EAP Channel Bindings

Charles Clancy
Katrin Hoeper

IETF 75
Stockholm, Sweden
July 27-31, 2009

Document Status

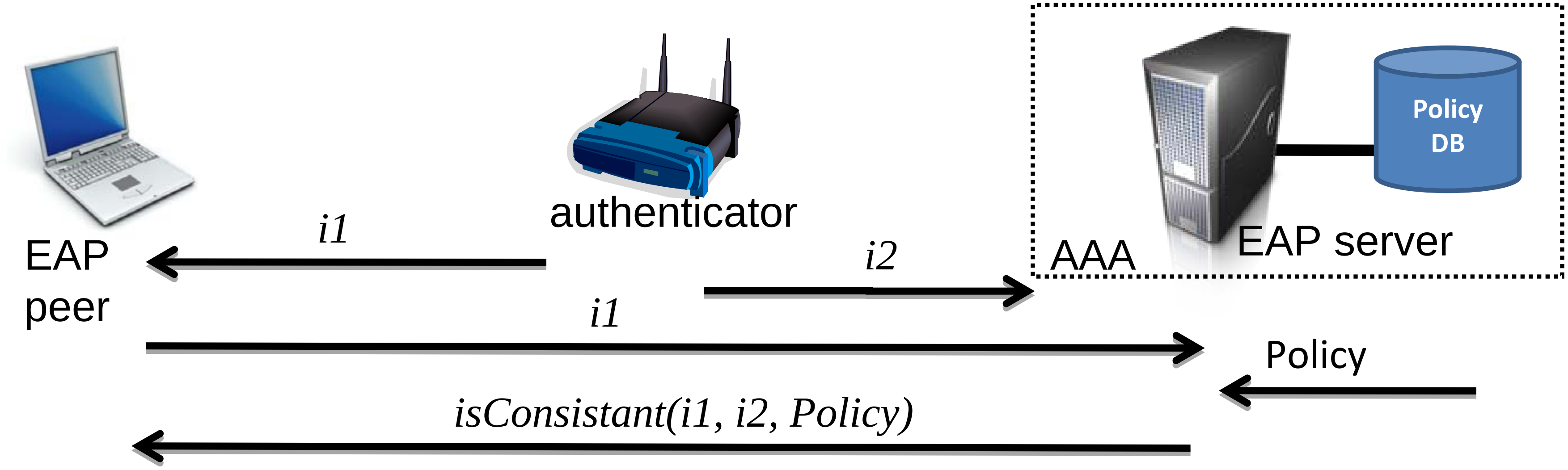
- <draft-ietf-emu-chbind-01> submitted in March `09
  - presented at IETF 74
  - consensus that draft is ready for WGLC
  - Klaas submitted detailed review in April `09
- <draft-ietf-emu-chbind-02> submitted in May `09
  - tried to address Klaas comments
  - more discussions on the list
- <draft-ietf-emu-chbind-03> submitted in July `09
  - address remaining open issues

Discussion 1: scope of draft

- What aspect of channel bindings should and can be solved by the proposed protocol?
  - mitigate lying NAS problem
  - mitigate lying provider problem
  - check whether peer is authorized to access requested services in manner described by NAS

Discussion 1: scope of draft (cont'd)

- Solution: specify channel binding protocol
  - protocol includes verification of channel binding info which requires access to local policy DB
  - general issues for setting up DB discussed; how rules are derived from policies is out of scope



Discussion 2: what is verified?

- Channel binding information
  - i1: any info part of the NAS beacon/EAP Identity request
  - i2: any AAA attribute exchanged between authenticator and AAA server as part of on-going authentication session
  - rules derived from network policies & stored in local DB
- Channel binding verifications, check whether
  1. the authenticator is lying to the peer (i1 false?)
  2. the authenticator (or AAA intermediaries) is lying to the AAA server (i2 false?)
  3. the authenticator (or AAA intermediaries) is violating any policy-based rules (i1 & i2 consistent and satisfy DB rules?)

Discussion 3: why do we need DB or why can’t AAA do the job?

- Comparing i1 and i2 is good, but this is <u>not</u> sufficient, because
  - i1 and i2 may be both false
  - i2 likely not sufficient to detect lying providers due to “message laundering” by AAA intermediaries
  - i1 is not restricted to AAA attributes
    - not all information of interest can be encoded in AAA attributes and defining numerous new AAA attributes seems like a bad idea!
- Using a policy DB needed to check
  - against trustworthy set of information
  - consistency of i1 and i2 rather than equality, e.g. do MAC and IP address belong to the same device
  - whether provided information violates network policies
  - whether peer is authorized to access requested services in the manner described by the NAS

Discussion 4: how do we verify?

- Verification steps:
  - check whether i1 complies with rules in DB
  - check whether i2 complies with rules in DB
  - with aid of DB, check consistency of i1 and i2

- Assumptions:
  - local DB containing rules and network information in place
  - EAP server has access to i2

Conclusion

- How many people have read -03 version?

- Ready for WG last call?