Chapter 8: Network Security

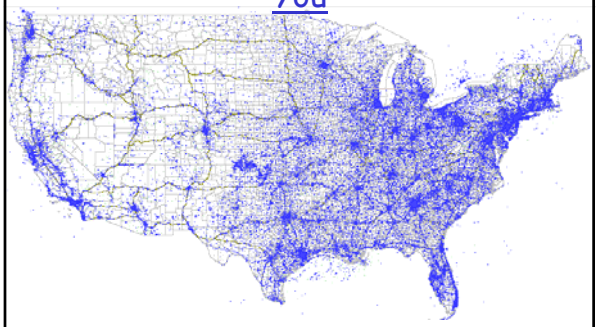
Chapter goals:

- understand principles of network security:
  - cryptography and its *many* uses beyond "confidentiality"
  - authentication
  - message integrity
  - key distribution
- security in practice:
  - firewalls
  - security in application, transport, network, link layers

Questions of Interest

	Practice	Research
Location & Privacy	How are users being tracked?	What constitutes "location privacy"?
Security	How safe are users?	What motivates users to protect themselves?

220,000 Cell Towers Can Find You



http://www.towermaps.com/images/nationwide5.gif

Millions of Wi-Fi Access Points Can Find You

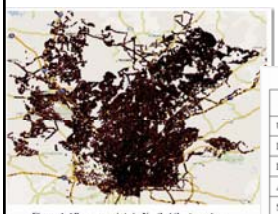


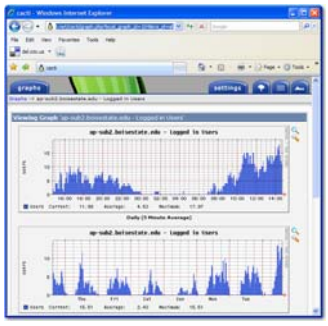
Figure 4. All access points in North Atlanta region.

Table 2. Access Point Density

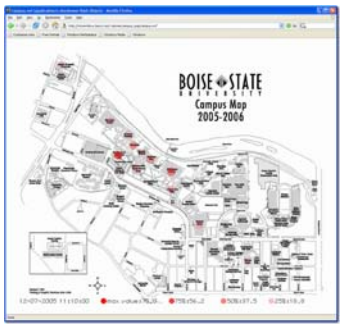
Region	Area (km²)	Access Points	Density (APs/km²)
U.S.	9,166,600	5,615,451	0.6
Las Vegas	240	26,069	109
Kansas City	270	29,438	109
Atlanta	460	65,364	142
San Francisco	213	69,502	326
Seattle	165	64,923	395
Boston	225	164,072	729
Manhattan	105	194,651	1,854

