6 Understanding Internet Technologies and Security

(Lecture 10)

Discovering the Internet, 5th Edition

Objectives

- Describe the infrastructure of the Internet
- Discuss GPS and identify wireless location-based services
- Explain the convergence of the Internet with telephony and conferencing
- Discuss internal and external network security threats, transactional risks, and virtual private networks

Internet Infrastructure

- Network Service Providers
  - **Network service providers (NSPs)** provide the public and private network infrastructure for the Internet that enables wireless, cellular, and other capabilities
    - AT&T, Sprint, Verizon, T-Mobile, and others
  - An **Internet exchange point (IXP)** is a physical infrastructure that enables ISPs to communicate among their networks, which limits the upstream traffic an ISP must handle
    - **Metropolitan Area Exchange (MAE)** – a specific type of high-speed Ethernet connection within a metropolitan area
  - **Peering** is the exchange of Internet traffic and router information between NSPs and ISPs at an exchange point

Internet Infrastructure

TCP/IP Stack

- **TCP/IP stack** –set of standard Internet protocols on which communications across the Internet and many private networks rely
  - TCP, IP, and UDP are core subprotocols required for all TCP/IP transmissions
- **IP network** is another name for a network running TCP/IP

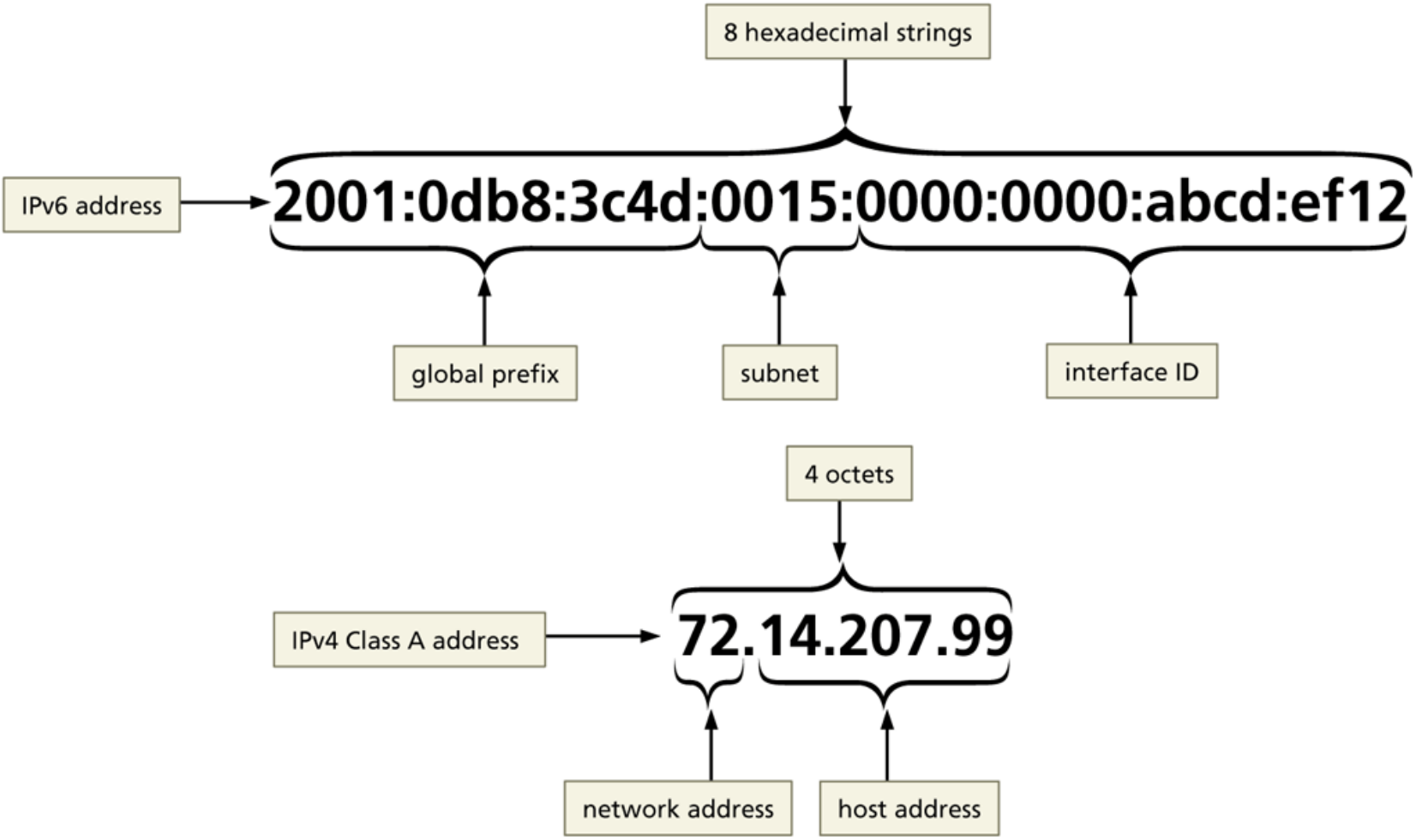
TCP/IP Stack

Subprotocol	Description
Address Resolution Protocol (ARP)	Converts a computer's IP address to its physical MAC address.
Dynamic Host Configuration Protocol (DHCP)	Automatically assigns IP addresses to network devices.
File Transfer Protocol (FTP)	Enables uploading and downloading of files between a local and remote computer.
Hypertext Transfer Protocol (HTTP)	Allows web servers and web browsers to communicate.
Internet Control Message Protocol (ICMP)	Sends error messages to routers and host computers when problems occur with data transmissions.
Internet Message Access Protocol version 4 (IMAP4)	Provides remote access to a mail server, allowing users to manage their stored messages; functions similar to POP3.
Internet Protocol (IP)	Sends packets and provides routers with the address information needed to deliver the packets.
Post Office Protocol version 3 (POP3)	Manages storage of email messages on a mail server and forwarding of email messages from a mail server to a user's mailbox.
Reverse ARP (RARP)	Converts a computer's physical MAC address to its IP address.
Simple Mail Transfer Protocol (SMTP)	Routes email messages from mail server to mail server across an IP network such as the Internet.
Telnet	Allows a computer to act as a terminal for logging on to remote devices such as a computer or router.
Transmission Control Protocol (TCP)	Breaks data into packets, verifies packet integrity, and reassembles error-free packets at their destination.
User Datagram Protocol (UDP)	Sends packets without checking for errors or verifying receipt of the packets. UDP is used to broadcast live video or audio over the Internet.

