Business Data Communications and Networking

11th Edition

Jerry Fitzgerald and Alan Dennis

John Wiley & Sons, Inc

Dwayne Whitten, D.B.A
Mays Business School
Texas A&M University

Copyright 2011 John Wiley & Sons, Inc

Chapter 10

Network Security

Copyright 2011 John Wiley & Sons, Inc

Outline

10.1 - Introduction: Security threats and network controls

10.2 - Risk assessment

10.3 - Ensuring Business Continuity:

- **Preventing, detecting and correcting for disruption, destruction and disaster**

10.4 - Intrusion prevention:

- **Preventing, detecting, and correcting intrusions**

10.5 - Best practice recommendations

10.6 – Implications for Management

Copyright 2011 John Wiley & Sons, Inc

10.1 Introduction

- **Security has always been a major business concern**
  - ***Physical assets*** **are protected with locks, barriers, guards.**
  - ***Information assets*** **are protected with passwords, coding, certificates, encryption.**
- **Computers and Internet have redefined the nature of information security**
- **Laws and enforcement in cyber crime**
  - **Slow to catch-up**
  - **Breaking into a computer is now a federal crime in the U.S.**
  - **New laws against cyberborder crimes, yet difficult to enforce, sentences are typically very light**

Copyright 2011 John Wiley & Sons, Inc

Computer Security Incidents

- **Computer security increasingly important**
  - **More sophisticated tools for breaking in**
  - **Viruses, worms, credit card theft, identity theft leave firms with liabilities to customers**
- **Incidents are escalating at increasing rate**
- **Computer Emergency Response Team (CERT) was formed at Carnegie Mellon University with US DoD support**
  - **responds and raises awareness of computer security issues, www.cert.org**
- **Worldwide annual information security losses may be $2 trillion**

Copyright 2011 John Wiley & Sons, Inc

Financial Impact of Security

- **2005 Computer Security Institute/FBI Computer Crime and Security Survey**
  - **70% of the respondents reported security breaches in the last 12 months**
  - **60% reported a financial loss due to security breaches**
  - **Average loss: $350,000**
- **Security issues can impact consumer confidence**
- **70% of all email sent worldwide was spam in 2006**
- **New laws on data privacy and financial information include Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPPA)**

Copyright 2011 John Wiley & Sons, Inc

Why Networks Need Security

- **Organizations vulnerable due to dependency on computing and widely available Internet access to its computers and networks**
- **Business loss potential due to security breaches**
  - **$350,000 average loss per incident**
  - **Reduced consumer confidence as a result of publicity**
  - **Loss of income if systems offline**
- **Protecting organizations' data and application software**
  - **Value of data and applications far exceeds cost of networks**
  - **Firms may spend about $1,250/employee on network security**

Copyright 2011 John Wiley & Sons, Inc

Primary Goals in Providing Security: "CIA"

- ***Confidentiality***
  - **Protection of data from unauthorized disclosure of customers and proprietary data**
- ***Integrity***
  - **Assurance that data have not been altered or destroyed**
- ***Availability***
  - **Providing continuous operations of hardware and software so that parties involved can be assured of uninterrupted service**

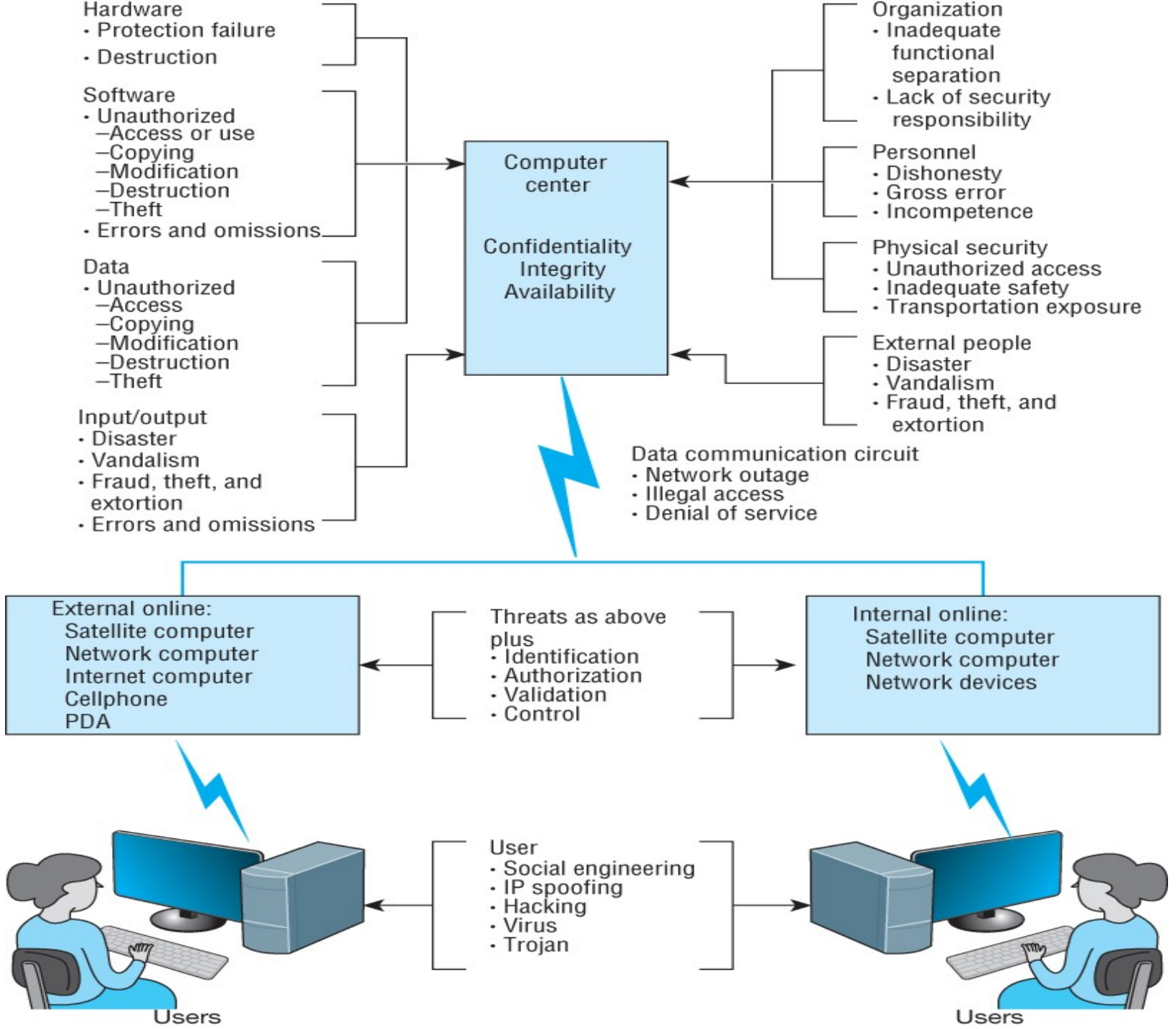
Copyright 2011 John Wiley & Sons, Inc

Types of Security Threats

- **Business continuity planning related threats**
  - **Disruptions**
    - **Loss or reduction in network service**
    - **Could be minor or temporary (a circuit failure)**
  - **Destructions of data**
    - **Viruses destroying files, crash of hard disk**
  - **Disasters (Natural or manmade disasters)**
    - **May destroy host computers or sections of network**
- **Intrusion**
  - **Hackers gaining access to data files and resources**
  - **Most unauthorized access incidents involve employees**
  - **Results: Industrial spying; fraud by changing data, etc.**

Copyright 2011 John Wiley & Sons, Inc

Threats to a computer center



Network Controls

- **Mechanisms that reduce or eliminate the threats to network security**
- **Types of controls:**
  - ***Preventative controls***
    - **Mitigate or stop a person from acting or an event from occurring (e.g., locks, passwords, backup circuits)**
    - **Act as a deterrent by discouraging or restraining**
  - ***Detective controls***
    - **Reveal or discover unwanted events (e.g., auditing)**
    - **Documenting events for potential evidence**
  - ***Corrective controls***
    - **Remedy an unwanted event or a trespass (e.g., reinitiating a network circuit)**

Copyright 2011 John Wiley & Sons, Inc

Securing the Network

- **Securing the network requires personnel designated to be accountable for controls:**
  - **Develop network controls**
  - **Ensure that controls are operating effectively**
  - **Update or replace controls when necessary**
- **Need to be reviewed periodically for usefulness, verification and testing:**
  - **Ensure that the control is still present (verification)**
  - **Determine if the control is working as specified (testing)**
  - **Is the control still working as it was specified?**
  - **Are there procedures for temporary overrides on control?**

Copyright 2011 John Wiley & Sons, Inc

10.2 Risk Assessment

- **A key step in developing a secure network**
- **Assigns level of risks to various threats**
  - **By comparing the nature of threats to the controls designed to reduce them**
- **Use a control spreadsheet**
  - **List down network assets on the side**
  - **List threats across the top**
  - **List the controls that are currently in use to address each threat in the corresponding cells**
  - **Allows optimization of controls based on risk**

