COMPUTER SECURITY

EGCO342 INFORMATION TECHNOLOGY IN DAILY LIFE

KANAT POOLSAWASD
DEPARTMENT OF COMPUTER ENGINEERING
MAHIDOL UNIVERSITY

Cybercrime

- Cybercrime is any criminal action perpetrated primarily through the use of a computer
  - Programs damaging computers
  - Stealing identities online
  - Attacking corporate Web sites
- Cybercriminals are individuals who use computers, networks, and the Internet to perpetrate crime.

Computer Threats

Viruses

Viruses infect computers through email attachments and file sharing. They delete files, attack other computers, and make your computer run slowly. One infected computer can cause problems for all computers on a network.

Hackers

Hackers are people who “trespass” into your computer from a remote location. They may use your computer to send spam or viruses, host a Web site, or do other activities that cause computer malfunctions.

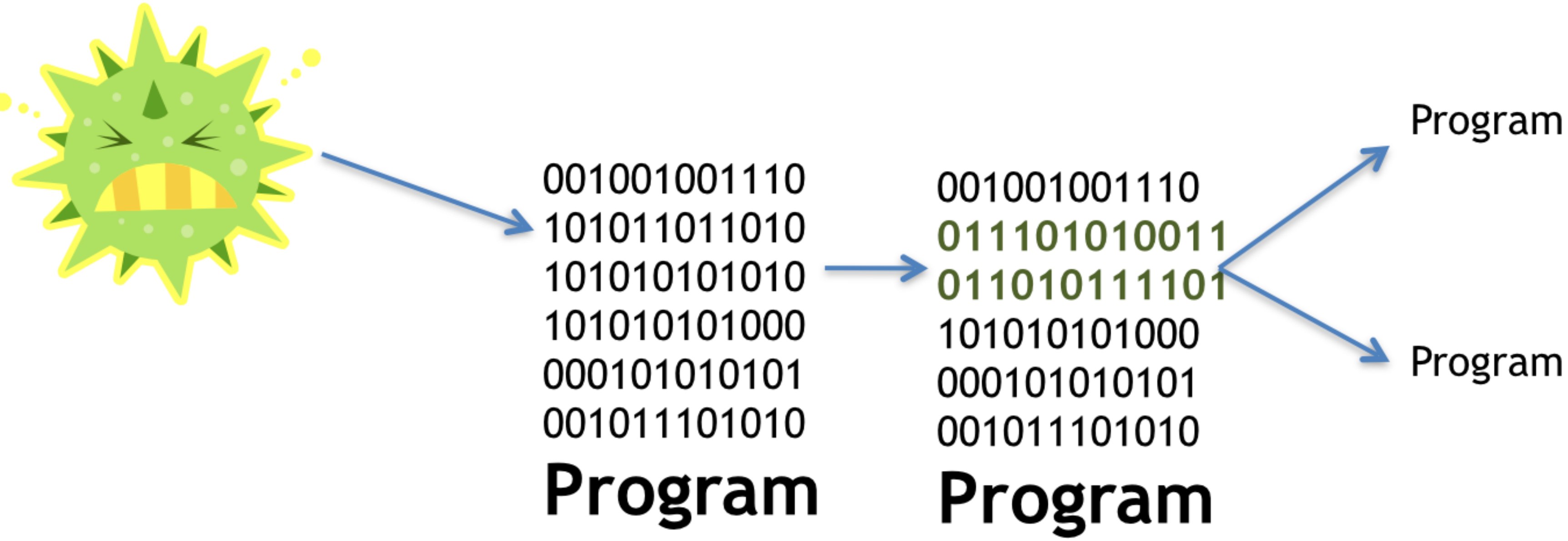
Identity Thieves

People who obtain unauthorized access to your personal information, such as Social Security and financial account numbers. They then use this information to commit crimes such as fraud or theft.

Spyware

Spyware is software that “piggybacks” on programs you download, gathers information about your online habits, and transmits personal information without your knowledge. It may also cause a wide range of other computer malfunctions.

