9. Information Assurance and Security, Protecting Information Resources

Alexander Nikov

Learning Objectives

- Explain why information systems are vulnerable to destruction, error, and abuse.
- Describe the business value of security and control.
- Describe the components of an organizational framework for security and control.
- Describe the tools and technologies used for safeguarding information resources.

You’re on Facebook? Watch Out!

- Facebook – world’s largest social network
- Problem – Identity theft and malicious software
  - Examples:
    - Feb 2010 18-month hacker scam for passwords, resulted in Trojan horse download that stole financial data
    - Koobface worm
    - Spam campaigned aimed at stealing logins
- Illustrates: Types of security attacks facing consumers
- Demonstrates: Ubiquity of hacking, malicious software
1. System Vulnerability and Abuse

2. Business Value of Security and Control

3. Establishing a Framework for Security and Control

4. Technologies and Tools for Protecting Information Resources

**Why systems are vulnerable**

- Accessibility of networks
- Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
- Software problems (programming errors, installation errors, unauthorized changes)
- Disasters
- Use of networks/computers outside of firm’s control
- Loss and theft of portable devices

**Contemporary Security Challenges And Vulnerabilities**

- 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

The architecture of a Web-based application typically includes 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.
**Internet vulnerabilities**

- Network open to anyone
- Size of Internet means abuses can have wide impact
- Use of fixed Internet addresses with cable or DSL modems creates fixed targets hackers
- Unencrypted VOIP
- E-mail, P2P, IM
  - Interception
  - Attachments with malicious software
  - Transmitting trade secrets

**Wireless security challenges**

- Radio frequency bands easy to scan
- SSIDs (service set identifiers)
  - Identify access points
  - Broadcast multiple times
  - Can be identified by sniffer programs
  - War driving
    - Eavesdroppers drive by buildings and try to detect SSID and gain access to network and resources
    - Once access point is breached, intruder can use OS to access networked drives and files

**Wi-Fi Security Challenges**

Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

**Malware (malicious software)**

- Viruses
  - Rogue software program that attaches itself to other software programs or data files in order to be executed
- Worms
  - Independent computer programs that copy themselves from one computer to other computers over a network.
- Worms and viruses spread by
  - Downloads (drive-by downloads)
  - E-mail, IM attachments
  - Downloads on Web sites and social networks
Malware (cont.)

- Smartphones as vulnerable as computers
  - Study finds 13,000 types of smartphone malware
- Trojan horses
  - Software that appears benign but does something other than expected
- SQL injection attacks
  - Hackers submit data to Web forms that exploits site’s unprotected software and sends rogue SQL query to database
- Spyware
  - Small programs install themselves surreptitiously on computers to monitor user Web browsing activity and serve up advertising
  - Key loggers
    - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks
  - Other types:
    - Reset browser home page
    - Redirect search requests
    - Slow computer performance by taking up memory