http://www.cercs.gatech.edu/tech-reports/tr2006/git-cercs-06-10.pdf

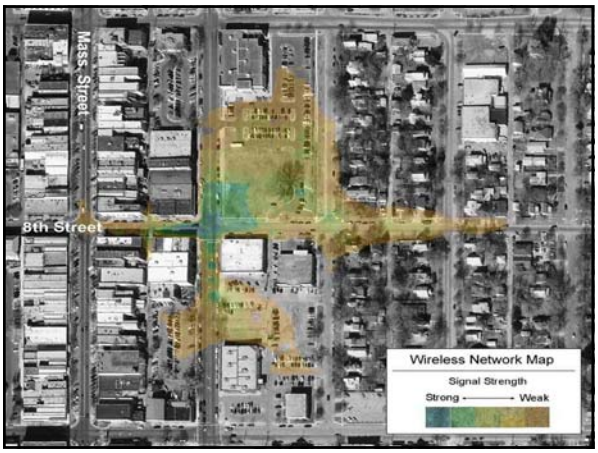
Wireless Usage Volume Over Time

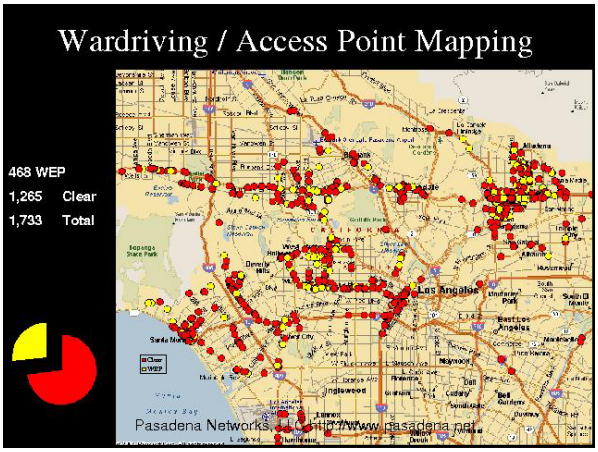


Wireless Usage Locations Over Time



Wireless Users in Real Time





Sources of Threats

- Three sources of security problems are: human error and mistakes, malicious human activity, and natural events and disasters.
- *Human errors and mistakes* include accidental problems caused by both employees and nonemployees.
  - An example is an employee who misunderstands operating procedures and accidentally deletes customer records.
  - This category also includes poorly written application programs and poorly designed procedures.

Sources of Threats (Continued)

- The second source of security problems is *malicious human activity.*
  - This category includes employees and former employees who intentionally destroy data or other systems components.
  - It also includes hackers who break into a system and virus and worm writers who infect computer systems.
  - Malicious human activity also includes outside criminals who break into a system to steal for financial gain; it also includes terrorism.
- *Natural events and disasters* are the third source of security problems.
  - This category includes fires, floods, hurricanes, earthquakes, tsunamis, avalanches, and other acts of nature.
  - Problems in this category include not only the initial loss of capability and service, but also losses stemming from actions to recover from the initial problem.

Problem Types

- Five types of security problems are:
  - Unauthorized data disclosure
  - Incorrect data modification
  - Faulty service
  - Denial of service
  - Loss of infrastructure

Figure 11-1 Security Problems and Sources

		Source		
		Human Error	Malicious Activity	Natural Disasters
Problem	Unauthorized data disclosure	Procedural mistakes	Pretexting Phishing Spoofing Sniffing Computer crime	Disclosure during recovery
	Incorrect data modification	Procedural mistakes Incorrect procedures Ineffective accounting controls System errors	Hacking Computer crime	Incorrect data recovery
	Faulty service	Procedural mistakes Development and installation errors	Computer crime Usurpation	Service improperly restored
	Denial of service	Accidents	DOS attacks	Service interruption
	Loss of infrastructure	Accidents	Theft Terrorist activity	Property loss

Unauthorized Data Disclosure

- *Unauthorized data disclosure* can occur by human error when someone inadvertently releases data in violation of a policy.
  - An example at a university would be a new department administrator who posts student names, numbers, and grades in a public place.
- The popularity and efficacy of search engines has created another source of inadvertent disclosure.
- Employees who place restricted data on Web sites that can be reached by search engines may mistakenly publish proprietary or restricted data over the Web.

Unauthorized Data Disclosure (Continued)

- **Pretexting** occurs when someone deceives by pretending to be someone else.
  - A common scam involves a telephone caller who pretends to be from a credit card company and claims to be checking the validity of credit card numbers.
- **Phishing** is a similar technique for obtaining unauthorized data that uses pretexting via email.
  - The *phisher* pretends to be a legitimate company and sends an email requesting confidential data, such as account numbers, Social Security numbers, account passwords, and so forth.

Unauthorized Data Disclosure (Continued)

- **Spoofing** is another term for someone pretending to be someone else.
  - *If you pretend to be your professor, you are spoofing your professor.*
- **IP spoofing** occurs when an intruder uses another site's IP address as if it were that other site.
- **Email spoofing** is a synonym for phishing.