Computer Threats: Viruses



001001001110
101011011010
101010101010
101010101000
000101010101
001011101010

Program

001001001110
011101010011
011010111101
101010101000
000101010101
001011101010

Program

Program

Program

What Viruses Do

- Main purpose
  - Replicate themselves and copy code to as many other files as possible
- Secondary objectives
  - Slow down networks
  - Display annoying messages
  - Destroy files or contents of hard drive

Catching a Virus

- If exposed to an infected file, the virus will try to copy itself and infect a file on your computer
- Sources of virus infection
    - Downloading infected audio and video files
    - Shared flash drives
    - Downloading or executing a file attached to e-mail

Types of Viruses (1)

- Viruses can be grouped into five categories based on behavior and method of transmission
  - **Boot-sector viruses**
    - Replicates itself into hard drive's master boot record
  - **Logic bombs and time bombs**
    - Logic bomb is triggered when certain logical conditions are met
    - Time bomb is triggered by the passage of time or on a certain date

Types of Viruses (2)

- Worms
  - Use transport methods like e-mail and networks to spread without human interaction
- Script and macro viruses
  - Script is mini-program hidden on Web sites that is executed without user's knowledge
  - Macro virus attaches itself to a document that uses macros

Types of Viruses (3)

- **Encryption viruses**
  - Run program that searches for common types of data files
  - Compress files using a complex encryption key that makes files unusable
  - Asks for payment to receive the program to decrypt your files

Virus Classifications

- Viruses can also be classified by methods they take to avoid detection
  - **Polymorphic viruses**
    - Periodically rewrite themselves to avoid detection
  - **Multipartite viruses**
    - Infect multiple file types
  - **Stealth viruses**
    - Erase their code from the hard drive and reside in the active memory

Antivirus Software (1)

- Antivirus software is designed to detect viruses and protect your computer
- Popular antivirus software companies
    - Symantec
    - Kaspersky
    - AVG
    - McAfee
- Comprehensive Internet security packages protect you from other threats

Antivirus Software (2)

- Designed to detect suspicious activity
  - Scan files for virus signatures (unique code)
  - Identifies infected files and type of virus
  - Provides choice of deleting or repairing infected file
  - Places virus in secure area (quarantining)
  - Records key attributes about file and rechecks these statistics during scan (inoculating)

Software Updates

- Make sure antivirus software and your operating system are up to date and contain latest security patches
    - Windows operating system has automatic update utility called Windows Update
    - Mac OS X has similar utility

Computer Threats: Hackers

- Anyone who unlawfully breaks into a computer system
- Types of hackers
  - White-hat or ethical hackers
  - Black-hat hackers
  - Grey-hat hackers

Problems Hackers Cause

- Steal credit and debit cards information from hard drives
- Break into sites that contain credit card information
- Capture login ID and password using packet analyzer or key logger
- Use information to purchase items illegally
- Sell credit card numbers and information

Trojan Horses and Rootkits

- Trojan horse appears to be useful but while it runs it does something malicious in background
- Rootkits are programs (or sets of programs) that allow hackers to gain access to your computer and take control without your knowledge
- Zombie is computer controlled by hacker

Denial-of-Service (DoS) Attacks

- In a denial-of-service (DoS) attack, users are denied access to computer system because hacker is making repeated requests
- When flooded with requests, the system shuts down
- Distributed denial-of-service (DDoS) attack launches attacks from more than one zombie computer

Critical Infrastructures - Compound Attacks

- Critical infrastructures include gas, power, water, banking and finance, transportation, communications.
- All dependent to some degree on information systems, and automated control systems (SCADA).
- Employ some or all of aforementioned cyber attacks techniques.
- Possibly combined with conventional (physical) terror attacks.
- Consequences include devastating disruption in communication and commerce, blocked access to critical systems, or loss of life.

How Hackers Gain Access

- Direct access
  - Installing hacking software
- Indirect access
  - Through Internet connection
  - Logical ports

Restricting Access to Your Digital Assets

- Keep hackers out
    - Prevent them from accessing computer
    - Protect your digital information
        - Use passwords
    - Hide activities from prying eyes

Firewalls

- Software program or hardware designed to protect computers from hackers
  - Consider installing both for maximum protection
- Software firewalls
  - Most operating systems include firewall
  - Many security suites include firewall software
- Hardware firewall devices
  - Routers
  - Keep unused logical ports closed

Password Protection

- Strong passwords are difficult to guess
  - At least 14 characters, including numbers, symbols, and upper and lowercase letters
  - Not a single word or a word from a dictionary
  - Not easily associated with you (birth date, name of pet, nickname)
  - Use different passwords for different Web sites
  - Never tell anyone or write down password
  - Change password regularly (every month)

Managing Your Passwords

- Well-constructed passwords can be hard to remember
- Password-management software remembers passwords for you
- Most security suites and Web browsers provide password-management tools

Lorrie Faith Cranor:

What’s wrong with your pa$$w0rd ?

