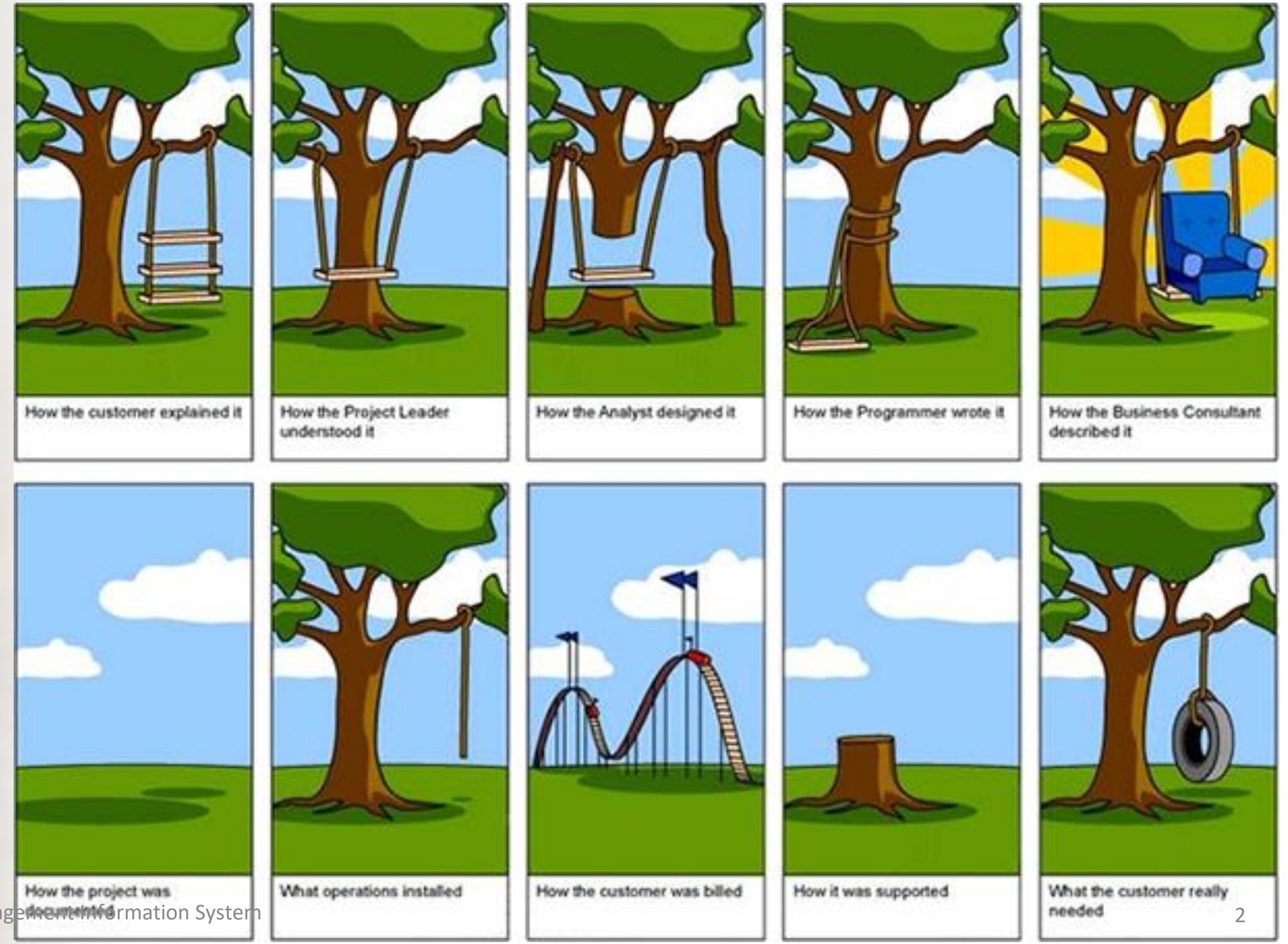
Week 9 Review

- Choices in System Acquisition
  - Outsourcing
  - Licensing
  - Software as a Service
  - User Application Development


