

Securing Information Systems

Reading:

Laudon & Laudon
chapter 7

Additional Reading:

Brien & Marakas
chapter 11

Outline

- ❑ System Vulnerability and Abuse
- ❑ Business Value of Security and Control
- ❑ Establishing Framework for Security/Control
- ❑ Technologies and Tools for Protecting Information Resource

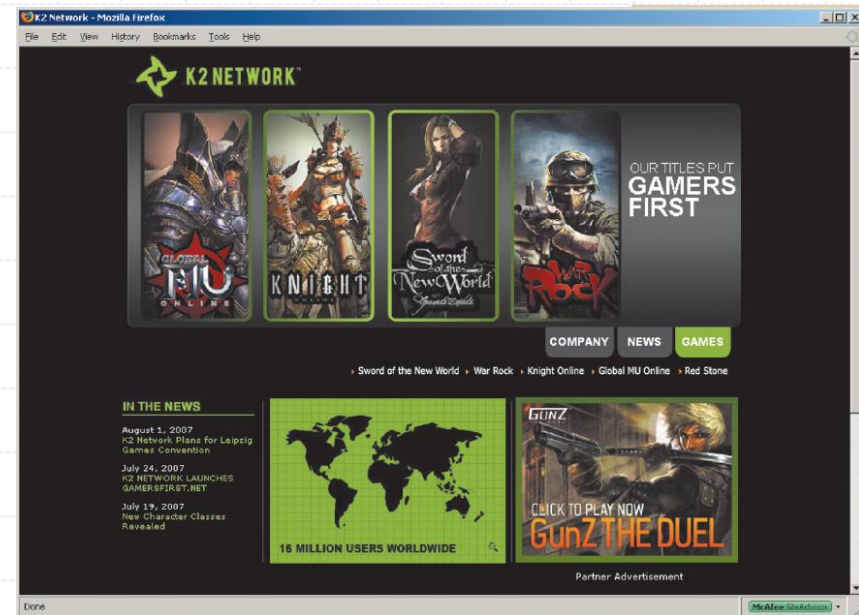
Security for Online Games

➤ Problem

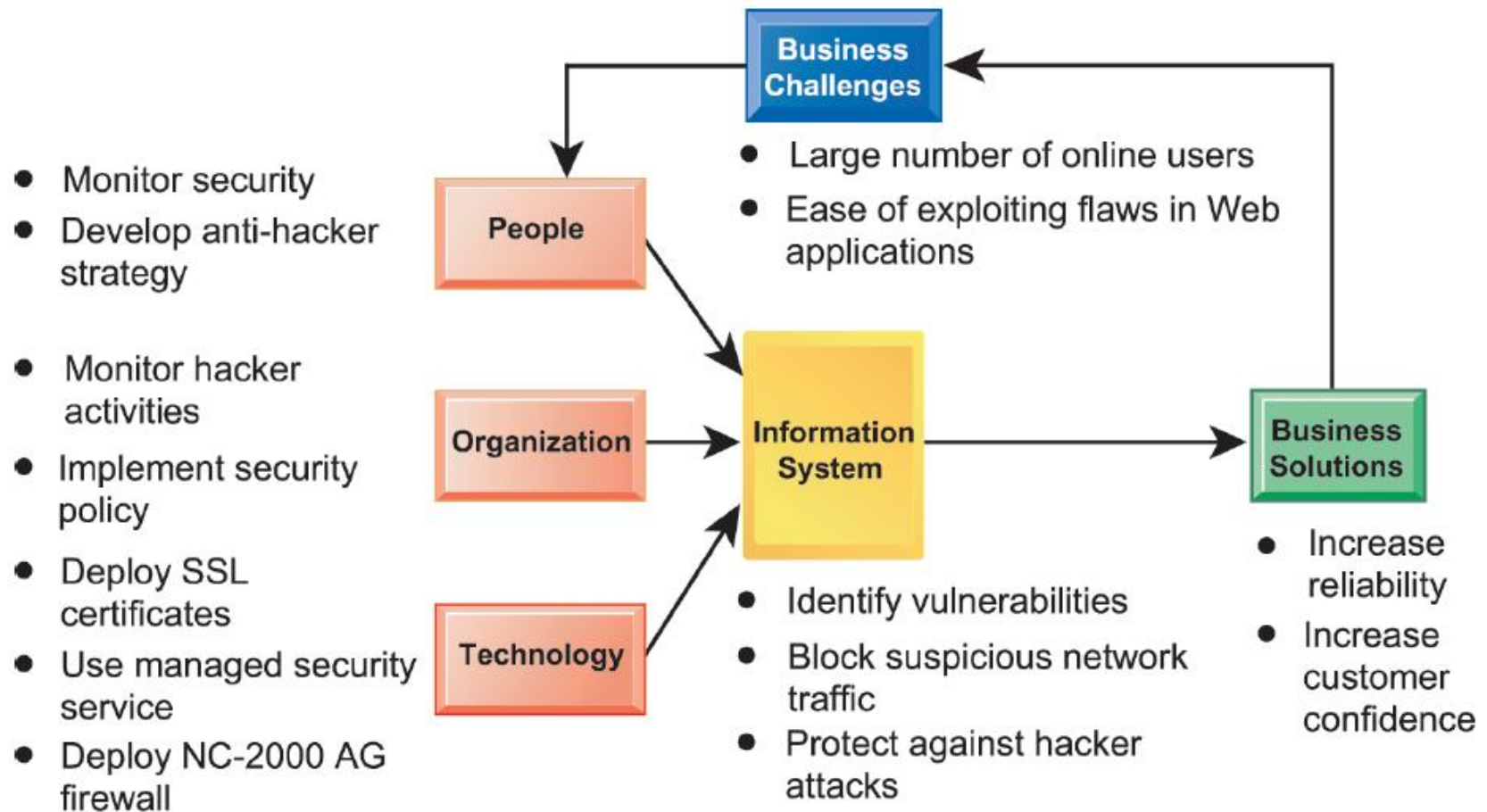
- Threat of attacks from hackers hoping to steal information or gaming assets
- K2 would lose great deal of money & reputation if its websites not working
- Relied on SSL encryption to secure communication with players

➤ Solution

- Deploy an advanced security system to identify threats & reduce hacking
- NetContinuum's NC-2000 AG firewall & Cenzic's ClickToSecure service work in tandem to minimize the chance of security breach
- Cenzic's service remotely probes K2's applications as a hacker would and makes suggestions/upgrades
- NetContinuum's firewall box sits in front of a web server to examine network traffic and block suspicious traffic
- Demonstrates IT's role in combating cyber crime.
- Illustrates digital technology's role in achieving security on the Web



Security for Online Games



System Vulnerability and Abuse

➤ System Security

- An unprotected computer without firewall or antivirus software
 - ◆ Disabled within minutes and may take days to recover
- An Make security and control a top policy

➤ What is Security?

- Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems

➤ What is Control?

- Methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards

Why Systems are Vulnerable?

Large amount of data stored in electronic form → Several kind of threats

- **Hardware problems**

- ◆ Breakdowns, configuration errors, damage from improper use or crime

- **Software problems**

- ◆ Programming errors, installation errors, unauthorized changes

- **Disasters**

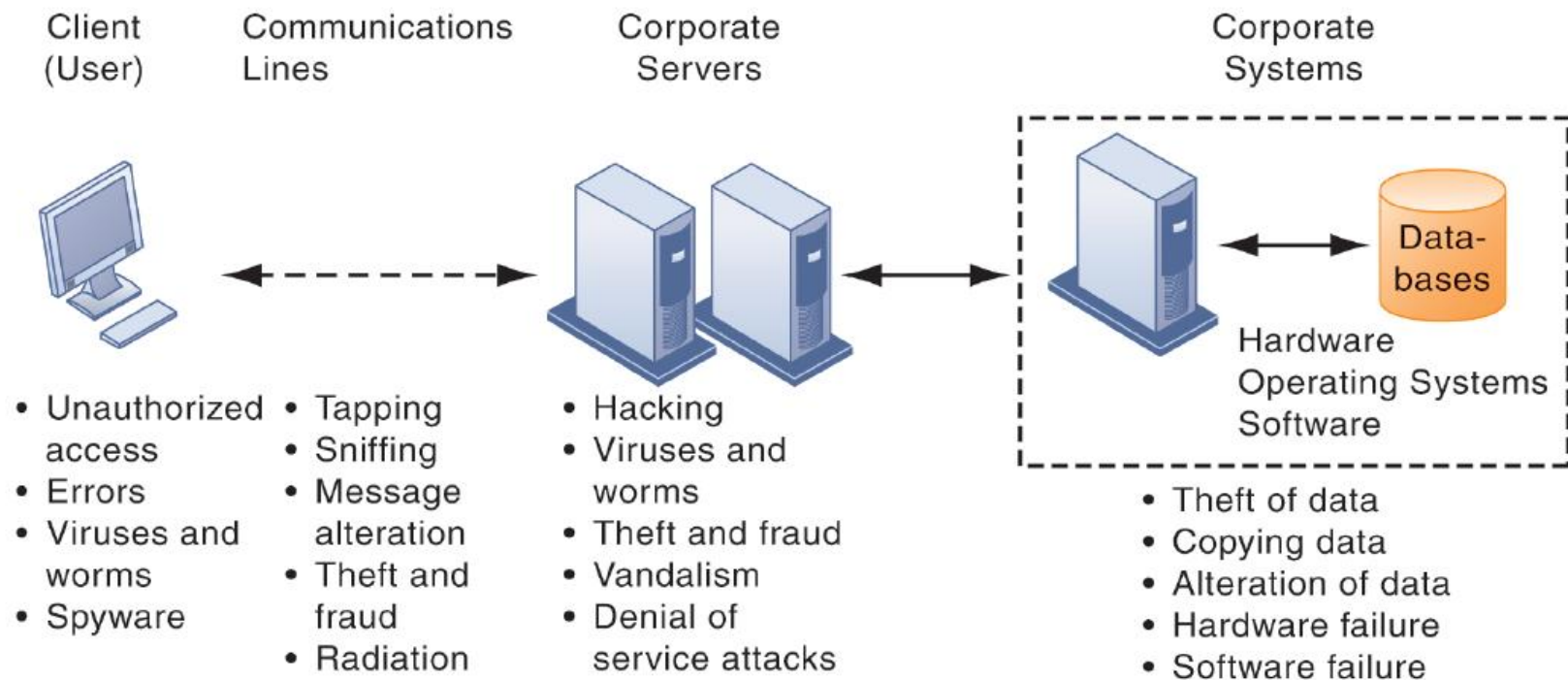
- ◆ Power failures, flood, fires, etc.

- **Use of networks/computers outside of firm's control**

- ◆ Example - with domestic or offshore outsourcing vendors

Contemporary Security Challenges

- The architecture of a Web-based application - a Web client, a server, and corporate information systems linked to databases
- Each of these components presents security challenges and vulnerabilities
- Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network



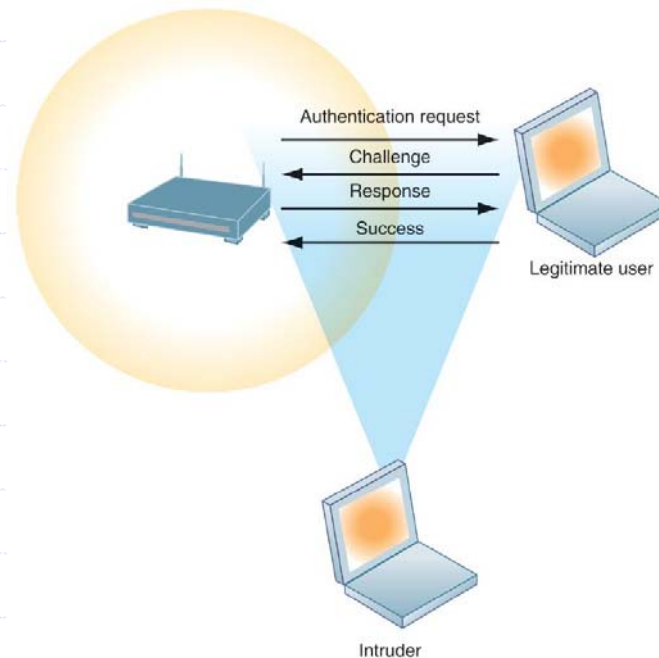
System Vulnerability and Abuse

➤ Internet Vulnerability

- Network open to anyone
- Size of Internet means abuses can have wide impact
- Use of fixed Internet addresses with permanent connections to Internet eases identification by hackers
- E-mail attachments
- E-mail used for transmitting trade secrets
- IM messages lack security, can be easily intercepted

System Vulnerability and Abuse

➤ Wi-Fi Security Challenges



- Wireless Network – Vulnerable - RF bands are easy to scan
- Wired Equivalent Privacy (WEP)
 - ◆ Initial security standard for Wi-Fi
 - ◆ Built in all 802.11 products → Optional, Not very effective
 - ◆ WEP requires access points and all users to share 40 bit encrypted password
 - ◆ Can be decrypted by hackers from small amount of traffic
 - ◆ Stronger encryption and authentication systems → Available, Willingness to install them

