NTP Security Model

David L. Mills
University of Delaware
http://www.eecis.udel.edu/~mills
mailto:mills@udel.edu

Sir John Tenniel; *Alice's Adventures in Wonderland*, Lewis Carroll

NTP security model

- NTP operates in a mixed, multi-level security environment including symmetric key cryptography, public key cryptography and unsecured.
- NTP timestamps and related data are considered public values and never encrypted.
- Time synchronization is maintained on a master-slave basis where synchronization flows from trusted servers to dependent clients possibly via intermediate servers operating at successively higher stratum levels.
- A client is authentic if it can reliably verify the credentials of at least one server and that server messages have not been modified in transit.
- A client is proventic if by induction each server on at least one path to a trusted server is authentic.

Intruder attack scenarios

- An intruder can intercept and archive packets forever, as well as all the public values ever generated and transmitted over the net.
- An intruder can generate packets faster than the server, network or client can process them, especially if they require expensive cryptographic computations.
- In a wiretap attack the intruder can intercept, modify and replay a packet. However, it cannot permanently prevent onward transmission of the original packet; that is, it cannot break the wire, only tell lies and congest it. It is generally assumed that the modified packet cannot arrive at the victim before the original packet.
- In a middleman or masquerade attack the intruder is positioned between the server and client, so it can intercept, modify and replay a packet and prevent onward transmission of the original packet. It is generally assumed that the middleman does not have the server private keys or identity parameters.