Copyright 2011 John Wiley & Sons, Inc

Sample Control Spreadsheet

Threats / Assets (with Priority)	Disruption, Destruction, Disaster					Intrusion		
	Fire	Flood	Power Loss	Circuit Failure	Virus	External Intruder	Internal Intruder	Eaves-drop
(92) Mail server								
(90) Web server								
(90) DNS server								
(50) Computers on sixth floor								
(50) Sixth-floor LAN circuits								
(80) Building A backbone								
(70) Router in building A								
(30) Network software								
(100) Client database								
(100) Financial database								

Copyright 2011 John Wiley & Sons, Inc

Network Assets

- **Identify the assets on the network**
  - **Organization's data files most important**
  - **Mission-critical applications also very important**
    - **Programs critical to survival of business**
  - **Hardware, software components**
    - **Important, but easily replaceable**
- **Evaluate assets based on their importance**
- **Prioritizing assets is a business decision, not a technology decision**
- **Value of an asset is a function of:**
  - **Its replacement cost**
  - **Personnel time to replace the asset**
  - **Lost revenue due to the absence of the asset**

Copyright 2011 John Wiley & Sons, Inc

Types of Assets

Hardware	• Servers, such as mail servers, web servers, DNS servers, DHCP servers, and LAN file servers • Client computers • Devices such as hubs, switches, and routers
Circuits	• Locally operated circuits such LANs and backbones • Contracted circuits such as MAN and WAN circuits • Internet access circuits
Network Software	• Server operating systems and system settings • Applications software such as mail server and web server software
Client Software	• Operating systems and system settings • Application software such as word processors
Organizational Data	• Databases with organizational records
Mission critical applications	• For example, for an Internet bank, the Web site is mission critical

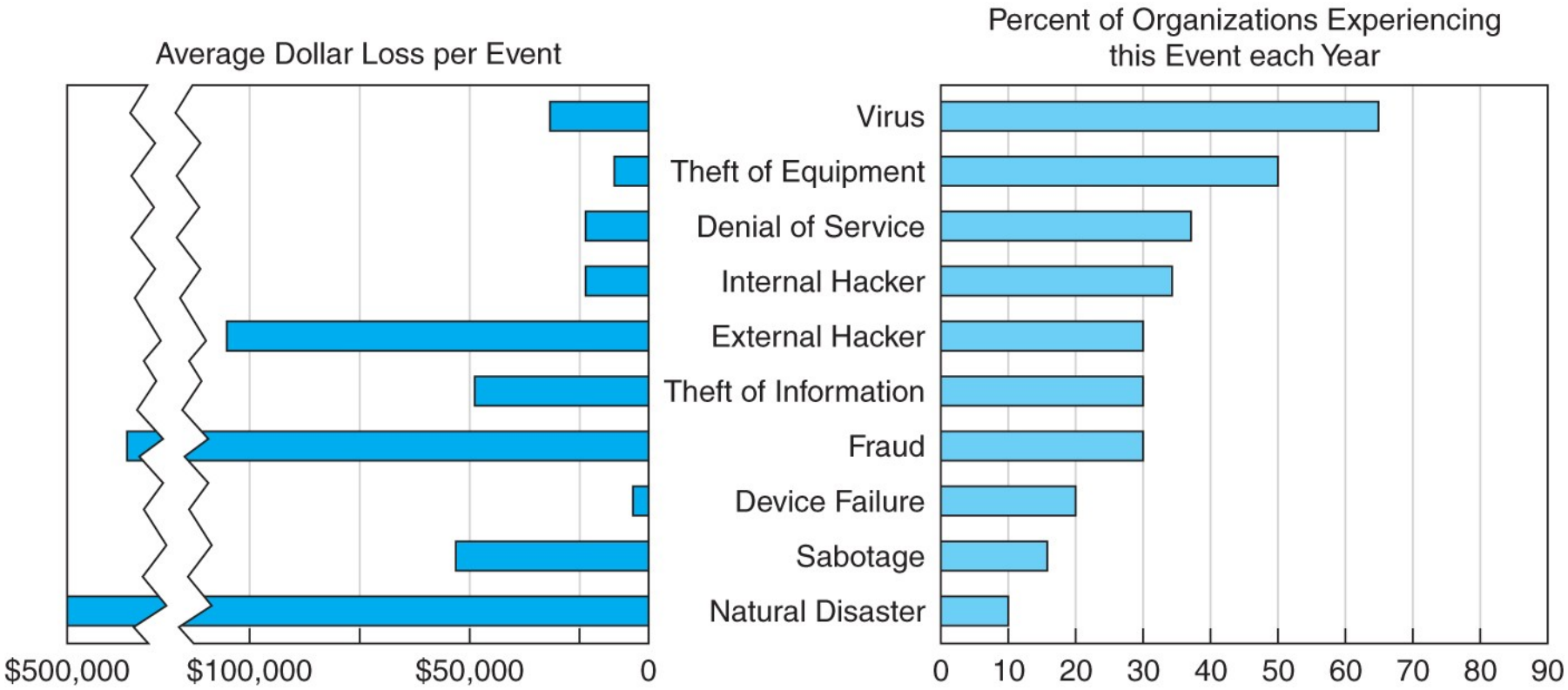
Copyright 2011 John Wiley & Sons, Inc

Security Threats

- **Identify threats**
  - **Any potentially adverse occurrence that can**
    - **Harm or interrupt the systems using the network, or**
    - **Cause a monetary loss to an organization**
- **Rank threats according to**
  - **Their probability of occurrence**
  - **Likely cost if the threat occurs**
- **Take the nature of business into account**
  - **Example: Internet banking vs. a restaurant**
    - **Bank's web site: has a higher probability of attack and much bigger loss if happens**
    - **Restaurant web site: much less likely and small loss**

Copyright 2011 John Wiley & Sons, Inc

Likelihood and Costs of Threats



Copyright 2011 John Wiley & Sons, Inc

Common Security Threats

THREATS:

- Virus infection is most likely event
- Intrusion
  - By internal employees and external hackers
  - High cost to recover in terms of financials and publicity
- Device failure (not necessarily by a malicious act)
- Device theft, Natural Disaster
- Denial of Service attacks
  - External attacks blocking access to the network
- Big picture messages:
  - Viruses: most common threat with a fairly high cost
  - External intrusion is now greater threat than own employees

COST OF THREATS:

- Costs may be $33,000 per virus that infects an average number of computers
- External intrusion may cost an average of $100,000 per incident
- Internal intrusion happens about as frequently as external intrusion, external is rising
- Natural disasters happen to about 20 percent of organizations each year
- Denial of Service attacks could cost Amazon.com $10 million per hour, organizations typically lose $100,000 to $200,000 per hour
- Cost of lost work for a single LAN may be $1000 to $5000 per hour

Copyright 2011 John Wiley & Sons, Inc

Identify and Document Controls

- **Identify existing controls and list them in the cell for each asset and threat**
- **For each asset and the specific threat**
  - **Describe each control that**
    - **Prevents,**
    - **Detects and/or**
    - **Corrects that threat**
  - **Place each control and its role in a numeric list (without any ranking)**
  - **Place the number in the cell (in the control spreadsheet)**
    - **Each cell may have one or more controls**

Copyright 2011 John Wiley & Sons, Inc

Sample Control Spreadsheet

Threats / Assets (with Priority)	Disruption, Destruction, Disaster					Intrusion		
	Fire	Flood	Power Loss	Circuit Failure	Virus	External Intruder	Internal Intruder	Eavesdrop
(92) Mail server	1, 2	1, 3	4	5, 6	7, 8	9, 10, 11	9, 10	
(90) Web server	1, 2	1, 3	4	5, 6	7, 8	9, 10, 11	9, 10	
(90) DNS server	1, 2	1, 3	4	5, 6	7, 8	9, 10, 11	9, 10	
(50) Computers on sixth floor	1, 2	1, 3			7, 8	10, 11	10	
(50) Sixth-floor LAN circuits	1, 2	1, 3						
(80) Building A backbone	1, 2	1, 3		6				
(70) Router in building A	1, 2	1, 3				9	9	
(30) Network software					7, 8	9, 10, 11	9, 10	
(100) Client database					7, 8	9, 10, 11	9, 10	
(100) Financial database					7, 8	9, 10, 11	9, 10	

Controls

1. Disaster recovery plan
2. Halon fire system in server room; sprinklers in rest of building
3. Not on or below ground level
4. Uninterruptable power supply (UPS) on all major network servers
5. Contract guarantees from interexchange carriers
6. Extra backbone fiber cable laid in different conduits
7. Virus checking software present on the network
8. Extensive user training about viruses and reminders in monthly newsletter
9. Strong password software
10. Extensive user training about password security and reminders in monthly newsletter
11. Application-layer firewall

Copyright 2011 John Wiley & Sons, Inc

Evaluate the Network's Security

- **Evaluate adequacy of the controls and resulting degree of risk associated with each threat**
- **Establish priorities for dealing with threats to network security**
  - **Which threats to be addressed immediately?**
- **Assessment can be done by**
  - **Network manager, or**
  - **A team of experts called a Delphi team, yields better results and analysis**
    - **Chosen (3-9 people) for their in-depth knowledge about the network and environment being reviewed**
    - **Includes key managers because they are important for implementing final results**

