EAP Channel Bindings

Charles Clancy
Katrin Hoeper

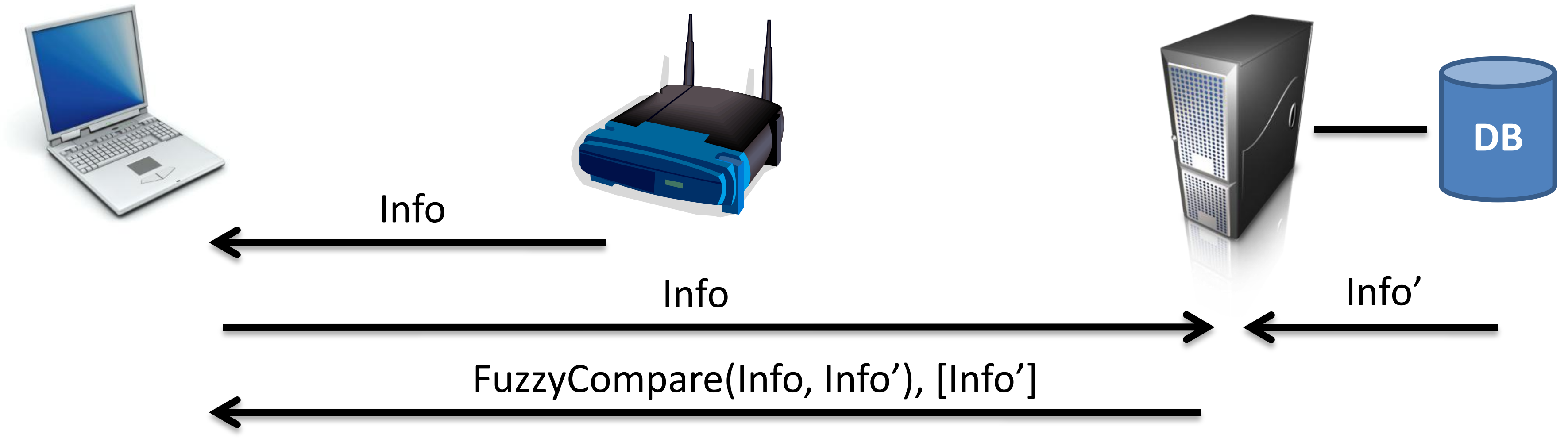
IETF 72
Dublin, Ireland
1 August 2008

Document Overview

- Two documents
  - draft-clancy-emu-aaapay-01
    - Defines mechanism for transporting Diameter AVPs for many existing EAP methods
  - draft-clancy-emu-chbind-01
    - Defines how to use this transport to achieve EAP channel bindings

Basic Approach

- Peer sends advertised network information to server during EAP authentication
- Server performs "fuzzy" comparison of the information and sends a notification to the client as to the accuracy
- Server optionally sends what the server should have advertised to the peer for peer to perform validation



CHBIND Document Status

- Version -00 submitted before IETF 71
- Version -01 presented at IETF 71
- Version -01 submitted in June
- Bernard did review of -00 in June
  - Many issues already addressed in -01
- Joe did a review of -01 in July

Resolved Issues

- Misstatement of lying NAS problem
  - Clarified through the introduction of the DB
- Lack of applicability to the roaming case
  - Clarified enterprise versus service provider case
  - DB info for roaming authenticator less specific
  - Channel binding addresses different threats
- Discussion of “fuzzy” comparisons
  - Clarified with the DB

Resolved Issues, cont

- Exploration of operations implications
  - Use of DB means more information needs to be provisioned with authenticators
  - No changes to AAA protocols required
  - No changes to authenticators required
  - Need to update existing EAP methods
- Motivation
  - Additional text in -01 provides further motivation
  - Threats in service provider versus enterprise cases

Open Issues

- Discussion of lower-layer channel bindings
  - Work item, will be included in section 6
- No problem statement or requirements section
  - Problem statement added, but could add additional requirements
- Clear distinction between 3748 vs 5056 channel bindings definitions
  - Single sentence indicating difference; description could be lengthened if necessary

Open Issues from Joe’s Review

- Definition of channel bindings and relation to RFC 5056 still needs work
  - Will address in next revision
- Discuss general solution using [AAAPAY] as a transport example
  - Will address in next revision
- Improve definition and motivation for “fuzzy” comparisons
  - Debugging, accounting, and cases where there may be multiple right answers

Open Issues from Joe’s Review

- Where does validation occur?
  - EAP server may want to export info to AAA layer and allow AAA server to perform validation
    - DB connected to AAA server, not EAP server
  - Can add clarificatory text
- Need requirements for EAP methods, AAA protocols, and EAP lower layers
  - Put examples about specific lower layers in appendix
  - Can address in the next revision

Conclusion

- Draft definitely needs more work
- Next version will address issues from reviews received so far
- Request additional WG review on upcoming revision
- Request adoption as WG item to satisfy channel bindings charter requirement