



# Business Data Communications & Networking:

12<sup>th</sup> Edition

---

## Chapter 11: Network Security



Sadiq M. Sait, PhD  
Professor  
College of Computing Science and Mathematics  
Director, Office of Planning & Quality

Fall 2023

# PROLOGUE

- ❑ This chapter describes why networks need security and how to provide it.
- ❑ The first step in any security plan is **risk assessment**, understanding the **key assets** that need protection and assessing the risks to each.
- ❑ A variety of steps can be taken to **prevent, detect, and correct** security problems due to **disruptions, destruction, disaster, and unauthorized access**.
- ❑ **Objectives:**
  - ❑ Be familiar with the major threats to network security
  - ❑ Be familiar with how to conduct a risk assessment
  - ❑ Understand how to ensure business continuity (BC)
  - ❑ Understand how to prevent intrusion

## 11.1 INTRODUCTION

- ❑ The introduction of computers and the Internet has changed security.  
We now need **more than physical locks**, codes, etc.
- ❑ The rise of the Internet has completely redefined the nature of information security.
- ❑ Now, companies face global threats to their networks and, more importantly, to their data.
- ❑ Viruses and worms have long been a problem, **but credit card theft and identity theft, two of the fastest-growing crimes**, pose immense liability to firms who fail to protect their customers' data.
- ❑ Laws have been **slow** to catch up, despite the fact that breaking into a computer in the United States—even without causing damage—is now a federal crime punishable by a fine and/or imprisonment.
- ❑ Nonetheless, we have a new kind of **transborder** cybercrime against which laws may apply but that will be very difficult to enforce.
- ❑ For example, Verizon's 2013 security report concluded that
  - ❑ at least **174 million electronic records** had been compromised in more than 855 separate security incidents.
  - ❑ These incidents included not only viruses but also industrial espionage, fraud, **extortion**, and identity theft.

## 11.1 INTRODUCTION

- ❑ The years when creating a virus was for fun are long gone.
- ❑ The goal of these attacks was money.
- ❑ Large companies Zappos and Target have been victims of cyberattacks, and millions of the credit card information of millions of their customers have been stolen.
  - ❑ A company of any size can be the target of an attack. According to Symantec, more than 50% of all targeted companies had fewer than 2,500 employees because they often have weaker security.
- ❑ Many organizations, private and public, focus on helping individuals, organizations, and governments to protect themselves from criminals operating on the Internet (cyber criminals).
- ❑ These include **CERT (Computer Emergency Response Team)** at Carnegie Mellon University, APWG (Anti-Phishing Working Group), the Russian-based Kaspersky Lab, McAfee, and Symantec.

## 11.1 INTRODUCTION

- ❑ There are three main reasons why there has been an increase in computer security over the past few years.
- ❑ **First:** **Earlier was a hobby**, now being a cybercriminal is a **profession**.
- ❑ There are professional organizations that one can hire to break into computer networks of specific targets to **steal information**.
  - ❑ **Ethical hacking (when a company hires another company to test its security).**
- ❑ Hackers work for a fee to steal information, intellectual property, or computer code.
  - ❑ These attacks are called **targeted attacks**, in which cybercriminals not only try to exploit technical vulnerabilities but also try to **“hack the human”** via social engineering or **phishing** emails.
- ❑ These targeted attacks can be very sophisticated, and any organization can become a victim because every organization has data that can be of value to cybercriminals.

## 11.1.1 Why Networks Need Security? yy

- ❑ Organizations have become increasingly dependent on data communication networks (mission critical) for their daily business communications,
- ❑ The rise of the Internet, providing opportunities to connect computers and mobile devices anywhere in the world, has significantly increased the **vulnerability** of an organization's assets.
- ❑ The **losses associated** with security failures **can be huge**.
  - ❑ An average annual loss of about \$350,000 sounds large enough, but this is just the tip of the iceberg.
  - ❑ **The potential loss of consumer confidence from a well-publicized security break-in can cost much more in lost business.**
  - ❑ More important than these, however, are the potential losses from the **disruption** of application systems that run on computer networks.
- ❑ Bank of America, one of the largest banks in the United States, estimates that it would cost the bank **\$50 million if its computer networks were unavailable for 24 hours**.
- ❑ Protecting customer privacy and the risk of identity theft also drive the need for increased network security.
  - ❑ In 1998, the European Union passed strong data privacy laws that fined companies for disclosing information about their customers.
  - ❑ In the United States, HIPAA and California law fines up to **\$250,000** for each unauthorized disclosure of customer information

## 11.1.2 Types of Security Threats yy

- ❑ For many people, security means preventing intrusion, such as preventing an attacker from breaking into your computer.
- ❑ Security is much more than an intrusion.
- ❑ There are three primary goals in providing security: (i) confidentiality, (ii) integrity, and (iii) availability (also known as **CIA**).
  - ❑ **Confidentiality**: Protection of organizational data from unauthorized disclosure of customer and proprietary data.
  - ❑ **Integrity**: Is the assurance that data have not been altered or destroyed.
  - ❑ **Availability**: This means providing continuous operation of the organization's hardware and software so that staff, customers, and suppliers can be assured of no interruptions in service.
- ❑ There are many potential threats to confidentiality, integrity, and availability.
- ❑ There can be threats to (see Figure 11-1 in the text):
  - ❑ a computer center
  - ❑ the data communication circuits, and
  - ❑ the attached computers
- ❑ In general, security threats can be classified into two broad categories:
  - ❑ **ensuring business continuity** and
  - ❑ **preventing unauthorized access**.

## 11.1.2 Types of Security Threats (contd)

- ❑ Preventing unauthorized access, also referred to as intrusion, refers primarily to confidentiality, but also to integrity
- ❑ The intruder may **change** important data.
- ❑ Intrusion is often viewed as external attackers gaining **access to organizational data files and resources** from across the Internet.
  - ❑ However, almost half of all intrusion incidents involve **employees**.
- ❑ Intrusion may have only minor effects.
  - ❑ A curious intruder may simply **explore** the system, gaining knowledge that has little value.
- ❑ **A more serious intruder may be a competitor** bent on industrial **espionage** who could attempt to gain access to
  - ❑ information on **products** under development, or
  - ❑ **the details and price of a bid** on a large contract, or
  - ❑ a thief trying to steal customer credit card numbers or
  - ❑ information to carry out identity theft.
- ❑ Worse still, the intruder could change files to commit **fraud** or **theft** or could destroy **the information to injure the organization**



## 11.1.3 Network Controls

- ❑ **Developing a secure network means developing controls.**
- ❑ Controls are software, hardware, **rules**, or procedures that **reduce** or **eliminate** the threats to network security.
- ❑ **Controls prevent, detect, and/or correct** whatever might happen to the organization because of **threats** facing its computer-based systems.
  
