INST0031
Systems Management

Lecture 6

Security and Controls

Learning Outcomes

- Understand the organizational needs for information security and control.
- Realize what information security is concerned with and what are its objectives
- See the logical relationship among threats, risks and controls.
- Analyze why information systems need special protection from destruction, error, and abuse.
- Assess the business value of security and control.
- Be familiar the most important tools and technologies for safeguarding information resources.
- Know the process for implementing an information security policy.

Feed the bear!

Security???

There is NONE

Or else…

Questions

- Why are information systems vulnerable to destruction, error, and abuse?
- What is the business value of security and control?
- What are the components of an organizational framework for security and control?
- What are the most important tools and technologies for safeguarding information resources?

Securing information systems

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

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses.
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity
  - Utility

Information Trends

- Three trends:
  - More information is being created, stored, processed and communicated using computers and computer-based networks
  - Computers are increasingly interconnected, creating new pathways to valuable information assets
  - Threats to information assets are becoming more widespread and more sophisticated
- Productivity and competitiveness, are tied to the first two trends, the third trend makes it inevitable that companies are increasingly vulnerable to corruption, destruction or exploitation of valuable information

Information Security

- Information security is comprised of **methods** and **technologies** that are used to protect the:
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation

  of information and actions but also of the computers and networks that create, process, store and communicate our information

What is a computer virus?

- A computer program in machine code
- "Lives" on disk and in memory
- Causes irritation or damage
- Capable of reproduction
- Is dangerous to the health of your system!

Why Systems are Vulnerable

- **Networks**
  - Potential for unauthorized access, abuse, or fraud is not limited to single location but can occur at any access point in network
  - Vulnerabilities exist at each layer and between layers
- **Internet vulnerabilities**
  - Public network, so open to anyone
  - Size of Internet means abuses may have widespread impact
  - E-mail, instant messaging vulnerable to malicious software, interception
- **Software vulnerability**
  - Software errors are constant threat to information systems
- **Patches**
  - Created by software vendors to update and fix vulnerabilities
  - However, maintaining patches on all firm's devices is time consuming and evolves more slowly than malware

Why Systems are Vulnerable

- **What motivates an individual or organisation to create a computer virus?**
- **Malicious software (malware)**
  - **Computer virus**
    - Rogue software program that attaches to other programs or data files
    - Payload may be relatively benign or highly destructive
  - **Worm:**
    - Independent program that copies itself over network

- **Viruses and worms spread via:**
  - Downloaded software files
  - E-mail attachments
  - Infected e-mail messages or instant messages
  - Infected disks or machines

Why Systems are Vulnerable

- **Trojan horse**
  - Software program that appears to be benign but then does something other than expected
  - Does not replicate but often is way for viruses or malicious code to enter computer system
- **Spyware**
  - Small programs installed surreptitiously on computers to monitor user Web surfing activity and serve advertising
- **Key loggers**
  - Record and transmit every keystroke on computer
  - Steal serial numbers, passwords

