug	Virus	Infects programs when they run, causing them to fail or perform incorrectly. SatanBug was designed to interfere with antivirus programs so they could not detect it.
1996	Concept	Virus Worm	One of the first viruses to be written in Microsoft Word's macro language, Concept travels with infected Word document files. When an infected document is opened, Concept places macros in Word's default document template, which infects any new Word documents created on that computer.
1999	Melissa	Virus Worm	A Microsoft Word macro virus that spreads by e-mailing itself automatically from one user to another. It inserts comments from "The Simpsons" television show and confidential information from the infected computer. Melissa spread throughout the world in a few hours. Many large companies were inundated by Melissa. For example, Microsoft closed down its e-mail servers to prevent the spread of this virus within the company.

FIGURE 10-5 Computer viruses, worms, and Trojan horses: 2000-2007

Year	Name	Type	Description
2000	ILOVEYOU	Virus Worm	Arrives attached to an e-mail message with the subject line "ILOVE YOU" and infects any computer on which the attachment is opened. It sends itself to addresses in any Microsoft Outlook address book it finds on the infected computer and can destroy music and photo files stored on infected computers. When launched, it clogged e-mail servers in many large organizations and slowed the operation of the entire Internet.
2001	Code Red	Virus Worm Trojan Horse	Code Red can infect Web servers and personal computers. It defaces Web pages and can be transmitted from Web servers to personal computers. It can give hackers control over Web server computers. Code Red can reinstall itself from hidden files after it is removed.
2001	Nimda	Virus Worm	Nimda modifies Web documents and certain programs on the infected computer. It also creates multiple copies of itself using various file names. It can be transmitted via e-mail, a LAN, or from a Web server to a Web client.
2002	BugBear	Virus Worm Trojan Horse	BugBear is spread through e-mail and through local area networks. It identifies antivirus software and attempts to disable it. BugBear can log keystrokes and store them for later transmission through a Trojan Horse program that it installs on the infected computer. This program gives hackers access to the computer and allows file uploads and downloads.
2002	Klez	Virus Worm	Klez is transmitted as an e-mail attachment and overwrites files, creates hidden copies of the original files, and attempts to disable antivirus software.
2003	Slammer	Worm	Slammer's primary purpose was to demonstrate how rapidly a worm could be transmitted on the Internet. It infected 75,000 computers in its first ten minutes of propagation.
2003	Sobig	Trojan Horse	Sobig turns infected computers into spam relay points. Sobig transmits mass e-mails with copies of itself to potential victims.
2004	MyDoom	Worm Trojan Horse	MyDoom turns the infected computer into a zombie that will participate in a denial of service attack on a specific company's Web site.

Year	Name	Type	Description
2004	Sasser	Virus Worm	Written by a German high school student, Sasser finds computers with a specific security flaw and then infects them. The infected computers are slowed by the virus, often to the point that they must be rebooted.
2005	Zotob	Worm Trojan Horse	Zotob peforms port scans and infects computers that appear to have a specific security flaw. Once installed on a target computer, Zotob can log keystrokes, capture screens, and steal authentication credentials and CD software keys. Infected computers can also be used as zombies for mass mailing or attacking other computers.
2006	Nyxem	Worm Trojan Horse	Nyxem disables security and file sharing software, destroys files created by Microsoft Office programs. It activates on the third of each month and spreads itself by mass mailing.
2006	Leap	Worm Virus	Leap (also called Oompa-Loompa) infects programs that run on the Macintosh OS-X operating system. Delivered over the iChat instant messaging system, it can only spread within a specific network.
2007	Storm	Worm Trojan Horse	Storm gathers infected computers into a botnet from which it launches spam. Spread as an email containing phony news clips with an attachment that it alleges is a news film.

