Server assist with PRE

MLS interim 2019-1

Server assist

- Server assist is a mechanism to save bandwidth:
  - The server stores the tree (structure and public keys)
  - The server can provide part of the tree to clients (e.g. a specific copath)
  - The clients send data to be cached to the server alongside handshake messages

PRE

- In every epoch, new nodes are encrypted under a key exported from the key schedule
- Existing nodes from previous epochs can be re-encrypted by the server to the current key
- Clients just provide a unidirectional “re-encryption key”

Properties

- Encryption keys inherit FS and PCS from key schedule
- Confidentiality: The server never learns the cleartext
- Integrity: The server cannot replace nodes
- To be confirmed: PRE preserves FS and PCS

Benefit

- Considerably reduces privacy concerns around server assist
- New clients only need an init secret from a peer, everything else can be downloaded from the server