Examples of Malicious Code

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conficker (aka</td>
<td>Worm</td>
<td>First detected in November 2008. Uses flaws in Windows software to take over</td>
</tr>
<tr>
<td>Downup)</td>
<td></td>
<td>machines and link them into a virtual computer that can be commande</td>
</tr>
<tr>
<td></td>
<td>Downup)</td>
<td>d from control. Has more than 5 million computers worldwide under its contro</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lle. Difficult to eradicate.</td>
</tr>
<tr>
<td>Storm</td>
<td>Worm/Trojan</td>
<td>First identified in January 2007. Spreads via e-mail spam with a fake attach</td>
</tr>
<tr>
<td></td>
<td>horse</td>
<td>ment. Infected up to 10 million computers, causing them to join its zombie</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network of computers engaged in criminal activity.</td>
</tr>
<tr>
<td>Sasser.ftp</td>
<td>Worm</td>
<td>First appeared in May 2004. Spread over the Internet by attacking random IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>addresses. Causes computers to continually crash and reboot, and infected ce</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mputers to search for more victims. Affected millions of computers worldwide,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disrupting British Airways flight check-ins, operations of British coast guard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>stations, Hong Kong hospitals, Taiwan post office branches, and Australia's</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Westpac Bank. Sasser and its variants caused an estimated $14.8 billion to $18.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>billion in damage worldwide.</td>
</tr>
<tr>
<td>MyDoom.A</td>
<td>Worm</td>
<td>First appeared on January 26, 2004. Spreads as an e-mail attachment. Sends</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e-mail to addresses harvested from infected machines, forging the sender’s ad</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dress. At its peak this worm lowered global Internet performance by 10 percent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and Web page loading times by as much as 50 percent. Programmed to stop spre</td>
</tr>
<tr>
<td>Sobig.F</td>
<td>Worm</td>
<td>First detected on August 19, 2003. Spreads via e-mail attachments and sends</td>
</tr>
<tr>
<td></td>
<td></td>
<td>massive amounts of mail with forged sender information. Deactivated itself o</td>
</tr>
<tr>
<td></td>
<td></td>
<td>n September 10, 2003, after infecting more than 1 million PCs and doing $50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>billion in damage.</td>
</tr>
<tr>
<td>ILOVEYOU</td>
<td>Virus</td>
<td>First detected on May 3, 2000. Script virus written in Visual Basic script and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overw</td>
</tr>
<tr>
<td></td>
<td></td>
<td>riters e-mail, music, and other files with a copy of itself and did an estima</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ted $10 billion to $15 billion in damage.</td>
</tr>
<tr>
<td>Melissa</td>
<td>Macro virus/</td>
<td>First appeared in March 1999. Word macro script mailing infected Word file t</td>
</tr>
<tr>
<td></td>
<td>worm</td>
<td>o first 50 entries in user's Microsoft Outlook address book. Infected 15 to 29</td>
</tr>
<tr>
<td></td>
<td></td>
<td>percent of all business PCs, causing $300 million to $600 million in damage.</td>
</tr>
</tbody>
</table>

Spoofing and Sniffer

- Spoofing
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Redirecting Web link to address different from intended one, with site masquerading as intended destination
- Sniffer
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, etc.

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
Denial-of-service attacks

- Denial-of-service attacks (DoS)
  - Flooding server with thousands of false requests to crash the network.
- Distributed denial-of-service attacks (DDoS)
  - Use of numerous computers to launch a DoS
  - Botnets
    - Networks of “zombie” PCs infiltrated by bot malware
    - Deliver 90% of world spam, 80% of world malware
    - Grum botnet: controlled 560K to 840K computers

Computer crime

- Defined as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”
- Computer may be target of crime, e.g.:
  - Breaching confidentiality of protected computerized data
  - Accessing a computer system without authority
- Computer may be instrument of crime, e.g.:
  - Theft of trade secrets
  - Using e-mail for threats or harassment

Examples of Computer Crime

<table>
<thead>
<tr>
<th>COMPUTERS AS TARGETS OF CRIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breaching the confidentiality of protected computerized data</td>
</tr>
<tr>
<td>Accessing a computer system without authority</td>
</tr>
<tr>
<td>Knobly accessing a protected computer to commit fraud</td>
</tr>
<tr>
<td>Intentionally accessing a protected computer and causing damage, negligently or deliberately</td>
</tr>
<tr>
<td>Knobly transmitting a program, program code, or command that intentionally causes damage to a protected computer</td>
</tr>
<tr>
<td>Threatening to cause damage to a protected computer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COMPUTERS AS INSTRUMENTS OF CRIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of trade secrets</td>
</tr>
<tr>
<td>Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video</td>
</tr>
<tr>
<td>Schemes to defraud</td>
</tr>
<tr>
<td>Using e-mail for threats or harassment</td>
</tr>
<tr>
<td>Intentionally attempting to intercept electronic communication</td>
</tr>
<tr>
<td>Illegally accessing stored electronic communications, including e-mail and voice mail</td>
</tr>
<tr>
<td>Transmitting or possessing child pornography using a computer</td>
</tr>
</tbody>
</table>

Identity theft, Phishing and Evil twins

- 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
Pharming, Click fraud, Cyberterrorism and Cyberwarfare

- **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
- **Cyberterrorism and Cyberwarfare**

Internal threats: employees

- Security threats often originate inside an organization
- Inside knowledge
- Sloppy security procedures
  - User lack of knowledge
- Social engineering:
  - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information

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 exploits often created faster than patches be released and implemented

