CHANNEL BINDINGS:
THE TRAIN DEPARTS THE STATION
SAM HARTMAN
PAINLESS SECURITY, LLC
IETF 78
JULY 28, 2010
Since IETF 77

- List discussion:
  - Use cases
  - Proxies
  - Tunnel interactions
- New draft published; new editor
Changes to Draft

- Update examples in introduction
- Discuss cases where one EAP server may be involved in enterprise and roaming
- Describe secure association protocol approach; not for this document
- Talk about levels of trust
Send Comments

- Send comments on problem statement and introduction
- Confirm we have consensus by IETF 79
Protocol

- General approach similar to `clancy-emu-aaapay`?
- Do we need more than 1 RT?
- Do we need non-AAA channel binding data?
- Propose using specific channel-binding AVP even for things like TTLS.
Advantage: using 1.5 RTs allows the server to indicate what information it needs.

Disadvantage: Adds complexity.

Do methods that have MTU/fragmentation constraints support 1.5 RTTs?