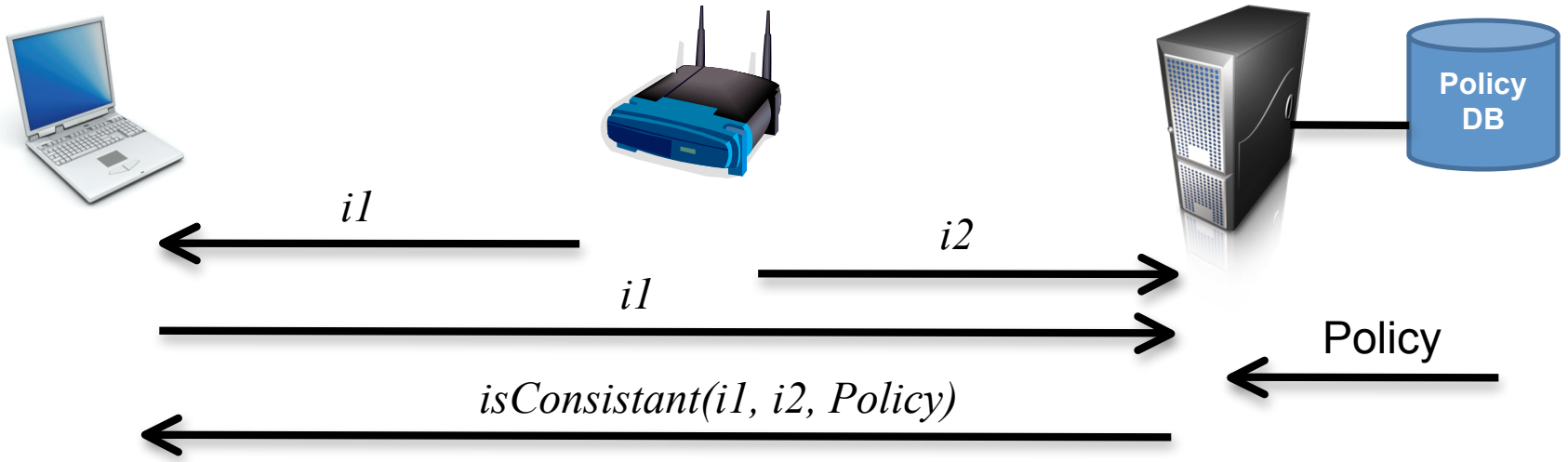
EAP Channel Bindings

Charles Clancy
Katrin Hoeper

IETF 73
Minneapolis, USA
17 November 2008

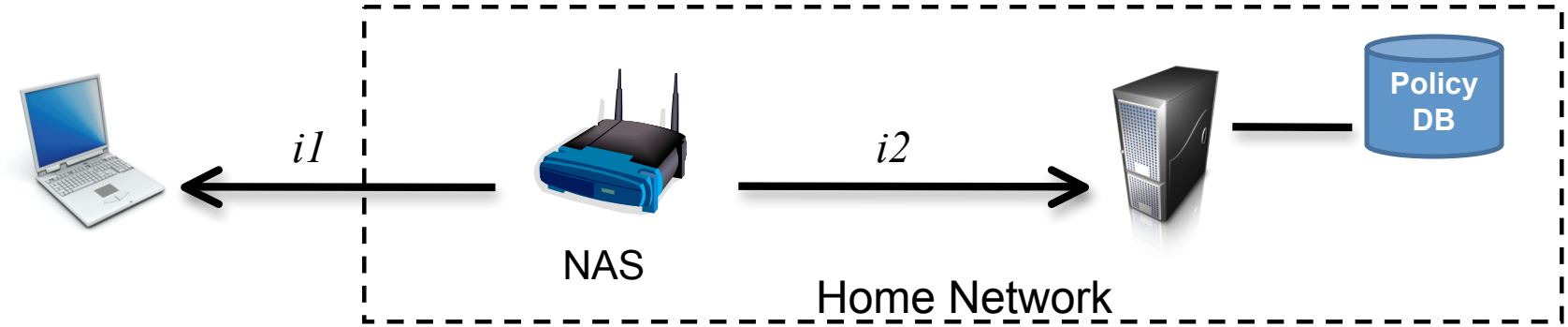
Basic Approach

- During an EAP execution
  - peer sends advertised network information *i1* to server
  - server checks whether *i1* from the peer, *i2* from the last AAA hop and the respective policy are consistent
  - server sends notification to the peer indicating the result

