Advanced Unix System Administration

Lecture 13
March 14, 2007

Steven Luo
<sluo+decal@OCF.Berkeley.EDU>

The Domain Name System

- Structure of DNS
  - Hierarchical system, each part of hierarchy separated by dots
  - DNS servers are delegated authority over parts of the DNS zone by lower DNS servers
  - 13 “root” DNS servers store the delegations for the lowest level
- Name resolution
  - Start at root, inquire who is authoritative for each part of name, until we get to the top

The Domain Name System

- DNS resource records (RRs)
  - Fields: name, type (2 bytes), class (2 bytes), TTL (32 bit integer), data length (16 bits), data
  - DNS can store many different types of information; each is assigned a number
    - Types: A (1, IPv4 address), AAAA (28, IPv6 address), CNAME (5, alias), MX (15, mail exchanger), PTR (12, reverse DNS), TXT (16), SOA (6, start of authority), NS (2, name server)
  - Records also have a class – the only useful one nowadays is IN (1, Internet)

The Domain Name System

- DNS over-the-wire format
  - Queries can go over UDP or TCP
    - UDP is recommended, but queries are limited to 512 bytes
  - Fields
    - Transaction ID (2 bytes), flags (2 bytes: query/response, opcode, authoritative, truncated, recursion desired, recursion available, reserved, answer authenticated, reply code), questions, answers, authoritative answers, additional answers

Applications

- SSL/TLS
  - Used for securing other application protocols
  - Client connects to server, two negotiate a cipher
  - Server sends back a certificate with a key
  - This key is used to negotiate a session key
  - Rest of the traffic in the session is encrypted with the session key

Applications

- HTTP
  - Developed to transfer web pages, now used for general file transfer and other purposes
  - One of many text-based protocols
  - Request syntax:
    - [command] [parameters] [HTTP version]
    - Additional headers separated by \r\n and ended by two \r\n
  - Reply syntax:
    - [HTTP version] [status code]
    - Headers, two \r\n, data

Applications

- HTTP con't
  - Common requests: GET, HEAD, POST
  - Reply codes: 200 (OK), 302 (Moved), 403 (Forbidden), 404 (Not Found), 500 (Internal Server Error), 503 (Service Unavailable)
- FTP
  - Text-based control protocol, but more complicated
  - Active mode: client connects to port 21 and gives a port for server to send it data on

Applications

- FTP con't
  - Passive mode: client connects to port 21, server sends random port for client to connect to receive data on
- DHCP
  - Used for autoconfiguration of clients
    - Client broadcasts DHCPDISCOVER to network
    - DHCP servers reply with DHCPOFFER containing config information
    - Client broadcasts DHCPREQUEST with source address of server whose offer was accepted
    - Server sends DHCPACK to acknowledge the lease