Copyright 2011 John Wiley & Sons, Inc

10.3 Ensuring Business Continuity

- **Make sure that organization's data and applications will continue to operate even in the face of disruption, destruction, or disaster**
- **Continuity Plan includes two major parts:**
  1. **Development of controls**
     - **To prevent these events from having a major impact**
  2. **Disaster recovery plan**
     - **To enable the organization to recover if a disaster occurs**

Copyright 2011 John Wiley & Sons, Inc

Specifics of Continuity Plan

- **Preventing Disruption, Destruction, and Disaster**
  - **Preventing Viruses**
  - **Preventing Denial of Service Attacks**
  - **Preventing Theft**
  - **Device Failure Protection**
  - **Disaster Protection**
- **Detecting Disruption, Destruction, and Disaster**
- **Correcting Disruption, Destruction, and Disaster**
  - **Disaster Recovery Plan**
  - **Disaster Recovery Outsourcing**

Copyright 2011 John Wiley & Sons, Inc

Preventing Computer Viruses

- **Viruses spreads when infected files are accessed**
  - **Macro viruses attach themselves to other programs (documents) and spread when the programs are executed (the files are opened)**
- **Worms**
  - **Special type of virus that spread itself without human intervention (sends copies of itself from computer to computer)**
- **Anti-virus software packages check disks and files to ensure that they are virus-free**
- **Incoming e-mail messages are most common source of viruses**
  - **Check attachments to e-mails, use filtering programs to 'clean' incoming e-mail**

Copyright 2011 John Wiley & Sons, Inc

Preventing Denial of Service Attacks

- **DoS attacks**
  - **Network disrupted by a flood of messages that prevents messages from normal users**
    - **Flooding web servers, email servers so server cannot respond**
- **Distributed DoS (DDoS) come from many different computers**
  - **DDoS agents on several machines are controlled by a DDoS handler, may issue instructions to computers to send simultaneous messages to a target computer**
- **Difficult to prevent DoS and DDoS attacks**
  - **Setup many servers around the world**
  - **Use Intrusion Detection Systems**
  - **Require ISPs to verify that all incoming messages have valid IP addresses**

Copyright 2011 John Wiley & Sons, Inc

DOS and DDOS Approaches

- ***Traffic filtering:*** verify all incoming traffic source addresses for validity (requires a lot of processing)
- ***Traffic limiting:*** When a flood of packets are entering the network, limit incoming access regardless of source (some may be legitimate)
- ***Traffic anomaly detectors:*** Perform analysis of traffic to see what normal traffic looks like, block abnormal patterns

Copyright 2011 John Wiley & Sons, Inc

Theft Protection

- **Security plan must include an evaluation of ways to prevent equipment theft**
- **Equipment theft**
  - **A big problem**
    - **About $1 billion lost each year to theft of computers and related equipment**
  - **Attractive good second hand market making these items valuable to steal**
- **Physical security is key component**

Copyright 2011 John Wiley & Sons, Inc

Device Failure Protection

- A key principal in preventing disruption, destruction and disaster
- Examples of components that provide redundancy
  - Uninterruptible power supplies (UPS)
    - A separate battery powered power supply
    - Can supply power for minutes or even hours
    - Some run on generators.
  - Fault-tolerant servers (with redundant components)
  - Disk mirroring
    - A redundant second disk for every disk on the server
    - Every data on primary disk is duplicated on mirror
  - Disk duplexing (redundant disk controllers)
- Can apply to other network components as well
  - Circuits, routers, client computers, etc.

Copyright 2011 John Wiley & Sons, Inc

Disaster Protection

- **More difficult to do since the entire site can be destroyed by a disaster**
- **Avoid disaster by:**
  - **Decentralizing the network resources**
  - **Storing critical data in at least two separate locations (in different parts of the country)**
- **Best solution**
  - **Have a completely redundant network that duplicates every network component, but in a different location**
- **Other steps**
  - **Depends on the type of disaster to be prevented**
    - **Flood: Locate key components away from rivers**
    - **Fire: Install fire suppression systems**

Copyright 2011 John Wiley & Sons, Inc

Disaster Recovery Plans (DRPs)

- **Identify clear responses to possible disasters**
- **Provide for partial or complete recovery of data, application software, network components, and physical facilities**
- **Includes backup and recovery controls**
  - **Make backup copies of all data and SW routinely**
  - **Encrypt them and store them offsite**
  - **Some use CDP, or Continuous Data Protection with copies of all data and transactions by time stamp for ease of restoration**
- **Should include a documented and tested approach to recovery, with formal testing**
- **Plan for loss of main database or long outages of data center**

Copyright 2011 John Wiley & Sons, Inc

Elements of a DRP

- **Names of decision making managers in charge of disaster recovery**
- **Staff assignments and responsibilities**
- **List of priorities of “fix-firsts”**
- **Location of alternative facilities**
- **Recovery procedures for data communications facilities, servers and application systems**
- **Actions to be taken under various contingencies**
- **Manual processes**
- **Plan updating and testing procedures**
- **Safe storage of data, software and the disaster recovery plan itself**

Copyright 2011 John Wiley & Sons, Inc

Two-Level DRPs

- **Level 1:**
  - **Build enough capacity and have enough spare equipment**
    - **To recover from a minor disaster (e.g., loss of a major server or portion of the network)**
  - **Could be very expensive**
- **Level 2: Disaster Recovery Outsourcing**
  - **Rely on professional disaster recovery firms**
    - **To provide second level support for major disasters**

Copyright 2011 John Wiley & Sons, Inc

Disaster Recovery Firms

- **Offer a range of services**
  - **Secure storage for backups**
  - **A complete networked data center that clients can use in disasters**
  - **Complete recovery of data and network within hours**
- **Expensive, used by large organizations**
  - **May be worthwhile when millions of dollars of lost revenue may be at stake**

Copyright 2011 John Wiley & Sons, Inc

10.4 Intrusion Prevention

- **Types of intruders**
  - **Casual intruders**
    - **With Limited knowledge (“trying doorknobs”)**
    - **Script kiddies: Novice attackers using hacking tools**
  - **Security experts (hackers)**
    - **Motivation: the thrill of the hunt; show off**
    - **Crackers: hackers who cause damage**
  - **Professional hackers (espionage, fraud, etc)**
    - **Breaking into computers for specific purposes**
  - **Organization employees**
    - **With legitimate access to the network**
    - **Gain access to information not authorized to use**

Copyright 2011 John Wiley & Sons, Inc

Intrusion Prevention

- **Requires a *proactive* approach that includes routinely testing the security systems**
- **Best rule for high security**
  - **Do not keep extremely sensitive data online**
  - **Store them in computers isolated from the network**
- **Security Policy**
  - **Critical to controlling risk due to access**
  - **Should define clearly**
    - **Important assets to be safeguarded and Controls needed**
    - **What employees should do**
    - **Plan for routinely training employees and testing security controls in place**

Copyright 2011 John Wiley & Sons, Inc

Elements of a Security Policy

- **Names of decision making managers**
- **Incident reporting system and response team**
- **Risk assessment with priorities**
- **Controls on all major access points to prevent or deter unauthorized external access**
- **Controls within the network to ensure internal users cannot exceed their authorized access**
- **An acceptable use policy**
- **User training plan on security**
- **Testing and updating plans**

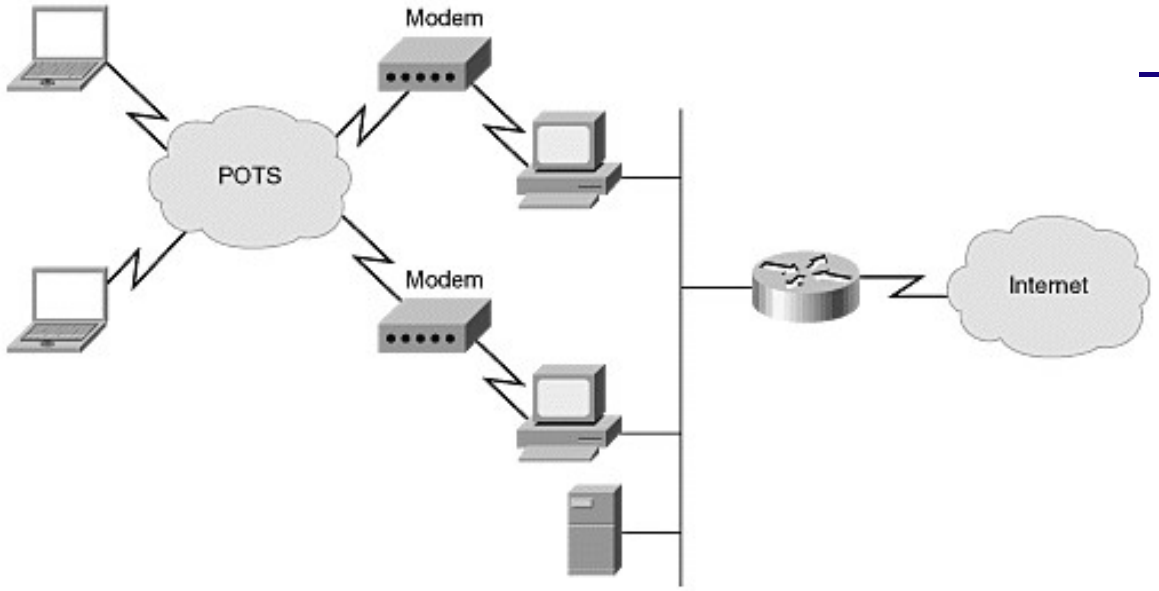
Copyright 2011 John Wiley & Sons, Inc

Securing Network Perimeter

- **Basic access points into a network**
  - **LANs inside the organization**
  - **Dial-up access through a modem**
  - **Internet (most attacks come in this way)**
- **Basic elements in preventing access**
  - **Perimeter Security and Firewalls**
  - **Network Address Translation (NAT) Proxy servers**
  - **Physical Security**
  - **Dial-in security**

Copyright 2011 John Wiley & Sons, Inc

– Dial-in security



- The need to support dial-in users might prove to be the security administrator's largest challenge. This is especially true if users are allowed to dial (via POTS or ISDN) in directly to their workstations or servers, bypassing all other security methods.
- User insist that the normal security precautions need to be bypassed because of special circumstances.
- For example, the argument can be made that direct access of the hardware is required for debugging purposes. Or a connection must be made for testing purposes without interference or delays imposed by security methods. This scenario can be differentiated from one where there is a central device on the network for dial-in access (such as a Cisco access server or a single Windows NT RAS server) by the fact that there are multiple entries into the network.