Malware, Adware, and Spyware

- Malware
  - Software that has malicious intent
- Adware
  - Displays sponsored advertisements
  - Pop-up windows
- Spyware
  - Unwanted piggyback programs that download with other software you install from Internet that transmit information about you

Spam

- Unwanted or junk e-mail
- Avoid spam in primary e-mail account
    - Create free Web-based e-mail account
    - Use spam filter
    - Read privacy policy
    - Don’t reply to spam to remove yourself from list
    - Subscribe to e-mail forwarding service

Cookies

- Small text files that Web sites automatically store on hard drive to make return visit more efficient and better geared to your interests
- Web site assigns ID number to computer
- Provide Web sites with information about browsing habits
- Some sites sell information cookies collect
- Not a security threat

Protecting Yourself … from Yourself!

- Keep your data safe from damage
  - Accidental
  - Intentional
- Keep unscrupulous individuals from tricking you into revealing sensitive information

Protecting Your Personal Information

- Never share:
  - Social Security number
  - Phone number
  - Date of birth
  - Street address
- Social networks ask for potentially sensitive information
  - Use privacy settings

Backing Up Your Data (1)

- Data faces three major threats:
  - Unauthorized access
  - Tampering
  - Destruction
- Backups are copies of files that can replace originals
- Store backups away from computer in at least two different places

Backing Up Your Data (2)

- Types of files to back up
  - Program files without media
  - Data files you create
- Types of backups
  - Incremental backup (partial backup)
  - Image backup (system backup)
- Backup data files frequently

Backing Up Your Data (3)

- Location of backup files
  - Online sites
  - Local drives
  - Network-attached storage (NAS) devices and home servers
- Performing file backups
  - Windows Backup and Restore utility
  - Mac OS X Time Machine feature

Social Engineering

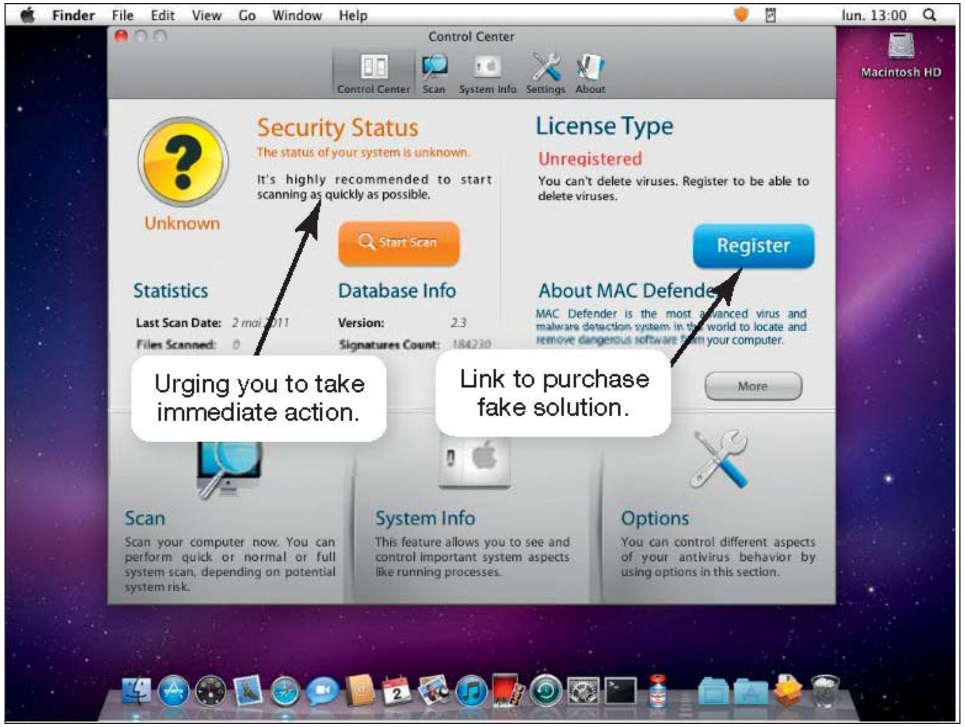
- Any technique that entices individuals to reveal sensitive information
- Pretexting creates a scenario that sounds legitimate
  - Bank calling to confirm personal details
  - Information can then be used to commit fraud
- Most common form of pretexting is phishing

Phishing and Pharming

- Phishing lures users to reveal personal information that could lead to identity theft
    - E-mail messages look legitimate
- Pharming is when malicious code is planted on your computer
    - Alters browser's ability to find Web addresses
    - Directed to bogus Web sites that gather personal information

Scareware

- Type of malware downloaded onto computer that tries to convince you that computer is infected with virus
- Then directed to site to buy fake removal tools



Security Status

The status of your system is unknown.