Internet Infrastructure

- IP Addresses
  - In addition to a MAC address, each node on an IP network has a **logical address**, called an IP address
  - IP address is the unique address of each node on a network
    - The current IP standard, **IPv6**, lengthens IP addresses from 32 bits to 128 bits

Internet Infrastructure

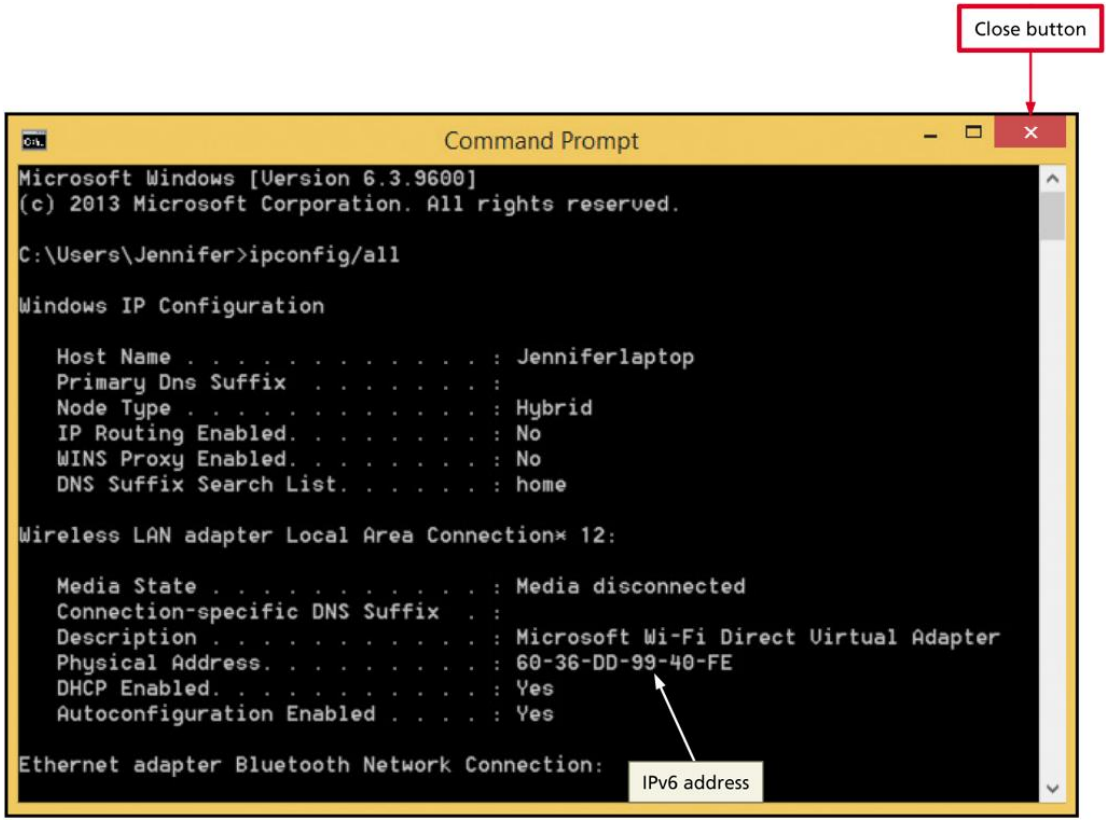


Internet Infrastructure

- IP Addresses (continued)
  - **Classful routing system** used originally
  - **Classless routing system**, called **Classless Inter-Domain Routing (CIDR)** allows network administrators to expand the number of network nodes assigned to an IP address
    - Used extensively on the Internet
    - Used in large private networks

Viewing a Networked Computer's IP Address

- Open the Command Prompt window.
- Enter ipconfig /all at the command-line prompt to instruct the operating system to display all IP information about your networked computer.
- Press the ENTER key to display your computer's host name, IP address, and other IP information.



