Outline for June 6, 1997

1. Greetings and Felicitations
2. Example Analysis: NTP v 2
   a. 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.
   b. Delay compensation: statistical in nature, calculates delay and clock offset relative to peer
   c. Access Control: trusted (can synchronize to), friendly (can synchronize), all others (ignore) -- relies on unauthenticated source information in packet
   d. Authentication: optional, uses pairwise secret keys. Authenticator excluded from integrity checking; no key distribution mechanism. Keys assigned on per-host (not per-path) basis.
3. Analysis of NTP: Masquerade
   a. Send packets with bogus source; peer determined by source and destination.
   b. Effect: if fake host kknown to victim and can synchrinize 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
4. 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
5. 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
6. Denial of Service
   a. Clock runs on its own power; can cause large errors
7. 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.