Firewalls

- **Prevent intruders by securing Internet connections**
  - **From making unauthorized access and denial of service attacks to your network**
- **Could be a router, gateway, or special purpose computer**
  - **Examines packets flowing into and out of the organization's network**
  - **Restricts access to that network**
  - **Placed on every connection that network has to Internet**
- **Main types of firewalls**
  - **Packet level firewalls (a.k.a., packet filters)**
  - **Application-level firewalls (a.k.a., application gateway)**

Copyright 2011 John Wiley & Sons, Inc

Packet-level Firewalls

- **Examines the source and destination address of every packet passing through**
  - **Allows only packets that have acceptable addresses to pass**
  - **Examines IP Addresses and TCP port IDs only**
    - **Packet filtering firewall is unaware of applications and what the intruder is trying to do**
- **Access Control Lists**
  - **A set of rules for a packet-level firewall**
  - **Can be used to**
    - **permit packets into a network**
    - **deny packets entry**

Copyright 2011 John Wiley & Sons, Inc

IP Spoofing

- **"IP spoofing" remains a problem**
  - **Done by simply changing the source address of incoming packets from their real address to an address inside the organization's network**
    - **Firewall will pass this packet as it looks like a valid internal IP address**
    - **Many firewalls know to discard incoming packets with internal IP addresses**

Copyright 2011 John Wiley & Sons, Inc

Application-Level Firewalls

- **Acts as an intermediate host computer (between outside clients and internal servers)**
  - **Forces anyone to login to this firewall and allows access only to authorized applications (e.g., Web site access)**
  - **Separates a private network from the rest of the Internet**
    - **Hides individual computers on the network behind the firewall**
- **Some prohibit external users downloading executable files**
  - **Software modifications done via physical access**
- **Requires more processing power than packet filters which can impact network performance**

Copyright 2011 John Wiley & Sons, Inc

Network Address Translation (NAT)

- **Used by most firewalls to shield a private network from public network**
  - **Translates between private addresses inside a network and public addresses outside the network**
  - **Done transparently (unnoticed by external computers)**
  - **Internal IP addresses remain hidden**
- **Performed by NAT proxy servers**
  - **Uses an address table to do translations**
  - **Ex: a computer inside accesses a computer outside**
    - **Change source IP address to its own address**
    - **Change source port number to a unique number**
      - **Used as an index to the original source IP address**
    - **Performs reverse operations for response packets**

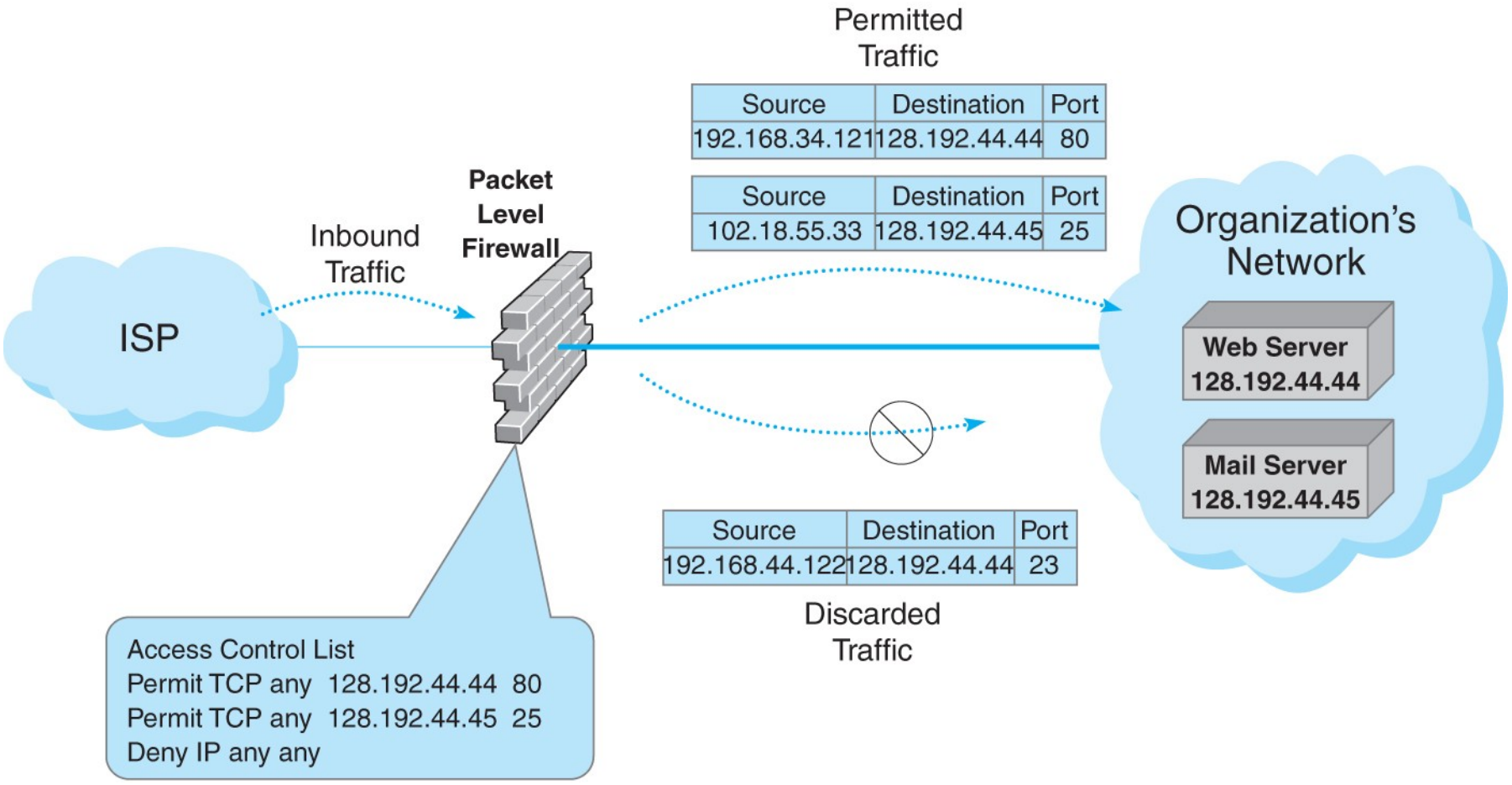
Copyright 2011 John Wiley & Sons, Inc

Using Private Addresses with NAT

- **Used to provide additional security**
- **Assigns private IP addresses to devices inside the network**
  - **Even if they are discovered, no packets with these addresses will be delivered (publicly illegal IP address)**
  - **Example: Assigned by ICANN: 128.192.55.xx**
    - **Assign to NAT proxy server: 128.192.55.1**
    - **Assign to internal computers: 10.3.3.xx**
      - **10.x.x.x is reserved for private networks (never used on Internet)**
    - **No problem for users as handled by NAT proxy server, but big problem for intruders**
- **Additional benefit is that it gives ability to have more internal IP addresses for an organization**