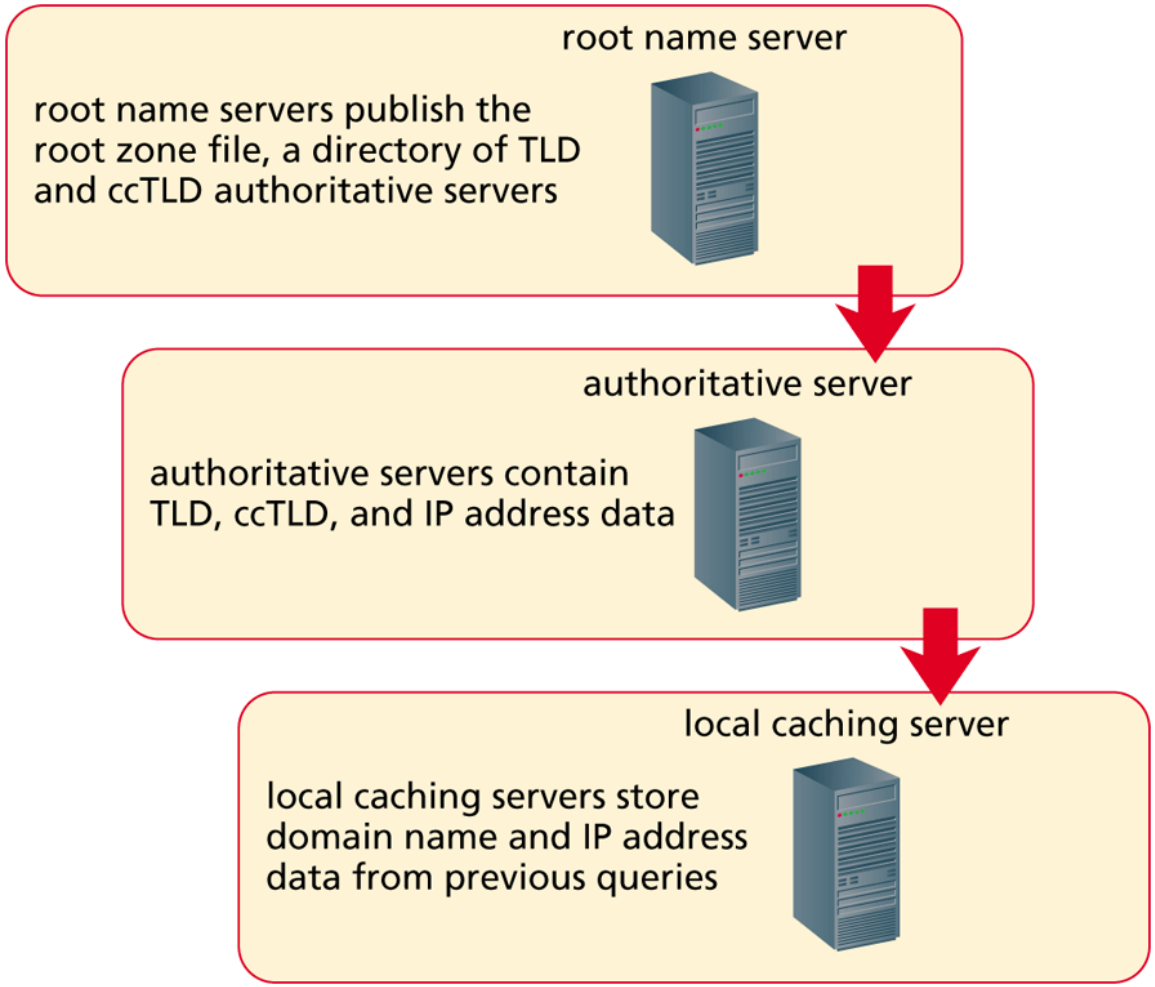
Internet Infrastructure

- Domain Name System (DNS)
  - The DNS is a hierarchy of servers used to translate domain names into IP addresses in a process called **resolving** the domain name
  - Twelve different organizations, such as VeriSign, NASA, the University of Maryland, and the University of Southern California, operate the **root name servers**

Internet Infrastructure

- Domain Name System (DNS) (continued)
  - **Authoritative servers** contain IP information for the TLD and ccTLD domains and their registrants
  - Caching servers **operated** by ISPs and company IT departments contain stored domain name and IP address information
  - **DNS namespace** consists of all information in the DNS databases
  - Process of resolving a domain name begins with local caching server

Internet Infrastructure



Internet Infrastructure

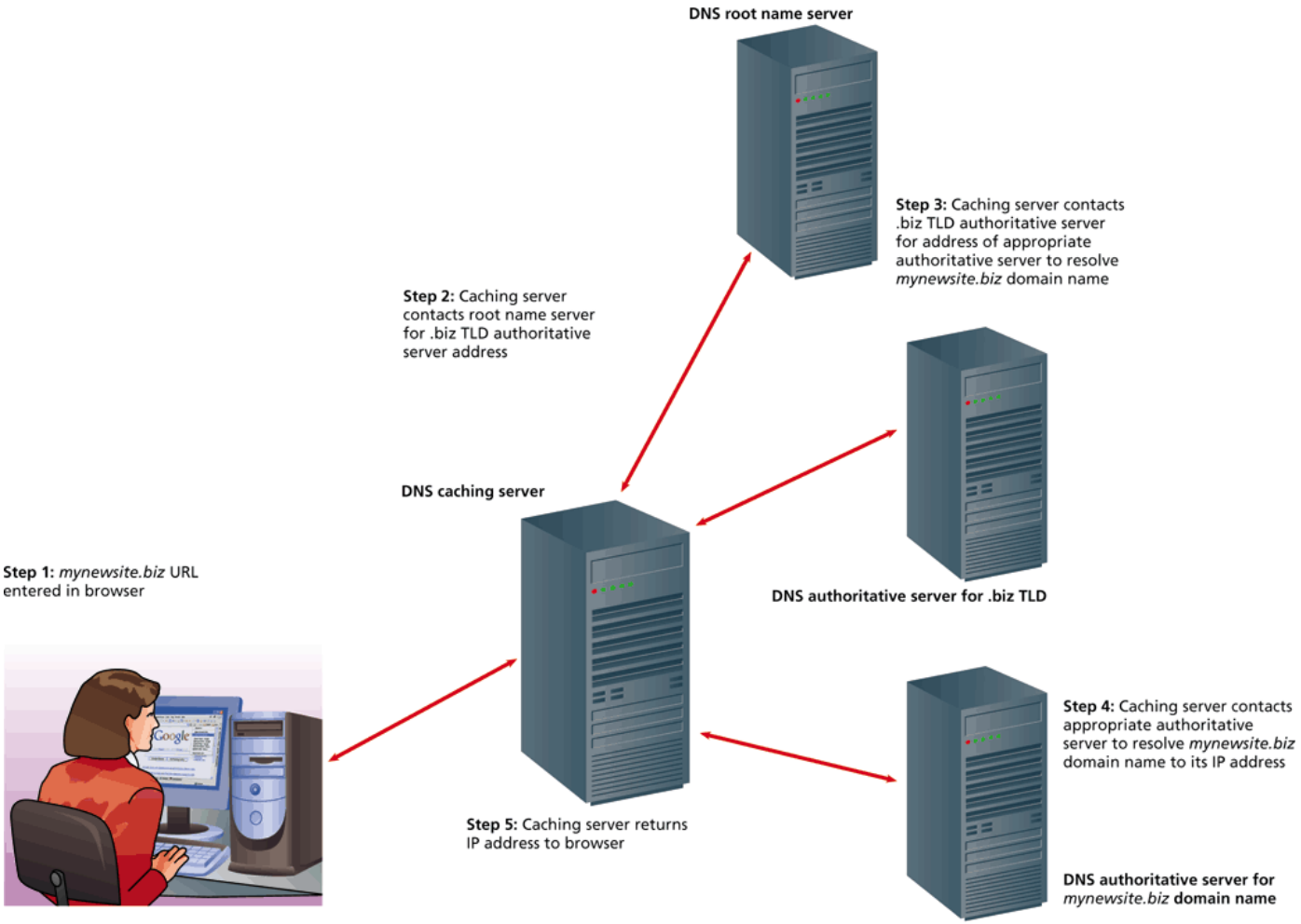
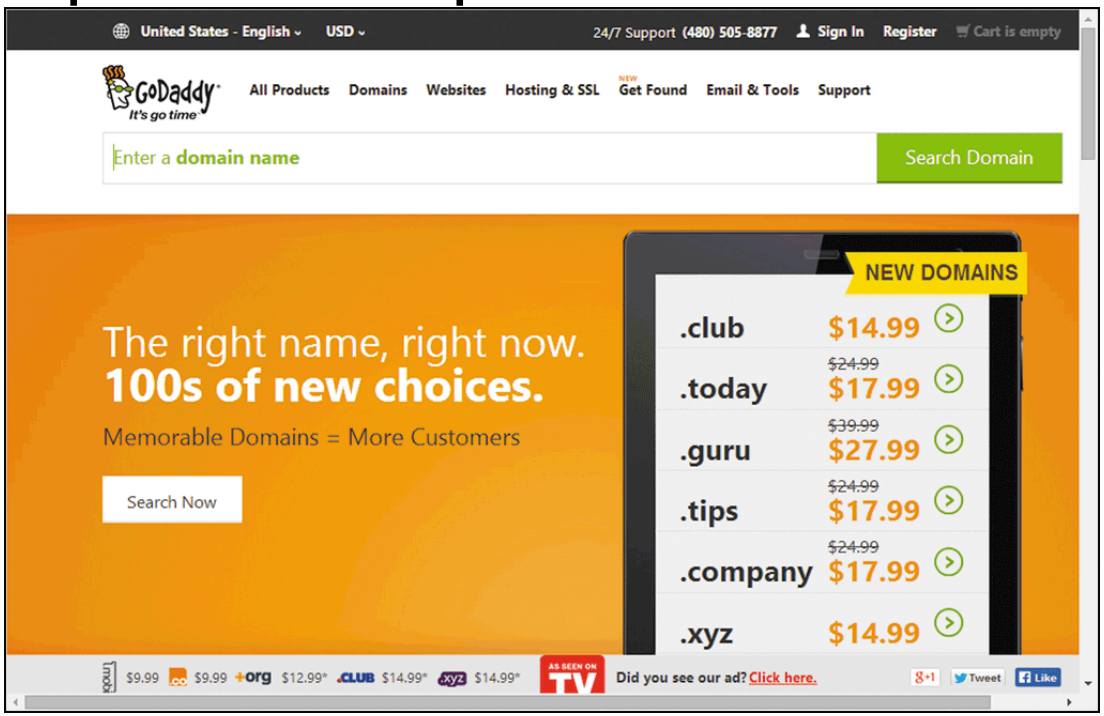