FIGURE 10-5 Computer viruses, worms, and Trojan horses: 2000-2007 (cont'd)

FIGURE 10-6 Computer viruses, worms, and Trojan horses: 2008 - 2015

Year	Name	Type	Description
2008	Conficker	Worm Trojan Horse	Conficker can reinstall itself when removed and remains on more than 7 million computers. Can launch a barrage of spam e-mail or a crippling denial-of-service attack on any Web site.
2009	Clampi	Worm Trojan Horse	Activated in 2009 after laying dormant for years. Captures usernames and passwords for more than 4000 financial institution Web sites. Perpetrators can this information to make purchases or transfer funds from victim accounts.
2009	URLzone	Worm Trojan Horse	Monitors user activity and hijacks session when victim logs into a financial institution Web site that it is programmed to recognize. Transfers money from victim's accounts to confederates, who take their cut, then buy goods shipped to a foreign address used by the perpetrator.
2010	Stuxnet	Worm Trojan Horse	Spreads through Microsoft Windows, but targets industrial software and equipment built by Siemens. The first worm designed to attack such systems, experts believe it was created to damage Iranian uranium enrichment systems.
2010	VBManie	Virus Trojan Horse	Transmitted by e-mail messages with the subject header "here you have." The message states that the attachment is "The Document I told you about."
2011	Anti-spyware 2011	Virus Trojan Horse	Posing as an anti-virus program, it disables anti-virus programs already installed on the victim computer. It also blocks Internet access so the disabled anti-virus program cannot obtain updates that might restore it.
2011	ZeuS/SpyEye variants	Worm Trojan Horse	These two Trojans were merged to create a series of new variants designed to attack mobile banking information stored on computers.
2013	Cryptolocker	Worm Trojan Horse	Encrypts files on the attacked computer and demands a ransom payment for the key needed to unlock the files.
2014	Regin	Worm Trojan Horse	Infection occurs by visiting a spoofed Web page that installs Regin, which in turn installs additional versions of itself, making detection difficult. It spies on user operations and is intended for long-term monitoring of the target computer.
2015	TeslaCrypt	Worm Trojan Horse	A Cryptolocker variant that identifies game software installed on the attacked computer, encrypts the game files, and demands a ransom payment for the decryption key.

Digital Certificates

- Digital certificate is an e-mail attachment or program embedded in Web page that verifies identity
  - Contains a means to send encrypted communication
  - Used to execute online transactions, send encrypted email and make electronic funds transfers
- Certification authority (CA) issues digital certificates to organizations, individuals with six elements
  - Owner's identification and public key, validity dates, serial number, issuer name and digital signature
    - Key is a long binary number used with encryption algorithm to "Lock" protected message characters

Digital Certificates (cont'd.)

- Identification requirements vary between CAs
  - Driver's license, notarized form, fingerprints
- More stringent rules adopted in 2008 after hackers obtained falsified digital certificates
  - Secure Sockets Layer-Extended Validation (SSL-EV) requires extensive confirmations
- Annual fees range from $100 to more than $1000
- Digital certificates expire after period of time
  - Provides protection by requiring credentials be resubmitted for evaluation

Steganography

- Process of hiding information within another piece of information which can be used for malicious purposes
- Provides a way for hiding an encrypted file within another file
  - Casual observer cannot detect anything important in container file
  - Two-step process where encrypting file protects it from being read and steganography makes it invisible
- Al Qaeda used steganography to hide attack orders

Physical Security for Client Devices and Client Security for Mobile Devices

- Client computers require physical security
  - Fingerprint readers: more protection than passwords
  - Biometric security devices use an element of a person's biological makeup to provide identification
    - Signature recognition, eye or palm scanners, veins
- Access passwords help secure mobile devices
  - Remote wipe clears all personal data and can be added as an app or done through e-mail
- Many users install antivirus software
  - Rogue apps contain malware or collect information and forward to perpetrators

Communication Channel Security and Secrecy Threats

- Internet was designed to provide redundancy, not to be secure
  - Remains unchanged from original insecure state
- Secrecy is the prevention of unauthorized information disclosure
  - Technical issue requiring sophisticated physical and logical mechanisms such as encryption of emails
- Privacy is the protection of individual rights to nondisclosure which is a legal matter
  - Should supervisors be allowed to randomly read employee emails?

Secrecy Threats (cont'd.)