- ❑ **Preventive controls** **mitigate** or stop a person from acting or an event from occurring.
  - ❑ For example, a password can prevent illegal entry
- ❑ **Detective controls** reveal or discover unwanted events.
  - ❑ For example, software that looks for illegal network entry can detect these problems.
- ❑ **Corrective controls** remedy an unwanted event or an intrusion.
  - ❑ Computer programs or humans verify and check data to correct errors or fix a security breach so it will not recur in the future.

## 11.2 RISK ASSESSMENT

- ❑ **The first step** in developing a secure network is to conduct a risk assessment.
- ❑ There are several commonly used risk assessment frameworks that provide strategies for analyzing and prioritizing the security risks systems/networks.
- ❑ A risk assessment should be simple.
- ❑ After reading a risk assessment, anyone should be able to see which systems and network components are at high risk for attack or abuse.
- ❑ Also, the reader should be able to see **what controls** have been implemented to protect him/her and what new controls need to be implemented.
- ❑ Three risk assessment **frameworks** are commonly used:
  - ❑ Operationally Critical Threat, Asset, and Vulnerability Evaluation (**OCTAVE**) from the Computer Emergency Response Team
  - ❑ Control Objectives for Information and Related Technology (**COBIT**) from the Information Systems Audit and Control Association
  - ❑ Risk Management Guide for Information Technology Systems (**NIST** guide) from the National Institute of Standards and Technology
- ❑ Each of these frameworks offers a slightly different process with a different focus. However, they share five common steps: **(1) Develop risk measurement criteria (2). Inventory IT assets (3). Identify threats (4). Document existing controls (5). Identify improvement.**

## 11.2.1 Develop Risk Measurement Criteria

- ❑ **Risk measurement criteria are the measures used to evaluate the way a security threat could affect the organization.**
  - ❑ For example, suppose a hacker broke in and stole customer credit card information from a company server. One immediate impact to the organization is financial because some customers are likely to stop shopping, at least in the short term.
  - ❑ There may also be legal impact because some countries and/or states have laws concerning the unauthorized release of personal information.
  - ❑ There also may be longer-term impacts on the company's **reputation**.
- ❑ Each organization needs to develop its own set of potential business impacts, but the five most commonly considered impact areas are (i) **financial** (revenues and expenses), (ii) **productivity** (business operations), (iii) **reputation** (customer perceptions), (iv) **safety** (health of customers and employees), and (v) **legal** (potential for fines and litigation).
- ❑ However, some organizations add other impacts and not all organizations use all of these five because some may not apply. It is important to remember that these impacts are for information systems and networks,

## 11.2.1 Develop Risk Measurement Criteria (contd)

- ❑ The next step is to **prioritize** them.
- ❑ Not all impact areas are equally important (some high, low or medium)
  - ❑ For example
    - ❑ For a hospital, safety may be the highest priority and financial the lowest.
    - ❑ In contrast, for a restaurant, information systems and networks may pose a low (or nonexistent) safety risk (because they are not involved in food safety) but a high priority reputation risk (if, for example, credit card data were stolen).
- ❑ The next step is to develop specific measures of what could happen in each impact area and what we would consider a high/medium/low impact.
  - ❑ For example, one financial impact could be a decrease in sales. What would we consider a low financial impact in terms of a decrease in sales: 1%? 2%? What would be a high impact on sales? These are business decisions, not technology decisions, so they should be made by the business leaders.
- ❑ Figure 11-2 has sample risk measurement criteria for a Web-based bookstore. As you can see, only four of the impact areas apply here.

## 11.2.1 Develop Risk Measurement Criteria (contd)

- ❑ Because information systems and network security problems would not harm the safety of employees or customers.
- ❑ However, it would be a different case if this were a pharmaceutical company.
  - ❑ A threat, such as **malware** (software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system), could cause changes in how a drug is prepared, potentially harming customers (patients) and employees.

Impact Area	Priority	Low Impact	Medium Impact	High Impact
Financial	High	Sales drop by less than 2%	Sales drop by 2%–10%	Sales drop by more than 10%
Productivity	Medium	Increase in annual operating expenses by less than 3%	Increase in annual operating expenses between 3% and 6%	Increase in annual operating expenses by more than 6%
Reputation	High	Decrease in number of customers by less than 2%	Decrease in number of customers by 2%–15%	Decrease in number of customers by more than 15%
Legal	Medium	Incurring fines or legal fees less than \$10,000	Incurring fines or legal fees between \$10,000 and \$60,000	Incurring fines or legal fees exceeding \$60,000

**FIGURE 11-2** Sample risk measurement criteria for a Web-based bookstore

## 11.2.2 Inventory IT Assets

- ❑ An asset is something of value and can be either hardware, software, data, or applications. Figure 11-3 defines six common categories of IT assets.
- ❑ An important type of asset is the mission-critical application, which is an information system that is critical to the survival of the organization.
- ❑ Other details in figure below.

**FIGURE 11-3**

Types of assets.

DNS = Domain Name Service; DHCP = Dynamic Host Control Protocol; LAN = local area network; WAN = wide area network

Hardware	<ul style="list-style-type: none"><li>• Servers, such as mail servers, Web servers, DNS servers, DHCP servers, and LAN file servers</li><li>• Client computers</li><li>• Devices such as switches and routers</li></ul>
Circuits	<ul style="list-style-type: none"><li>• Locally operated circuits such as LANs and backbones</li><li>• Contracted circuits such as WAN circuits</li><li>• Internet access circuits</li></ul>
Network software	<ul style="list-style-type: none"><li>• Server operating systems and system settings</li><li>• Application software such as mail server and Web server software</li></ul>
Client software	<ul style="list-style-type: none"><li>• Operating systems and system settings</li><li>• Application software such as word processors</li></ul>
Organizational data	<ul style="list-style-type: none"><li>• Databases with organizational records</li></ul>
Mission-critical applications	<ul style="list-style-type: none"><li>• For example, for an Internet bank, its Web site is mission-critical</li></ul>

