Channel Bindings

Katrin Hoeper

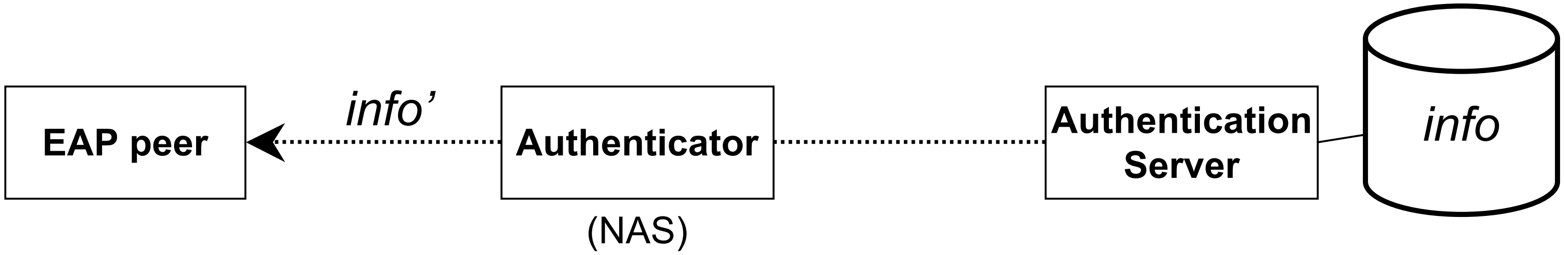
khoeper@nist.gov

Outline

- Why do we need channel bindings?
- What are channel bindings anyway?
- How can a channel binding draft help?

Potential Attacks

- Rogue authenticators in pass-through mode may launch “lying NAS attack”
  - Advertize false information to peer
    - e.g. false SSID, services, roaming fees, etc.
    - users might sometimes not care who provides service but always care about correct billing

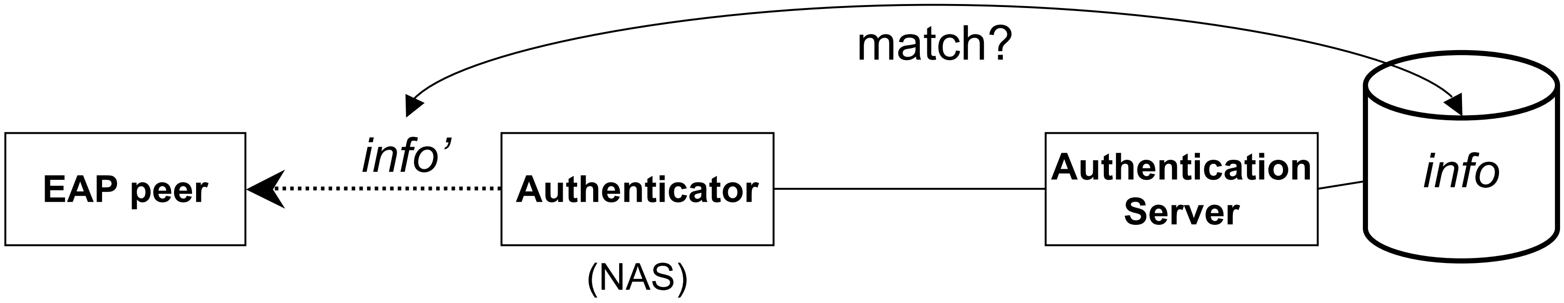


Why is EAP prone to such attacks?

- Limitations
  1. Peer unable to validate *info’*
     - No pre-shared keys or PKI
     - Not capable to verify authorization
  2. Server unaware of what was advertized to peer
     - No consistency check of advertised *info’* and stored *info*
- Potential solutions must address one limitation
  - No. 1 requires changing infrastructure
  - No. 2 can be addressed by adding channel binding

Channel Bindings

- Idea: bind information advertized by authenticator to the channel
- Definition: *EAP channel bindings (c.b.)*
  - – Check consistency of information advertized to peer and known by the server by an authenticator acting as pass-through device during an EAP session



Use Cases

- Enterprise Networks
  - Single administrative domain
  - AS can know & validate all information for all NASes
    - including the identifiers that are advertized to peers
- Service Provider Networks
  - Multiple administrative domains, bound with roaming relationships, contracts
  - AS can’t know information for all NASes in all domains
  - AS can validate some advertised information based on contractual agreements

Channel bindings should be added to EAP methods because…

1. Peers can’t directly authenticate NASes and check their authorization; EAP c.b. provides simplest solution.
   - Reuse trust relationship between peer ↔ AS
   - Validate against pre-provisioned *info* on AS
2. EAP c.b. provides a general higher layer-independent solution to the lying NAS problem
   - Prevents attacks on EAP as well as on higher layer protocols that depend on EAP and involve the NAS
3. It is efficient & secure without modifying EAP framework

How does a c.b. draft help?

- Instead of individual solutions and analyses for each EAP method, a c.b. draft provides
  - A definition of c.b. and the addressed problems
  - One general c.b. technique incl. security analysis applicable to existing and future EAP methods
  - Specifications of type and format of c.b. data
- A c.b. draft enhances the security of existing methods and accelerates processing current drafts

What should be specified?

- Define channel binding in EAP context
  - Goals, attacks, trust model …
- Define channel binding technique
  - What information should be bound to channel
    - identifiers, service info, domains, fee structure, etc
  - How is this information exchanged
    - data format, encapsulation in EAP flow, etc
  - Who performs consistency check and how
    - server and/or peer, comparison method, notification, etc
  - How are messages protected
    - end-to-end integrity protection, specify keys, MACs, etc
- Optionally
  - means to extend and add new bindings in the future

Existing Work

- General
  - RFC 5056 “On the Use of Channel Bindings to Secure Channels”, N. Williams
- EAP-related personal drafts
  - <draft-clancy-emu-aaapay-00>
  - <draft-clancy-emu-chbind-00>
- Previous documents
  - <draft-hiller-eap-tlv-00>, expired
  - <draft-salowey-eap-protectedtlv-02>, expired
  - <draft-ohba-eap-channel-binding-02>, expired

Questions?

Comments?

Volunteers?