Copyright 2011 John Wiley & Sons, Inc

How Packet Level Firewalls Work



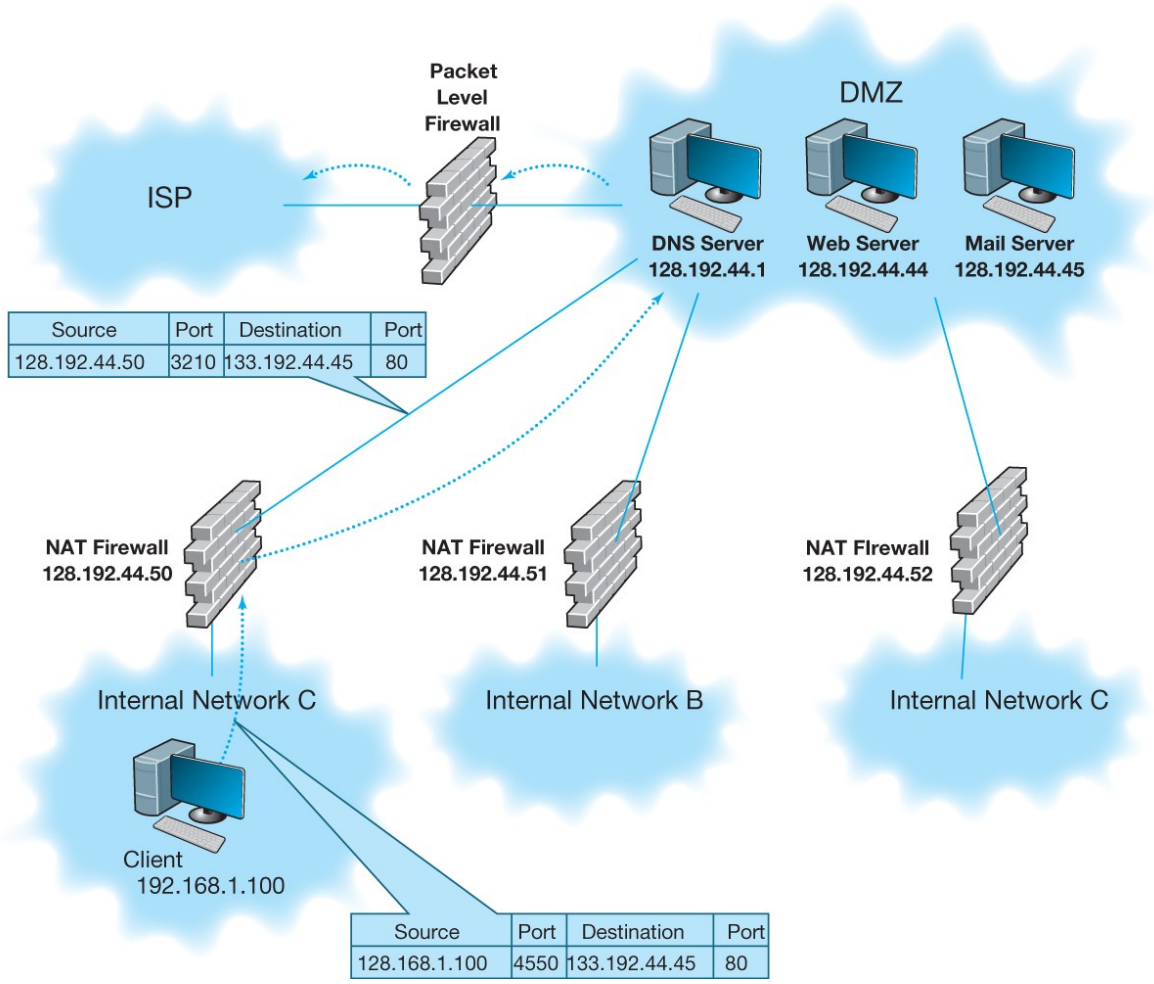
Copyright 2011 John Wiley & Sons, Inc

NAT Proxy Servers

- **Becoming popular; replacing firewalls**
- **Slow down message transfer**
- **Require at least two separate DNS servers**
  - **For use by external users on Internet**
  - **For use by internal users (internal DNS server)**
- **Use of combined, layered approach**
  - **Use layers of NAT proxy servers, packet filters and application gateways**
  - **Maintaining online resources (for public access) in a "DMZ network" between the internal networks and the Internet**

Copyright 2011 John Wiley & Sons, Inc

A Network Design Using Firewalls



Copyright 2011 John Wiley & Sons, Inc

Physical Security

- **Means preventing outsiders from gaining access into offices, server rooms, equipment**
  - **Secure both main and remote facilities**
- **Implement proper access controls to areas where network equipment is located**
  - **Only authorized personnel to access**
  - **Each network component to have its own level of physical security**
    - **Have locks on power switches and passwords to disable keyboard and screens**
  - **Be careful about distributed backup and servers**
    - **Good for continuity, but bad for unauthorized access**
    - **More equipment and locations to secure**

Copyright 2011 John Wiley & Sons, Inc

Personnel Matters

- **Also important to**
  - **Provide proper security education**
  - **Perform background checks**
  - **Implement error and fraud controls**
- **Reduces the possibility of attackers posing as employees**
  - **Example: Become employed as janitor and use various listening devices/computers to access the network**
- **Areas vulnerable to this type of access:**
  - **Wireless LANs (easiest target)**
  - **Network Cabling**
  - **Network Devices**

Copyright 2011 John Wiley & Sons, Inc

Securing Network Cables

- **Easy targets for eavesdropping**
  - **Often run long distances and usually not checked regularly**
  - **Easier to tap into local cables**
    - **Easier to identify individual circuits/channels**
- **Control physical access by employees or vendors to connectors and cables**
  - **Secure local cables behind walls and above ceilings**
  - **Keep equipment room locked and alarm controlled**
- **Choose a cable type harder to tap**
  - **Harder to tap into fiber optic cables**
  - **Pressurized cables: generates alarms when cut**

Copyright 2011 John Wiley & Sons, Inc

Securing Network Devices

- **Should be secured in locked wiring closets**
  - **More vulnerable: LAN devices (controllers, switches, bridges, routers, etc.,)**
    - **A sniffer (LAN listening device) can be easily hooked up to these devices**
    - **Use secure switches: requires special code before a new computers are connected**

Copyright 2011 John Wiley & Sons, Inc

Dial-in Security

- **Routinely change modem numbers**
- **Use automatic number identification (ANI)**
  - **Only users dialing in from authorized locations are granted access based on phone number**
    - **ANI: allows the user to dial in from several prespecified locations**
- **Use one-time only passwords**
  - **For traveling employees who can't use ANI**

Copyright 2011 John Wiley & Sons, Inc

Server and Client Protection

- **Security Holes**
- **Operating Systems**
- **Trojan Horses**
- **Encryption**

Copyright 2011 John Wiley & Sons, Inc

Security Holes

- **Made by flaws in network software that permit unintended access to the network**
  - **A bug that permits unauthorized access**
  - **Operating systems often contain security holes**
  - **Details can be highly technical**
- **Once discovered, knowledge about the security hole quickly circulated on the Internet**
  - **A race can then begin between**
    - **Hackers attempting to break into networks through the security hole and**
    - **Security teams working to produce a patch to eliminate the security hole**
  - **CERT: major clearing house for Internet-related holes**

Copyright 2011 John Wiley & Sons, Inc

Other Security Holes

- **Flawed policies adopted by vendors**
  - **New computers come with preinstalled user accounts with well known passwords**
    - **Managers forgetting to change these passwords**

Copyright 2011 John Wiley & Sons, Inc

Operating Systems

- **American government's OS security levels**
  - **Minimum level (C2): provided by most OSs**
  - **Medium Level (B2): provided by some**
  - **Highest level (A1 and A2): provided by few**
- **Windows vs. Linux**

Copyright 2011 John Wiley & Sons, Inc

OS Security: Windows vs. Linux

- **Windows**
  - **Originally written for one user one computer**
    - **User with full control**
    - **Applications making changes to critical parts of the system**
      - **Advantages: More powerful applications without needing user to understand internals; feature rich, easy to use applications**
      - **Disadvantages: Hostile applications taking over the system**
- **Linux**
  - **Multi-users with various access rights**
  - **Few system administrators with full control**