It's highly recommended to start scanning as quickly as possible.

License Type

Unregistered

You can't delete viruses. Register to be able to delete viruses.

Statistics

Last Scan Date: 2 mai 2011

Files Scanned: 0

Database Info

Version: 2.3

Signatures Count: 184230

About MAC Defender

MAC Defender is the most advanced virus and malware detection system in the world to locate and remove dangerous software from your computer.

Scan

Scan your computer now. You can perform quick or normal or full system scan, depending on potential system risk.

System Info

This feature allows you to see and control important system aspects like running processes.

Options

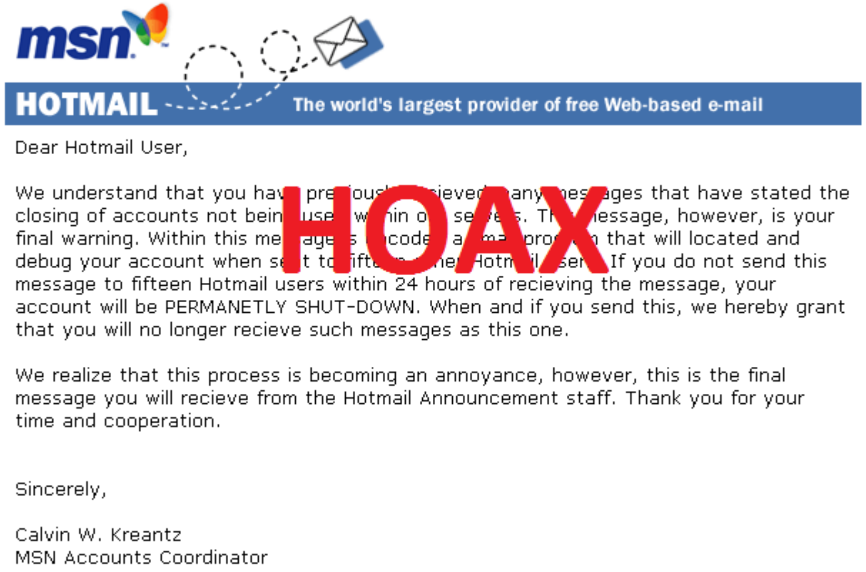
You can control different aspects of your antivirus behavior by using options in this section.

Urging you to take immediate action.

Link to purchase fake solution.

Hoaxes

- Attempt to make someone believe something that is untrue
  - Target large audiences
  - Practical joke, agents of social change, or time wasters
  - Mostly by e-mail



HOTMAIL The world's largest provider of free Web-based e-mail

Dear Hotmail User,

We understand that you have previously recieved many messages that have stated the closing of accounts not being used within our servers. This message, however, is your final warning. Within this message is encoded a mail program that will located and debug your account when sent to fifteen other Hotmail users. If you do not send this message to fifteen Hotmail users within 24 hours of recieving the message, your account will be PERMANETLY SHUT-DOWN. When and if you send this, we hereby grant that you will no longer recieve such messages as this one.

We realize that this process is becoming an annoyance, however, this is the final message you will recieve from the Hotmail Announcement staff. Thank you for your time and cooperation.

Sincerely,

Calvin W. Kreantz
MSN Accounts Coordinator

Cryptography (1)

- Cryptography
  - The field of study related to encoded information (comes from Greek word for "secret writing")
- Encryption
  - The process of converting plaintext into ciphertext
  - Encrypted (Information) cannot be read.
- Decryption
  - The process of converting ciphertext into plaintext
  - Decrypted (Encrypted (Information)) can be.