How the customer explained it
How the Project Leader understood it
How the Analyst designed it
How the Programmer wrote it
How the Business Consultant described it
How the project was documented
What operations installed
How the customer was billed
How it was supported
What the customer really needed

Management Information Systems (MINSYST)

Week Ten

Objectives

- Identify the primary goals of information security
- Enumerate the main types of risks to information systems
- Improve security of information systems and the information it stores

Goals of Information Security

- Protecting IT resources is a primary concern
- Securing corporate ISs is becoming increasingly challenging

Goals of Information Security

- The major goals of information security are to:
  - Reduce the risk of systems ceasing operation
  - Maintain information confidentiality
  - Ensure the integrity and reliability of data resources
  - Ensure the uninterrupted availability of resources
  - Ensure compliance with policies and laws

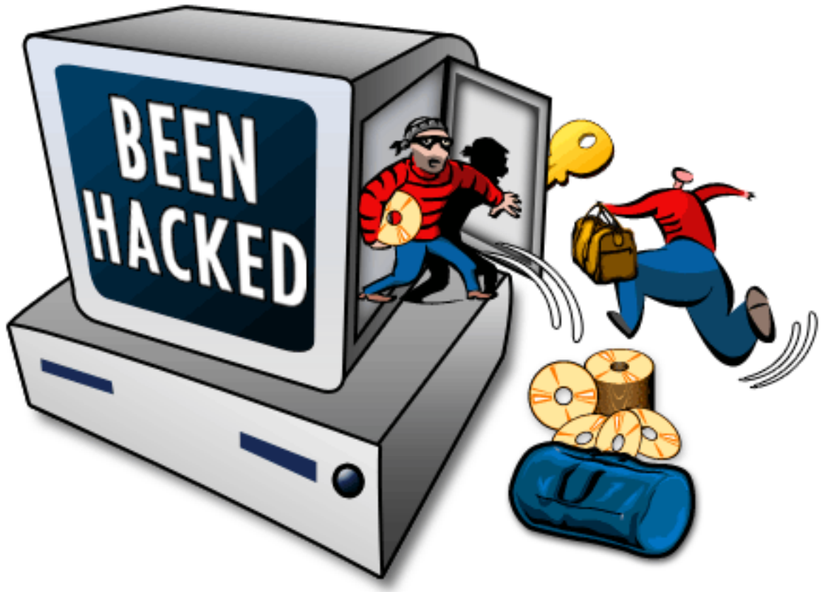
Risks to Information Systems

- Downtime: the period of time during which an IS is not available
- Extremely expensive: average losses of:
  - $2,500/minute for CRM systems
  - $7,800/minute for e-commerce applications
  - $4 billion lost annually in the U.S. due to downtime

Risks

Risks to Hardware

- Major causes of damage to hardware include:
  - Natural disasters
  - Blackouts and brownouts
  - Vandalism



Risks to Data and Applications

- Data and applications are susceptible to disruption, damage, and theft
  - Theft of information and identity theft
  - Data alteration, data destruction, and Web defacement
  - Computer viruses, worms, and logic bombs
  - Non-malicious mishaps

Risks to Online Operations

- Many hackers try daily to interrupt online businesses
- Types of attacks include:
  - Unauthorized access
  - Data theft
  - Defacing of Web pages
  - Denial of service
  - Hijacking

Denial of Service

- *Denial of service (DoS)*: an attacker launches a large number of information requests
- *Distributed denial of service (DDoS)*: an attacker launches a DoS attack from multiple computers
  - Usually launched from hijacked personal computers called "zombies"

Computer Hijacking

- *Hijacking*: using some or all of a computer's resources without the consent of its owner
  - Done by installing a software bot on the computer
  - Main purpose of hijacking is usually to send spam

Errors & Accidents

- Human errors
- Procedural errors
- Software errors
- ‘Dirty data’ problems
- Electromechanical problems

Security

Controls

- *Controls*: constraints and restrictions imposed on a user or a system
  - Application reliability and Data Entry Controls
  - Backup
  - Access Controls
  - Atomic Transactions
  - Audit Trail

