Announcements

- Reading: 7.2
- Midterm #2 was returned
  - Mean 67.2, Stddev 15.6
  - Min 34, max 96
- HW#2 (due Tuesday Dec. 7)
  - 4-1, 4-28, 4-40, 7-17, 7-15

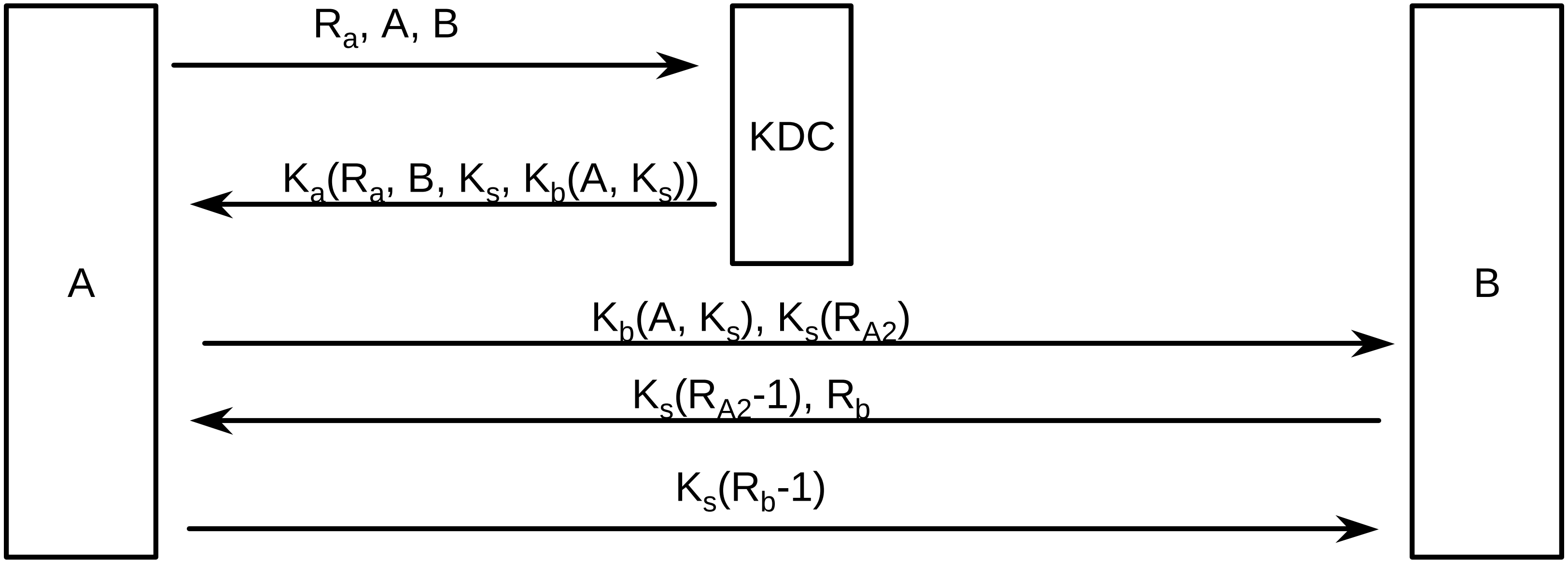
Project Related Issues

- Port numbers are your abstraction
- Timeout in recv

Key Distribution Center

- Problem with Private Key Authentication
  - Need to establish key
  - for n people need n^2 keys
  - keys must be established via **out-of-band** communication
- Solution: Key Distribution Center (KDC)
  - trusted party used to assist in authentication
  - each party establishes a private key with the center
- have KDC trans-code a message with a session key
  - A sends to KDC <A, $K_A(B, K_s)$>
  - KDC sends to B <$K_b(A, K_s)$>
  - open to replay attack
    - T logs KDC to B message **and** all traffic using K_s

Needham-Schroeder Authentication


R_a, A, B
KDC
$K_a(R_a, B, K_s, K_b(A, K_s))$
A
B
$K_b(A, K_s), K_s(R_{A2})$
$K_s(R_{A2}\text{-}1), R_b$
$K_s(R_b\text{-}1)$

