## Chapter 8: Network Security

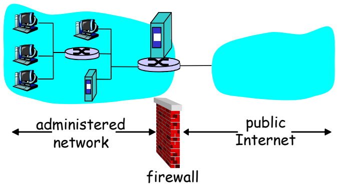
Chapter goals:

- 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

## Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



## Firewalls: Why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections.

prevent illegal modification/access of internal data.

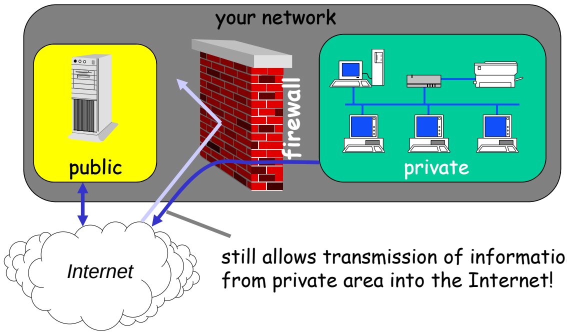
- e.g., attacker replaces CIA's homepage with something else

allow only authorized access to inside network (set of authenticated users/hosts)

two types of firewalls:

- application-level
- packet-filtering

## Implement a firewall



still allows transmission of information from private area into the Internet!

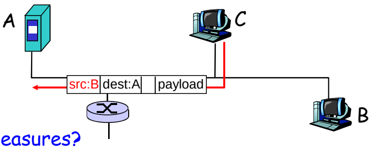
## Limitations of firewalls and gateways

- IP spoofing: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.

## Internet security threats

IP Spoofing:

- can generate "raw" IP packets directly from application, putting any value into IP source address field
- receiver can't tell if source is spoofed
- e.g.: C pretends to be B

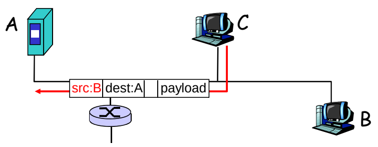


Countermeasures?

## Internet security threats

IP Spoofing: ingress filtering

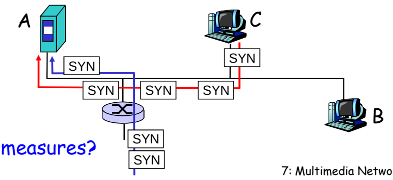
- routers should not forward outgoing packets with invalid source addresses (e.g., datagram source address not in router's network)
- great, but ingress filtering can not be mandated for all networks



## Internet security threats

Denial of service (DOS):

- flood of maliciously generated packets "swamp" receiver
- Distributed DOS (DDOS): multiple coordinated sources swamp receiver
- e.g., *C* and remote host SYN-attack *A*

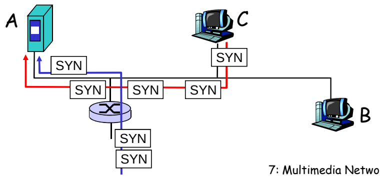


Countermeasures?

## Internet security threats

Denial of service (DOS): countermeasures

- filter out flooded packets (e.g., SYN) before reaching host: throw out good with bad
- traceback to source of floods (most likely an innocent, compromised machine)



## Stay informed

- subscribe to mailing lists (CERT/CC advisories, BugTraq, NTBugTraq, Microsoft security advisories, …)
- check for new exploits

## Apply patches

- advisories often offer links to vendor patches
- if those are absent, consider a temporary service restriction

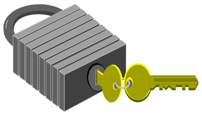
sites still report successful IMAP attacks, although patches have been available for more than three years

## Monitor system activity and integrity

- store logs in a safe place
- check logs for suspicious entries
- compare checksums on essential binaries and configuration files *(Tripwire)*
- monitor incoming connections *(Argus)*
- test systems with scanners *(SATAN, ISS)*

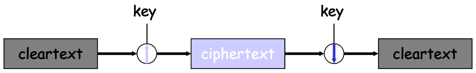
## Use encryption

- encrypt your remote sessions
- encourage use of email encryption (e.g. PGP - Pretty Good Privacy)
- encrypt sensitive data on servers



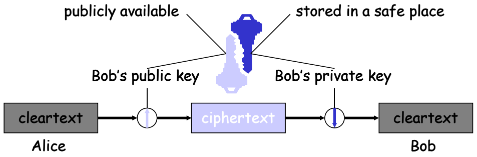
## Symmetric encryption

- users/devices/programs share a secret key used for encryption and decryption:



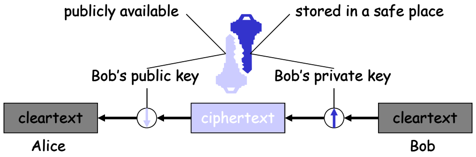
## Asymmetric encryption

- key consists of a complementary public and private part



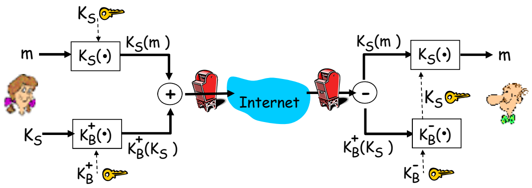
## Digital signatures

- digital signatures encrypt only "message digests", not the whole message



## Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.