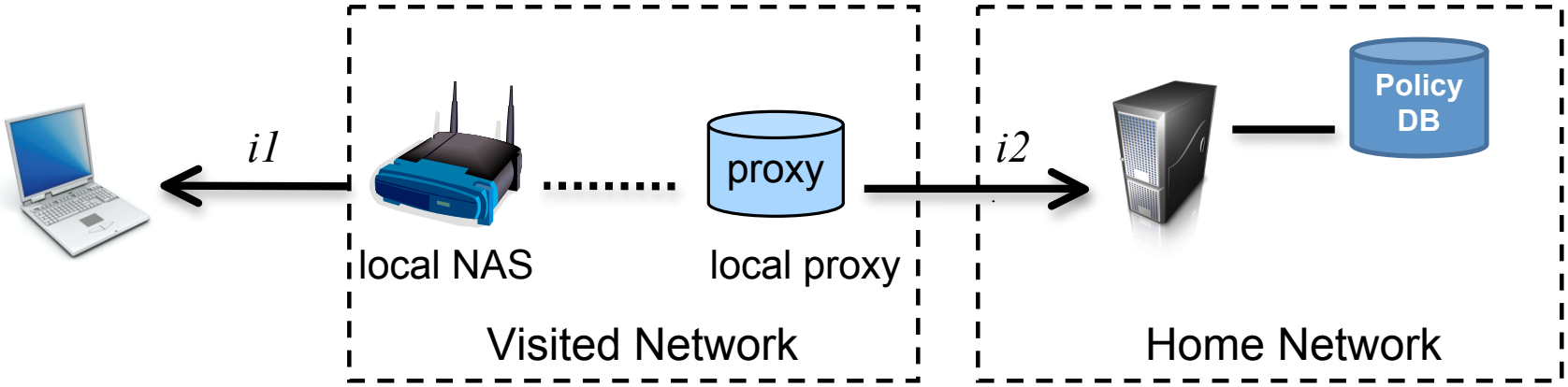


Network Models

- Enterprise network



- Service provider network



Document Status

- Version -00 submitted before IETF 71
- Version -01 presented at IETF 71
  - submitted in June
- Version -02 submitted after IETF 72
  - addressed comments from EMU meeting
  - addressed Joe's comments
- Version -03 submitted in October
- Version -04 submitted in November
  - addressed Bernard's comments on -02 &03

Resolved Issues

- NAS information not used for authorizations
  - sometimes important which NAS (authenticator) the peer is connected to, e.g. if EAP server controls access to several networks
  - including NAS information into channel binding verification, thus, improving EAP's ability to provide authorization

Resolved Issues-(ii)

- Information *i1* not sufficiently described
  - described differences for enterprise and service provider models
  - provided examples of attributes
    - in general: NAS-Port Type, Cost information
    - IEEE 802.11: Called-Station-Id
    - IEEE 802.11r: Mobility-Domain-Id
    - IEEE 802.11s: Mesh-Key-Distributor-Domain-Id

Resolved Issues–(iii)

- Last hop information not utilized in verification
  - added information *i2* from last AAA hop to channel binding verification
  - explored impact of local proxies in service provider scenario and discussed usefulness and verifiability of "laundered" information
  - defined which AAA attributes can and should be validated
    - User-Name, NAS-IP-Address, Called-Station-Id, Calling-Station-Id, NAS-Identifier, NAS-Port-Type

Resolved Issues–(iv)

- Misstatement of “lying NAS” problem in roaming case
  - in service provider networks the lying entity is not necessarily the local NAS
    - could be lying local authentication server or local proxies
  - introduced “lying provider problem”
  - EAP channel bindings detect if one (or more) of the local entities is lying

Resolved Issues–(v)

- Incomplete comparison of main EAP channel binding approaches
  - removed “fuzzy comparisons”
  - described policy-based comparisons
  - added more advantages to exchanging plaintext information
    - “logging mode”
    - consistent information canonicalization and formatting unnecessary

Resolved Issues–(vi)

- Lack of transport protocol description
  - defined transport protocol requirements and explored options
    - channel binding protocol must be transported after keying material has been derived between peer and server
    - transport protocol for carrying channel binding information MUST support end-to-end message integrity protection
    - transport protocol SHOULD provide confidentiality
    - [I-D.clancy-emu-aaapay] is one possible option

Resolved–(vii)

- Missing privacy discussion
  - if channel binding messages contain identifiers of peer and/or network entities, the privacy property of the executed EAP method may be violated
  - discussed privacy violations as part of the “Security Considerations”

Resolved–(viii)

- Lack of operations and management considerations
  - analyzed system impact (Section 10.1)
  - explored required modifications to EAP peers & EAP servers
  - provided examples how server database can be set up more cost efficiently
    - auto-population phase (secure environment)
    - self-learn approach
    - incremental implementation

Resolved–(ix)

- Lack of examples on how EAP channel bindings prevent attacks
  - added Appendix describing attacks
    - enterprise subnetwork masquerading
    - forced roaming
    - downgrading attacks
    - bogus beacons in IEEE 802.11r
    - forcing false authorization in IEEE 802.11i

Open Issues

- Cost-benefit analysis
  - only provide impact discussion
  - no hard numbers on how much a deployment would cost and how much money would be saved by supporting channel bindings

Open Issues–(ii)

- Lower layer binding
  - need a way to transport the RSN-IE
  - define attributes for IEEE 802.16, wired 802.1x, PPP, IKEv2, 3GPP2, PANA

Conclusion

- Request support with open issues
- Request WG review of -04 version
- Request adoption as WG item to satisfy channel bindings charter requirement