Unauthorized Data Disclosure (Continued)

- **Sniffing** is a technique for intercepting computer communications.
  - With wired networks, sniffing requires a physical connection to the network.
  - With wireless networks, no such connection is required.
  - **Drive-by sniffers** simply take computers with wireless connections through an area and search for unprotected wireless networks.
  - Even protected wireless networks are vulnerable.
- Other forms of computer crime include breaking into networks to steal data such as customer lists, product inventory data, employee data, and other proprietary and confidential data.

Faulty Service

- *Faulty service* includes problems that result because of incorrect system operation.
- Faulty service could include incorrect data modification, as previously described.
- It also could include systems that work incorrectly, by sending the wrong goods to the customer or the ordered goods to the wrong customer, incorrectly billing customers, or sending the wrong information to employees.
- **Usurpation** occurs when unauthorized programs invade a computer system and replace legitimate programs.
- Faulty service can also result from mistakes made during the recovery from natural disasters.

Denial of Service

- Human error in following procedures or a lack of procedures can result in **denial of service.**
  - For example, humans can inadvertently shut down a Web server or corporate gateway router by starting a computationally intensive application.
- *Denial-of-service attacks* can be launched maliciously.
  - A malicious hacker can flood a Web server, for example, with of millions of bogus services requests that so occupy the server that it cannot service legitimate requests.
  - Natural disasters may cause systems to fail, resulting in denial of service.

Loss of Infrastructure

- Human accidents can cause *loss of infrastructure.*
  - Examples are a bulldozer cutting a conduit of fiber-optic cables and the floor buffer crashing into a rack of Web servers.
  - Theft and terrorist events also cause loss of infrastructure.
    - A disgruntled, terminated employee can walk off with corporate data servers, routers, or other crucial equipment.
- Natural disasters present the largest risk for infrastructure loss.
  - A fire, flood, earthquake, or similar event can destroy data centers and all they contain.

The Security Program

- A security has three components:
  - Senior management involvement:
    - Senior management must establish the security policy
      - This policy sets the stage for the organization to respond to threats.
    - Senior management must manage risk by balancing the costs and benefits of the security program.
  - Safeguards of various kinds.
    - Safeguards are protections against security threats.
    - Safeguards involve computer hardware and software, data, procedures and people.
  - Incident response
    - A security program consists of the organization's planned response to security incidents.

Figure 11-2 Security Safeguards as They Relate to the Five Components

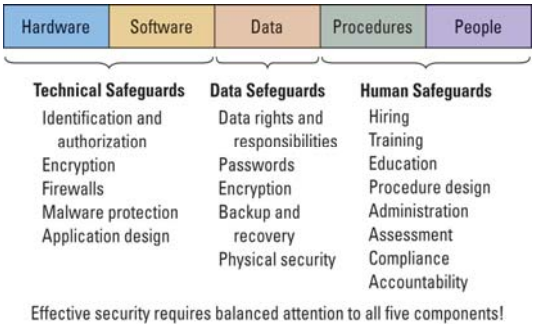


Figure 11-5 Technical Safeguards

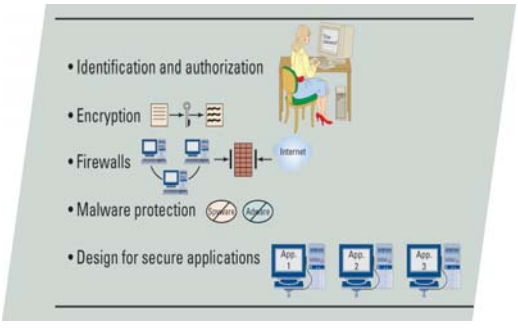
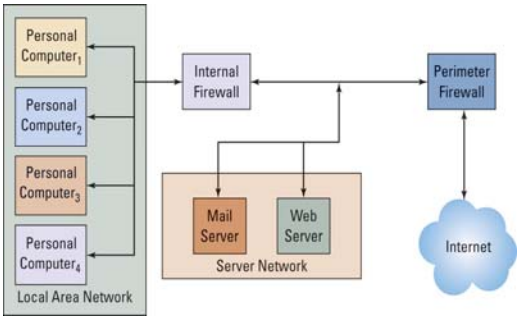


Figure 11-8 Use of Multiple Firewalls



Malware Protection

- The term **malware** has several definitions.
- Our focus will be on the broadest one: *malware* is viruses, worms, Trojan horses, spyware, and adware.