Malicious Software

➤ Malware

- Viruses

- ◆ Rogue software program that attaches itself to other software programs or data files in order to be executed, Payload

- Worms

- ◆ Independent computer programs that copy themselves from one computer to other computers over a network

- Trojan horses

- ◆ Software program that appears to be benign but then does something other than expected

- Key loggers

- ◆ Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks

Malicious Software

➤ Adware

- Software that purports to serve a useful purpose
- But also allows Internet advertisers to display advertisements (pop-up and banner ads)
- Without the consent of the computer's user

➤ Spyware

- Adware that employs the user's Internet connection in the background without your permission or knowledge
- Captures information about you and sends it over the Internet

➤ 200+ virus & worms targeted mobile phones in 2006

➤ Web 2.0 applications (*blogs, wikis, MySpace*)

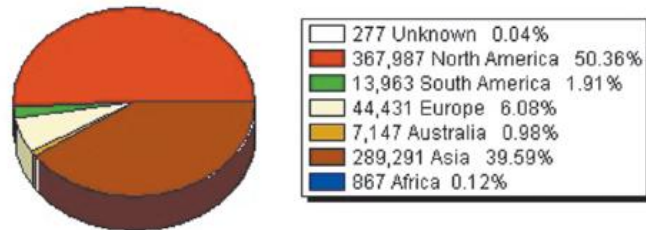
- Users can post software codes as permissible contents
- Launched automatically as these pages are viewed
- In Nov'06 *Wikipedia* was employed to distribute *malware* – info about security patch

➤ US Consumers lost 7.9 b\$ → Malware, online scam

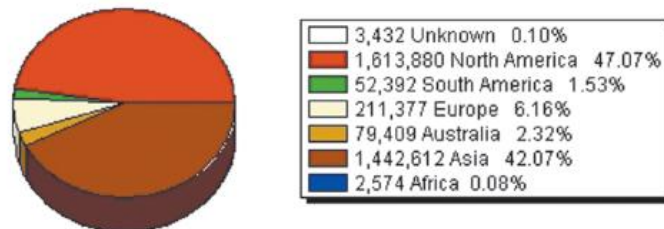
System Vulnerability and Abuse

- Regional distribution of worms and computer viruses worldwide (Example)

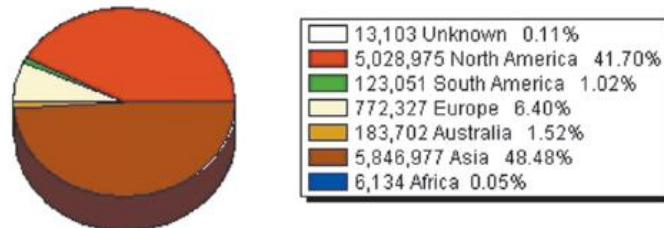
Viruses Detected During the Past 24 Hours



Viruses Detected During the Past 7 Days



Viruses Detected During the Past 30 Days



Copyright (c) 1989-2007 Trend Micro Incorporated. All rights reserved.



Hackers and Computer Crime

➤ Hackers Vs Crackers

- Activities include
 - ◆ System intrusion
 - ◆ System damage
 - ◆ Cybervandalism
 - Intentional disruption, defacement, destruction of Web site or corporate information system

➤ Spoofing

- Faking an e-mail address or Web page to trick users into passing along critical information like passwords or credit card numbers
- Redirecting Web link to address different from intended one, with site masquerading as intended destination

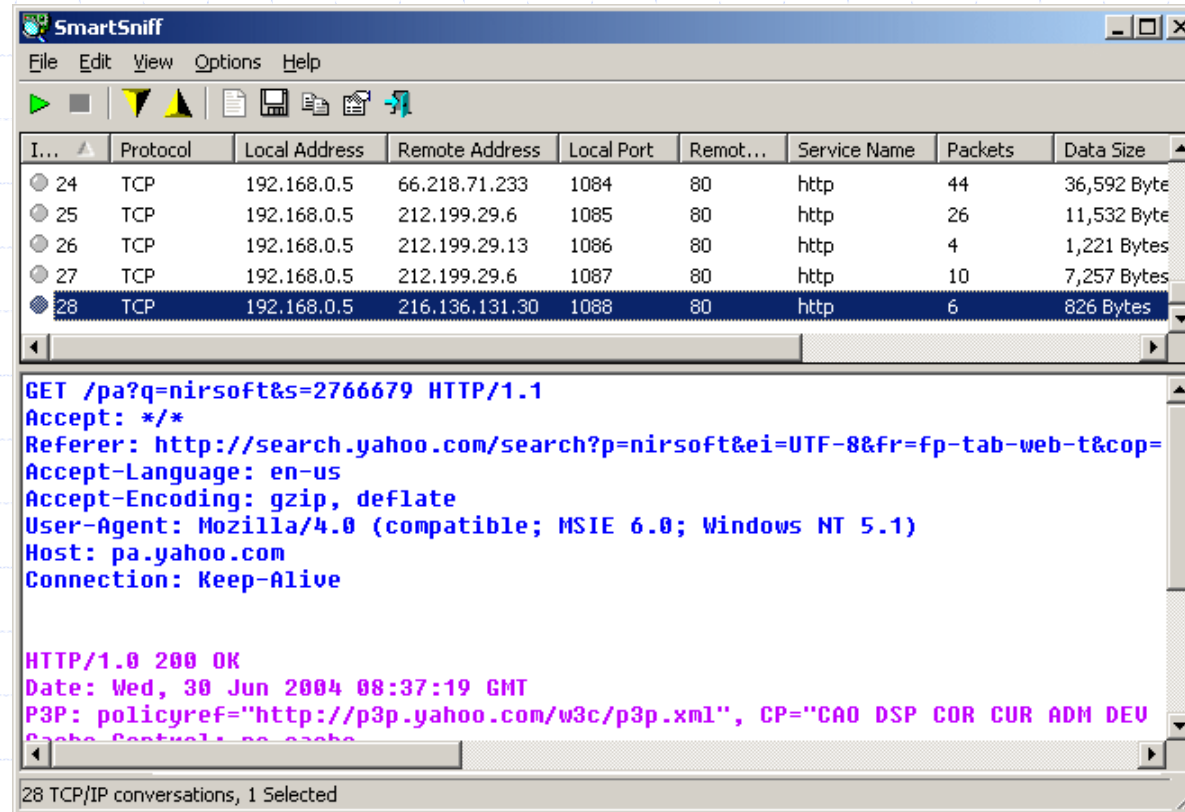
➤ Sniffer

- Eavesdropping program that monitors information traveling over network
- Programs that search individual packets of data as they pass through the Internet
- Legitimate use → Identify potential network trouble spot or criminal activity in network
- Capturing passwords or entire contents
- Enables hackers to steal proprietary information (e-mail, company files)