Application Reliability and Data Entry Controls

- A reliable application is one that can resist inappropriate usage such as incorrect data entry or processing
- Controls also translate business policies into system features

Backup

- *Backup*: periodic duplication of all data
- Data backup not enough; must be routinely transported off-site as protection from a site disaster

Access Controls

- *Access controls*: measures taken to ensure only authorized users have access to a computer, network, application, or data
- Three types of access controls:
  - What you know
  - What you have
  - Who you are

Access Controls

- Security card is more secure than a password
- *Biometric*: uses unique physical characteristics such as fingerprints, retinal scans, or voiceprint

Atomic Transactions

- *Atomic transaction*: a set of indivisible transactions
  - All of the transactions in the set must be completely executed, or none can be
  - Ensures that only full entry occurs in all the appropriate files to guarantee integrity of the data
  - Is also a control against malfunction and fraud

Audit Trail

- *Audit trail*: a series of documented facts that help detect who recorded which transactions, at what time, and under whose approval
- *Information systems auditor*: a person whose job is to find and investigate fraudulent cases

Security Measures

- Organizations can protect against attacks using various approaches, including:
  - Firewalls
  - Authentication
  - Encryption
  - Digital signatures
  - Digital certificates

Firewalls and Proxy Servers

- *Firewall*: the best defense against unauthorized access over the Internet
- *DMZ*: demilitarized zone approach
- *Proxy server*: represents another server

Authentication and Encryption

- *Authentication*: the process of ensuring that you are who you say you are
- *Encryption*: coding a message into an unreadable form

Authentication and Encryption

- Encryption programs scramble the transmitted information
  - Plaintext
  - Ciphertext
- Encryption uses a mathematical algorithm and a key

Authentication and Encryption

- Public key encryption
  - *Symmetric encryption*: when the sender and the recipient use the same key
  - *Asymmetric encryption*: both a public and a private key are used