Figure 6-24 The process of resolving a domain name using the DNS begins with a local caching server.

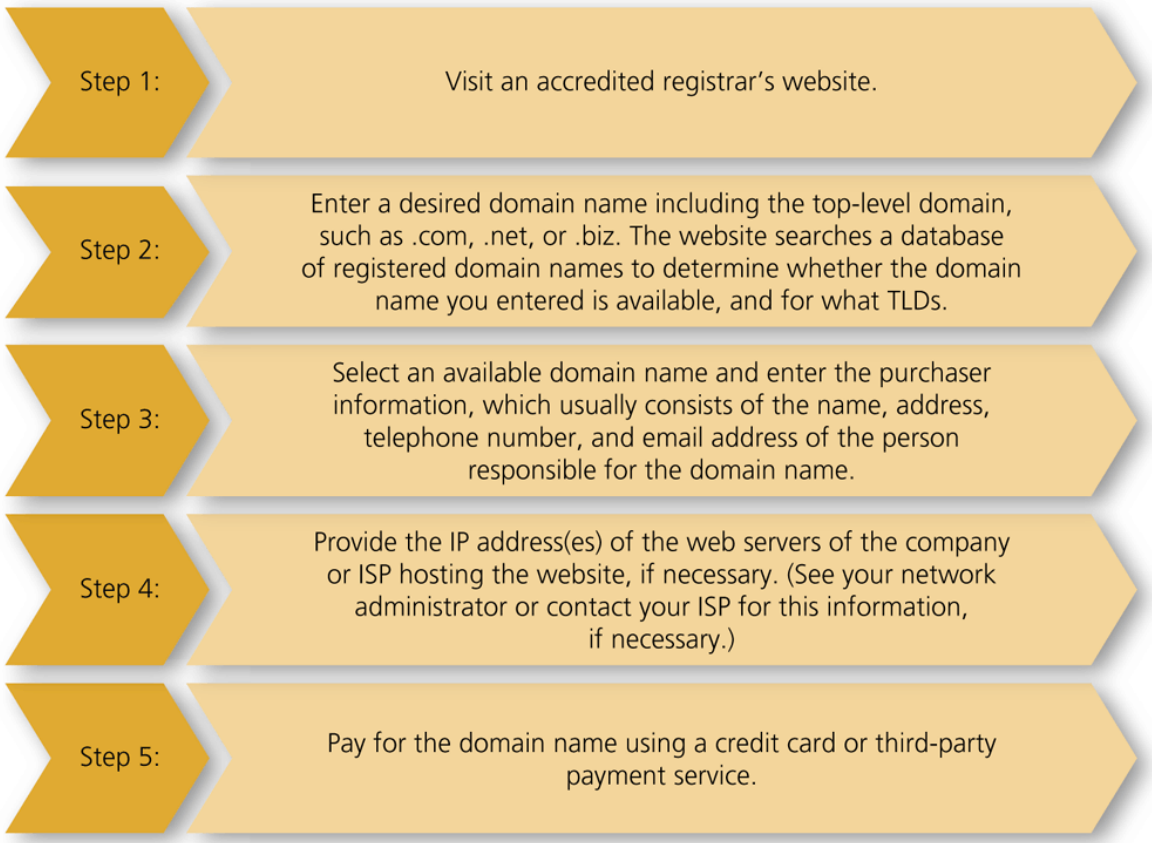
Internet Infrastructure

- Domain Name System (DNS) (continued)
  - **Shared Registration System (SRS)** is registration system that allows private companies, called **accredited registrars**, to handle registration of domain names