Hackers and Computer Crime

➤ Sniffer

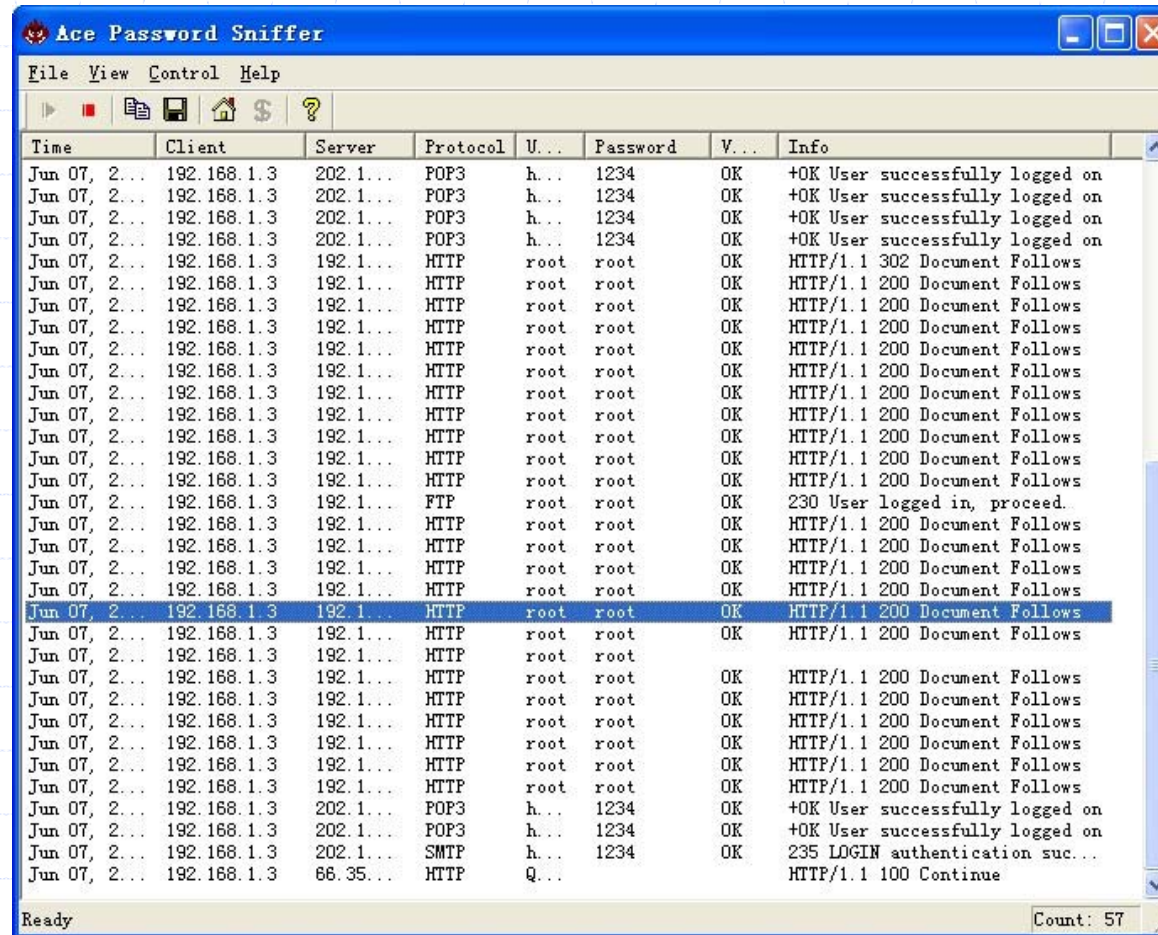
Freeware - capture TCP/IP packets that pass through your network adapter



Hackers and Computer Crime

➤ Password Sniffer

Can listen on your LAN and enables *network administrators* or *parents* to capture passwords of any network user. Currently, Password Sniffer can monitor and capture passwords through FTP, POP3, HTTP, SMTP, Telnet, and etc.



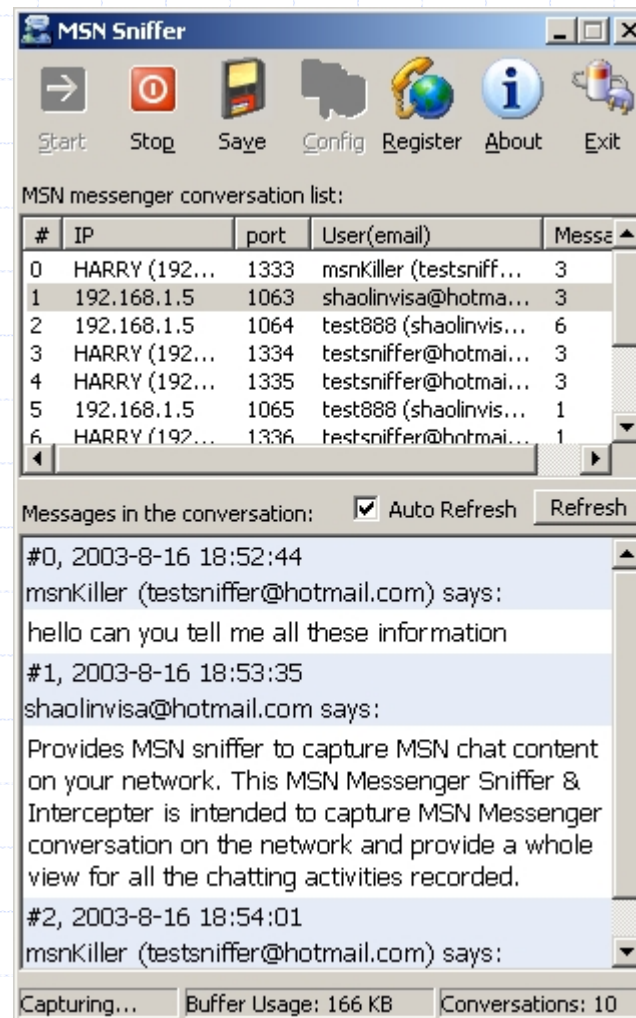
The screenshot shows the 'Ace Password Sniffer' application window. It has a menu bar (File, View, Control, Help) and a toolbar with icons for play, stop, save, home, and help. The main area is a table with columns: Time, Client, Server, Protocol, U..., Password, V..., and Info. The table contains 30 rows of captured traffic data. The status bar at the bottom shows 'Ready' and 'Count: 57'.