Asset	Importance	Most Important Security Requirement	Description	Owner(s)
Customer database	High	<ul style="list-style-type: none"> <li>■ Confidentiality</li> <li>■ Integrity</li> <li>■ Availability</li> </ul>	This database contains all customers' records, including address and credit card information.	VP of Marketing CIO
Web server	High	<ul style="list-style-type: none"> <li>■ Confidentiality</li> <li>■ Integrity</li> <li>■ Availability</li> </ul>	This is used by our customers to place orders. It is very important that it would be available 24/7.	CIO
Mail server	Medium	<ul style="list-style-type: none"> <li>■ Confidentiality</li> <li>■ Integrity</li> <li>■ Availability</li> </ul>	This is used by employees for internal communication. It is very important that no one intercepts this communication as sensitive information is shared via email.	CIO
Financial records	High	<ul style="list-style-type: none"> <li>■ Confidentiality</li> <li>■ Integrity</li> <li>■ Availability</li> </ul>	These records are used by the C-level executives and also by the VP of operations. It is imperative that nobody else but the C-team be able to access this mission information.	CFO
Employees' computers	Low	<ul style="list-style-type: none"> <li>■ Confidentiality</li> <li>■ Integrity</li> <li>■ Availability</li> </ul>	Each employee is assigned to a cubical that has a desktop computer in it. Employees provide customer service and support for our Web site using these computers.	Division directors

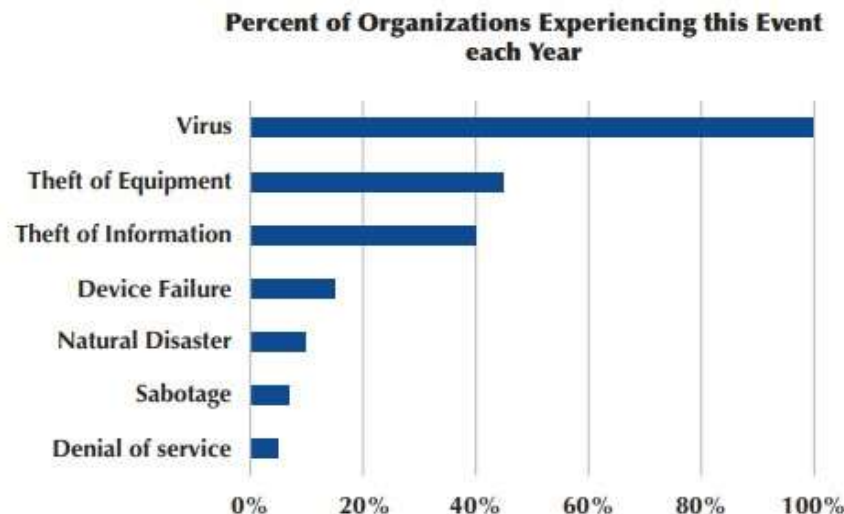
**FIGURE 11-4** Sample inventory of assets for a Web-based bookstore



## 11.2.3 Identify Threats

- ❑ **A threat is any potential occurrence that can do harm**, interrupt the systems using the network, or cause a monetary loss to the organization.
- ❑ Figure 11-5 summarizes the most common types of threats and their likelihood of occurring based on several surveys in recent years.
- ❑ This figure shows the percentage of organizations affected each year by each threat but not whether the threat caused damage;
  - ❑ for example, 100% of companies reported experiencing one or more viruses each year, but in most cases, the antivirus software prevented any problems.
- ❑ The actual probability of a threat to your organization depends on your business.
  - ❑ An Internet bank, for example, is more likely to be a target of theft of information than a restaurant with a simple Web site.

**FIGURE 11-5**  
Likelihood of a threat





## 11.2.3 Next Step: Threat Scenarios

- ❑ A threat scenario describes how an asset can be compromised by one specific threat.
  - ❑ An asset can be compromised by more than one threat, so it is common to have more than one threat scenario for each asset.
  - ❑ For example, the confidentiality, integrity, and/or availability of the client data database can be compromised by information theft (confidentiality), sabotage (integrity), or a natural disaster such as a tornado (availability).
- ❑ Figure 11-6 provides an example of a threat scenario for one asset (the customer database) of a Web-based bookstore.
  - ❑ The top half of the threat scenario describes the risk associated with the asset from the threat
  - ❑ the bottom half (shaded in color) describes the existing controls implemented to protect the asset from this threat.
- ❑ Finally, we can calculate the relative **risk score** by multiplying the **impact score by the likelihood**.
- ❑ Figure 11-7 shows the threat scenario for a tornado. Observe that tornado risk score is 14, that is, information theft is a greater risk than a tornado.

**FIGURE 11-6 Threat scenario for theft of customer information: Top Half**

<b>Asset</b>	Customer database		
<b>Asset Importance</b>	High		
<b>Threat</b>	Theft of information		
<b>Description</b>	An external hacker or a disgruntled current or former employee can gain unauthorized access to the client data and distribute it to a third party.		
<b>Likelihood</b>	Medium (2)		
<b>Impact on</b>	<div><input checked="" type="checkbox"/> Confidentiality</div> <div><input type="checkbox"/> Integrity</div> <div><input type="checkbox"/> Availability</div>		
<b>Impact Area</b>	<b>Priority</b>	<b>Impact</b>	<b>Score</b>
Financial	High (3)	Medium (2)	6
Productivity	Medium (2)	High (3)	6
Reputation	High (3)	High (3)	9
Legal	Medium (2)	Medium (2)	4
		<b>Impact Score</b>	<b>25</b>
<b>Risk Score</b> (Likelihood × Impact Score)	<b>50</b>		

**FIGURE 11-6 Threat scenario for theft of customer information: Bottom Half**

<b>Adequacy of Existing Controls</b>	<b>Medium</b>
<b>Risk Control Strategy</b>	<input type="checkbox"/> Accept <input checked="" type="checkbox"/> Mitigate <input type="checkbox"/> Share <input type="checkbox"/> Defer
<b>Risk Mitigation Controls</b>	
<b>Encryption</b>	The database is encrypted.
<b>Firewall</b>	A firewall is installed on the router in front of the database to prevent unauthorized access.
<b>Personnel Policy</b>	All employees have their log-in credentials removed within 24 hours of their resignation or termination.
<b>Training</b>	Employees have to attend annual security training that focuses on information disclosure policy, phishing and social engineering techniques to ensure they do not provide their passwords to anyone.
<b>Automatic screen lock</b>	Each employee's computer will lock if the computer hasn't been used for five minutes so that if an employee leaves his or her desk without logging off, someone else cannot gain unauthorized access to the employee's computer.