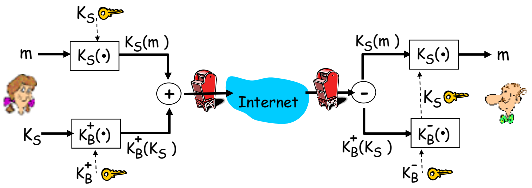


Alice:

- generates random *symmetric* private key, $K_S$.
- encrypts message with $K_S$ (for efficiency)
- also encrypts $K_S$ with Bob's public key.
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob.

## Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.

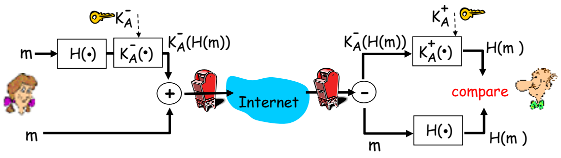


Bob:

- uses his private key to decrypt and recover $K_S$
- uses $K_S$ to decrypt $K_S(m)$ to recover m

## Secure e-mail (continued)

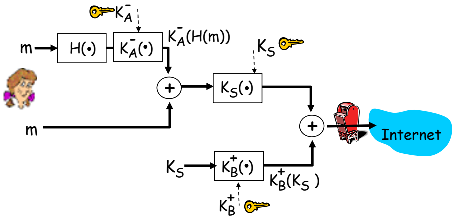
- Alice wants to provide sender authentication message integrity.



- Alice digitally signs message.
- sends both message (in the clear) and digital signature.

## Secure e-mail (continued)

- Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

## Pretty good privacy (PGP)

- Internet e-mail encryption scheme, de-facto standard.
- uses symmetric key cryptography, public key cryptography, hash function, and digital signature as described.
- provides secrecy, sender authentication, integrity.
- inventor, Phil Zimmerman, was target of 3-year federal investigation.

A PGP signed message:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZ
   P9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

## Secure sockets layer (SSL)

- transport layer security to any TCP-based app using SSL services.
- used between Web browsers, servers for e-commerce (shttp).
- security services:
  - server authentication
  - data encryption
  - client authentication (optional)
- server authentication:
  - SSL-enabled browser includes public keys for trusted CAs.
  - Browser requests server certificate, issued by trusted CA.
  - Browser uses CA's public key to extract server's public key from certificate.
- check your browser's security menu to see its trusted CAs.

## SSL (continued)

Encrypted SSL session:

- Browser generates *symmetric session key*, encrypts it with server's public key, sends encrypted key to server.
- Using private key, server decrypts session key.
- Browser, server know session key
  - All data sent into TCP socket (by client or server) encrypted with session key.
- SSL: basis of IETF Transport Layer Security (TLS).
- SSL can be used for non-Web applications, e.g., IMAP.
- Client authentication can be done with client certificates.

## Network Security (summary)

Basic techniques......

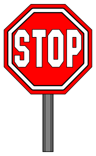
- cryptography (symmetric and public)
- authentication
- message integrity
- key distribution

.... used in many different security scenarios

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

## Prevention traps

- there is no perfect protection, not even with firewalls
- don't trust out-of-the-box solutions and "zero administration" concepts



## After the incident

- consult your security policy
- if you do not have a security policy
  - consult with management
  - consult with your legal counsel
  - contact law enforcement agencies
  - notify others within your organization
- document all of the steps you take in recovering

## Regain control

- disconnect compromised systems from the network
- copy an image of the compromised systems

## Analyze the intrusion

- look for modifications made to system software and configuration files
- look for modifications to data
- look for tools and data left behind by the intruder
- review log files
- look for signs of a network sniffer
- check other systems on your network

## Things to check

- logs in /var/adm or /var/log (have they been tampered with?)
- users' .bash_history files
- regular files and directories in /dev
- list of recently changed files
  - find /bin –mtime –5 –print
- compare saved binaries with current ones
- compare MD5 checksums

## Contact the relevant organizations

- Incident Response Teams
  - list of FIRST teams at http://www.first.org/
  - list of European teams at http://www.terena.nl/cert/
- other sites involved in the incident
  - whois.ripe.net (Europe)
  - whois.arin.net (Americas)
  - whois.apnic.net (Asian-Pacific)

## Recover from the intrusion

- install a clean version of your operating system
- disable unnecessary services
- install all vendor security patches
- consult advisories and external security bulletins
- change passwords

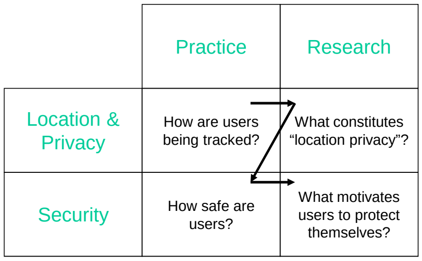
## Disclosure of information

- when communicating with others about the incident, think about:
  - do you know who you are talking with?
  - is the other site also compromised?
  - is someone else reading the messages?
  - what kind of information can you submit to others?