| Time | Client | Server | Protocol | U... | Password | V... | Info |
|--------------|-------------|----------|----------|------|----------|------|---------------------------------|
| Jun 07, 2... | 192.168.1.3 | 202.1... | POP3 | h... | 1234 | OK | +OK User successfully logged on |
| Jun 07, 2... | 192.168.1.3 | 202.1... | POP3 | h... | 1234 | OK | +OK User successfully logged on |
| Jun 07, 2... | 192.168.1.3 | 202.1... | POP3 | h... | 1234 | OK | +OK User successfully logged on |
| Jun 07, 2... | 192.168.1.3 | 202.1... | POP3 | h... | 1234 | OK | +OK User successfully logged on |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 302 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | FTP | root | root | OK | 230 User logged in, proceed. |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 192.1... | HTTP | root | root | OK | HTTP/1.1 200 Document Follows |
| Jun 07, 2... | 192.168.1.3 | 202.1... | POP3 | h... | 1234 | OK | +OK User successfully logged on |
| Jun 07, 2... | 192.168.1.3 | 202.1... | POP3 | h... | 1234 | OK | +OK User successfully logged on |
| Jun 07, 2... | 192.168.1.3 | 202.1... | SMTP | h... | 1234 | OK | 235 LOGIN authentication suc... |
| Jun 07, 2... | 192.168.1.3 | 66.35... | HTTP | Q... | | | HTTP/1.1 100 Continue |

Hackers and Computer Crime

➤ MSN Sniffer

Intended to capture *MSN Messenger conversation* on the network and provide a whole view for all the chatting activities recorded.



Hackers and Computer Crime

➤ Denial-of-service attacks (DoS)

- Flooding server with thousands of false requests to crash the network
- Hammering a website's equipment with too many requests for information
- Clogging the system, slowing performance or even crashing the site
- Very Costly for busy e-commerce websites

➤ Distributed denial-of-service attacks (DDoS)

- Use of numerous computers to launch a DoS
- Botnets
 - ◆ Infected PC's becomes *slave* or *zombie* – serving master computer elsewhere
 - ◆ Networks of *zombie* PCs infiltrated by *bot malware*

➤ War dialing

- Programs that automatically dial thousands of telephone numbers in search of a way in through a modem connection

➤ Logic bombs

- An instruction in a computer program that triggers a malicious act

➤ Buffer overflow

- A technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory

Hackers and Computer Crime

➤ Password Crackers

- Software that can guess passwords

➤ Social Engineering

- Gaining access to computer systems
- By talking unsuspecting company employees out of valuable information such as passwords

➤ Dumpster Driving

- Sifting through a company's garbage to find information to help break into their computers

Hackers and Computer Crime

➤ Computer Crime

- Any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution
- **Computer may be target of crime**
 - ◆ Breaching confidentiality of protected computerized data
 - ◆ Accessing a computer system without authority
- **Computer may be instrument of crime**
 - ◆ Theft of trade secrets
 - ◆ Using e-mail for threats or harassment

➤ Identity theft

- Theft of personal Information (social security id, driver's license or credit card numbers) to impersonate someone else

➤ Phishing

- Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data.

➤ Evil twins

- Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet, try to capture passwords or credit card numbers

Hackers and Computer Crime

➤ Pharming

- Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser

➤ Click fraud

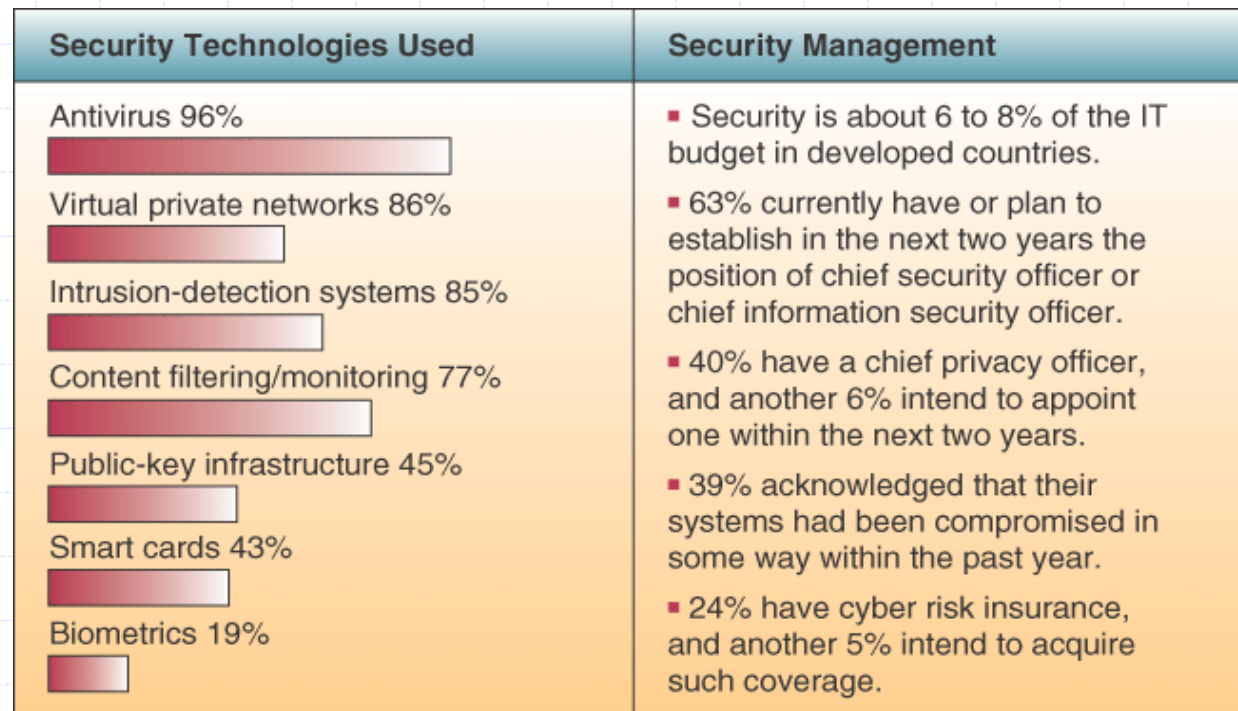
- Occurs when individual or computer program fraudulently clicks on online ad *without any intention of learning more about the advertiser* or making a purchase
- Serious problem at websites (e.g. Google) that feature pay per click advertising, 3rd party to weaken firms
- Google attempts to monitor click fraud, efforts not in public domain

