SEND IPSEC PROTOCOL

draft-send-ipsec-00.txt

Jari Arkko, Ericsson
James Kempf, DoCoMo
Bill Sommerfeld, SUN Microsystems
Brian Zill, Microsoft

http://www.piuha.net/~jarkko/publications/send/drafts

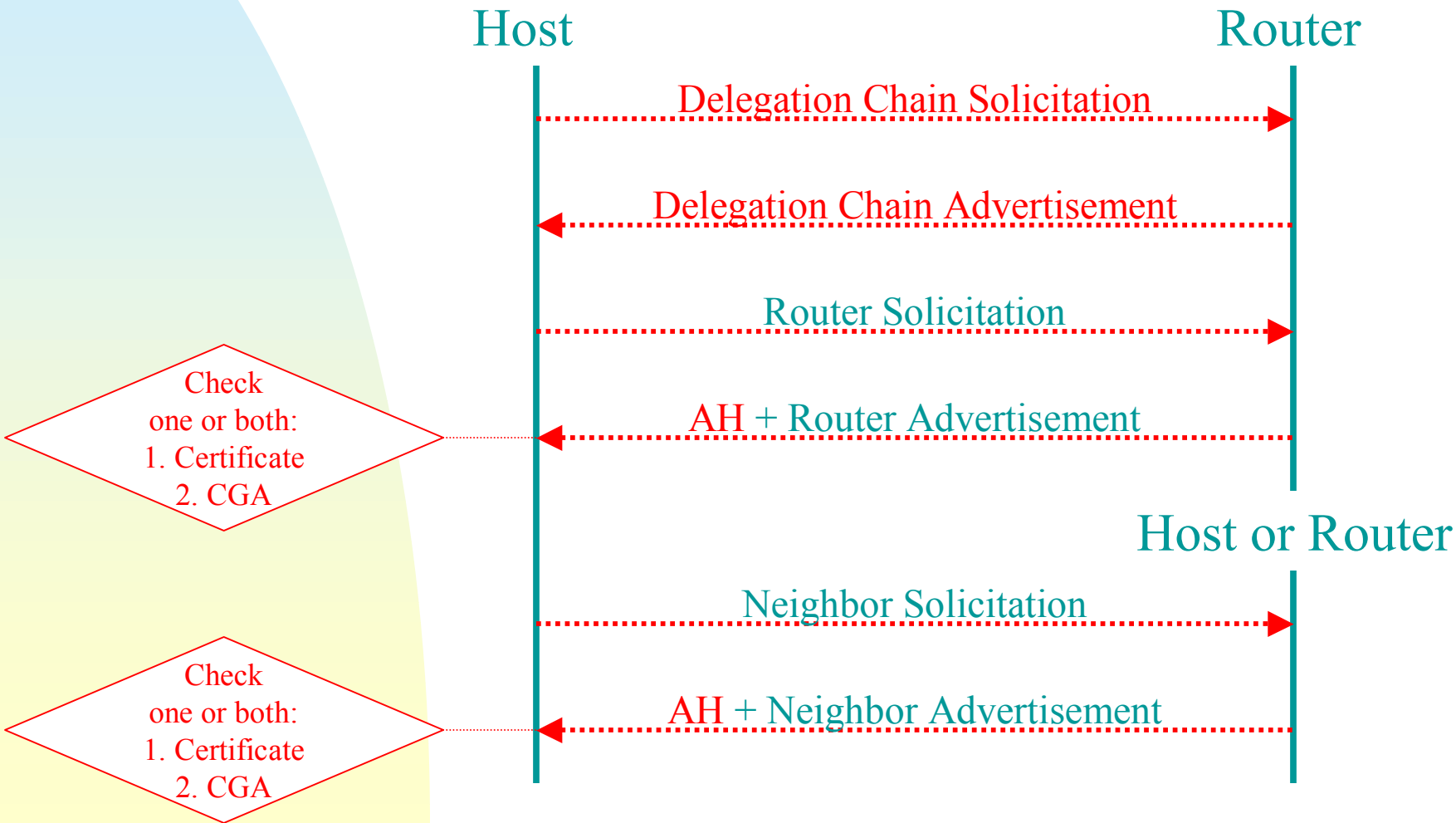
Outline

- IPR
- Protocol operation
- Open issues

IPR Issues

- The CGA mechanisms are likely under IPR claims from several companies
- This functionality is optional
- Ericsson IPR statement has been posted to the list

Protocol Operation



Open Issues

Currently open issues:

- Split the document?
- CGA derivation details?
- General case for transitions phase
- Computational efforts
- Proxy ND
- How to protect solicitations?
- ...

Split the document?

- Complaints
  - Document is too large
  - Hard to analyze without CGAs
- One possible split
  - Delegation chain discovery
  - CGA addresses
  - IPsec AH-RSA-Sig transform
  - SEND document (refers to the above components)
- Which WGs?

CGA derivation details

- Current draft approach:
  - Derives one hash value, used as the address
  - Certain number of extra hash bits required to be zero
  - The purpose of this is to defend against CGA attacks as more CPU power becomes available
- Drawback:
  - generation of CGA addresses, e.g., care-of addresses upon movements is costly
- Tuomas Aura used two steps:
  - Additional addresses from the same CGA address can be generated efficiently

General case for the transition phase

- SEND/ND interoperation allowed
  - Router acts as a router between “secure” and “insecure” sets of hosts
  - Hosts are either secure or insecure
  - Accordingly, either see only ND or AH ND packets
- Remaining problems
  - Can an ND-only router participate?
  - Can a SEND-only router participate?
  - Does a host need to be both ND and SEND?
  - Is the current transition scheme the best one? Should we use Proxy ND?

Computational efforts

- AH-RSA-Sig uses PK operations
- Precomputation is hard
  - On a solicited advertisement, typically the destination is different
  - On an unsolicited advertisement, at least the timestamp is different
- Possible solutions
  - We can choose the time at which we precompute, but can't send it more than once
  - CGA hash check is fast
- Denial-of-service concerns?

Proxy ND

- Can SEND work with proxy ND?
  - Mobile IPv6 home agent
  - Host - host ND where no common trusted CA
  - ND - SEND transition?
- Some solution ideas exist...
- But we need more thought on where this would be
  - Necessary
  - Useful
  - Possible

How to protect solicitations?

- Solicitations may have an effect
  - Update peer link-layer address
  - Inform peer that DAD is in progress
- Solutions?
  - Remove the above functions
  - Protect even solicitations with AH
    - Layering problem with IPsec:
      - Source = unspecified
      - Claimed address @ application layer
    - Add an option in IP or AH to carry the address?
  - ICMP option solution vs. IPsec AH