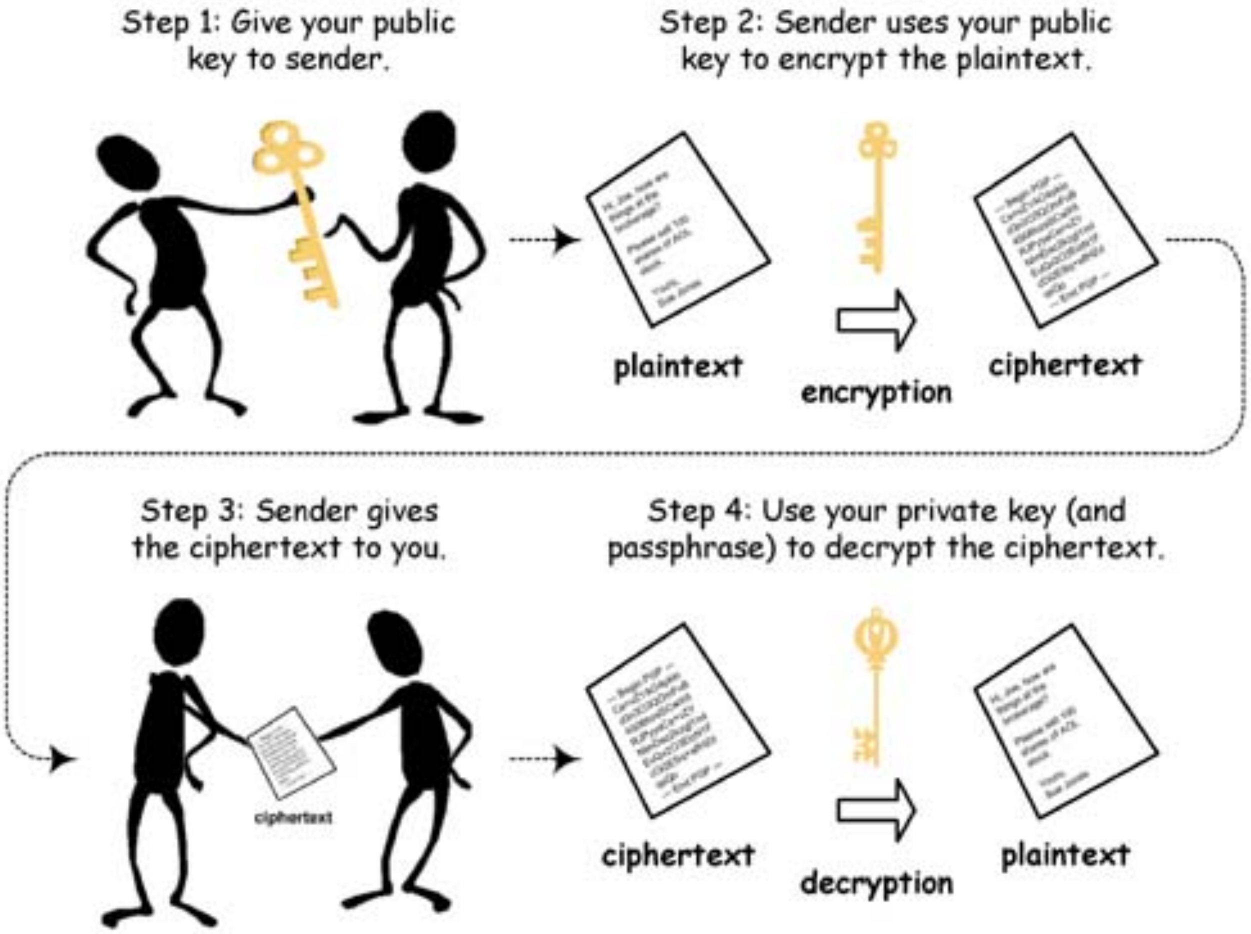
Cryptography (2)

- Cipher
  - An algorithm used to encrypt and decrypt text
- Key
  - The set of parameters that guide a cipher
- Neither is any good without the other

