ICS 351: Today's plan

- HTTP cookies
- DNS reminder
- SNMP
HTTP cookies

- HTTP is a stateless protocol: a server has no real way to identify a client, so a request may or may not be connected with prior requests.
- Instead, a server may offer a client a cookie, a small amount of data that is only meaningful to the server.
- On subsequent related requests to the same server, the client will send back the cookie, to confirm that the requests are connected.
- Cookies have an expiration time -- most legitimate cookies expire quickly.
- Cookies can also be used to attempt to track users as they visit multiple sites, by embedding in the several sites a small image (or other content) served from the same server.
- Similar tracking can be done by tracking accesses based on the IP number of the connecting client.
DNS reminder

- DNS provides name to IP address resolution
- Domain names are grouped into zones
- a DNS server provides translation (resolution) for the names in one zone
- a DNS query contains question Resource Records
- a DNS response may contain answer RRs, name server RRs, and additional RRs
Simple Network Management Protocol

- suppose a system administrator has to manage a large number of machines
- for example, three web servers, a DHCP server, a backup server, a Network Attached Storage (NAS) server, a mail server, and a few printers
- a large KVM might be useful, but also has limitations:
  - all the servers must be in close physical proximity
  - there cannot be multiple, remote consoles
  - there is no way to get alerts from systems that need attention
- SNMP uses the network to report status information and alerts about remote systems
- SNMP messages are carried over UDP
- values can be loaded on demand (pull model), but when needed and configured appropriately, alerts are sent independently by the systems being managed (push)
SNMP needs a machine-independent way to indicate which item of information is being requested or sent.

Logically, the entire universe of information that can be accessed is built into a large tree: the Management Information Base or MIB.

The tree is extensible so individuals and organization can add their own subtrees -- private MIBs.

The tree is universal and known to all.

The path through the tree is sufficient to indicate one specific item (corresponding to a variable in a programming language).

The path through the tree can be indicated by a sequence of numbers, the number of left siblings of the path being taken.

For example, 0.2.7.5.14.1.7.0 is such an Object Identifier (OID).

OIDs are useful for enumerating arrays of objects, e.g., network interfaces, routing table entries.
SNMP basic operation

- A network management station is used by the system administrator to monitor multiple systems.
- A management agent must run on every managed device, get the required information, and provide it on request.
- The network management station may send GET requests to get one or more objects from specific agents.
- The network management station may also send SET requests to modify one or more objects on specific agents.
- Agents will send TRAP or INFORM alerts to network management stations that they have been configured to alert.
- Because it uses UDP, SNMP (like DNS) cannot assume that its operations will be successful.
HTTP reminder

- all HTTP is rendered using ASCII. This makes it easy to read, a little harder to parse
- for example, an HTTP request might look like this:

```plaintext
GET /~esb/ HTTP/1.1
Host: www2.ics.hawaii.edu
...
```

- a corresponding HTTP reply might look like this:

```plaintext
HTTP/1.1 200 OK
Date: Thu, 19 Nov 2009 05:18:56 GMT
...
```

- in each case, the first line describes the main request or result:
  - o in the request, the method can be GET, HEAD, POST, or a few others,
  - o the path is specified immediately after the request,
  - o the protocol version follows the path
  - o in the reply, the version comes first, followed by the result code, both as a number and as a string
  - the remaining lines of the header give more details, sometimes essential details (e.g. the content type and content length)
  - each header ends with an empty line