- Theft of sensitive or personal information is a significant electronic commerce threat
  - **Sniffer programs** record information passing through computer or router handling Internet traffic
  - Backdoor allows users to run a program without going through the normal authentication procedures
    - May be left by programmers accidently or intentionally
  - Stolen corporate info (Eavesdropper example)
- Several companies offer anonymous Web services that hide personal information from sites visited

Integrity Threats

- Also known as active wiretapping, exists when an unauthorized party alters message information stream
  - Cybervandalism is electronic defacing of a Web site
  - Masquerading (spoofing) is pretending to be someone else or a fake Web site representing itself as original
- Domain name servers (DNSs) are Internet computers that link domain names to IP addresses
  - Perpetrators substitute their Web site address in place of real one
- Phishing expeditions trick victims into disclosing confidential info (banking and payment systems)

Necessity Threats

- The purpose of a necessity threat, which usually occurs as a delay attack, denial attack, or denial-of-service DoS) attack, is to disrupt normal computer processing, or deny processing entirely
  - Intolerably slow-speed computer processing
  - Renders service unusable or unattractive
  - Distributed denial-of-service (DDoS) attack uses botnets to launch simultaneous attack on a Web site
-

Encryption Solutions and Encryption Algorithms

- Encryption is the coding of information by using a mathematically based program and a secret key to produce a string of characters that is unintelligible
  - Cryptography is the science of studying encryption
    - Converts text that is visible but has no apparent meaning
- Encryption programs transforms normal text (plain text) into cipher text (unintelligible characters string)
  - Encryption algorithm is the logic behind the program
  - Includes mathematics to do transformation
- Decryption program is an encryption-reversing procedure that decodes or decrypts messages

Encryption Algorithms and Hash Coding

- Encryption algorithm property is that message cannot be deciphered without key used to encrypt it
- Hash coding uses a hash algorithm to calculate a number (hash value) from a message
  - Unique message fingerprint
  - Can determine if message was altered during transit
    - Mismatch between original hash value and receiver computed value

Asymmetric Encryption

- Also known as public-key encryption, encodes messages using two mathematically related numeric keys
  - Public key is freely distributed and encrypts messages using encryption algorithm
  - Private key is secret and belongs to key owner
    - Decrypts all messages received
- Pretty Good Privacy (PGP) is a popular public-key encryption technology
  - Uses several different encryption algorithms
  - Free for individuals and sold to businesses

Symmetric Encryption

- Also known as private-key encryption, encodes message with a single numeric key to encode and decode data
  - Both sender and receiver must know the key
  - Very fast and efficient but does not work well in large environments because of number of keys required
  - The key must be guarded
- Data Encryption Standard (DES) was first U.S. government private-key encryption system
  - Triple Data Encryption Standard (Triple DES, 3DES) was a stronger version of DES

Comparing Asymmetric and Symmetric Encryption Systems

- Advantages of public-key (asymmetric) systems
  - Small combination of keys required
  - No problem in key distribution
  - Implementation of digital signatures possible
- Disadvantage is that public key systems are significantly slower than private-key systems
- Public-key systems complement rather than replace private-key systems