## 11.2.4 Document Existing Controls

- ❑ Once the specific assets, threat scenarios, and risk scores have been identified, we develop a risk control strategy, which is 'how to address a risk?'.
  - ❑ A risk can be **accepted**, **mitigated**, **shared**, or **deferred**.
  - ❑ If you accept the risk, then you take no action.
  - ❑ Risk **mitigation**:
    - ❑ Involves some control to counter a threat or minimize the impact.
    - ❑ An organization can implement several types of controls, such as using **antivirus software**, implementing state-of-the-art **firewalls**, or providing security **training** for employees.
  - ❑ An organization can decide to **share** the risk. In this case, it purchases *insurance* against the risk.
  - ❑ Defer the risk: When there is a need to collect additional information.
  - ❑ Then list the controls (will discuss shortly)
  - ❑ Then Assessment: Assessment produces a value relative to the risk:
    - ❑ High adequacy: means the controls are expected to strongly control the risks in the threat scenario
    - ❑ Medium adequacy means some improvements are possible
    - ❑ Low adequacy means improvements are needed to effectively mitigate or share the risk.
  - ❑ Once again, some organizations use more complex scales such as a letter grade (A, A-, A+, B, etc.) or 100-point scales.

## 11.3 ENSURING BUSINESS CONTINUITY

- ❑ Business continuity means that the organization's data and applications will continue to operate even in the face of disruption, destruction, or disaster.
- ❑ A business continuity plan has two major parts:
  - ❑ the development of controls that will prevent these events from having a major impact on the organization, and
  - ❑ a disaster recovery plan that will enable the organization to recover if a disaster occurs.
- ❑ Major threats to BC include **viruses**, **theft**, **denial of service attacks**, **device failure**, and **disasters**.
- ❑ BC planning is sometimes **overlooked** because intrusion is more often the subject of news reports

## 11.3.1 Virus Protection: Viruses

- ❑ **Special attention must be paid to preventing computer viruses.**
  - ❑ Some are harmless and just cause nuisance messages, but others are serious, such as destroying data.
- ❑ In most cases, disruptions or the destruction of data are local and affect only a small number of computers (usually easy to deal with)
- ❑ Some viruses cause widespread infection,
- ❑ Most viruses attach themselves to other programs or to special parts on disks. **As those files execute or are accessed, the virus spreads.**
- ❑ Macro viruses: are contained in documents, emails, or spreadsheet files, and spread when an infected file is opened.
- ❑ Some viruses change their appearances as they spread, making detection more difficult.

## 11.3.1 Virus Protection: Viruses and Worms

- ❑ A **worm** is special type of virus that **spreads itself** without human intervention.
- ❑ Many viruses **attach themselves to a file** and require a person to copy the file, but a worm copies itself from computer to computer.
- ❑ **Worms spread when they install themselves on a computer and then send copies of themselves to other computers, sometimes by email, sometimes via security holes in software.**
- ❑ The best way to prevent the spread of viruses is to install **antivirus** software
- ❑ Most organizations automatically install antivirus software on their computers, but many people fail to install them on their **home computers**.
- ❑ Antivirus software is **only as good as its last update**, so it is critical that the software be updated regularly. Be sure to set your software to **update automatically** or do it manually on a regular basis (**Researchers estimate that 10 new viruses are developed every day**).
- ❑ Viruses are often spread by downloading files from the Internet, so do not copy or download files of unknown origin (e.g., music, videos, screen savers), or at least check every file you do download. Always check all files for viruses before using them (even those from friends!).
- ❑ There are also Trojan Horses:
- ❑ All these can be classified as Malware, spyware, adware, and rootkits.

## 11.3.2 Denial-of-Service Attack

- ❑ DoS attack: The attacker attempts to **disrupt** the network by **flooding** it with messages so that the network cannot process messages from normal users.
- ❑ **The simplest approach is to flood a Web server, mail server, and so on, with incoming messages.** The server attempts to respond to these, but there are so many messages that it cannot.
- ❑ **Most attackers use tools that enable them to put false source IP addresses on the incoming messages so that it is difficult to recognize a message as a real message or a DoS message and filter it.**
- ❑ **A distributed denial-of-service (DDoS) attack is even more disruptive.**
  - ❑ Here, the attacker breaks into and takes control of many computers on the Internet (often several hundred to several thousand) and plants software on them called a DDoS agent (or sometimes a **zombie** or a **bot**).
  - ❑ And uses software called a DDoS handler (sometimes called a **botnet**) to **control the agents**.
  - ❑ The handler issues instructions to the computers under the attacker's control.



## 11.3.2 Denial-of-Service (contd) Prevention

- ❑ Approach 1: **Configure the main router** that connects your network to the Internet (or the firewall) to verify that the **source address of all incoming messages is in a valid address range** for that connection (called **traffic filtering**).
  - ❑ For example, if an incoming message has a source address from inside your network, then it is obviously a false address.
- ❑ Approach 2: A second approach is to configure the main router (or firewall) to **limit the number of incoming packets that could be DoS/DDoS attack packets** to enter the network, regardless of their source (called **traffic limiting**).
  - ❑ The **disadvantage** is that during an attack, some **valid packets** from regular customers will be **discarded**, and lost.
- ❑ Approach 3: Use a special-purpose device, called a **traffic anomaly detector**, installed in front of the main router (or firewall) **to perform traffic analysis**.
  - ❑ This device **monitors normal traffic patterns** and learns what normal traffic looks like.
  - ❑ Most DoS/DDoS attacks target a specific server or device so when the anomaly detector recognizes a sudden burst of abnormally high traffic destined to a specific server or device, it quarantines but allows normal traffic to flow through into the network.
  - ❑ The anomaly detector reroutes the quarantined packets to a traffic anomaly analyzer (see Figure 11-9). This is a better approach.

### 11.3.3 Theft Protection

- ❑ An often overlooked security risk is theft.
- ❑ Industry sources estimate that more than \$1 billion is lost to computer theft each year, with many of the stolen items ending up on Internet auction sites (e.g., eBay).
- ❑ Physical security is a key component of theft protection.
- ❑ Most organizations require anyone entering their offices to go through some level of physical security.
  - ❑ For example, most offices have security guards and require all visitors to be authorized by an organization employee (KAUST).
  - ❑ In universities, computer equipment and network devices are protected by locked doors or security cables so that someone cannot easily steal them. One of the most common targets for theft is laptop computers.
  - ❑ More laptop computers are stolen from employees' homes, cars, and hotel rooms than any other device.
  - ❑ Airports are another common place for laptop thefts.
  - ❑ It is hard to provide physical security for traveling employees, but most organizations remind their employees to take special care when traveling with laptops.