Outline

1. System Vulnerability and Abuse
2. **Business Value of Security and Control**
3. Establishing a Framework for Security and Control
4. Technologies and Tools for Protecting Information Resources
**Business Value of Security and Control**

- Failed computer systems can lead to significant or total loss of business function
- Firms now more vulnerable than ever
  - Confidential personal and financial data
  - Trade secrets, new products, strategies
- A security breach may cut into firm’s market value almost immediately
- Inadequate security and controls also bring forth issues of liability

**Legal and regulatory requirements for electronic records management and 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

**Electronic evidence and Computer forensics**

- Electronic evidence
  - Evidence for white collar crimes often in digital form
    - Data on computers, e-mail, instant messages, e-commerce transactions
  - Proper control of data can save time and money when responding to legal discovery request
- 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

**Outline**

1. System Vulnerability and Abuse
2. Business Value of Security and Control
3. Establishing a Framework for Security and Control
4. Technologies and Tools for Protecting Information Resources
**Information systems controls**

- Information systems controls
  - Manual and automated controls
  - General and application controls
- General controls
  - 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, and manual procedures to create overall control environment

**Types of general Controls**

<table>
<thead>
<tr>
<th>TYPE OF GENERAL CONTROL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software controls</td>
<td>Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.</td>
</tr>
<tr>
<td>Hardware controls</td>
<td>Ensure that computer hardware is physically secure, and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.</td>
</tr>
<tr>
<td>Computer operations controls</td>
<td>Overse see the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.</td>
</tr>
<tr>
<td>Data security controls</td>
<td>Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.</td>
</tr>
<tr>
<td>Implementation controls</td>
<td>Audit the systems development process at various points to ensure that the process is properly controlled and managed.</td>
</tr>
<tr>
<td>Administrative controls</td>
<td>Formalize standards, rules, procedures, and control disciplines to ensure that the organization’s general and application controls are properly executed and enforced.</td>
</tr>
</tbody>
</table>

**Application controls**

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

**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

<table>
<thead>
<tr>
<th>EXPOSURE</th>
<th>PROBABILITY</th>
<th>LOSS RANGE (AVG)</th>
<th>EXPECTED ANNUAL LOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power failure</td>
<td>30%</td>
<td>$5K - $200K ($102,500)</td>
<td>$30,750</td>
</tr>
<tr>
<td>Embezzlement</td>
<td>5%</td>
<td>$1K - $50K ($25,500)</td>
<td>$1,275</td>
</tr>
<tr>
<td>User error</td>
<td>98%</td>
<td>$200 - $40K ($20,100)</td>
<td>$19,698</td>
</tr>
</tbody>
</table>
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

Identity management

- Business processes and tools to identify valid users of system and control access
  - Identifies and authorizes different categories of users
  - Specifies which portion of system users can access
  - Authenticates users and protects identities
- Identity management systems
  - Captures access rules for different levels of users

Security Profiles For A Personnel System

These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.

Disaster recovery and Business continuity planning

- Disaster recovery planning: Devises plans for restoration of disrupted services
- 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 which systems restored first
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.

### Outline

1. System Vulnerability and Abuse
2. Business Value of Security and Control
3. Establishing a Framework for Security and Control
4. Technologies and Tools for Protecting Information Resources

### Identity management and authentication

- Identity management software
  - Automates keeping track of all users and privileges
  - Authenticates users, protecting identities, controlling access
- Authentication
  - Password systems
  - Tokens
  - Smart cards
  - Biometric authentication

### Sample Auditor’s List Of Control Weaknesses

This chart is a 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.

<table>
<thead>
<tr>
<th>Function: Loans</th>
<th>Prepared by: J. Ericson</th>
<th>Received by: T. Benson</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location: Pearls, IL</td>
<td>Date: June 16, 2011</td>
<td>Review date: June 28, 2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nature of Weakness and Impact</th>
<th>Chance for Error/Abuse</th>
<th>Notification to Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>User accounts with missing passwords</td>
<td>Yes/No</td>
<td>Justification</td>
</tr>
<tr>
<td>Network configured to allow some sharing of system files</td>
<td>Yes</td>
<td>Leaves system open to unauthorized outsiders or attackers</td>
</tr>
<tr>
<td>Software patches can update production programs without final approval from Standards and Controls group</td>
<td>No</td>
<td>Exposes critical system files to hostile parties connected to the network</td>
</tr>
</tbody>
</table>

FIGURE 8-4

9-37

9-38

9-39

9-40
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

The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic.