Spyware and Adware

- **Spyware** programs are installed on the user's computer without the user's knowledge.
- Spyware resides in the background and, unknown to the user, observes the user's actions and keystrokes, monitors computer activity, and reports the user's activities to sponsoring organizations.
- Adware is similar to spyware in that it is installed without the user's permission and resides in the background and observes user behavior.
- Most adware is benign in that it does not perform malicious acts or steal data.
- Adware produces pop-up ads and can also change the user's default window or modify search results and switch the user's search engine.

Figure 11-9 Spyware and Adware Symptoms

- Slow system start up
- Sluggish system performance
- Many pop-up advertisements
- Suspicious browser homepage changes
- Suspicious changes to the taskbar and other system interfaces
- Unusual hard-disk activity

Malware Safeguards

- Install antivirus and antispyware programs on your computer.
- Set up your anti-malware programs to scan your computer frequently.
- Update malware definitions.
- Open email attachments only from known sources.
- Promptly install software updates from legitimate sources.
- Browse only in reputable Internet neighborhoods.

Malware Is a Serious Problem

- America Online (AOL) and the National Cyber Security Alliance conducted a malware study using Internet users in 2004.
- They asked the users a series of questions and then, with the users permission, they scanned the users computers to determine how accurately the users understood malware problems on their own computers.

Figure 11-10 Malware Survey Results

Question	User Response	Scan Results
Do you have a virus on your computer?	Yes: 6%	Yes: 19%
	No: 44%	No: 81%
	Don't know: 50%	
Average (maximum) number of viruses on infected computer		2.4 (213)
How often do you update your antivirus software?	Last week: 71%	Last week: 33%
	Last month: 12%	Last month: 34%
	Last 6 months: 5%	Last 6 months: 6%
	Longer than 6 months: 12%	Longer than 6 months: 12%
Do you think you have spyware or adware on your computer?	Yes: 53%	Yes: 80%
	No: 47%	No: 20%
Average (maximum) number of spyware/adware components on computer		93 (1,059)
Did you give permission to someone to install these components on your computer?	Yes: 5%	
	No: 95%	

Source: AOL/NCSA Online Safety Study, October 2004, *staysafeonline.info/news/safety-study-V04.pdf* (accessed March 2005).

Security Guide-Metasecurity

- Metasecurity is security about security
  - "How do we secure the security system?"
- The accounting profession has dealt with some of these problems for decades and has developed a set of procedures and standards know as **accounting controls.**
  - In general, these controls involve procedures that provide checks and balances, independent reviews of activity logs, control of critical assets, and so forth.
  - Properly designed and implemented, such controls will catch the help-desk representative performing unauthorized account transfers.

Security Guide-Metasecurity (Continued)

- Many computer networks threats are new, proper safeguards are under development, and some threats are not yet known.
  - The safeguards for some problems have unexpected consequences.
- Ironically, the answers for many metasecurity problems lie in openness.
  - Encryption experts generally agree that any encryption algorithm that relies on secrecy is ultimately doomed, because the secret will get out.
- Metasecurity extends to the data, procedures, and people components as well.

Useful links

- http://www.cert.org/ (CERT/CC)
- http://www.sans.org/ (SANS Institute)
- http://www.ciac.org/ (CIAC)
- http://www.first.org/ (Forum of Incident Response and Security Teams)
- http://www.securityfocus.com/
- http://www.cerias.purdue.edu/hotlist/ (Center for Education and Research in Information Assurance and Security)

Network Security (summary)

Basic techniques……

- cryptography (symmetric and public)
- authentication
- message integrity
- key distribution

…. used in many different security scenarios

- secure email
- secure transport (SSL)
- IP sec
- 802.11