## 11.3.4 Device Failure Protection

- ❑ Eventually, every computer network device, cable, or leased circuit will fail. It's just a matter of time. Network managers have to be prepared for failure.
- ❑ The best way to prevent a failure from impacting business continuity is to build redundancy into the network. A second redundant component.
  - ❑ For example, if the Internet connection is important to the organization, the network designer ensures that there are at least two connections to the Internet—**each provided by a different common carrier.**
    - ❑ This means, of course, that the organization now requires two routers to connect to the Internet because there is little use in having two Internet connections if they both run through the same router.
- ❑ This same design principle applies to the organization's internal networks.
  - ❑ If the core backbone is important (and it usually is), then the organization must have two core backbones, each served by different devices.
    - ❑ Each distribution backbone that connects to the core **backbone (e.g., a building backbone that connects to a campus backbone) must also have two connections (and two routers) into the core backbone.**
  - ❑ The next logical step is to ensure that each access layer LAN also has two connections to the distribution backbone.

## 11.3.4 Device Failure Protection (contd).

- ❑ Redundancy also applies to servers. Most organizations use a server farm.
- ❑ Some organizations use fault-tolerant servers that contain many redundant components so that if one of its components fails, it will continue to operate.
- ❑ Redundant array of independent disks (RAID) is a storage technology that, as the name suggests, is made of many separate disk drives.
  - ❑ When a file is written to a RAID device, it is written across several separate, redundant disks. There are several types of RAID.

(a) **RAID 0 uses multiple disk drives** and therefore is faster than traditional storage because the data can be written or read in parallel across several disks rather than sequentially on the same disk. (b) **RAID 1 writes duplicate copies** of all data on at least two different disks; this means that if one disk in the RAID array fails, there is no data loss because there is a second copy of the data stored on a different disk. This is sometimes called **disk mirroring** because the data on one disk is copied (or mirrored) onto another. (c) RAID 2 provides error checking (during read and write). (d) **RAID 3 provides a better and faster error-checking** process than RAID 2. (e) **RAID 4 provides slightly faster read access than RAID 3 because of the way it allocates the data to different disk drives**. (f) RAID 5 provides slightly faster read and write access because of the way it **allocates the error-checking data** to different disk drives. (g) **RAID 6 can survive the failure of two drives with no data loss**.

### 11.3.4 Device Failure Protection (contd).

- ❑ Power outages are one of the most common causes of network failures.
- ❑ An uninterruptable power supply (UPS) is a device that detects power failures and permits the devices attached to it to operate as long as its battery lasts.
- ❑ UPS for home use is inexpensive and often provide power for up to 15 minutes—long enough for you to save your work and shut down your computer.
- ❑ UPS for large organizations often have batteries that last an hour and permit mission-critical servers, switches, and routers to operate until the organization's backup generator can be activated.

## 11.3.5 Disaster Protection

- ☐ Avoiding Disaster (some cannot be avoided! BC)
- ☐ **Recovering from Disaster. How? (Backup and recovery controls)**
- ☐ **Continuous Data Protection (CDP)**
  - ☐ Copies of all data and transaction are written to CDP servers
- ☐ **Disaster Recover Drill (like fire drill)**
- ☐ **Online Backup**
- ☐ **Disaster Recovery Outsourcing**

## 11.4 INTRUSION PREVENTION

- ☐ Security Policy
  - ☐ Critical to controlling risk due to intrusion
- ☐ Perimeter Security and Firewalls
  - ☐ Three basic access points where intruders must be stopped (Internet 70%, LANs and WLANs 30%)
  - ☐ A firewall is used to secure the Internet connection
- ☐ Firewalls?
  - ☐ A firewall is a router or special-purpose device that examines packets flowing into and out of a network
  - ☐ The network is designed so that a firewall is placed on every network connection between the organization and the Internet (Figure 11-12).
  - ☐ No access is permitted except through the firewall.
  - ☐ Some firewalls can detect and prevent denial-of-service attacks and unauthorized access attempts.
  - ☐ Three commonly used types of firewalls are (i) packet-level firewalls, (ii) application-level firewalls, and (iii) NAT firewalls

## 11.4 INTRUSION PREVENTION (contd)

- ❑ Four types of intruders

1. Casual
2. Experts in Security (but only for the thrill)
  - a. Hackers who cause damage are crackers
3. Professional hackers (who break into organizations, most dangerous)
4. The fourth type of intruder is also very dangerous. These are organization employees who have legitimate access to the network but who gain access to information they are not authorized to use.

- ❑ *The key principle in preventing intrusion is to be proactive. This means routinely testing your security systems before an intruder does. No network is completely safe. The best rule for high security is to do what the military does: Do not keep extremely sensitive data online.*



# Types of Firewalls

## ❑ Packet-Level Firewalls

- ❑ A packet-level firewall examines the source and destination address of every network packet that passes through it.
- ❑ In general, the addresses are examined only at the transport layer (TCP port ID) and network layer (IP address).
- ❑ Each packet is examined individually, so the firewall has no knowledge of what packets came before.
- ❑ This type of firewall is the simplest and least secure because it does not monitor the contents of the packets or why they are being transmitted and typically does not log the packets for later analysis.

The network manager writes a set of rules (called an access control list [ACL]) for the firewall so it knows what packets to permit into the network and what packets to deny entry.

