CONTROLLER - IKE

A secure case #2

What the heck is Controller-IKE
(or: What we want to change in case #2)

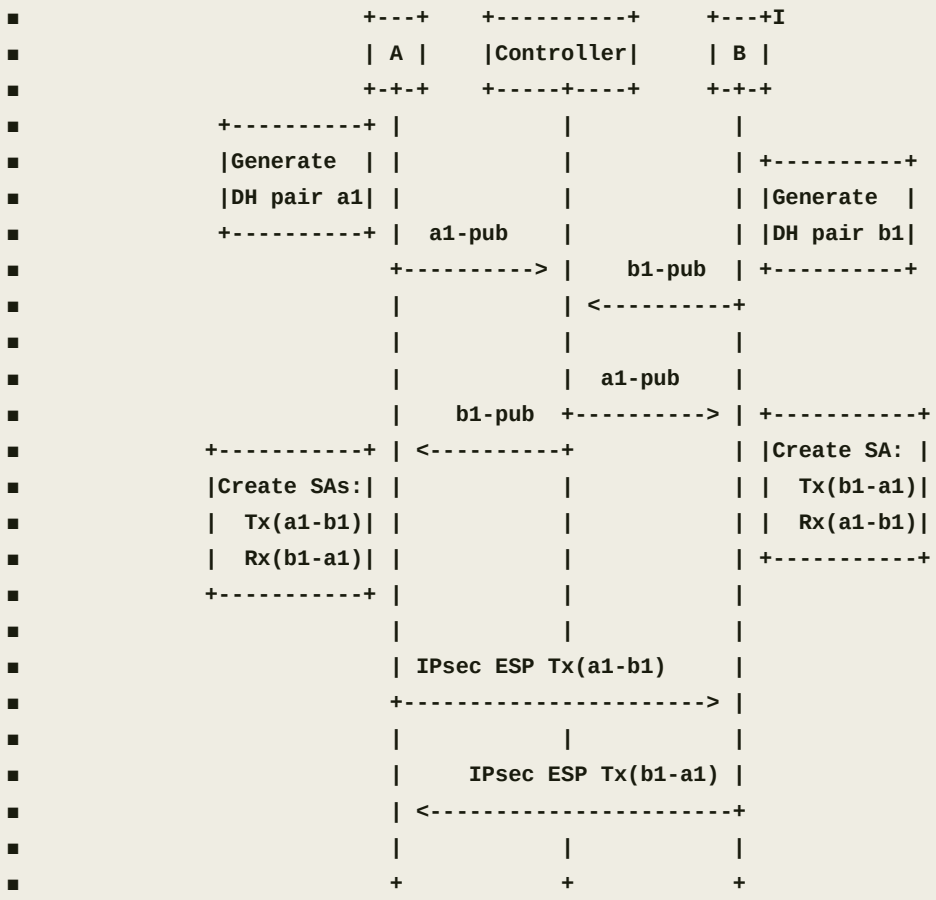
- This is a key exchange method; NOT a protocol and not for configuring NSF
  - *Suitable for securing case #2*
- DH based key exchange done through the controller
  - *All peers send their DH public value to the controller*
  - *Controller sends the list of all public values to to all peers*
  - *All peers calculate a unique pairwise secret for each other peer*
- No peer-to-peer messages
- That was easy…. What could go wrong?
  - *what happens when a peer re-keys? … when 10,000 peers all re-key?*

The “good” stuff

- Synchronization is the key
- With 4 rules, we actually make this work.
  - *Robust to loose timing*
  - *Works when peers rekey simultaneously*
- Meets security needs
  - *Controller is not a MITM for keys*

- Read the draft and find out more…

Initial key exchange



Authors

- David Carrel <carrel@cisco.com>
- Brian Weis <bew@cisco.com>