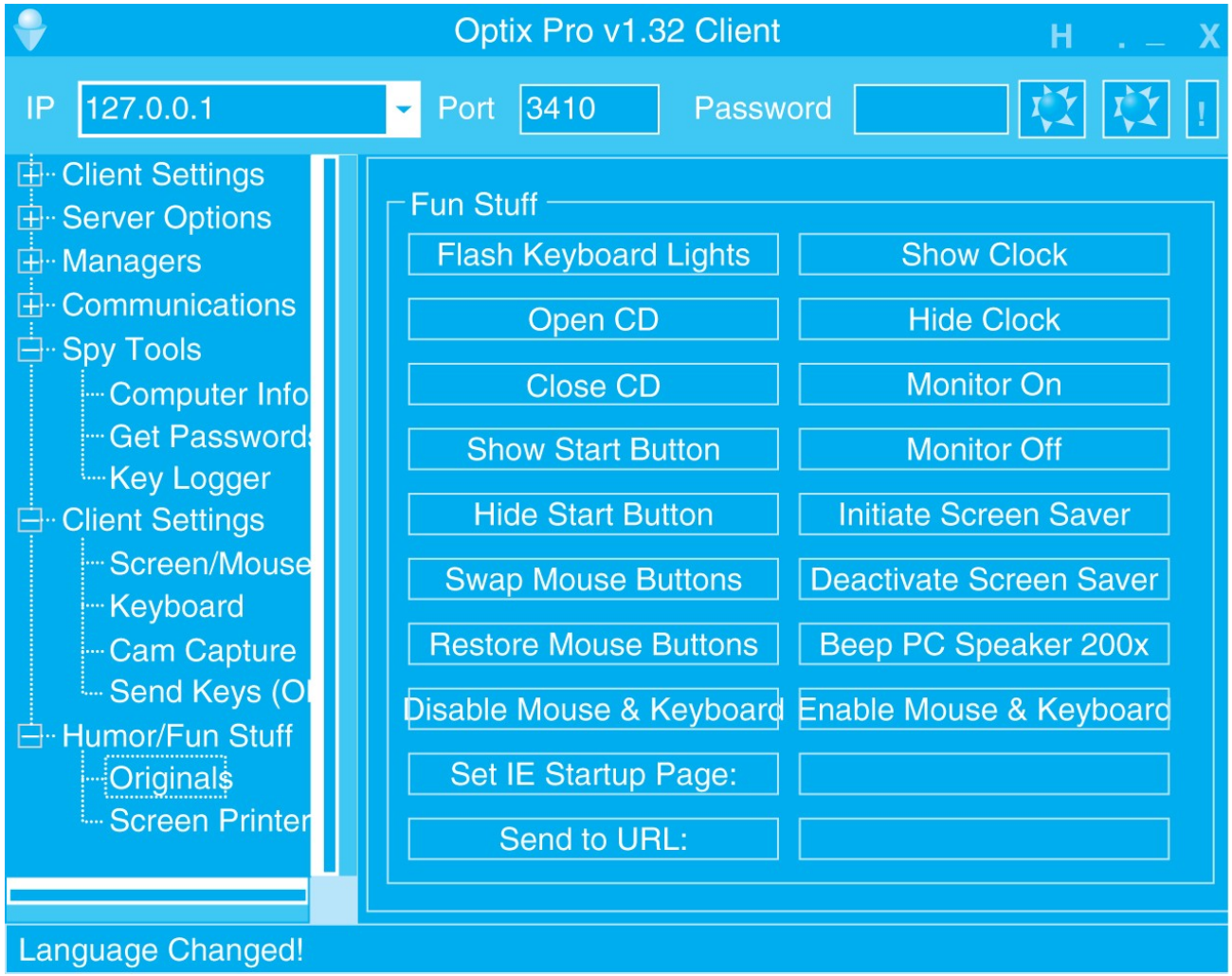
Copyright 2011 John Wiley & Sons, Inc

Trojan Horses

- **Remote access management consoles (rootkits) that enable users to access a computer and manage it from afar**
- **More often concealed in other software that is downloaded over Internet**
  - **Common carriers: Music and video files shared on Internet sites**
- **Undetected by even the best antivirus software**
- **Major Trojans**
  - **Back Orifice: attacked Windows servers**
    - **Gave the attacker the same right as the administrator**
  - **Morphed into tools such as MoSucker and Optix Pro**
    - **Powerful and easy to use**

Copyright 2011 John Wiley & Sons, Inc

Optix Pro Trojan Menu



Copyright 2011 John Wiley & Sons, Inc

Three Types of Trojans

- **Spyware**
  - **Monitors what happens on the target computer**
  - **Can record keystrokes**
- **Adware**
  - **Monitors users' actions**
  - **Displays pop-up advertisements on the screen**
- **DDos**

Copyright 2011 John Wiley & Sons, Inc

Encryption

- **One of the best way to prevent unauthorized access (more formally, cryptography)**
- **Process of disguising info by mathematical rules**
- **Main components of encryption systems**
  - **Plaintext: Unencrypted message**
  - **Encryption algorithm: Works like the locking mechanism to a safe**
  - **Key: Works like the safe's combination**
  - **Cipher text: Produced from the plaintext message by the encryption function**
- **Decryption - the same process in reverse**
  - **Doesn't always use the same key or algorithm.**
  - **Plaintext results from decryption**

Copyright 2011 John Wiley & Sons, Inc

Encryption Techniques

- **Symmetric (single key) encryption**
  - **Uses the same algorithm and key to both encrypt and decrypt a message**
  - **Most common**
- **Asymmetric (public key) encryption**
  - **Uses two different “one way” keys:**
    - **a public key used to encrypt messages**
    - **a private key used to decrypt them**
- **Digital signatures**
  - **Based on a variation of public key encryption**

Copyright 2011 John Wiley & Sons, Inc

Symmetric Encryption

- **Key must be distributed**
  - **Vulnerable to interception (an important weakness)**
  - **Key management – a challenge**
- **Strength of encryption**
  - **Length of the secret key**
    - **Longer keys more difficult to crack (more combinations to try)**
  - **Not necessary to keep the algorithm secret**
- **How to break an encryption**
  - **Brute force: try all possible combinations until the correct key is found**

Copyright 2011 John Wiley & Sons, Inc

Symmetric Encryption Techniques

- **Data Encryption Standard (DES)**
  - **Developed by the US government and IBM**
  - **Standardized and maintained by the National Institute of Standards and Technology (NIST)**
  - **A 56-bit version of DES: used commonly, but can be broken by brute force (in a day)**
  - **Not recommended for data needing high security**
- **Other symmetric encryption techniques**
  - **Triple DES (3DES): DES three times, effectively giving it a 168 bit key**
  - **Advanced Encryption Standard (AES), designed to replace DES; uses 128, 192 and 256 bit keys**
  - **RC4: a 40 bit key, but can use up to 256 bits**

Copyright 2011 John Wiley & Sons, Inc

Regulation of Encryptions

- **Considered a weapon by the U.S. government**
- **Regulated its export the same way the weapons are**
- **Present rule:**
  - **Prohibits the export of encryption techniques with keys longer than 64 bit without permission**
  - **Exemptions: Canada, European Union; American companies with foreign offices**
- **Focus of an ongoing policy debate between security agencies and the software industry**
  - **Many non-American companies and researchers developing more powerful encryption software**

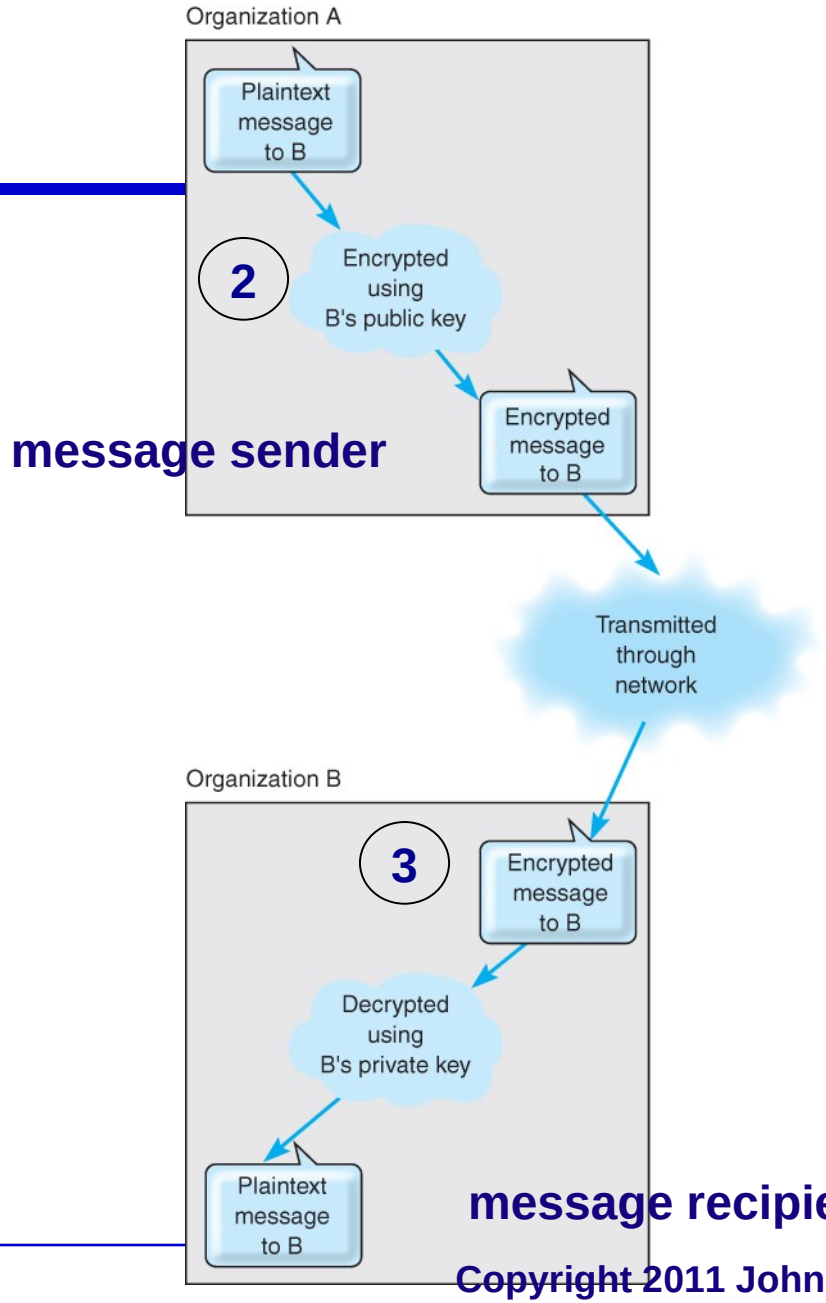
Copyright 2011 John Wiley & Sons, Inc

Asymmetric Encryption

- **Also known as Public Key Encryption (PKE)**
- **Most popular form of PKE: RSA**
  - **Named (1977) after the initials of its inventors: Rivest, Shamir, and Adelman**
  - **Forms the basis of Public Key Infrastructure (PKI)**
  - **Patent expired in 2000; Now many companies offer it**
- **Longer keys: 512 bits or 1,024 bits**
- **Greatly reduces the key management problem**
  - **Publicized Public keys easily accessible in a public directory**
  - **Never distributed Private keys (kept secret)**
  - **No need to exchange keys**
    - **Sender uses the receiver's public key to encrypt**
    - **Receiver uses their private key to decrypt**
    - **Public key cannot decrypt public key encrypted message, only private key will work**

Copyright 2011 John Wiley & Sons, Inc

PKE Operations



1

B makes its public key widely available (i.e. through the Internet)

No security hole is created by distributing the public key, since B's private key has never been distributed.