Software Vulnerability

- Commercial software contains flaws that create security vulnerabilities
 - Hidden bugs (program code defects)
 - ◆ Zero defects cannot be achieved because complete testing is not possible with large programs
 - Flaws can open networks to intruders
- Patches
 - Vendors release small pieces of software to repair flaws
 - However, amount of software in use can mean exploits created faster than patches be released and implemented
 - Security firms identify about 5000 vulnerabilities every year, in 2007
 - ◆ Symantec → Identified 39 vulnerabilities in *Microsoft IE*, 34 in *Mozilla* browsers, 25 in *Apple Safari*, 7 in *Opera*
- Failed computer systems can lead to significant or total loss of business function
- Firms now more vulnerable than ever
- A security breach may cut into firm's market value almost immediately

Software Vulnerability

- How large companies protect themselves from cybercrime



Business value of Security and Control

- Legal and Regulatory Requirements for Electronic Records Management
 - Firms face new legal obligations for the retention and storage of electronic records as well as for privacy protection
 - ◆ **HIPAA** → Medical security and privacy rules and procedures
 - ◆ **Gramm-Leach-Bliley Act** → Requires financial institutions to ensure the security and confidentiality of customer data
 - ◆ **Sarbanes-Oxley Act** → Imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally

Business value of Security and Control

➤ Electronic Evidence and Computer Forensics

- **Evidence for white collar crimes often found in digital form**
 - ◆ Data stored on computer devices, e-mail, instant messages, e-commerce transactions
- Proper control of data can save time, money when responding to *legal discovery request* (high cost)
 - ◆ Courts impose financial and even criminal penalties for improper destruction of electronic documents
- **Computer forensics**
 - ◆ Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law
 - ◆ Includes recovery of ambient and hidden data
 - ◆ Finding significant information in large volume of electronic data
 - ◆ Presenting the information to court of law

Framework for Security and Control

➤ Information Systems Controls

➤ General Control

- ◆ Govern design, security, and use of computer programs and security of data files in general throughout organization's information technology infrastructure.
- ◆ Apply to all computerized applications
- ◆ Combination of hardware/software/manual procedures to create overall control environment

➤ Types of General Control

- Software controls
- Hardware controls
- Computer operations controls
- Data security controls
- Implementation controls
- Administrative controls

➤ Application Controls

- Specific controls unique to each computerized application, payroll or order processing
- Include both automated and manual procedures
- Ensure that only authorized data are completely/accurately processed by application
- Include:
 - ◆ Input controls
 - ◆ Processing controls
 - ◆ Output controls

Framework for Security and Control

➤ Risk Assessment

- Determines level of risk to firm if specific activity or process is not properly controlled
 - ◆ Types of threat
 - ◆ Probability of occurrence during year
 - ◆ Potential losses, value of threat
 - ◆ Expected annual loss
- Example – *Online Order Processing System*
Risk Assessment, 30,000 orders per day

| EXPOSURE | PROBABILITY | LOSS RANGE | EXPECTED ANNUAL LOSS |
|---------------|-------------|---------------|----------------------|
| Power failure | 30% | \$5K - \$200K | \$30,750 |
| Embezzlement | 5% | \$1K - \$50K | \$1,275 |
| User error | 98% | \$200 - \$40K | \$19,698 |

Framework for Security and Control

➤ Security Policy

- Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals
- Drives other policies
 - ◆ **Acceptable use policy (AUP)**
 - Defines acceptable uses of firm's information resources and computing equipment
 - ◆ **Authorization policies**
 - Determine differing levels of user access to information assets

➤ Authorization Management Systems

- Establish where and when a user is permitted to access certain parts of a Web site or corporate database
- Allow each user access only to those portions of system that person is permitted to enter, based on information established by set of access rules, profile

System Vulnerability and Abuse

➤ Security Profiles of a Personnel System

| SECURITY PROFILE 1 | |
|---|-----------------|
| User: Personnel Dept. Clerk | |
| Location: Division 1 | |
| Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116 | |
| Data Field Restrictions | Type of Access |
| All employee data for Division 1 only | Read and Update |
| • Medical history data | None |
| • Salary | None |
| • Pensionable earnings | None |

| SECURITY PROFILE 2 | |
|--|----------------|
| User: Divisional Personnel Manager | |
| Location: Division 1 | |
| Employee Identification Codes with This Profile: 27321 | |
| Data Field Restrictions | Type of Access |
| All employee data for Division 1 only | Read Only |

Framework for Security and Control

➤ Disaster Recovery Planning

- Devises plans for restoration of disrupted services
- Focuses on technical issues
 - ♦ Which file to backup, maintenance of backup computer system
 - ♦ Example – MasterCard maintains duplicate computer centre in Kansas City, which serves as emergency backup of primary centre at St. Louis
- Disaster recovery firms
 - ♦ Comdisco disaster recovery services, SunGard availability services
 - ♦ Hot sites housing spare computers (running critical applications in emergency)

➤ Business Continuity Planning

- Focuses on restoring business operations after disaster
 - ♦ Both types of plans needed to identify firm's most critical systems
 - ♦ *Business impact analysis* to determine impact of an outage
 - ♦ Management must determine
 - Maximum amount of time business can survive with systems down
 - Which systems to be restored first

Framework for Security and Control

➤ The Role of Auditing

■ MIS Audit

- ♦ Examines firm's overall security environment as well as controls governing individual information systems
- ♦ Reviews technologies, procedures, documentation, training, and personnel.
- ♦ May even simulate disaster to test response of technology, IS staff, other employees.
- ♦ Lists and ranks all control weaknesses and estimates probability of their occurrence.
- ♦ Assesses financial and organizational impact of each threat

Framework for Security and Control

➤ Sample Auditor's List of Control Weakness

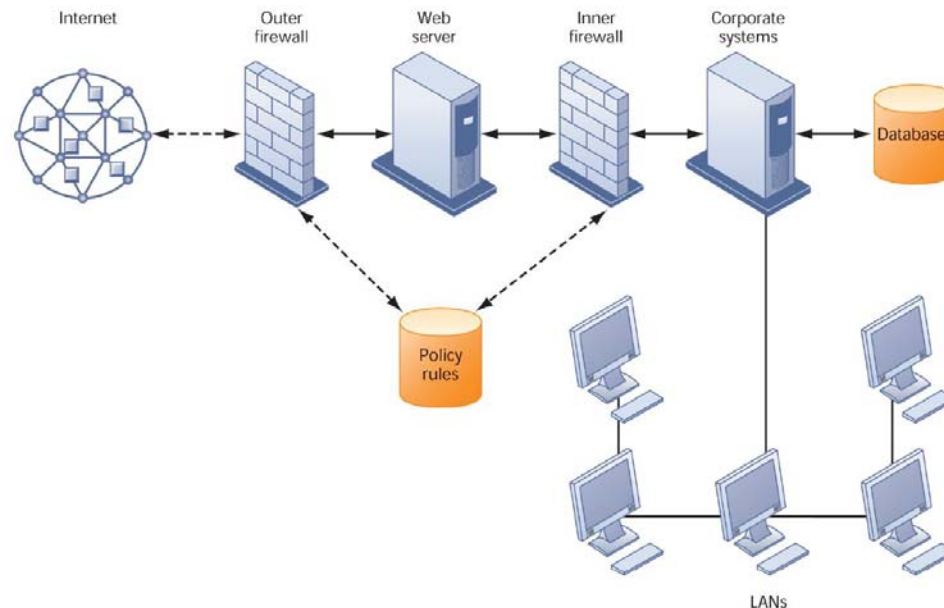
- Sample page from a *list of control weaknesses* that an auditor might find in a loan system in a local commercial bank
- This form helps auditors *record and evaluate control weaknesses* and shows the results of *discussing those weaknesses with management*, as well as any corrective actions taken by management.

