ICS 451: Today's plan

- Domain Name System:
  - DNS Protocol
- dig
- DNSSEC overview
DNS Protocol

- DNS has requests and replies (queries and answers)
- Each query is for a Resource Record (RR)
  - each answer is a RR
- Each message has a header followed by one or more RRs
- The message can be sent over UDP
  - or, with a length header, over TCP
- RFC 1035, and many more
DNS Message Structure

+------------------------+  
| Header                 |  
+------------------------+  
| Question               | the question for the name server  
+------------------------+  
| Answer                 | RRs answering the question  
+------------------------+  
| Authority              | RRs pointing toward an authority  
+------------------------+  
| Additional             | RRs holding additional information  
+------------------------+  

• from RFC 1035
<table>
<thead>
<tr>
<th>QR</th>
<th>Opcode</th>
<th>AA</th>
<th>TC</th>
<th>RD</th>
<th>RA</th>
<th>Z</th>
<th>RCODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QDCOUNT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANCOUNT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSCOUNT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARCOUNT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DNS Header Fields

- ID is used to match replies to requests
  - essentially random
- Opcode: 0 for query, 1 for inverse query
- Rcode (Response Code): 0 no error
- QD/AN/NS/AR count: number of questions/answers/name servers (authorities)/additional RRs
DNS Header Bits

- **QR**: 0 for query, 1 for response
- **AA**: this answer sent by an authoritative server
  - not authenticated, i.e. not secure
- **TC**: message was truncated
- **RD**: Recursion Desired
  - set in query, copied to response
- **RA**: Recursion Available
  - set in response if server provides recursion
Resource Record Structure

- Name (variable)
- Type (2 bytes)
- Class (2 bytes)
- TTL (4 bytes)
- RD length (2 bytes)
- RData (RDLength bytes)
RR Fields

- Name is the domain name
- TTL is the time in second this record may be cached
- RDLength is the length of the RData field
- RData is the actual data, e.g. IP address
  - questions have no TTL, RDLength, or RData
Types and Classes

- Types:
  - A (IPv4 address), AAAA (IPv6)
  - MX (mail server)
  - NS (name server)
  - CNAME (canonical name for an alias)
  - PTR (reverse lookup pointer)

- Only 1 Class: IN (1), the Internet
  - other classes are obsolete
A DNS Lookup

• Query carries a Query Name, followed by a Type and a Class
  – e.g. www.hawaii.edu, A, IN
  – typically 1 query, and no other records

• Response has:
  – answers: CNAME web00.its.hawaii.edu
    web00.its.hawaii.edu A 128.171.224.100
  – authority: hawaii.edu NS dns1.hawaii.edu
  – additional: dns1.hawaii.edu A 128.171.213.116
Encoding Names

- Domain Names are encoded as sequences of labels, each label up to 63 bytes long.
- Each label is 1 byte of length, then the name.
  - The root is a single byte of 0.
- Optimization: a label can be replaced by a 14-bit pointer preceded by two 1 bits.
  - The remaining 14 bits are an index into the message.
  - That is the beginning of another label.
Encoding Names – example

- web00.its.hawaii.edu appears as:
  - 5web003its6hawaii3edu0
- if the index of the 5 in the message is 45, and the 6 is at index 55 in the message
- dns1.hawaii.edu can be encoded as
  - 4dns1xC0 x37 (55 is x37)
- any further web00.its.hawaii.edu can be
  - xC0 x2D (45 is x2D)
- www.hawaii.edu is 3wwwxuC0 x37
Request and Reply IDs

- The requester generates a different ID for each request
- The server copies the ID field into the reply
- The requester ignores replies with different IDs

Security issue:
- if I can guess what you are going to query
- and I can guess your ID
- I can send you a spoofed reply
dig

• Domain Information Groper?
• Unix tool for DNS lookups
• Sends a query, prints the response

• many options!
$ dig @128.171.3.13 www.hawaii.edu a

;; QUESTION SECTION:
;www.hawaii.edu. IN A

;; ANSWER SECTION:
www.hawaii.edu. IN CNAME web00.its.hawaii.edu.
web00.its.hawaii.edu. IN A 128.171.224.100

;; AUTHORITY SECTION:
hawaii.edu. 1571 IN NS dns4.hawaii.edu.

;; ADDITIONAL SECTION:
dns4.hawaii.edu.1457 IN A 130.253.102.7
dns4.hawaii.edu.1457 IN AAAA 2001:468:508:2::7
DNSSEC motivation

- If I send a query and I get a response, how can I trust the response?
  - anyone who can intercept the query can send me an arbitrary response
  - e.g. an ISP that wants to redirect me
  - even without intercepting the query, an attacker may guess the query and the ID
- DNS is not secure: the response may give me an incorrect IP number
DNSSEC strategy

- client/resolver must know the **root key**
- the root key is used to sign a TLD key
- the TLD key is used to sign the lower key
- ... and so on
- client getting a record follows the chain back to the root key
- this confirms that the RR we received has been signed by someone known to the level above it
  - going back to the DNS root
DNSSEC weaknesses

• DNSSEC is not yet in widespread use
  – so an unauthenticated answer may be legit
• client/resolver must know the root key
• DNSSEC reveals zone data
  – which many admins prefer to keep secret
• DNSSEC provides authentication, but not confidentiality
• DNS is much more lightweight than DNSSEC