Why Systems are Vulnerable

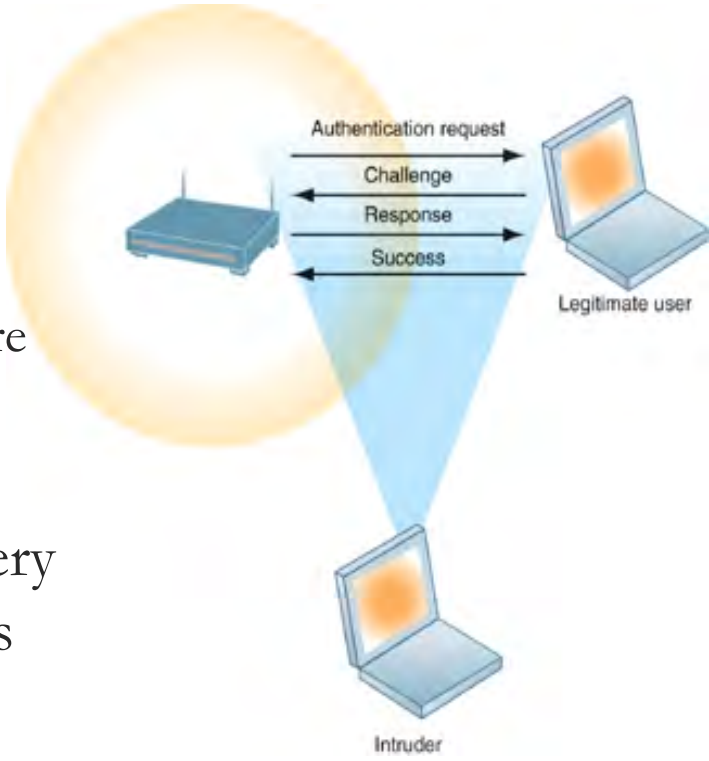
- **Spoofing:**
  - Misrepresentation, e.g. by using fake e-mail addresses or redirecting to fake Web site
- **Sniffing:**
  - Eavesdropping program that monitors information traveling over network
- **Denial-of-service (DoS) attack:**
  - Flooding network or Web server with thousands of false requests so as to crash or slow network
- **Distributed denial-of-service (DDoS) attack**
  - Uses hundreds or thousands of computers to inundate and overwhelm network from many launch points

Why Systems are Vulnerable

- **Identity theft**
  - Using key pieces of personal information (social security numbers, driver's license numbers, or credit card numbers) to impersonate someone else
- **Phishing**
  - Setting up fake Web sites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data
- **Evil twins**
  - Bogus wireless networks used to offer Internet connections, then to capture passwords or credit card numbers
- **Pharming**
  - Redirecting users to bogus Web page, even when individual types correct address into browser