| | | | | | |
|--|------------------------|---|----------------------------|---|--|
| Function: Loans Location: Peoria, IL | | Prepared by: J. Ericson Date: June 16, 2008 | | Received by: T. Benson Review date: June 28, 2008 | |
| Nature of Weakness and Impact | Chance for Error/Abuse | | Notification to Management | | |
| | Yes/ No | Justification | Report date | Management response | |
| User accounts with missing passwords | Yes | Leaves system open to unauthorized outsiders or attackers | 5/10/08 | Eliminate accounts without passwords | |
| Network configured to allow some sharing of system files | Yes | Exposes critical system files to hostile parties connected to the network | 5/10/08 | Ensure only required directories are shared and that they are protected with strong passwords | |
| Software patches can update production programs without final approval from Standards and Controls group | No | All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status | | | |

Technologies and Tools for Security

➤ Firewall

- Combination of hardware and software that prevents unauthorized users from accessing private networks
- Technologies include
 - ◆ **Static packet filtering**
 - ◆ **Network address translation (NAT)**
 - ◆ **Application proxy filtering**
- A Corporate Firewall



Technologies and Tools for Security

➤ Intrusion Detection Systems

- Monitor *hot spots* on corporate networks to detect and deter intruders
- Examines events as they are happening to discover attacks in progress
- Software looks for patterns indicative of known methods of computer attacks
 - ◆ Bad password, if important files have been removed/modified

➤ Antivirus and antispyware software

- Checks computers for presence of malware and can often eliminate it as well
- Require continual updating
- Leading Vendors
 - ◆ Antivirus → McAfee, Symantec, Trend Micro
 - ◆ Anti-spyware → Ad-aware, Spyware Doctor, Spybot

Technologies and Tools for Security

➤ Securing Wireless Networks

- WEP security can be improved
 - ♦ Activating it
 - ♦ Assigning unique name to network's SSID, Instruct router not to broadcast
 - ♦ Using it with VPN technology
- Wi-Fi Alliance finalized WAP2 (802.11i) specification, replacing WEP with stronger standards
 - ♦ Continually changing and longer keys, harder to crack
 - ♦ Encrypted authentication system with central server

Technologies and Tools for Security

➤ Encryption and Public Key Infrastructure

➤ Encryption

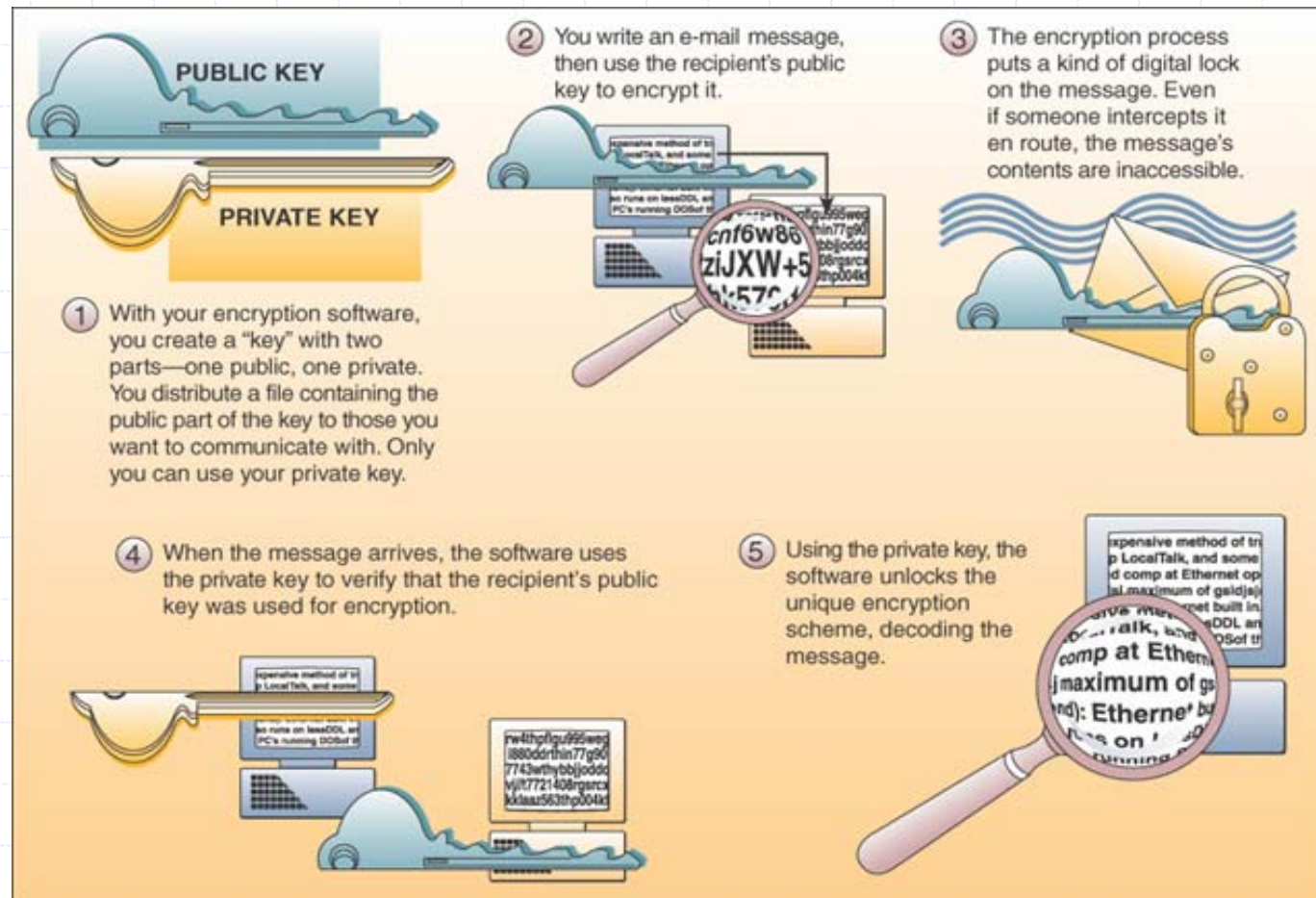
- Transforming text or data into cipher text that cannot be read by unintended recipients
- Two methods for encryption on networks
 - ◆ Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS) – Manages Encryption/Decryption activities
 - ◆ Secure Hypertext Transfer Protocol (S-HTTP) – another encryption protocol, limited to individual messages (SSL/TSL - secure connection)

➤ Two Methods of Encryption

- Symmetric key encryption
 - ◆ Sender and receiver use single, shared key
- Public key encryption
 - ◆ Uses two, mathematically related keys: Public key and private key
 - ◆ Sender encrypts message with recipient's public key
 - ◆ Recipient decrypts with private key

Technologies and Tools for Security

➤ How public key/private key encryption works?



