ICS 351: Today's plan

- DNS
- WiFi

Domain Name System

- Hierarchical system of names
- top-level domain names include .edu, .org, .com, .net, and many country top-level domains
- root is just "."
- so the fully qualified domain name is, e.g., www.hawaii.edu.
- administration of domains is delegated according to the hierarchy

Domain Name Service

- the domain names are administratively divided into zones
- each zone must be contiguous in the hierarchy tree:
- o .edu. is one zone
- o hawaii.edu. and most names below it are one zone,
- o ics.hawaii.edu. and all names below it are one zone,
- in the Internet, each zone should have at least two authoritative servers
- the root has 13 servers, A.root-servers.net through M.root-servers.net

Domain Name Service

- the domain names are administratively divided into zones
- each zone must be contiguous in the hierarchy tree:
  - .edu. is one zone
  - as is hawaii.edu. and most names below it,
  - but ics.hawaii.edu. and below are one zone
- in the Internet, each zone should have at least two authoritative servers
- the root has 13 servers, A.root-servers.net through M.root-servers.net, some of which are actually multiple servers

DNS Communications

- clients (resolvers) send requests to servers to resolve a domain name to an IP address or vice-versa
- DNS is designed to run over either TCP or UDP, but commonly runs over UDP for name resolution
- large transfers such as zone exchanges usually use TCP

zone file

- the network administrator must configure each of the servers with a description of name to IP address mappings
- this is loosely known as a zone file, even though several files might be needed to accomplish the overall configuration
- if there are multiple servers for one zone (should be at least two) their zone files should describe the same zone
- DNS names in zone files end in '.' if they are absolute, otherwise they are relative to the zone

DNS Resource Records

- `A` is not the only record that can be served:
- `MX` identifies the mail server for a given name
- `NS` identifies the name server for a given name
- `CNAME` identifies the "main" (canonical) name for a given name
- the `SOA` (start of authority) record can be used by a slave server to download the records from the master server

DNS Query

- a DNS client sends a query to any DNS server
- usually, every client is configured with the IP address of one or more DNS servers
- the servers authoritative for the zone know a given translation ("answer"), though other servers and clients may cache a translation
- since the DNS name space and the zones are arranged hierarchically, a DNS server always knows another server closer to the answer
- DNS names are encoded efficiently by replacing repeated strings with pointers: a.hawaii.edu and b.hawaii.edu become a.hawaii.edu and b.*pointer-to-previous-hawaii.edu*

DNS Query Response

- a server can respond to a query in one of three ways:
- o by returning the answer, if it is known or cached,
- o by returning the address of another server closer to the answer: this leads to the client performing an iterative query
- o by requesting the translation from a server closer to the answer, then returning the result to the client: this is a recursive query

ICS 351: Today's plan

- wireless 802.11 and WiFi.
- 802.11 security: WEP, 802.11i, WPA, WPA2.
- networking security
- wireless ad-hoc and mesh networks

ISM bands

- to operate most radios, a license is needed from a government body (in the U.S., the FCC)
- to operate a microwave oven, no license is needed
- microwave ovens work on the resonant frequency of water, 2.4GHz
- the 2.4GHz-2.5GHz band has been designated an **Industrial**, **Scientific**, and **Medical** (ISM) band, free to use worldwide without a license – as long as transmission power is limited – and some countries restrict part of this band

Using ISM bands

- ISM equipment needs to tolerate interference (e.g., from microwave ovens!)
- there are many ISM bands, but most are limited to only some countries
- due to the unprecedented availability of the 2.4GHz ISM band, many applications have been developed for it

Wireless 802.11/WiFi

- an early marketing term for 802.11 was WiFi (a pun on HiFi, High Fidelity audio equipment)
- 802.11 works mostly in the 2.4GHz ISM band, though 802.11a works in the 5GHz band
- many successive standards, 802.11 (1-2Mb/s), 802.11a (54Mb/s), 802.11b (11Mb/s), 802.11g (54Mb/s) and foreseeable future versions

802.11/WiFi Operation

- 802.11 has two modes: ad-hoc (point-to-point) and managed
- in managed mode, all communication is to or from a central access point
- end-nodes contend for the medium: this contention may result in collisions that require retransmissions

802.11 Security: WEP

- tapping a wired network requires physical access to the wires
- tapping a wireless network requires being in range of the signal
- originally, cryptographic Wired Equivalent Privacy (WEP) was introduced to hide the contents of the messages
- the original design for WEP was not widely published – unfortunately, this lead to a lack of serious examination of the protocol:
- security by obscurity often does not work

802.11 Security: WPA and WPA2

- unfortunately, WEP is sufficiently weak that it can be cracked by listening to a few minutes of busy traffic
- 802.11i introduced:
- o WiFi Protected Access (WPA), a simple but much stronger encryption protocol, and
- o WPA2, stronger than WPA and requiring more resources for implementation (including, in some cases, newer equipment)

networking security

- "in the clear" protocol can be easily broken when information is snooped: telnet, ftp, http, many email protocols
- encrypted protocol are secure against many attacks, including someone examining the data: ssh/scp, https, secure POP/IMAP, PGP
- most protocols are not secure against traffic analysis
- *host security* is more concerned with installing applications, running foreign code, firewalls/NATs, etc

security principles

- it is usually better to have more security than less security
- security that inconveniences users is more likely to be resisted or circumvented
- security can inadvertently lock out people who should have access
- data requiring security should not be sent unencrypted over the Internet, because some of the links may be accessible to adversaries
- data requiring security is still often sent unencrypted over the Internet, though data with monetary value is usually protected these days

wireless ad-hoc networks

- using the ad-hoc mode of 802.11, any machine ("node") may directly talk to any other node
- if nodes agree to forward data for each other, they can form a wireless ad-hoc network
- machines may move or go to sleep, so routing can be challenging
- also, the notion of a "link" is different for wired and wireless networks: successful wireless protocols take advantage of broadcasting
- generally machines should discover each other and automatically send data to the destination

wireless mesh networks

- a wireless mesh network consists of static wireless nodes
- possibly with some wired nodes coordinating to provide Internet access
- mobile nodes may obtain Internet access from nodes in a mesh network