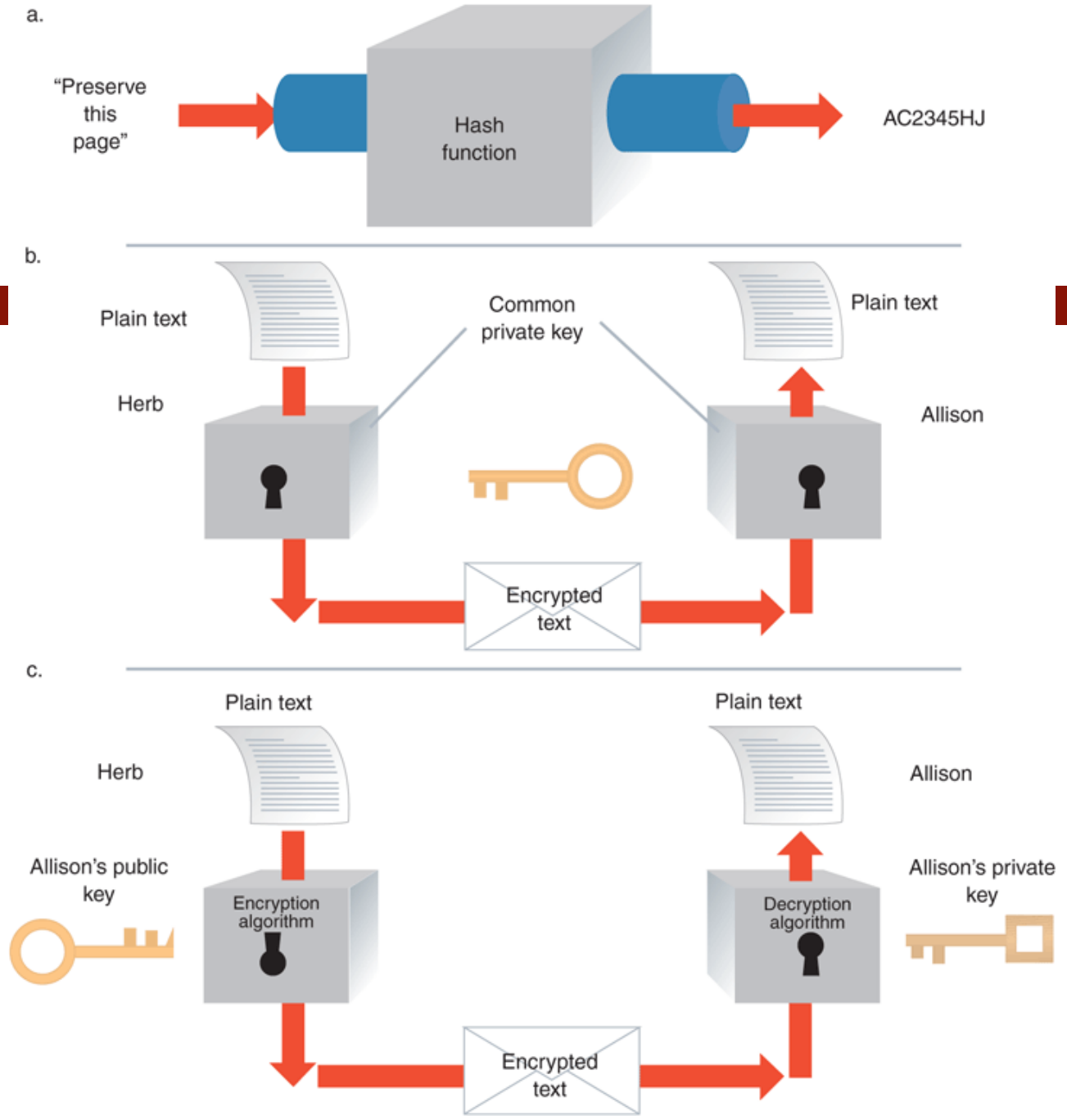

FIGURE 10-7
Comparison of (a) hash coding, (b) private-key, and (c) public-key encryption

Security for Server Computers and Password Attack Threats

- Server is the third link in client-Internet-server electronic commerce path
  - Web server administrator ensures security policies documented and implemented
- One of the most sensitive file on Web server is the file that holds Web server username-password pairs
  - Authentication information are stored in encrypted files
- Passwords threats include using easy passwords
  - Dictionary attack programs cycle through an electronic dictionary, trying every word and common name as password

Password Attack Threats (cont'd.)

- Solutions to threat include stringent requirements and company dictionary checks
- Passphrase is a sequence of words or text easy to remember but a good password or password hint
- Password manager software securely stores all of a person's passwords
  - User only needs to remember master password to get access to the program

admin

2917

password

abeginet

CBcarnqt

m1$$i0ns

n8p0zqr6

zyL3n&BpQ4

~96d$7Pr%}X\

<8?U1@3H+\[oSn$u@Mf>"FV\K^N!dE@sfi52%INO

FIGURE 10-10 Examples of passwords, from very weak to very strong