Outline for March 11, 1999

1. Greetings and felicitations!
2. Network Security
   a. Same issues as for general computer security; only mechanisms different
   b. Typically don't rely on network hardware to protect things
   c. Must use cryptography
3. Network Environment
   a. Quick review of ISO/OSI model
   b. Link v. end-to-end encryption
4. Security Threats and Countermeasures
   a. snooping
   b. modification
   c. masquerading
   d. replay
   e. delay
   f. denial of service
   g. repudiation of origin
   h. denial of receipt
5. Example Design: Electronic Mail
   a. Review desired security services
   b. Basis
   c. PEM protocol
   d. Certificate-based key management vs. secret key management
   e. Comparison to PGP
6. Example Existing Protocol: NTP v 2
   a. Protocol to synchronize clocks on the Internet
   b. Primary time servers: synced to an external time system (eg, atomic clocks)
   c. Go through cloud hierarchy (and cohorts), stratum layer (distance from primary) , synchronization
   d. Association modes: client (sends message to peer, can reset time), server (replies to sent message), broadcast (send out periodic messages); higher up, symmetric active and symmetric passive: association periodically sends out broadcast messages; on arrival, symmetric passive association is created, looks at source; if source at higher stratum, reply and terminate; otherwise, reply, and source synchronizes itself to peer. Also, allow control messages.
   e. Selection of source peer, smoothing of data: retains last 8 values of (delay, clock offset), and chooses point with lowest delay, and sets dispersion. Best source chosen from the sets (one per possible source).
   f. Packet receipt, sending: on receipt, if connections compatible, checks not a duplicate by looking at transmit times, checks the last packet received by peer was the last one sent; on failure, set sanity check **but continue** . Update association to reflect data in newly-0arrived packet; check peer clock, stratum level, validate 2-way communication. If sanity check set, exit. Else estimate delay, clock offset, dispersion, and update local clock.
   g. Delay compensation: statistical in nature, calculates delay and clock offset relative to peer
   h. Access Control: trusted (can synchronize to), friendly (can synchronize), all others (ignore) -- relies on unauthenticated source information in packet
   i. Authentication: optional, uses pairwise secret keys. Authenticator excluded from integrity checking; no key distribution mechanism.
7. asquerade
   a. Send packets with bogus source; peer determined by source and destination.
   b. Effect: if fake host known to victim and can synchronize clock, may be ignored due to sample processing and selection operations.
   c. Can cause offsets, delays to alter gradually; victim's clocks will drift
   d. If unknown to victim and can become clock source, can flood with 8 messages and assuming victim gets no

  others, can now control what is discarded; or, claim low stratum number. Either way, attacker tends to become source
  e. See request, send response before legitimate response; real one discatded

8. Analysis of NTP: Modification
   a. Alter a message to cause recipient to resynchronize, or to break an association
   b. Look at allgorithm; variables reset before packet alteration acted upon
   c. Can alter packet precision, time of sending, and time of last message reception; all others cause discard before changing time (but may change association parameters)
   d. precision: can increase round-trip delay or decrease it (to make it more likely impersonated host will be new time source)
   e. Other two: used to adjust clock offset and delay, so can affect choice of source and frequency of contact
   f. DoS: version, association mode deny services
   g. stratum alters stratum of peer, making it more likely to be a clock source
   h. poll: how often peer is polled (certain limits)
   i. distance: affects delay that victim percieves from primay, and hence affects clock source selection
9. Replay
   a. To cause recipient to resynchronize, or to disable an association
   b. Alternate 2 recorded packets; either they get tossed (new source) or victim isolated
   c. Can set clock backwards
10. Denial of Service
    a. Clock runs on its own power; can cause large errors
11. Fixes
    a. External
    b. Internal: use authentication and include the key index (authenticator). Change peer variables only after authenticating packets. Disallow clocks being set backwards.