## Global trends

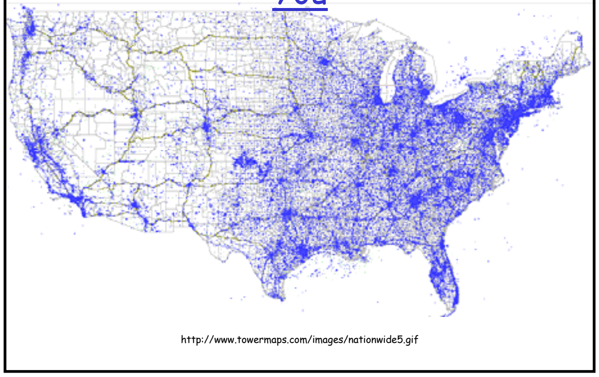
- readily available exploits and automation
  - increase in number of attacks
  - average intruder knows less
- growth in electronic commerce is forcing a change (although slow) in legislation and implementation of encryption mechanisms
- recurring types of attacks (buffer overruns)

## 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

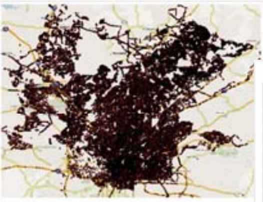


Figure 4. All access points in North Atlanta region.

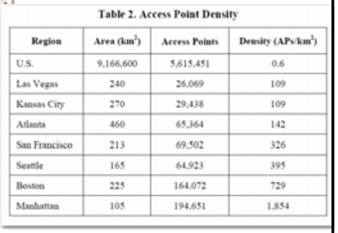
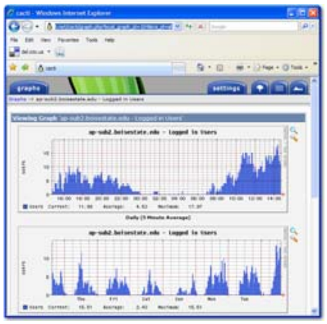


Table 2. Access Point Density

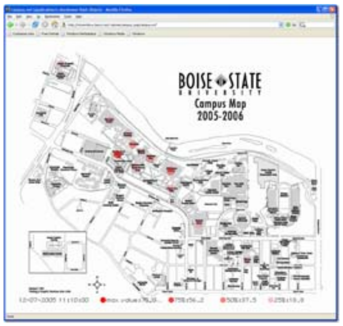
| Region | Area (km$^2$) | Access Points | Density (APs/km$^2$) |
|---|---|---|---|
| U.S. | 9,166,600 | 5,615,451 | 0.6 |
| Las Vegas | 240 | 26,069 | 109 |
| Kansas City | 270 | 29,438 | 109 |
| Atlanta | 460 | 65,364 | 142 |
| San Francisco | 213 | 69,502 | 326 |
| Seattle | 165 | 64,923 | 395 |
| Boston | 225 | 164,072 | 729 |
| Manhattan | 105 | 194,651 | 1,854 |

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

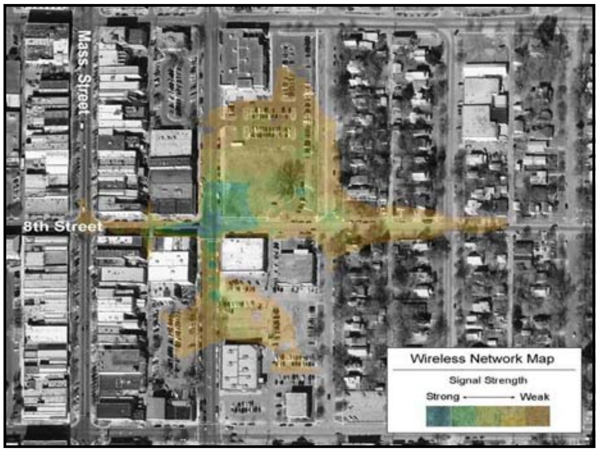
## Wireless Usage Volume Over Time


cacti - Windows Internet Explorer
graphs
settings
ap-sub2.boisestate.edu - Logged in Users
Daily (5 Minute Average)
ap-sub2.boisestate.edu - Logged in Users

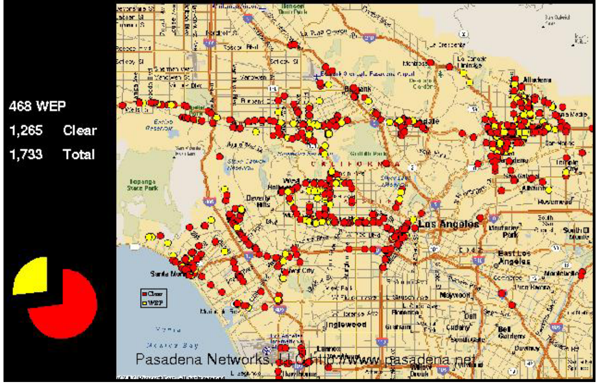
## Wireless Usage Locations Over Time



## Wireless Users in Real Time



## Wardriving / Access Point Mapping



## 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)