TESLA Documents update

MSEC meeting, August 2004

Ran Canetti

IBM Research

TESLA Reminder

- TESLA is an scheme for source authentication of multicast communication [Perrig, Canetti, Tygar, Song].
- Main characteristics:
  - Very efficient (comparable to MACs)
  - Handles high-bandwidth, lossy communication
  - Requires loose time synchronization
  - Incurs an authentication delay.

TESLA document map

- An “intro” document:
  - Describes the basic scheme. No implementation details, but should contain enough info to write an implementation document.
  - To be an informational RFC
- Two standards-track documents:
  - TESLA-ESP
  - TESLA-SRTP

Document status

- Intro draft:
  - Version 01 passed WG last call in Dec. 03.
  - Remarks from AD in March 04.
  - Version 02 published May 04.
  - Version 03 posted on the list yesterday.
  - The changes: Only clarifications and consistency corrections.

Document status

- TESLA-ESP draft:
  - Version 00 expired, relates to the old MESP format. (Was called tesla-mesp)
  - Version 01 (actually 00) of tesla-esp coming soon.
- TESLA-SRTP draft:
  - Next talk.

Questions to the audience

Are people interested in implementing TESLA?

- In ESP?
- In SRTP?
- With which key management protocol?

- Please come talk to me.