Internet Infrastructure

- Domain Name System (DNS) (continued)
  - Process of registering domain name varies by registrar
  - If chosen name is taken, reconsider website name

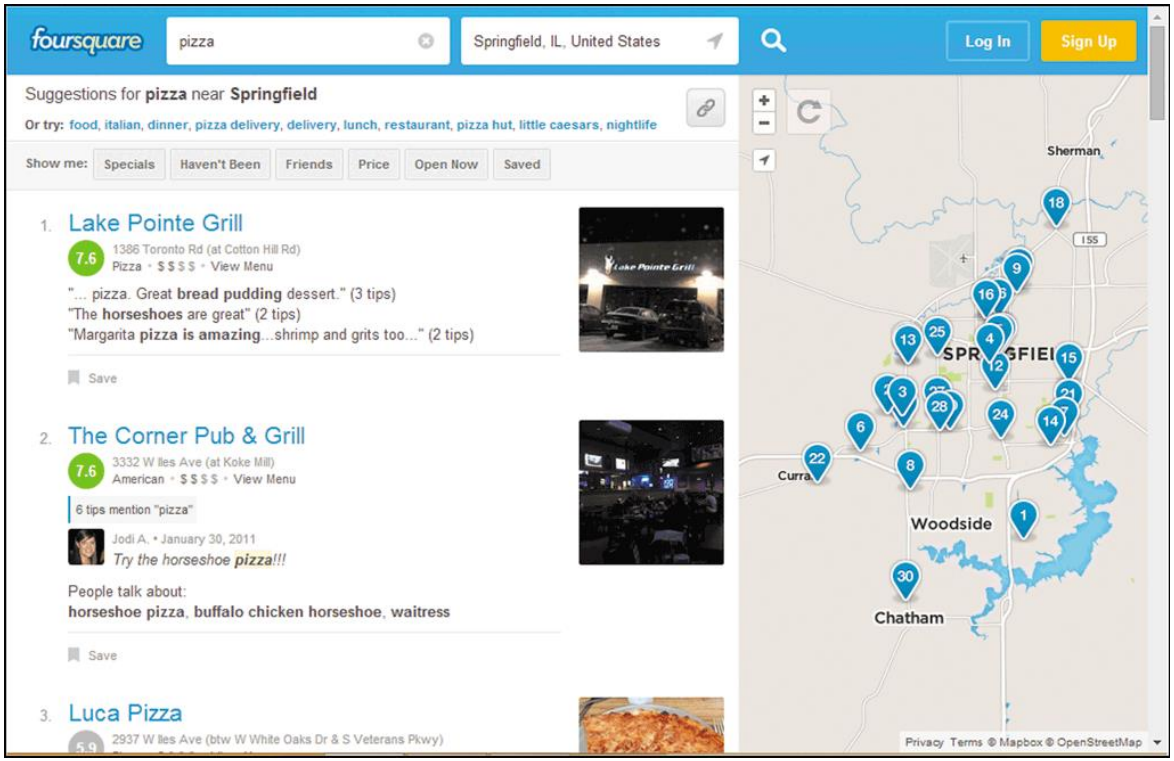


Location-Based Services and GPS

- **Location-based service (LBS)** is a wireless service offered to customers based on their physical location
  - Example: E9-1-1
- **Global Positioning System (GPS)** satellite network and receivers mounted in automobiles or placed in mobile phones, watches, tablets, or other handheld devices

Location-Based Services and GPS

- **Geosocial networking** is a term used to describe the combination of LBS with social networking providers



Internet Telephony and Web Conferencing

- Internet Telephony
  - **IP telephony** or **Voice over IP (VoIP)**
  - Uses TCP/IP and packet switching to send voice transmissions over private or public IP network
    - VoIP providers, such as Vonage, offer telephone services to homes and businesses over broadband Internet connections.
    - Computer to computer calling using special software, such as Skype

Internet Telephony and Web Conferencing

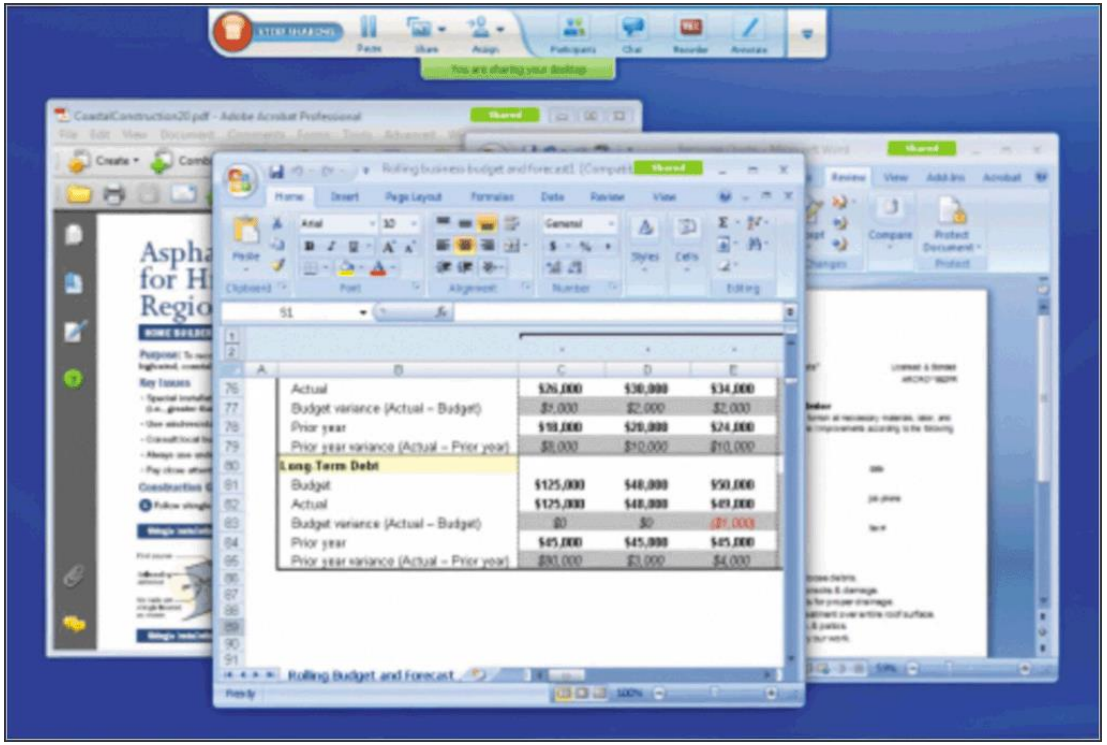
Virtual Meetings, Conversations, and Web Conferencing