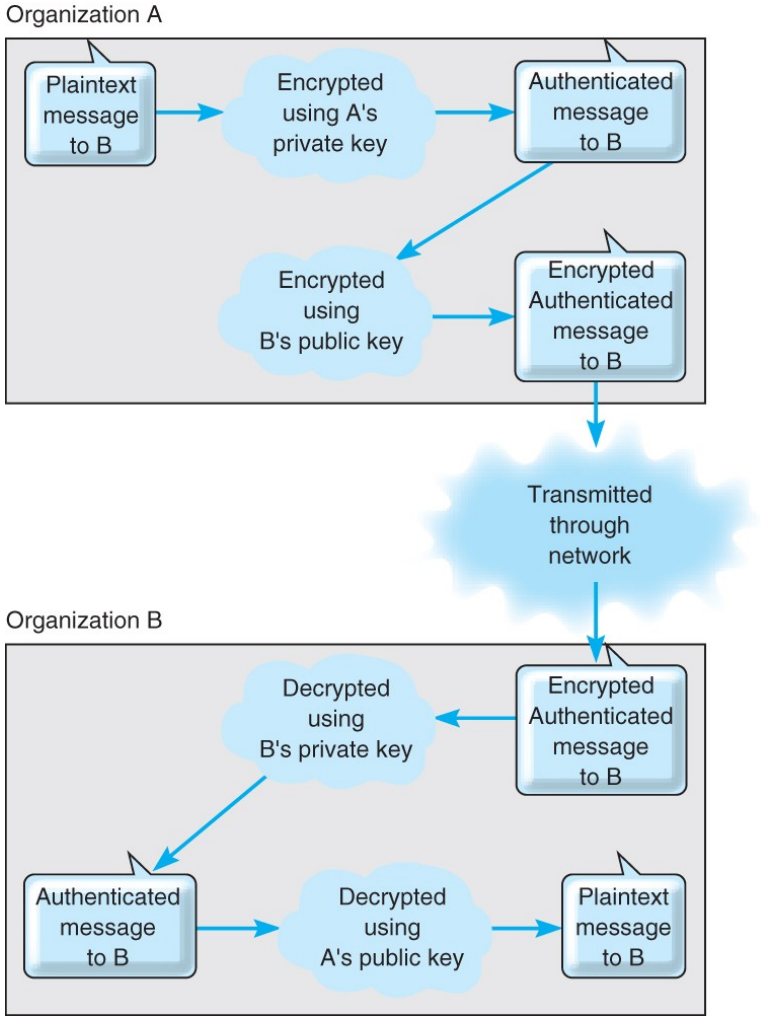
Copyright 2011 John Wiley & Sons, Inc

Authentication

- **Provide secure and authenticated message transmission, enabled by PKE**
- **Provides a proof identifying the sender**
  - **Important for certain legal transactions**
- **Digital Signature:**
  - **Includes the name of the sender and other key contents (e.g., date, time, etc.,)**
- **Use of PKE in reverse (applied to Digital Signature part of the message only)**
  - **Outgoing: Encrypted using the sender's private key**
  - **Incoming: Decrypted using the sender's public key**
    - **Providing evidence who the message originated from**

Copyright 2011 John Wiley & Sons, Inc

Transmission with Digital Signatures



Copyright 2011 John Wiley & Sons, Inc

Public Key Infrastructure (PKI)

- **Set of hardware, software, organizations, and policies to make PKE work on Internet**
  - **Solves the problem with digital signatures**
    - **How to verify that the person sending the message**
- **Elements of PKI**
  - **Certificate Authority (CA)**
    - **A trusted organization that can vouch for the authenticity of the person of organization**
  - **Certificate**
    - **A digital document verifying the identity of a digital signature's source**
  - **"Fingerprint"**
    - **A unique key issued by the CA for every message sent by the user (for higher security certification)**

Copyright 2011 John Wiley & Sons, Inc

Process with Certificate Authority

- **User registers with a CA (e.g., VeriSign)**
  - **Must provide some proof of Identity**
  - **Levels of certification: Examples:**
    - **Simple confirmation of an email address**
    - **Complete police style background check**
- **CA issues a digital certificate**
- **User attaches the certificate to transactions (email, web, etc)**
- **Receiver authenticates transaction with CA's public key**
  - **Contact CA to ensure the certificate is not revoked or expired**

Copyright 2011 John Wiley & Sons, Inc

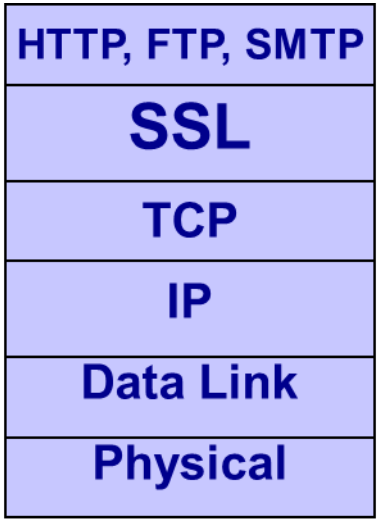
Pretty Good Privacy (PGP)

- **A PKE freeware package**
  - **Often used to encrypt e-mail**
- **Users make their public keys available**
  - **Example: Posting them on Web pages**
- **Anyone wishing to send an encrypted message to that person**
  - **Copies the public key from the Web page into the PGP software**
  - **Encrypts (via PGP software) and sends the message using that key**

Copyright 2011 John Wiley & Sons, Inc

Secure Sockets Layer (SSL)

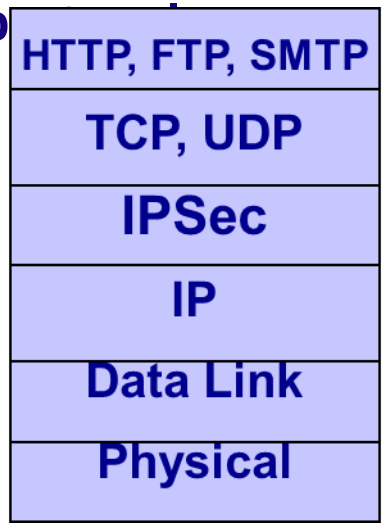
- **A protocol widely used on the Web**
  - **Between the application and layers**
- **Operations of SSL**
  - **Encrypts outbound packets from application layer before transport layer**
  - **Negotiation for PKI**
    - **Server sends its public key and encryption technique to be used (e.g., RC4, DES)**
    - **Browser generates a key for this encryption technique; and sends it to the server (by encrypting with server's public key)**
  - **Communications encrypted by using the key generated by browser**



Copyright 2011 John Wiley & Sons, Inc

IP Security Protocol (IPSec)

- **Another widely used encryption protocol**
  - **Can be used with other application layer p (not just for web applications)**
- **Operations of IPSec between A and B**
  - **A and B generate and exchange two random using Internet Key Exchange (IKE)**
  - **Then combine these two numbers to create encryption key to be used between A and B**
  - **Next, A and B negotiate the encryption technique to be used, such as DES or 3DES.**
  - **A and B then begin transmitting data using either:**
    - **Transport mode: only the IP payload is encrypted**
    - **Tunnel mode: entire IP packet is encrypted (needs a new header for routing in Internet**



Copyright 2011 John Wiley & Sons, Inc

User Authentication

- **Done to ensure that only the authorized users are**
  - **permitted into network**
  - **allowed into the specific resources**
- **Basis of user authentication**
  - **User profile**
  - **User accounts allow access based on something you have, know, or are**
  - **Password is something you know**
  - **Access cards and smart cards**
  - **Biometric is something you are**

Copyright 2011 John Wiley & Sons, Inc

User Profile

- **Assigned to each user account by the manager**
- **Determines the limits of what users have access to on a network**
  - **Allowable log-in day and time of day**
  - **Allowable physical locations**
  - **Allowable number of incorrect log-in attempts**
- **Specifies access details such as**
  - **Data and network resources a user can access**
  - **Type of access (e.g., read, write, create, delete)**

Copyright 2011 John Wiley & Sons, Inc

Forms of Access

- **Something you know:**
  - **Password based**
    - **Users gain access based on something they know**
    - **Not very secure due to poor choice of passwords**
  - **One-time passwords**
    - **Users connected to network obtains a password via:**
      - **A pager**
      - **A token system (a separate handheld device)**
      - **Time-based tokens (password changes every 60 s)**
- **Something you have:**
  - **Card based**
    - **Users gain access based on something they have**
      - **Smart cards, ATM cards**
    - **Typically used in conjunction with a password**