Technologies and Tools for Security

➤ Digital Certificate

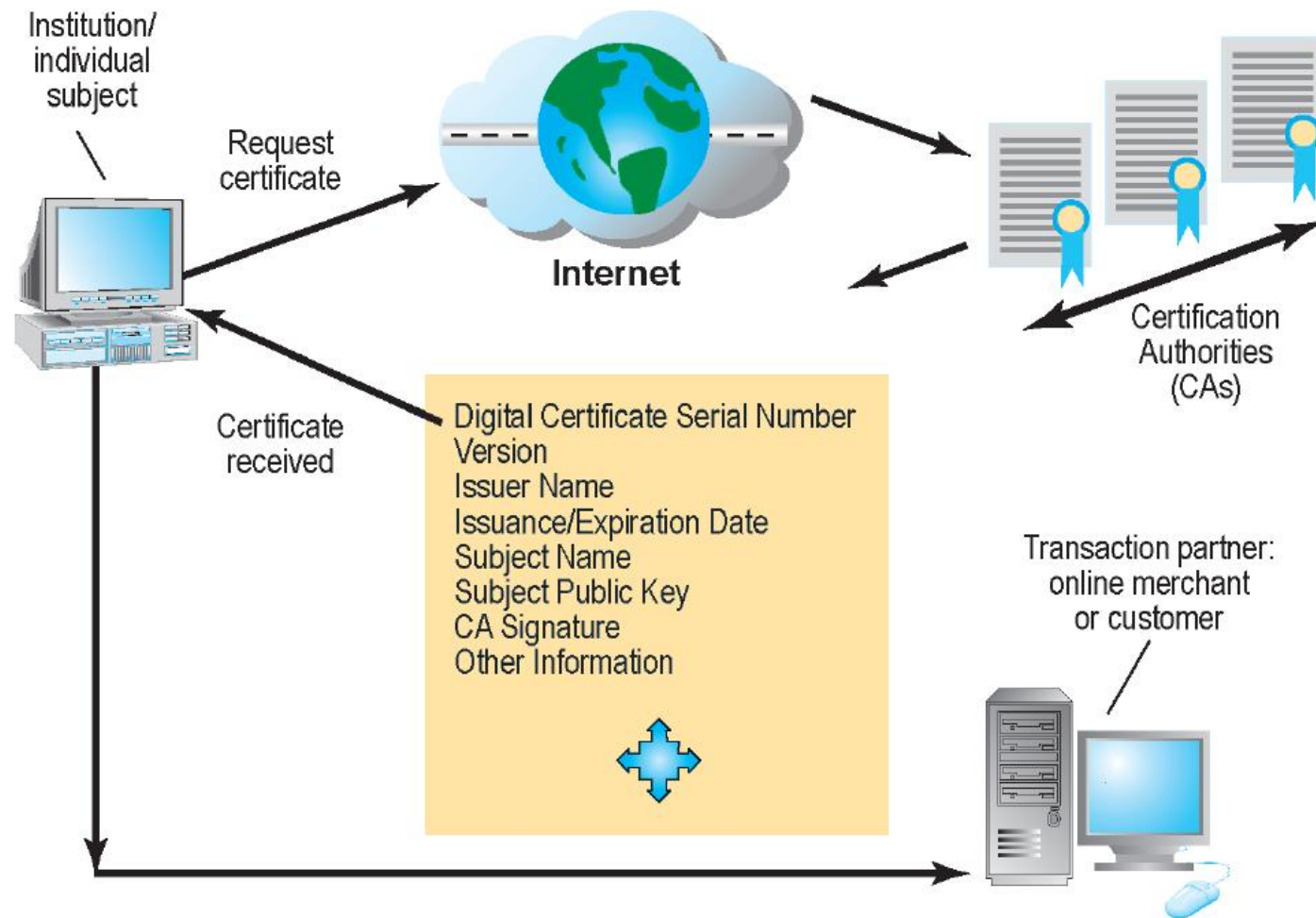
- Data file used to establish the identity of users and electronic assets for protection of online transactions
- Uses a trusted third party, certification authority (CA), to validate a user's identity
 - ◆ CA → *VeriSign, IdenTrust, KeyPost*
- CA verifies user's identity offline, stores information online in CA server, which generates encrypted digital certificate containing owner ID information and copy of owner's public key

➤ Public Key Infrastructure (PKI)

- Use of public key cryptography working with certificate authority
- Widely used in e-commerce

Technologies and Tools for Security

➤ Digital Certificates



Technologies and Tools for Security

➤ Ensuring System Availability

- Online transaction processing requires 100% availability, no downtime
- Fault-tolerant computer systems
 - ◆ For continuous availability, e.g. stock markets
 - ◆ Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service
- High-availability computing
 - ◆ Helps recover quickly from crash
 - ◆ Minimizes, does not eliminate downtime
- Recovery-oriented computing
 - ◆ Designing systems that recover quickly with capabilities to help operators pinpoint and correct source of faults in multi-component systems
- Controlling network traffic
 - ◆ Deep packet inspection (DPI) (video and music blocking)
- Security outsourcing
 - ◆ Managed security service providers (MSSPs)
 - ◆ Example → *VeriSign, Guardent, Counterpane, Symantec*

Technologies and Tools for Security

➤ Ensuring System Availability

- **Software Metrics:** Objective assessments of system in form of quantified measurements
 - ◆ Number of transactions in a specified time
 - ◆ Online response time
 - ◆ Payroll checks printed per hour
 - ◆ Known bugs per hundred lines of code
- **Early and regular testing**
- **Walkthrough**
 - ◆ Good testing begins even before the code is written
 - ◆ Review of specification or design document by small group of qualified people
- **Debugging**
 - ◆ Process by which errors are eliminated