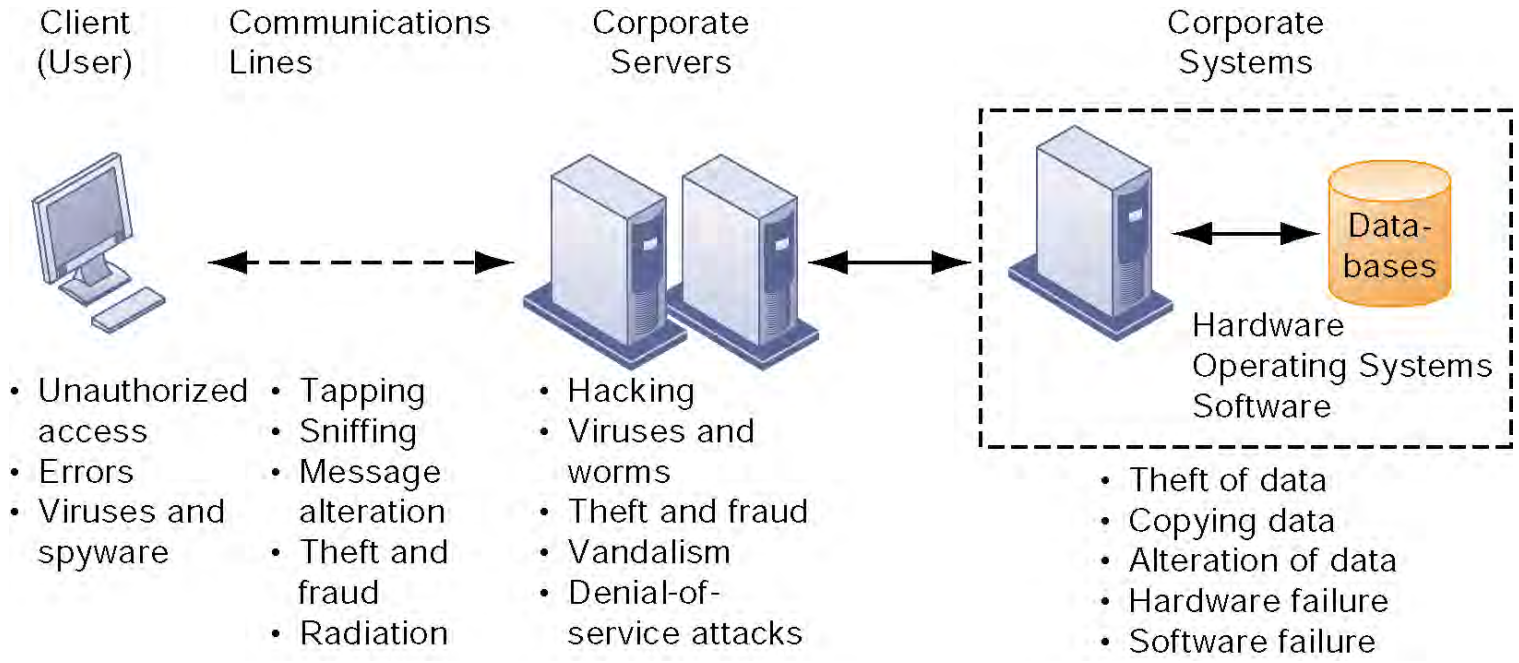
Why Systems are Vulnerable

- **Wireless security challenges**
  - Many home networks and public hotspots open to anyone, so not secure, communication unencrypted
  - LANs using 802.11 standard can be easily penetrated
    - *Service set identifiers (SSIDs)* identify access points in Wi-Fi network and are broadcast multiple times
  - WEP (Wired Equivalent Privacy): Initial Wi-Fi security standard not very effective as access point and all users share same password



Why Systems are Vulnerable

- Information systems are vulnerable:
  - to technical, organizational, and environmental threats
  - from internal and external sources.
- The weakest link in the chain is poor management.



Who are the "Opponents"?

- Internal threats
  - Employees
  - Service personnel
  - Visitors
- External Intruders
  - Former employees
  - Clients and Customers
  - "Crackers"
  - Thieves and Organized Crime
  - Business competitors

65%

35%

What are their Motives?

- Money, profit
- Access to additional resources
- Competitive advantage
  - Economic
  - Political
- Personal grievance, vengeance
- Curiosity
- Attention