Copyright 2011 John Wiley & Sons, Inc

Forms of Access

- **Something you are:**
  - **Users gain access based on something they are**
    - **Finger, hand, or retina scanning by a biometric system**
    - **Convenient; no need to remember passwords**
  - **Used in high-security applications**
  - **Low cost versions becoming available**
    - **Fingerprint scanners for less than $100**

Copyright 2011 John Wiley & Sons, Inc

Managing User Access

- **Create accounts and profiles when new personnel arrive**
- **Remove user accounts when someone leaves an organization**
  - **Often forgotten, creating big security problems**
  - **Many systems allows now to set an expiration dates to the accounts**
    - **When expires, deleted automatically**
- **Assign separate profiles and passwords to users using several different computers**
  - **Cumbersome for users and managers as well**
- **Adopt network authentication**
  - **Helps mange users automatically**

Copyright 2011 John Wiley & Sons, Inc

Network Authentication

- **Also called central authentication, single sign-on, directory services**
- **Requires user to login to an *authentication server***
  - **Checks id and password against a database**
  - **Issues a certificate**
- **Certificate used for all transactions requiring authentications**
  - **No need to enter passwords**
  - **Eliminates passwords changing hands**
- **Kerberos – most commonly used authentication protocol**

Copyright 2011 John Wiley & Sons, Inc

Preventing Social Engineering

- **Breaking security by simply asking how**
- **Attackers impersonate others on the phone to ask for information**
  - **Personal**
  - **Account**
  - **Company**
- **Attackers have good social skills and can manipulate people**
- **Phishing is an example**
  - **Sending an email to millions of users**
  - **Directing them to a fake website where they “log-in”**
  - **Attacker can then use this log-in information to get into their real account**

Copyright 2011 John Wiley & Sons, Inc

Managing Users

- **Screen and classify both users and data**
  - **Based on “need to know”**
- **Review the effect of any security software**
  - **Focus on restriction or control access to files, records, or data items**
- **Provide adequate user training on network security**
  - **Use self-teaching manuals, newsletters, policy statements, and short courses**
  - **May eliminate social engineering attacks**
- **Launch a well publicized security campaign**
  - **To deter potential intruders**

Copyright 2011 John Wiley & Sons, Inc

Detecting Unauthorized Access

- **Intrusion Prevention Systems (IPSs):**
  - **Network-based IPSs**
    - **Install IDPS sensors on network circuits and monitor packets**
    - **Reports intrusions to IPS Management Console**
  - **Host-based IPSs**
    - **Monitor all activity on the server as well as incoming server traffic**
  - **Application-based IPSs**
    - **Special form of host-based IPSs**
    - **Monitor just one application, such as a Web server**

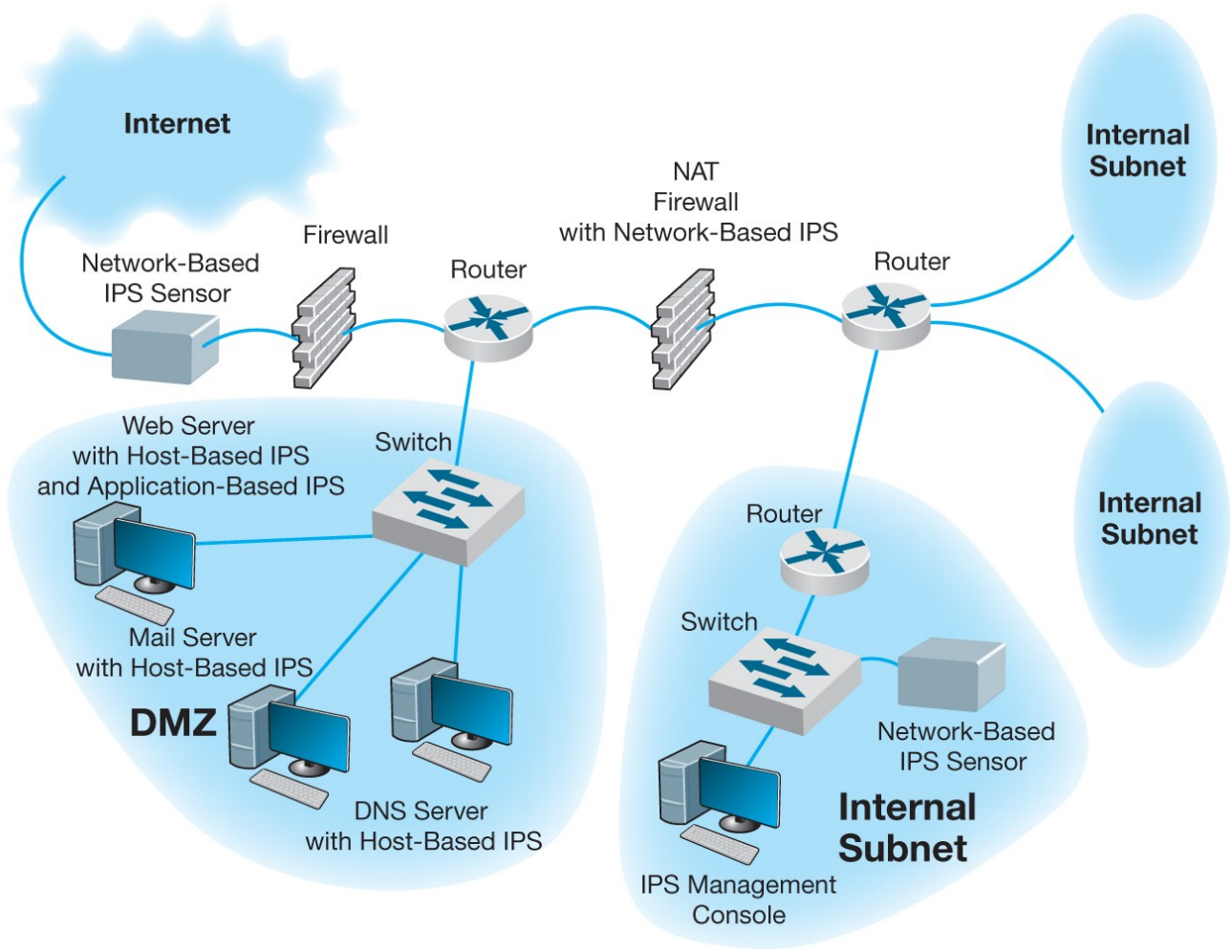
Copyright 2011 John Wiley & Sons, Inc

Techniques Used by IPSs

- **Misuse detection**
  - **Compares monitored activities with signatures of known attacks**
  - **If an attack is recognized the IPS issues an alert and discards the packet**
  - **Challenge: keep database current**
- **Anomaly detection**
  - **Operates in stable computing environments**
  - **Looks for major deviations from the "normal" parameters of network operation**
    - **e.g., a large number of failed logins**
  - **When detected, an alert is issued, packets discarded**
  - **Problem: false alarms (valid traffic different from normal)**

Copyright 2011 John Wiley & Sons, Inc

Use of IPS with Firewalls



Copyright 2011 John Wiley & Sons, Inc

Intrusion Recovery

- **Must have a clear plan to respond to breaches**
  - **Have an emergency response team (CERT for Internet)**
- **Steps to take once intrusion detected:**
  - **Identify where the security breach occurred and how it happened**
    - **Helps to prevents other doing it the same way**
    - **May report the problem to police**
  - **Use Computer Forensics area techniques**
    - **Use of computer analysis techniques to gather evidence for trials**
- **Entrapments – Use of honey pots**
  - **Divert attackers to a fake server (with interesting, but fake data used as bait)**
  - **Monitor access to this server; use it as a proof**

Copyright 2011 John Wiley & Sons, Inc

10.5 Best Practice Recommendations

- **Start with a clear disaster recovery plan and solid security policies**
- **Train individuals on data recovery and social engineering**
- **Use routinely antivirus software, firewalls, physical security, intrusion detection, and encryption**

Copyright 2011 John Wiley & Sons, Inc

Recommendations (Cont.)

- **Use of strong centralized desktop management**
  - **Prohibits individual users to change settings**
  - **Use regular reimaging of computers to prevent Trojans and viruses**
  - **Install most recent security patches**
  - **Prohibit al external software downloads**
- **Use continuous content filtering**
  - **Scan all incoming packets**
  - **Encrypt all server files and communications**
- **Enforce, vigorously, all written security policies**
  - **Treat violations as “capital offense,” a basis for firing**

Copyright 2011 John Wiley & Sons, Inc

10.6 Implications for Management

- **Security - fastest growing area in networking**
- **Cost of security expected to increase**
  - **More and sophisticated security tools to encounter ever increasing attacks**
  - **Network becoming mission critical**
  - **More and skilled staff providing security**
- **Expect tougher laws and better enforcement**
- **Security to become a major factor to consider in choosing software and equipment**
  - **More secure OSs, more secure application software, etc.**

Copyright 2011 John Wiley & Sons, Inc

Copyright 2011 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that permitted in section 117 of the 1976 United States Copyright Act without express permission of the copyright owner is unlawful. Request for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages caused by the use of these programs or from the use of the information herein.