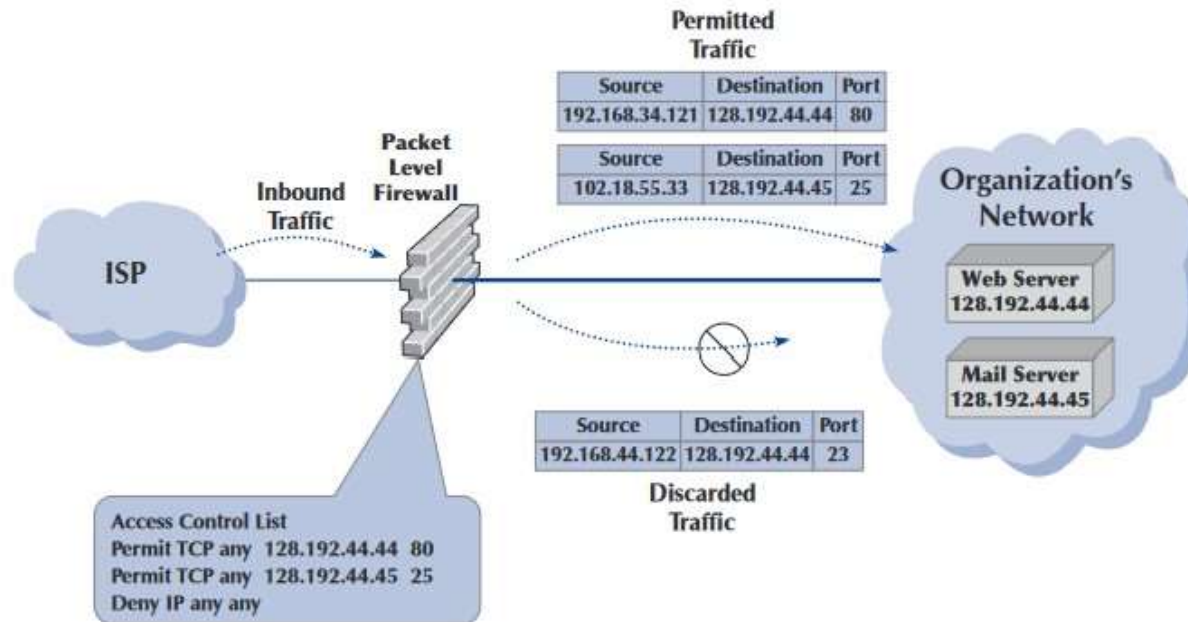
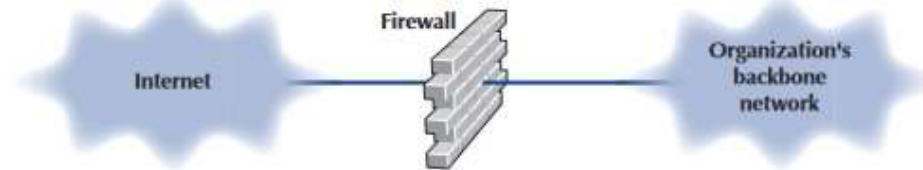
# Types of Firewalls

## ❑ Packet-Level Firewalls (contd)

- ❑ Suppose that the organization had a public Web server with an IP address of 128.192.44.44 and an email server with an address of 128.192.44.45 (see Figure 11-13).
- ❑ The network manager wants to make sure that no one outside of the organization can change the contents of the Web server (e.g., by using telnet or FTP).
- ❑ The ACL could be written to include a rule that permits the Web server to receive HTTP packets from the Internet (but other types of packets would be discarded). For example, the rule would say if the source address is anything, the destination IP address is 128.192.44.44, and the destination TCP port is 80, then permit the packet into the network;
- ❑ Likewise, we could add a rule to the ACL that would permit SMTP packets to reach the email server: If the source address is anything, the destination is 128.192.44.45 and the destination TCP port is 25, then permit the packet through (see Figure 11-13).
- ❑ The last line in the ACL is usually a rule that says to deny entry to all other packets.

# Firewalls

**FIGURE 11-12**  
Using a firewall to  
protect networks



**FIGURE 11-13** How packet-level firewalls work

## What is IP Spoofing?

- ❑ Although source IP addresses can be used in the ACL, they often are not used.
- ❑ Most hackers have software that can change the source IP address on the packets they send (called IP spoofing), so using the source IP address in security rules is not usually worth the effort.
- ❑ Some network managers do routinely include a rule in the ACL that denies entry to all packets coming from the Internet that have a source IP address of a subnet inside the organization, because any such packets must have a spoofed address and therefore obviously are an intrusion attempt.

## Application-Level Firewalls

- ❑ Is more expensive and more complicated to install and manage than a packet-level firewall, because it examines the contents of the application-level packet and searches for known attacks.
- ❑ Application-layer firewalls have rules for each application they can process.
  - ❑ For example, most application-level firewalls can check Web packets (HTTP), email packets (SMTP), and other common protocols.



## Firewall Architectures

- ❑ Many organizations use layers of NAT, packet-level, and application-level firewalls (Figure 11-14).
- ❑ Packet-level firewalls are used as an initial screen from the Internet into a network devoted solely to servers intended to provide public access (e.g., Web servers, public DNS servers).
- ❑ This network is sometimes called the DMZ (demilitarized zone) because it contains the organization's servers but does not provide complete security for them.
- ❑ This packet-level firewall will permit Web requests and similar access to the DMZ network servers but will deny FTP access to these servers from the Internet because no one except internal users should have the right to modify the servers.
- ❑ Each major portion of the organization's internal networks has its own NAT firewall to grant (or deny) access based on rules established by that part of the organization.

# Network Address Translation (NAT) Firewalls

- ☐ NAT is the process of converting between one set of public IP addresses that are viewable from the Internet and a second set of private IP addresses that are hidden from people outside of the organization.
- ☐ NAT is transparent, in that no computer knows it is happening.
- ☐ The most common reasons for NAT are IPv4 address conservation and security.
- ☐ If external intruders on the Internet can't see the private IP addresses inside your organization, they can't attack your computers.
- ☐ Most routers and firewalls today have NAT built into them, even inexpensive home-routers.
- ☐ The NAT firewall uses an address table to translate the private IP addresses used inside the organization into proxy IP addresses used on the Internet.
- ☐ When a computer inside the organization accesses a computer on the Internet, the firewall changes the source IP address in the outgoing IP packet to its own address.
- ☐ It also sets the source port number in the TCP segment to a unique number that it uses.
- ☐ When the external computer responds to the request, it addresses the message to the firewall's IP address.
- ☐ The firewall receives the incoming message, and after ensuring the packet should be permitted inside, changes the destination IP address to the private IP address before transmitting it on the internal network.

## Firewall Architectures: (contd)

- ❑ Many organizations use layers of NAT, packet-level, and application-level firewalls (Figure 11-14).
- ❑ Packet-level firewalls are used as an initial screen from the Internet into a network devoted solely to servers intended to provide public access (e.g., Web servers, public DNS servers).
- ❑ This network is sometimes called the DMZ (demilitarized zone) because it contains the organization's servers but does not provide complete security for them.
- ❑ This packet-level firewall will permit Web requests and similar access to the DMZ network servers but will deny FTP access to these servers from the Internet because no one except internal users should have the right to modify the servers.
- ❑ Each major portion of the organization's internal networks has its own NAT firewall to grant (or deny) access based on rules established by that part of the organization.



