Time Synchronization Protocols and Security

IETF tictoc working group

28 July 2011

Karen O'Donoghue

odonoghue@isoc.org

Agenda

- What has been done thus far?
- What are the basic aspects of the discussion around time/security?
- What are the potential types of security services?

Summary of initial survey

- Does the application require security? (if so, which one: authentication, encryption, traceability, others):
  - No – assuming a private network
    - 6 flavors of cellular backhauling
    - Circuit emulation
  - No answer
  - Possibly systems with legal requirements
    - Test and Measurement
  - Sometimes authentication
    - ToD / Internet
  - Authentication and encryption
    - Sensor networks
- Requirements matrix
  - client authentication, server authentication, transaction auth, intermediate device auth

Different aspects of the discussion

- What are the threats that need to be addressed for the synchronization protocol? (and thus what security services need to be provided?)
- What external security practices impact the security and performance of time keeping? (and what can be done to mitigate these impacts?)
- What are the security impacts of time synchronization protocol practices? (e.g. on-the-fly modification of timestamps)
- What are the dependencies between other security services and time synchronization?

Possible Security Services

- Authentication
  - Server/master authentication
  - Client/slave authentication
  - Intermediate device authentication
  - Transaction authentication
- Confidentiality
  - Data Encryption
- Traceability timestamps

Next Steps

- Additional volunteers to work on the document