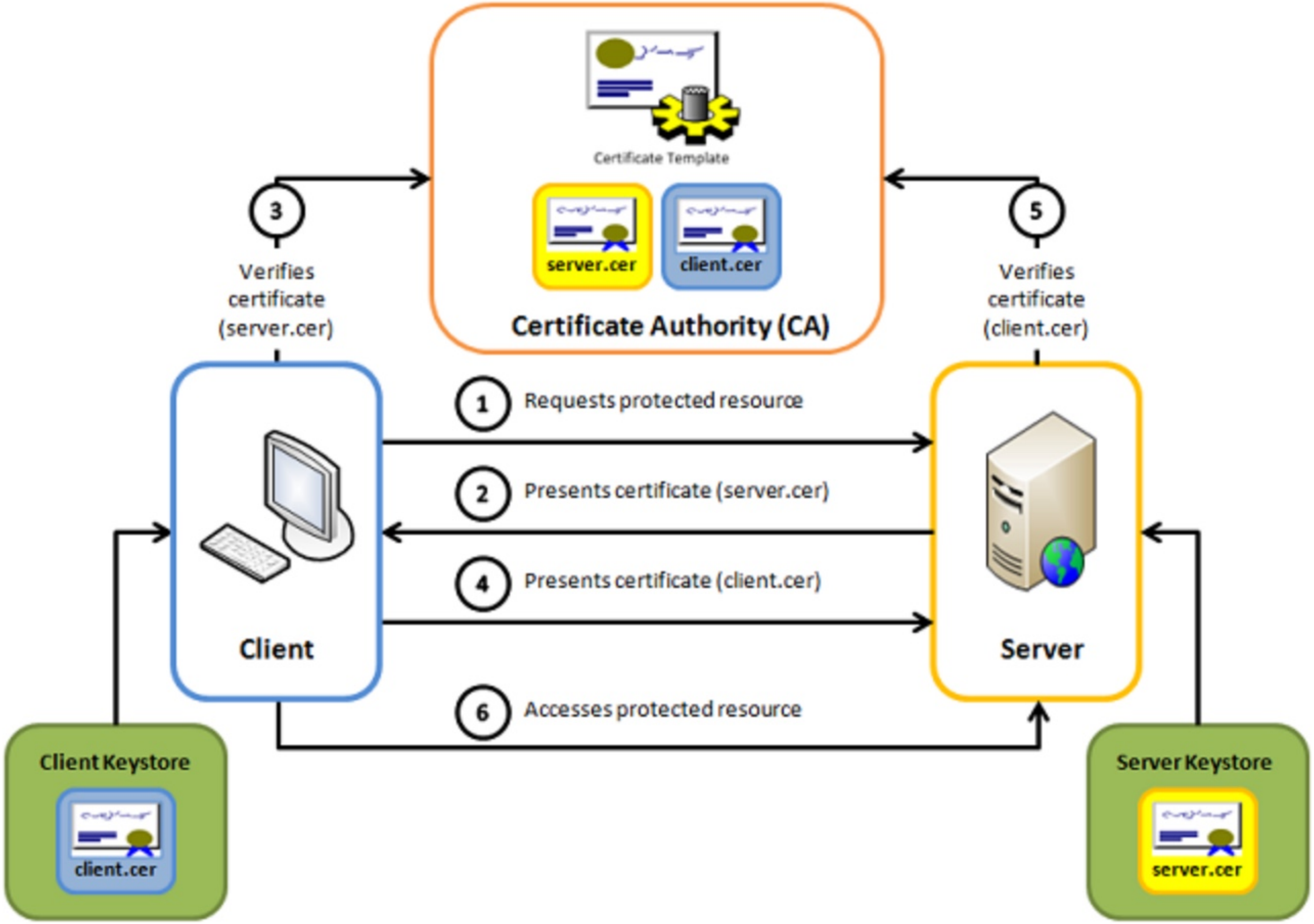
Cryptography (3)

- Substitution cipher
  - A cipher that substitutes one character with another
- Caesar cipher
  - A substitution cipher that shifts characters a certain number of positions in the alphabet
- Transposition ciphers
  - A cipher that rearranges the order of existing characters in a message in a certain way (e.g., a route cipher)