- A **virtual meeting** allows collaboration between participants, such as a group of employees, by allowing invitees to log on to their network and sign in to a meeting in which they communicate with each other as well as view, share, and work collaboratively on files
- **Video conferencing**, an expanded virtual meeting that sometimes includes hundreds or thousands of participants, involves real-time transmission of video and audio between two locations

Internet Telephony and Web Conferencing

Virtual Meetings, Conversations, and Web Conferencing

- A **virtual conversation** is a video chat using services such as Google Hangouts or FaceTime
- **Web conferencing** is a virtual meeting conducted using a browser and the web



Network Security Issues and Technologies

- Internal Network Security Threats
  - Security Policies and Procedures
  - Authorized Network Access
    - User ID and passwords

Effective Passwords

Do This	Do Not Do This
Z89$33Q	Wilson (last name)
D33f084	012664 (birthday)
66G13b9	apple
7y3MF98F	user

Network Security Issues and Technologies

- Internal Network Security Threats (continued)
  - **Biometrics** – using devices to measure biological data to identify a user
  - **Smart card –** plastic card the size of a credit card that contains memory chips that can store special access codes or biometric information
  - Wireless Network Security
    - **LAN jacking** or **war driving**
    - **Spoofing**
    - **Rogue WLAN**
  - Data Storage, Backup, and Restore
    - **Cloud storage**

Act of driving around with a laptop, antenna, and wireless card, looking for unsecured wireless networks to access

Technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network

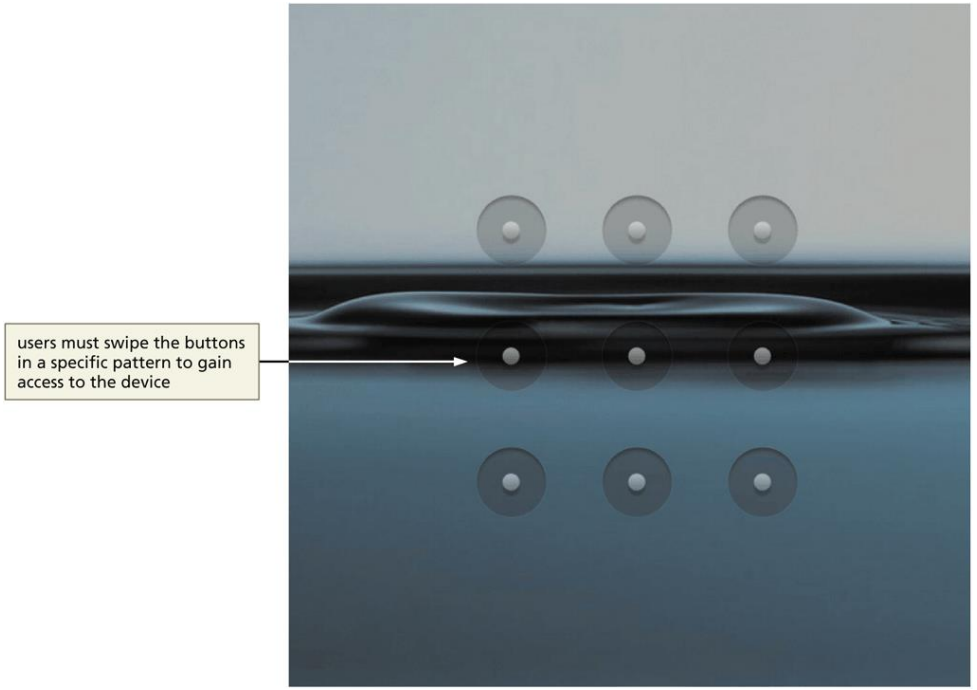
A hacker can create a rouge WLAN by installing a wireless router that uses network resources and exposes the network to security threats

Network Security Issues and Technologies

- Internal Network Security Threats (continued)
  - Disaster Recovery Planning
    - Techniques to protect against accidental or deliberate physical damage to network equipment and data
    - **Disaster recovery plan** covers how an organization deals with a natural or man-made disaster to ensure the organization's viability
- External Network Security Threats
  - Unauthorized Network Access
    - **Distributed denial of service (DDoS)** attacks
    - Hackers may break into network to steal account information, such as credit card numbers, user passwords, and other personal information to steal a person's identity, make unauthorized credit card purchases, or open accounts in a user's name for illegal purposes

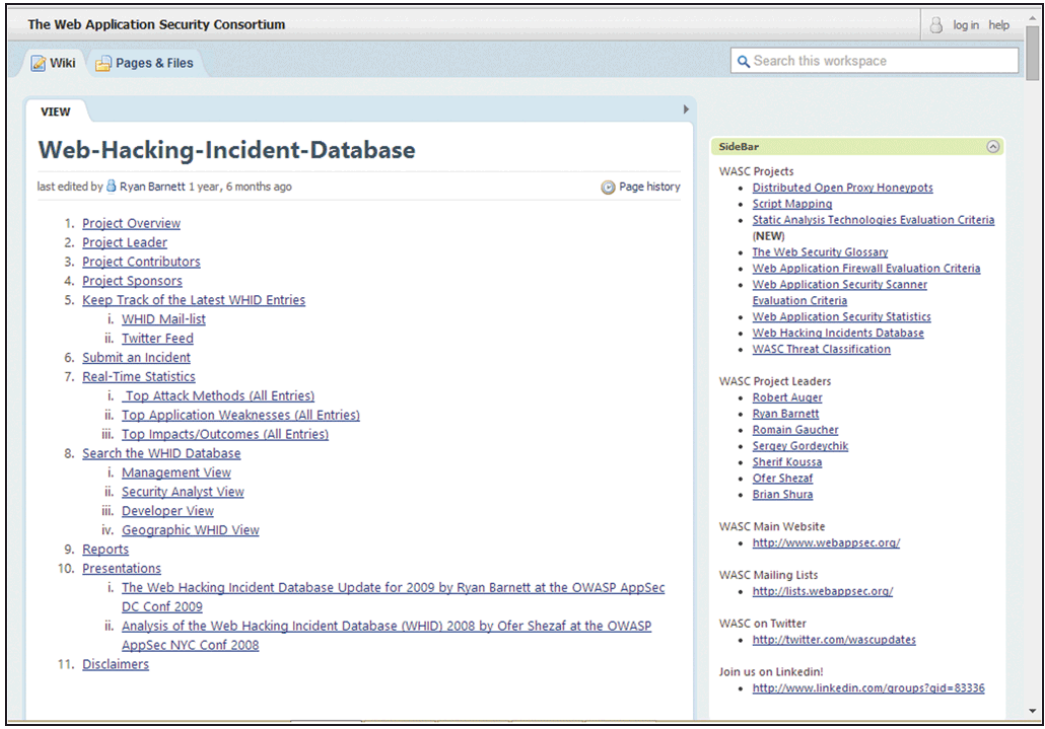
Network Security Issues and Technologies