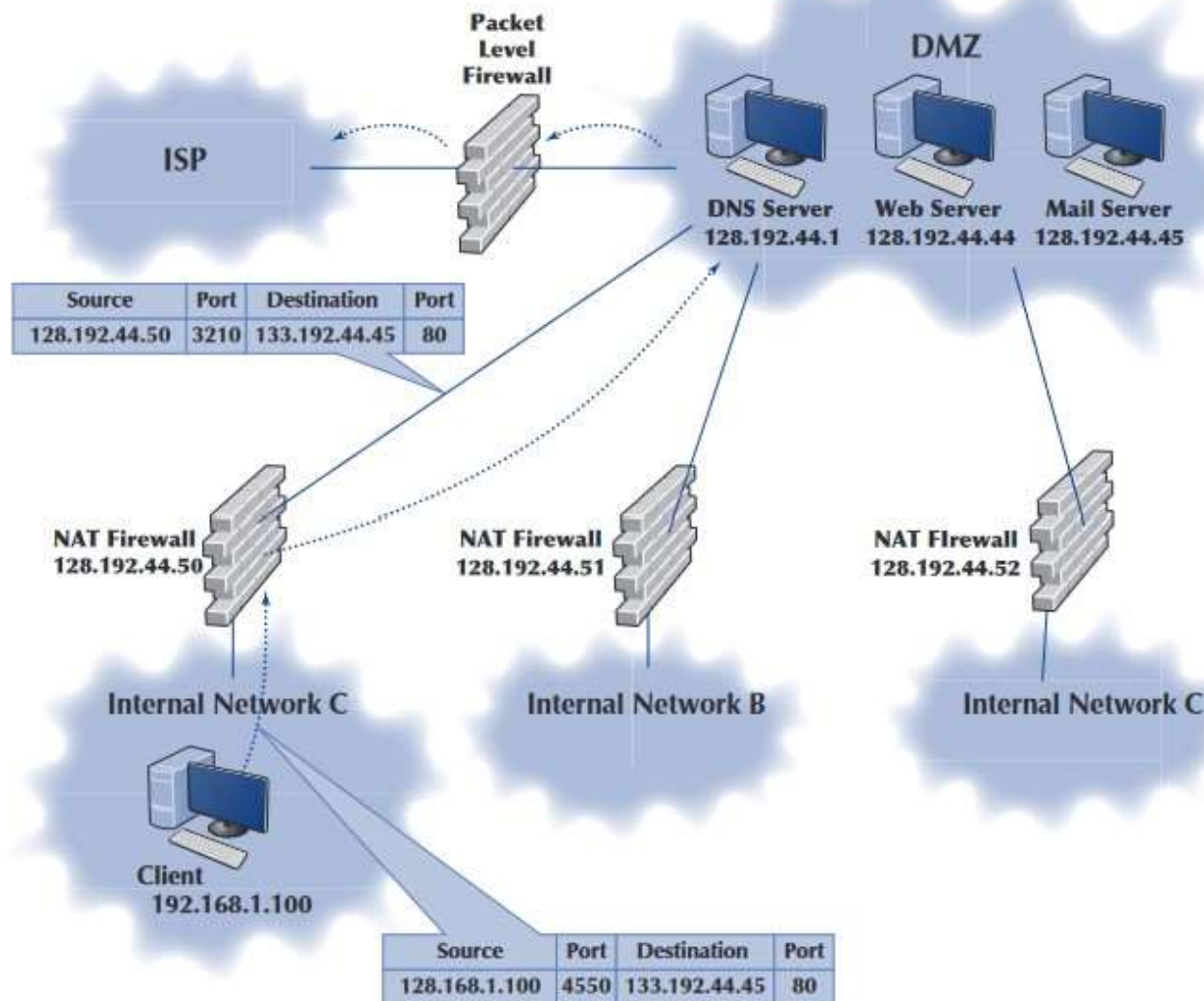


FIGURE 11-14 A typical network design using firewalls

## 11.4.4 Encryption

- ❑ **Best way** to prevent intrusion is encryption, which is a means of disguising information by the use of mathematical rules.
- ❑ Encryption is the process of **disguising** information (converting to **ciphertext**), whereas decryption is restoring it to readable form (**plaintext**).
- ❑ Encryption can be used to **encrypt files** stored on a computer or to **encrypt data in transit** between computers.
- ❑ Types of encryption: **symmetric** and **asymmetric**.
  - ❑ **Symmetric** encryption (also called **single key** encryption) is when the key used to encrypt a message is the same as the one used to decrypt it.
  - ❑ **Asymmetric** encryption is when the key used to decrypt a message is **different** from the key used to encrypt it.
- ❑ **KEY**: Is a small numeric value in terms of bits. Larger the key, more secure the encryption (**Brute Force** attacks become difficult).
- ❑ Key management in symmetric encryption is a problem because the key must be **shared**.

## 11.4.4 DES, 3DES, AES

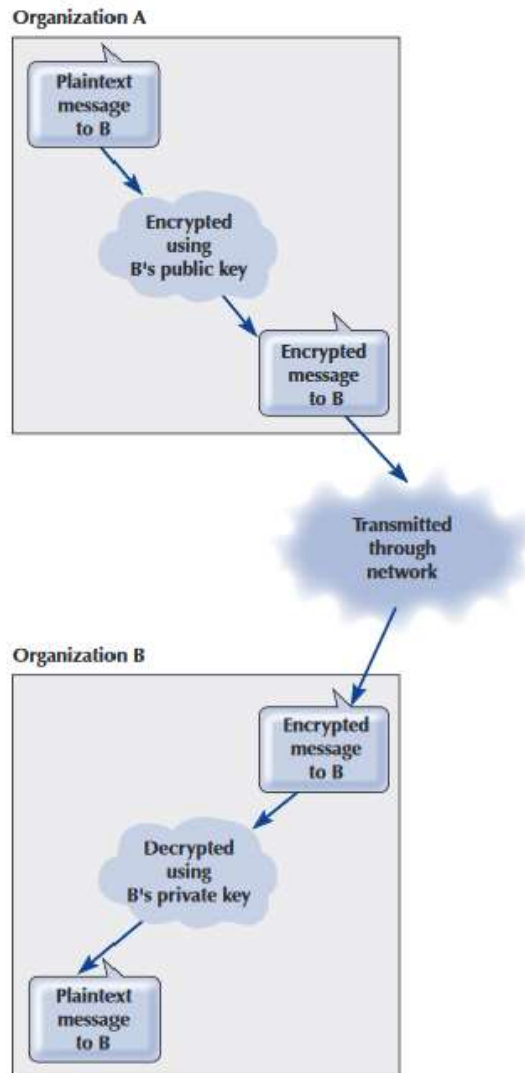
- ☐ DES, 56 bits, Symmetric. Can be cracked in 24 hours. Not safe, still used.
- ☐ 3DES is when DES is used 3 times. Key therefore is 3 times 56 bits.
- ☐ AES: This has replaced DES.
  - ☐ AES key sizes are 128, 192, and 256 bits.
  - ☐ It will require about 150 Trillion Years to crack AES (but with Quantum Computing this can change)
- ☐ RC4 (Rivest): Can use a key up to 256 bits, but usually 40 bits are used.
  - ☐ Faster to use than DES, but can be broken in a day or two.
- ☐ Present day US rules prohibit export of encryption tools the same way as defence material.
  - ☐ Encryption techniques longer than 64 bits cannot be exported (except to the EU and Canada).