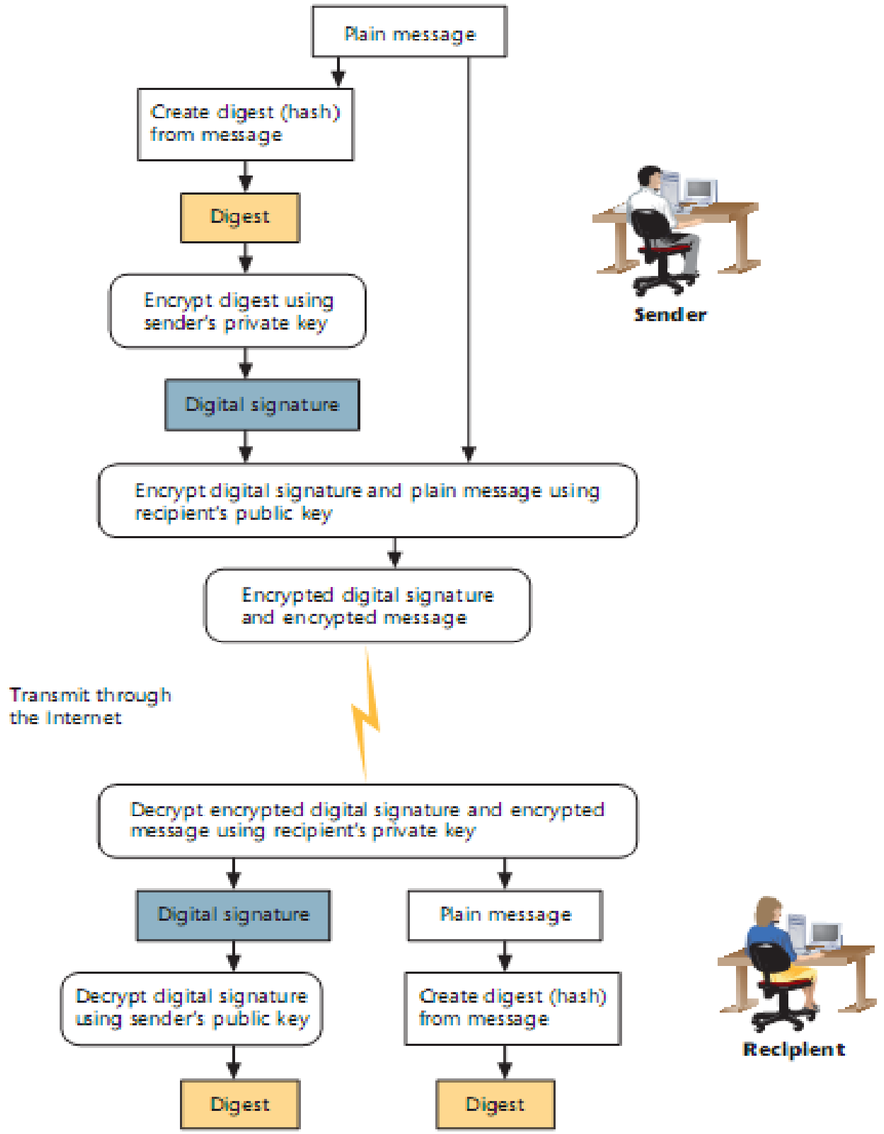
Authentication and Encryption

- *Transport Layer Security (TLS)*: a protocol for transactions on the Web that uses a combination of public key and symmetric key encryption
- *HTTPS*: the secure version of HTTP

Authentication and Encryption

- *Digital signature*: a means to authenticate online messages; implemented with public keys
  - *Message digest*: akin to the unique fingerprint of a file

FIGURE 14.6
Using digital signatures



Reference:
Oz, E. (2011). *Principles of Management Information Systems*. Cengage Learning.

Authentication and Encryption

- *Digital certificates*: computer files that associate one's identity with one's public key
- *Certificate authority (CA)*: a trusted third party
- A digital certificate contains its holder's name, a serial number, its expiration dates, and a copy of holder's public key

A digital certificate as shown in two different Web browsers

Reference:
Oz, E. (2011). *Principles of Management Information Systems*. Cengage Learning.

The Downside of Security Measures

- *Single sign-on (SSO)*: a user must enter his or her name/password only once
- Encryption slows down communication
- IT specialists must clearly explain the implications of security measures to upper management

Disaster Recovery

Recovery Measures

- Organizations must have recovery measures in place, in preparation for probable uncontrolled disasters
  - Redundancy may be used
  - Other measures must be taken

The Business Recovery Plan

- *Business recovery plan*: a plan about how to recover from a disaster
  - Disaster recovery plan, business resumption plan, business continuity plan
- Emphasis should be on the damage to the organization's business

The Business Recovery Plan

- Nine steps to develop a business recovery plan:
  - Obtain management's commitment to the plan
  - Establish a planning committee
  - Perform risk assessment and impact analysis
  - Prioritize recovery needs

The Business Recovery Plan

- Nine steps to develop a business recovery plan:
  - Select a recovery plan
  - Select vendors
  - Develop and implement the plan
  - Test the plan
  - Continually test and evaluate

Recovery Planning and Hot Site Providers

- Can outsource recovery plans to firms that specialize in disaster recover planning
- *Hot sites*: alternative sites that a business can use when a disaster occurs
  - Backup sites provide desks, computer systems, and Internet links

The Economics of Information Security

- Security measures should be regarded as analogous to insurance
- Spending for security measures should be proportional to the potential damage
- A business must assess the minimum acceptable rate of system downtime and ensure that the company can financially sustain the downtime

How Much Security Is Enough Security?

- Two costs should be considered:
  - Cost of the potential damage
  - Cost of implementing a preventative measure
- As the cost of security measures increases, the cost of potential damage decreases
- The company must define what needs to be protected
- Security measures should never exceed the value of protected system

Calculating Downtime

- Businesses should try to minimize downtime, but the benefit of greater uptime must be compared to the added cost
  - Mission-critical systems must be connected to an alternative source of power, duplicated with a redundant system, or both
  - Many ISs are now interfaced with other systems
  - Redundancy reduces downtime