- External Network Security Threats (continued)
  - Computer Viruses
  - Worm
  - Trojan horse
  - Protect again viruses with virus protection apps
    - Symantec
    - McAfee
    - Swipe codes



Network Security Issues and Technologies

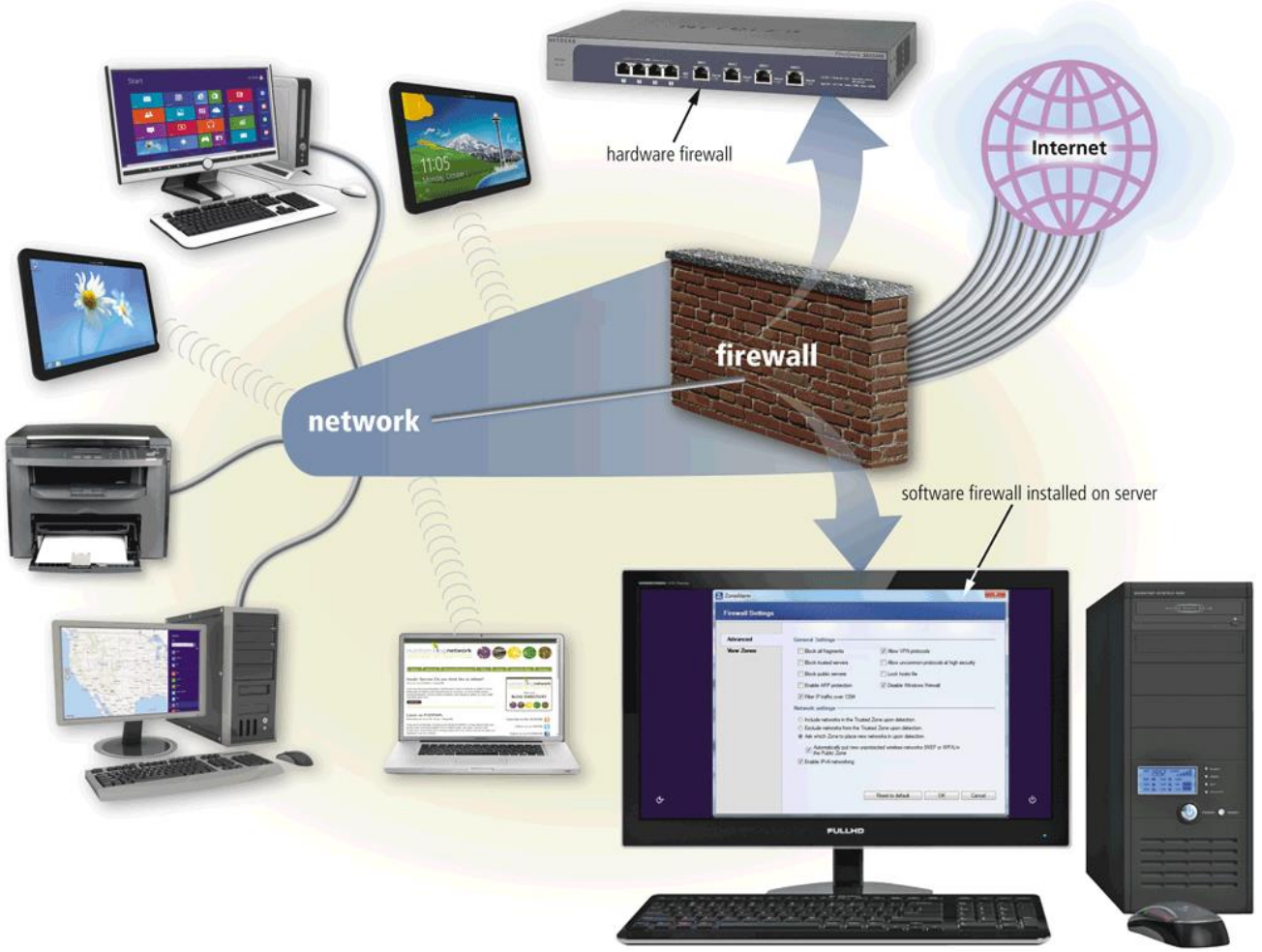
- External Network Security Threats (continued)
  - Web Page Hacking
    - **Hijacking** occurs when hackers redirect a URL to an alternate website
    - Web Application Security Consortium and its sponsored Web Hacking Incidents Database is a good learning resource



Network Security Issues and Technologies

- External Network Security Threats (continued)
  - Firewalls and Proxy Servers
    - **Network firewall** is a combination of hardware and software that filters traffic between private networks or between a private network and a public network, such as the Internet
    - **Proxy server** is a computer or application that hides an internal IP address from the outside world by substituting its own IP address for a source computer's IP address before sending outgoing email or webpage requests