Technologies and Tools for Protecting Information Resources

- 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
- Antivirus and antispyware software:
  - Checks computers for presence of malware and can often eliminate it as well
  - Require continual updating
- Unified threat management (UTM) systems

Securing wireless networks

- WEP security can provide some security by
  - Assigning unique name to network’s SSID and not broadcasting SSID
  - Using it with VPN technology
- Wi-Fi Alliance finalized WAP2 specification, replacing WEP with stronger standards
  - Continually changing keys
  - Encrypted authentication system with central server
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)
  - Secure Hypertext Transfer Protocol (S-HTTP)

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

Public Key Encryption

- 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 verifies user’s identity, stores information 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
Digital Certificates

Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

![Diagram of digital certificates]

FIGURE 8-7

Ensuring system availability

- 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

Ensuring system availability (cont.)

- Recovery-oriented computing
  - Designing systems that recover quickly with capabilities to help operators pinpoint and correct of faults in multi-component systems
- Controlling network traffic
  - Deep packet inspection (DPI)
    - Video and music blocking
- Security outsourcing
  - Managed security service providers (MSSPs)

Security in the cloud

- Responsibility for security resides with company owning the data
- Firms must ensure providers provides adequate protection:
  - Where data are stored
  - Meeting corporate requirements, legal privacy laws
  - Segregation of data from other clients
  - Audits and security certifications
- Service level agreements (SLAs)
Securing mobile platforms

- Security policies should include and cover any special requirements for mobile devices
  - Guidelines for use of platforms and applications
- Mobile device management tools
  - Authorization
  - Inventory records
  - Control updates
  - Lock down/erase lost devices
  - Encryption
- Software for segregating corporate data on devices

Ensuring software quality

- Software metrics: Objective assessments of system in form of quantified measurements
  - Number of transactions
  - Online response time
  - Payroll checks printed per hour
  - Known bugs per hundred lines of code
- Early and regular testing
- Walkthrough: Review of specification or design document by small group of qualified people
- Debugging: Process by which errors are eliminated

Video Case: IBM Zone Trusted Information Channel

http://www.youtube.com/watch?v=mPZrkeHMDJ8

Video Case 1
IBM Zone Trusted Information Channel

1. What are some common types of malicious software, or malware? What best describes the ‘man-in-the-middle’ type attack?

2. Provide some examples of each type of authentication factor. What are your experiences with each?

3. Can you think of any drawbacks of the ZTIC device?

4. How might malicious attackers try to get around devices like the ZTIC?

5. Do you foresee a future where malware is completely eliminated, or protections are so good that malware is no longer a threat? Explain your answer.
1. What are some common types of malicious software, or malware? What best describes the ‘man-in-the-middle’ type attack?

- Common types of malicious software include viruses, worms, Trojan horses, and spyware. A keylogger is a type of spyware that records the keystrokes of the user. Many of these types of malicious software are used in bank fraud-related activities. The ‘man-in-the-middle’ attack is most often executed by a Trojan installed on the user’s system.

2. Provide some examples of each type of authentication factor. What are your experiences with each?

- For example: a person question you need to answer to change your password for a site (a personal factor), a retinal scanner (a human factor), and the ZTIC (a technical factor).

3. Can you think of any drawbacks of the ZTIC device?

- One drawback of the device is that while the Internet is ubiquitous, you would need to bring the ZTIC everywhere you go to safely perform banking transactions anywhere, anytime.

4. How might malicious attackers try to get around devices like the ZTIC?

- Though the ZTIC might prevent attackers from performing any transactions themselves, more emphasis might be placed on acquiring other information from the user's hard drive, like account numbers, balances, and other transaction details.
5. Do you foresee a future where malware is completely eliminated, or protections are so good that malware is no longer a threat? Explain your answer.

- Malware is only a temporary phenomenon and is likely to be outpaced by preventive technologies, it's not likely this will happen. Too many people do not take efficient care of their computers for malware to die out completely.