Everyday Cyber Crime

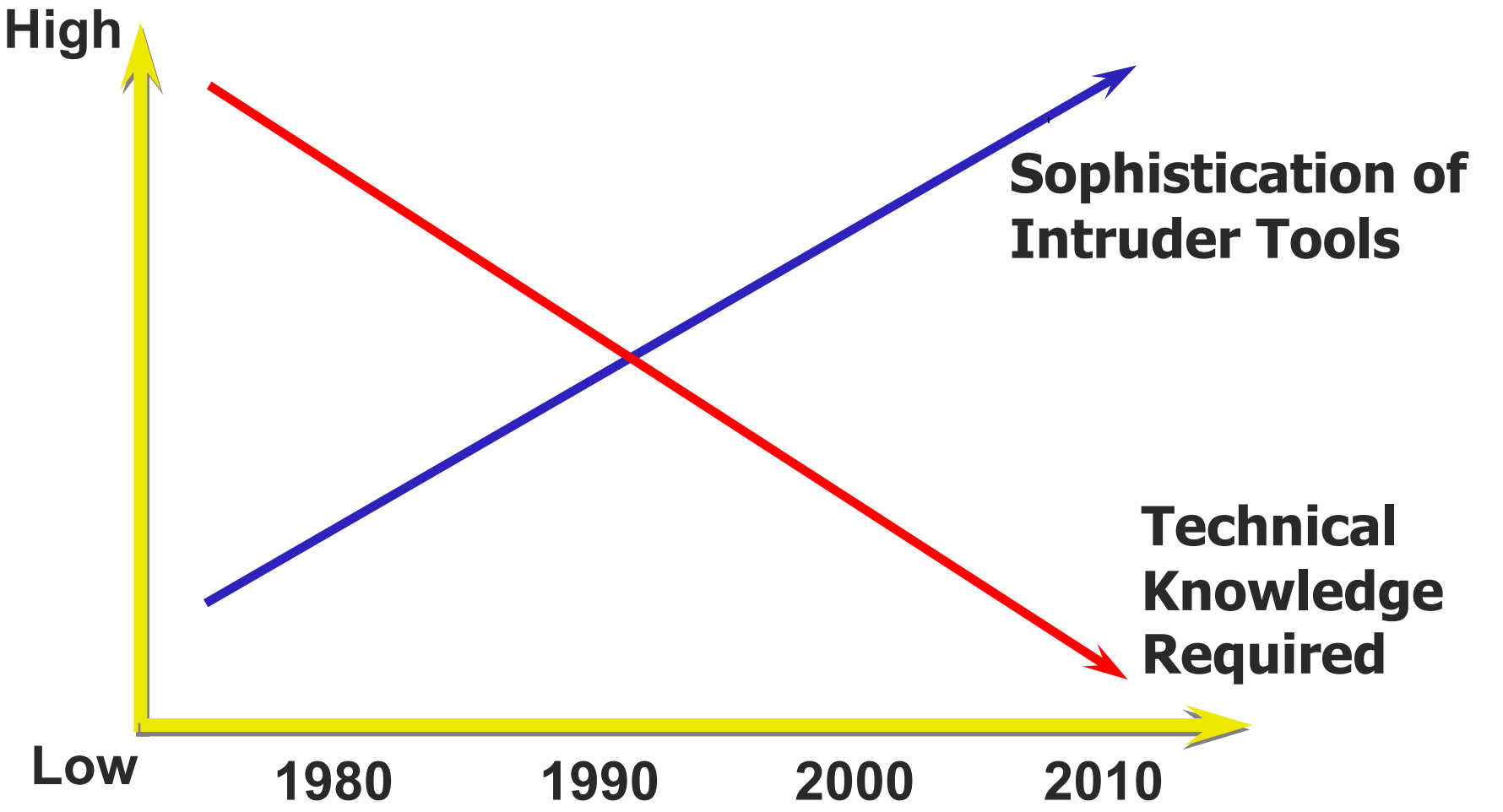
- https://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it?language=en
- How do you pick up a malicious online virus, the kind of malware that snoops on your data and taps your bank account? Often, it's through simple things you do each day without thinking twice. James Lyne reminds us that it's not only the NSA that's watching us, but ever-more-sophisticated cybercriminals, who exploit both weak code and trusting human nature.

Food for Thought …

- 90% of companies detected computer security breaches in the last 12 months
- 80% acknowledged financial losses due to computer breaches
- 74% cited the Internet as the most frequent origin of attack
- 40% detected denial of service attacks
- 40% detected system penetration from the outside
- 85% detected computer viruses

Source: CSI/FBI Computer Crime and Security Survey

Why are Security Incidents Increasing?



The virus analogy

- Health and precautions
  - importance of health
  - importance of healthy living
- How do you know you're ill?
  - real and imagined illness
  - incubation, chronic illness
  - going to the doctor

Dealing with viruses

- Diagnosis
  - via hunters
  - scan for known virus signatures
- Cure
  - via killers/disinfectants
  - erase or edit identified virus elements
- Prevention
  - via guardians
  - monitor for suspect activity

Problems with viral control

- New viruses
  - Signatures not on databases
  - Awareness of risk
  - Hoaxes
- Old viruses
  - Penetration and eradication
- People
  - Knowledge and gullibility
  - The weak link?

Tips for staying safe

- Minimise external contact
- Check incoming material
- Use tools regularly
- Keep tools up-to-date
- Write-protect disks
- Don’t boot from removeable media
- Keep backups
- Avoid high-risk/unknown sources

Tips for staying safe

Trust no-one!

The two key rules of virus control

- Check ALL incoming materials for viruses BEFORE use
- If you find a virus, tell the system manager and the supplier of the infected material
- The biggest source of virus infection is?

People not following the rules!

Questions?

OK...

Take a break!