Network Security Issues and Technologies



Network Security Issues and Technologies

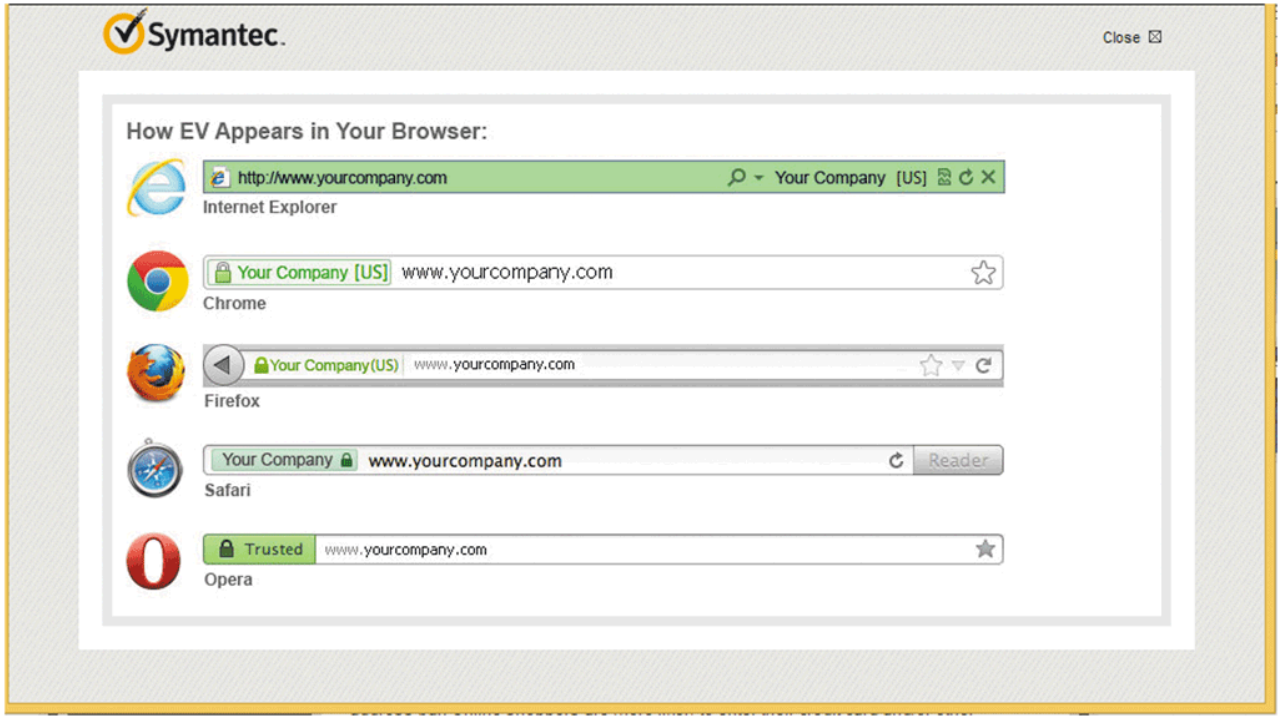
- External Network Security Threats (continued)
  - Internet Filtering Software
    - WebSpy
    - Websense
  - Security Audits
    - **Network security audit –** reviews overall security policies, employee security policy and procedure training, data backup and restore policies and procedures, and the physical security of network equipment and data
    - **Penetration testing –** security audit personnel try to hack into network

Network Security Issues and Technologies

- Transactional Risks
  - Authentication, integrity, nonrepudiation, confidentiality
  - **Encryption** – translating readable data into unreadable data to prevent unauthorized access or use
  - **Certificate authority (CA)** creates encryption keys (public and private) for a fee
    - **Public key** encrypts data and is posted by CA to publicly accessible directory
    - **Private key** is known only to organization and is used to decrypt incoming data

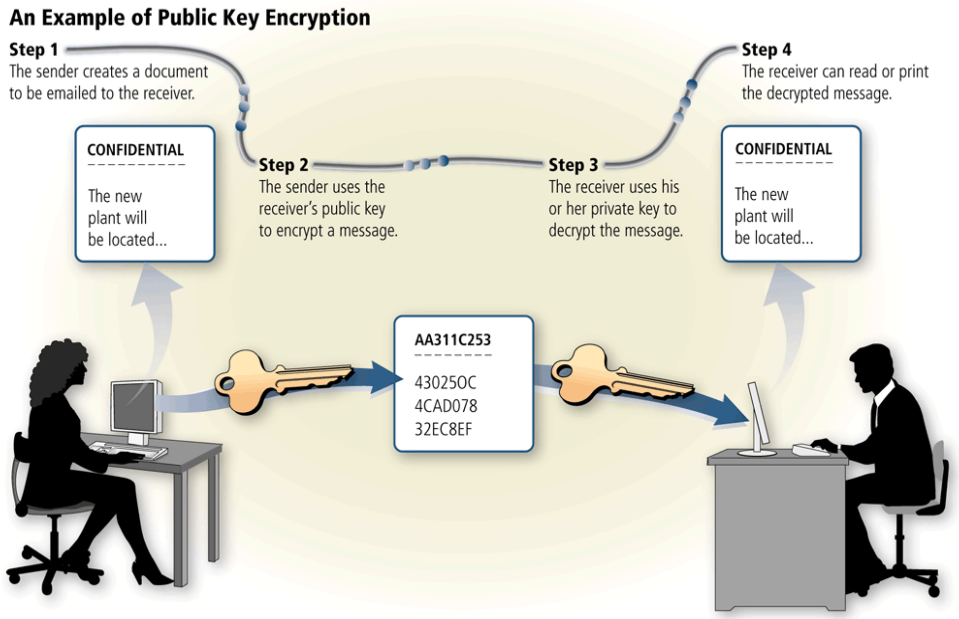
Network Security Issues and Technologies

- Transactional Risks (continued)
  - **Digital certificate** electronically authenticates organization's or individual's identity



Network Security Issues and Technologies

- Transactional Risks (continued)
  - **Public key infrastructure** is combination of organizations or individuals sending and receiving encrypted data, their public and private keys, and the CAs that issue the keys and digital certificates.



Virtual Private Networks

- A **virtual private network** uses a large public IP network, such as the Internet, to transmit its data
  - **Tunneling** is a process that encapsulates one protocol inside another protocol
  - At destination network, the IP protocol information is removed and the tunneling protocol transmits the data to its final destination computer
  - VPNs also use public and private key encryption, digital certificates and special security protocols