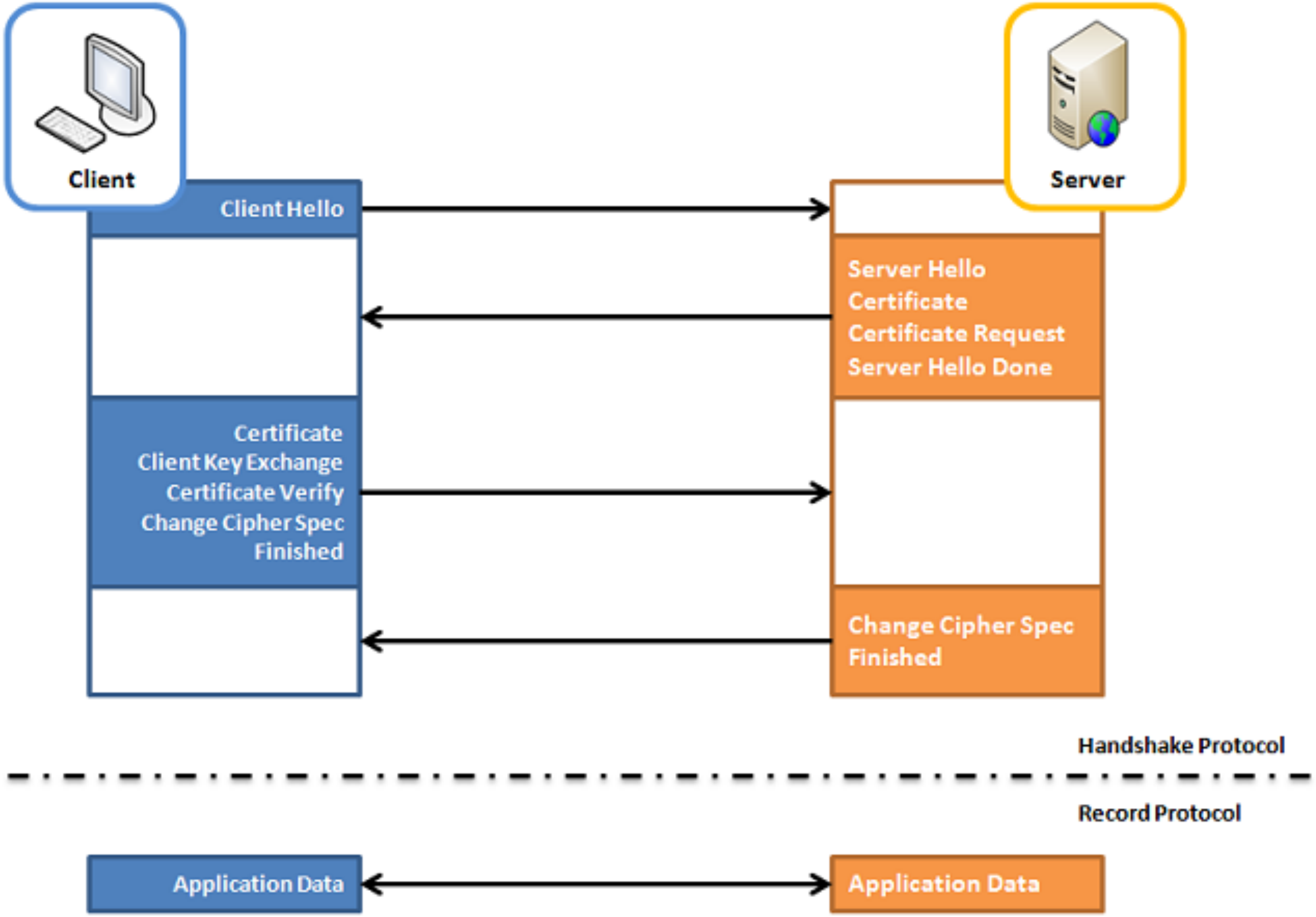
Public/Private Keys


Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
ciphertext
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
decryption
plaintext

Secure Socket Layer (SSL) (1)


Certificate Template
server.cer
client.cer
Certificate Authority (CA)
3
Verifies certificate (server.cer)
5
Verifies certificate (client.cer)
1
Requests protected resource
2
Presents certificate (server.cer)
4
Presents certificate (client.cer)
6
Accesses protected resource
Client
Server
Client Keystore
client.cer
Server Keystore
server.cer

Secure Socket Layer (SSL) (2)



Mutual SSL authentication handshake messages

Protecting Online Information

- Be smart about information you make available!!!!!
    - 25% of Facebook users don’t make use of its privacy controls or don’t know they exist
    - 40% of social media users post their full birthday, opening themselves up to identity theft
    - 9% of social media users become victims of information abuse

Avi Rubin: All your devices can be hacked

Assignment 8

- ให้แต่ละกลุ่มดูวิดีโอเรื่อง “บล็อกเชนเปลี่ยนแปลงการเงินและธุรกิจได้อย่างไร” พร้อมทั้งหาข้อมูลเพิ่มเติมเกี่ยวกับ “บล็อกเชน” (Blockchain) สรุปเนื้อหาไม่เกิน 1 หน้ากระดาษ เขียนลงใน comment ในเว็บไซต์ของรายวิชา