## 11.4.4 Public Key Encryption


- ❑ RSA, 1977, MIT, most popular, asymmetric, is the basis of today's PKI (public key infrastructure).
- ❑ There are two keys:
  - ❑ One key, the public key is used to encrypt the message
  - ❑ A second key, a private key, is used to decrypt.
  - ❑ Keys are often of length 512 bits, 1024 bits, or 2048 bits.
- ❑ Messages are encrypted by using public key, and cannot be decrypted without the private key.
- ❑ One way functions: Easy to calculate in one direction but impossible to “uncalculate” in the reverse direction.
- ❑ All public keys are widely publicised, and published in telephone book-style directories.
  - ❑ Therefore, key management is simple.

## 11.4.4 Public Key Encryption

**FIGURE 11-16**  
Secure transmission with  
public key encryption



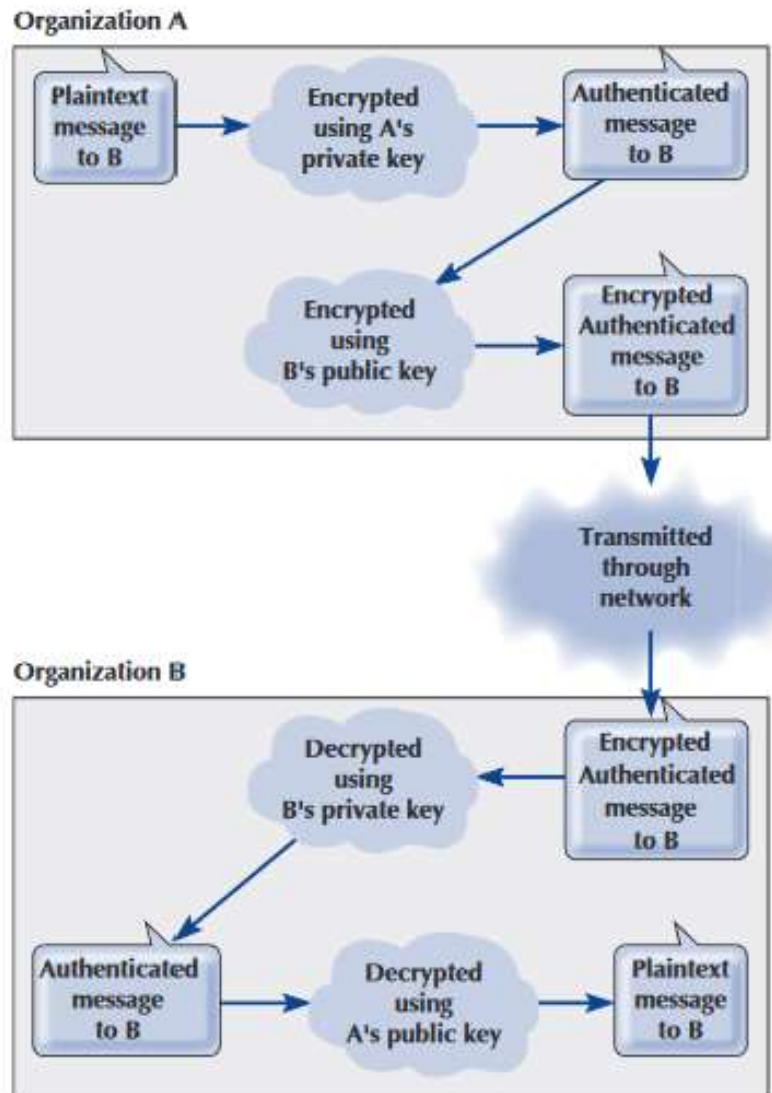
## 11.4.4 Public Key Encryption for Authentication

- ❑ Public key encryption also permits the use of digital signatures through a process of authentication.
- ❑ When one user sends a message to another, it is difficult to legally prove who actually sent the message. Legal proof is important in many communications: (contracts, bank transfers and buy/sell orders in currency and stock trading,
- ❑ Public key encryption algorithms are **invertible**, meaning that text encrypted with either key can be decrypted by the other.
- ❑ It is possible to do the inverse: encrypt with the private key and decrypt with the public key.
  - ❑ Because the private key is secret,  only the real user could use it to encrypt a message.
  - ❑ Thus, a digital signature or authentication sequence is used as a legal signature on many financial transactions.
  - ❑ This signature is usually the name of the signing party plus other key-contents such as unique information from the message (e.g., date, time, or dollar amount).
  - ❑ **The receiver uses the sender's public key to decrypt the signature block** and compares the result to the name and other key contents in the rest of the message to ensure a match.

## 11.4.4 Public Key Encryption for Authentication

**FIGURE 11-17**

Authenticated and secure transmission with public key encryption



## 11.4.4 Problem with Authentication (PKI, CA)

- ❑ It is possible for someone to create a Web site and claim to be “Organization A” when in fact the person is really someone else, and post a public key.
- ❑ This is where the Internet’s public key infrastructure (PKI) becomes essential.
- ❑ The PKI is a set of hardware, software, organizations, and policies designed to make public key encryption work on the Internet.
- ❑ PKI begins with a certificate authority (CA), a trusted organization that can vouch for the authenticity of the person or organization using authentication (VeriSign).
  - ❑ A person wanting to use a CA registers with the CA and provides some proof.
  - ❑ There are several levels of certification: simple confirmation from a valid email address to a complete police-style background check with the interview.
  - ❑ The CA issues a digital certificate that is the requestor’s public key encrypted using the CA’s private key as proof of identity.
  - ❑ This certificate is then attached to the user’s email or Web transactions, in addition to the authentication information.
  - ❑ The receiver then verifies the certificate by decrypting it with the CA’s public key—and contacts the CA to ensure that the certificate has not been revoked.
  - ❑ For higher security certifications, the CA requires that a unique “fingerprint” be issued by the CA for each message sent by the user.



## Finally, Some More Important Terminology/Tools

- ☐ NAT firewalls
- ☐ Application-Level Firewall
- ☐ DMZ
- ☐ Security holes
- ☐ Trojan Horses and rootkits
- ☐ Spyware, Adware, and DDoS agents
- ☐ Encryption and Cryptography
- ☐ PGP
- ☐ Phishing
- ☐ SSL
- ☐ IPSec
- ☐ Sniffer program
- ☐ Kerberos

