Computer Networks
ICS 651

- Ethernet summary
- HTTP
- HTTPS
- HTTP authentication
- network security

Ethernet Summary

- hub, switch, router, NAT+firewall
  - firewall blocks incoming connections, which prevents port scanning and some attacks
- home network setup is mostly automated
- designing larger networks requires consideration of traffic as well as security
- ethernets should be designed to be either strictly point-to-point (preferably full-duplex), or mostly unloaded

Our network so far

- DNS
- IP, ICMP, and routing
- TCP and UDP
- Ethernet and WiFi (and SLIP/serial ports)
- can carry data end-to-end, reliably or quickly
- can build robust, efficient, fast, inexpensive local area networks
- what is missing: why are we carrying the data?

Tasks for the application

- user interaction
- accomplishing specific tasks
- providing security
- encoding real-world data (and voice/video)
- "creating" and "consuming" data

application-layer functions

- client-server (or p2p) interactions
- sessions: logging in, user state
- security
- ultimate end-to-end evaluation of reliability (e.g. "reload" button in browser) and performance
- applications nest, e.g. social networking sites or banking applications are nested within the web

Some application-layer protocols

- HTTP
- HTTPS/SSL/TLS
- ssh
- SMTP/POP/IMAP
- NTP
- FTP
- telnet
- etc.

HTTP

- HyperText Transfer Protocol
- request and reply headers, both encoded in ASCII (HTTP/2 and HTTP/3 use binary)
- headers are variable length, with variable fields
- first line is required, some fields are required
- header ends at first empty line
- ancestry: FTP
- HTTP/1.1 allows multiple requests/replies to be sent on a single TCP connection
- in-class exercise: explain why this is an improvement over HTTP/1.0 (one request/reply per TCP connection)

HTTP/1.1 example

- an HTTP request might look like this:

```
GET /~esb/ HTTP/1.1
Host: www2.hawaii.edu
Accept: */*
Connection: close
```

- a corresponding HTTP reply might look like this:

```
HTTP/1.1 200 OK
Date: Tue, 27 Nov 2018 20:59:07 GMT
Server: Apache/2.2.15 (Red Hat)
Last-Modified: Mon, 06 Aug 2018 23:29:37 GMT
ETag: "20a3d58c-225e-572cca69b1e19"
Accept-Ranges: bytes
Content-Length: 8798
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
. . .
```

HTTP/2

- Two major changes from HTTP/1.1
  - allow multiple, interleaved requests per connection
  - compress header fields
- client can specify different priority for different requests
- flow control specifies to the server what data the client can actually use
- more complex than HTTP/1.1
- RFC 7540

HTTPS

- secure version of HTTP
- two types of protection:
  - authentication provides evidence that communication is occurring with the intended party (as identified by the URL)
  - encryption hides the contents of the communication (including passwords and credit card numbers) from eavesdroppers
- HTTPS is very similar to HTTP, except: SSL or TLS is used as an end-to-end secure tunnel (VPN) to connect the browser to the server (see RFC 2818)
- Transport Layer Security, or TLS (RFC 5246) provides authentication and secrecy using public-key cryptography to agree on a shared secret key
- this shared secret key is then used to encrypt the data

HTTPS authentication

- any public-key cryptosystem depends, for security, on knowing the other party's public key
- otherwise, man-in-the-middle attacks can easily succeed
- in https, the authenticity of a server's public key (correspondence between a public key and an IP+port number combination) is guaranteed by having the public key signed by a **certificate authority** (CA)
- most web browsers are pre-configured with the public keys of multiple certificate authorities, assumed trustworthy
- e.g. a list of CAs that firefox trusts
- the communication is safe as long as the certificate authority can be trusted (not always the case)
- servers usually authenticate clients in other ways, e.g. with a password or a credit card number or by access to an email address

Active Web

- the static web has been, and continues to be, was immensely successful as a repository of static information (of varying reliability)
- however, the user interaction model of the static web is limited to users clicking links
- for many purposes this is not adequate, including logging in or interacting with any graphic display
- so the web evolved to provide support for server-side and client-side code execution that could provide different models of interactivity and customization
- this code generally increases the vulnerability to attack of the client and the server
- client-side code (usually Javascript embedded in the web page) may make further requests from the server, either using HTTP or HTTPS, or a custom protocol
- cookies allow the server to store state on the client, for purposes of later authentication or identity matching

Network Security

- Alice and Bob are trying to communicate securely, Charlie wishes to do all sorts of mischief
- for example, if Charlie is the attacker in the middle, he can read all the messages between Alice and Bob, maybe remove some or all of them, and perhaps add his own
- this might be accomplished by owning or subverting a router, or with other tricks including ARP spoofing or DNS spoofing
- in theory, encryption protects the contents, authentication guarantees that the sender is a machine with the correct key
- as long as the correct public key is known, Public-Key Encryption works well
  - but relatively slowly – often RSA is used only initially, to exchange an AES key

Network security in practice

- in practice, applications have vulnerabilities:
  - array overflow (e.g. heartbleed) or stack overflow
  - being tricked into executing code or SQL commands (shellshock)
  - being designed for a different (e.g., secure) environment
  - not being secure against random or malicious inputs (shellshock)
  - side-channel attacks
- once the attacker can execute some code on a machine, privilege escalation might lead to executing other code as the superuser (root user)
- firewalls can prevent access to all applications other than the ones explicitly selected by a knowledgeable user -- but cannot protect permitted applications