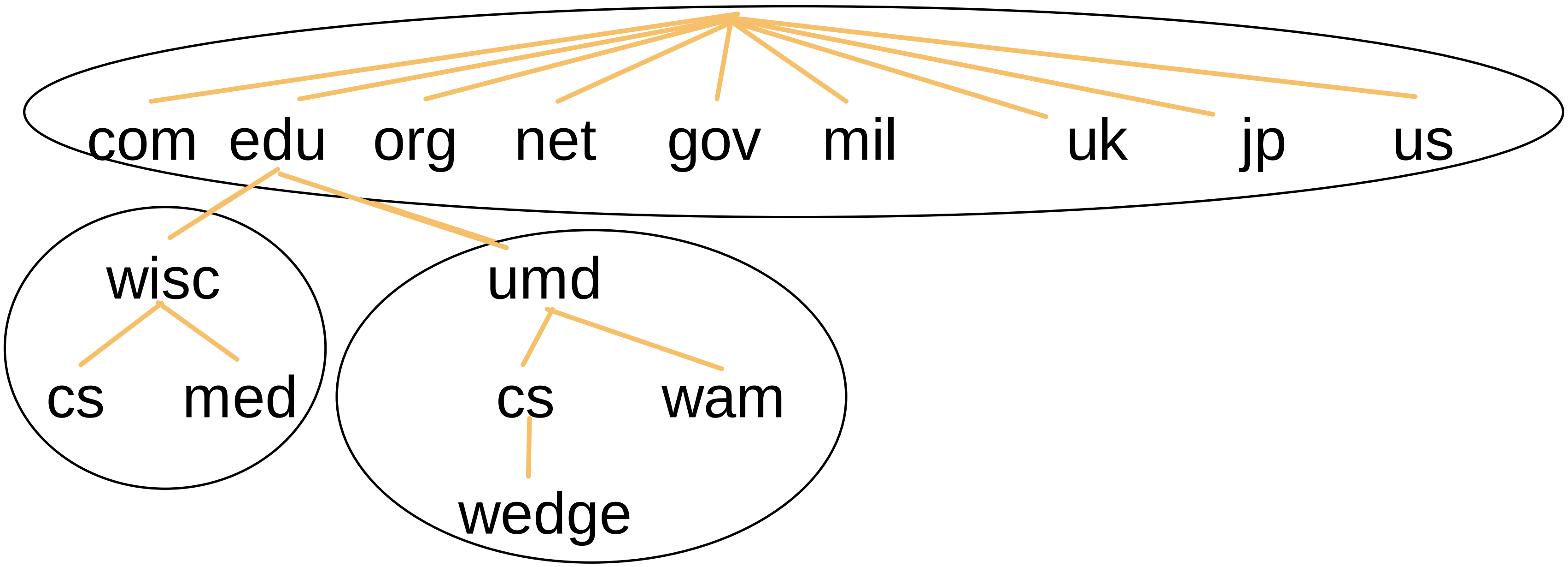
- R_A, R_{A2} and R_B random strings
  - used to prevent replay attacks
- If T ever gets K_s can establish contact with B
  - can prevent this with a slight variation of the algorithm
- Used in Kerberos Authentication System

Naming Hosts In the Internet

- Originally used a single file
  - all hosts had line line with name and IP Address
- Domain Naming System (DNS)
  - introduced in 1986
  - tree based structure to names
  - Names
    - full name must be less than 256 characters
    - each part can be up to 64 characters
    - are case insensitive
  - administration of subtrees can be deligated
    - each administrative region is called a zone

Examples of Domain Names

- Domains can be both roots of subtrees **and** hosts
  - For example: cs.umd.edu
- Top level country codes
  - required by PTTs outside of US



DNS (cont.)

- Resource Records
  - DNS is really a distributed, replicated database
- Several types of tuples in the database
  - SOA - Start of Authority information for a zone
  - A - IP Address record
  - MX - Mail exchanger
    - priority and destination (host name) to accept mail
  - NS - Name of the name server for this domain
  - CNAME - Canonical name (DNS name)
  - PTR - alias for an IP Address
  - HINFO - Host Info (CPU and OS type information)
  - TXT - other text information

Name Servers

- A collection of servers is used to run DNS
  - root servers: handle top level domains
  - have pointers to servers for deligated sub-domains
  - areas of the namespace covered by a server called a zone
- Zones
  - has one primary server (zone information stored on disk)
  - secondary name servers (get info from primary)
    - secondary server may be located outside of the zone
- Namelookup
  - start at current name server
  - if not found, resolve down tree to correct zone server
  - data may be cached in servers
    - this information may be out of data
    - **authoritative data** comes from the primary/secondary NS