HIP-EAP

Samu Varjonen
Helsinki Institute for Information Technology

IETF 75 - Stockholm, Sweden, 28.07.2009

Motivation

Humans are using the Internet
… are authenticated
… are access controlled

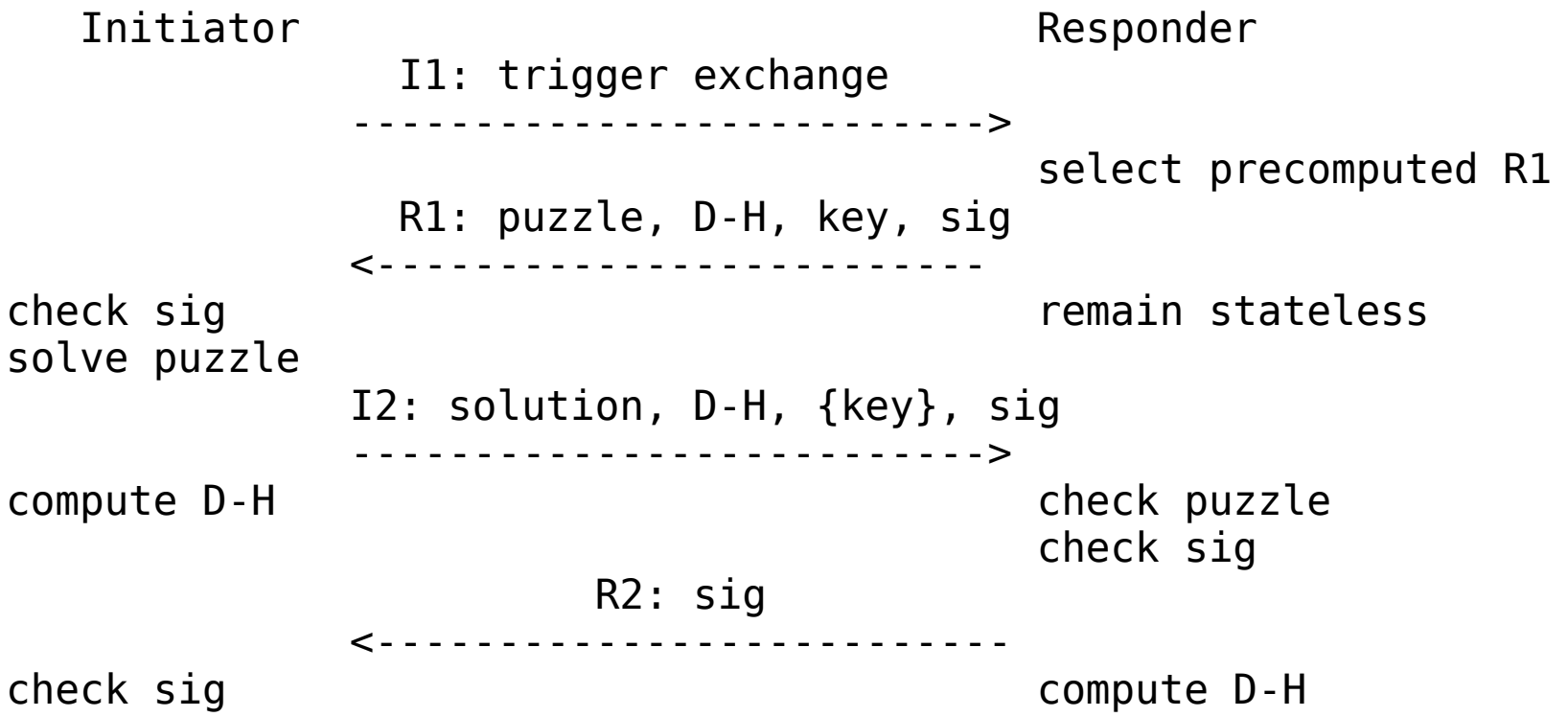
Humans

Authenticated by
… by passwords
… by OTPs
… by Token cards

NOTE!

We are only piggybacking existing authentication protocol

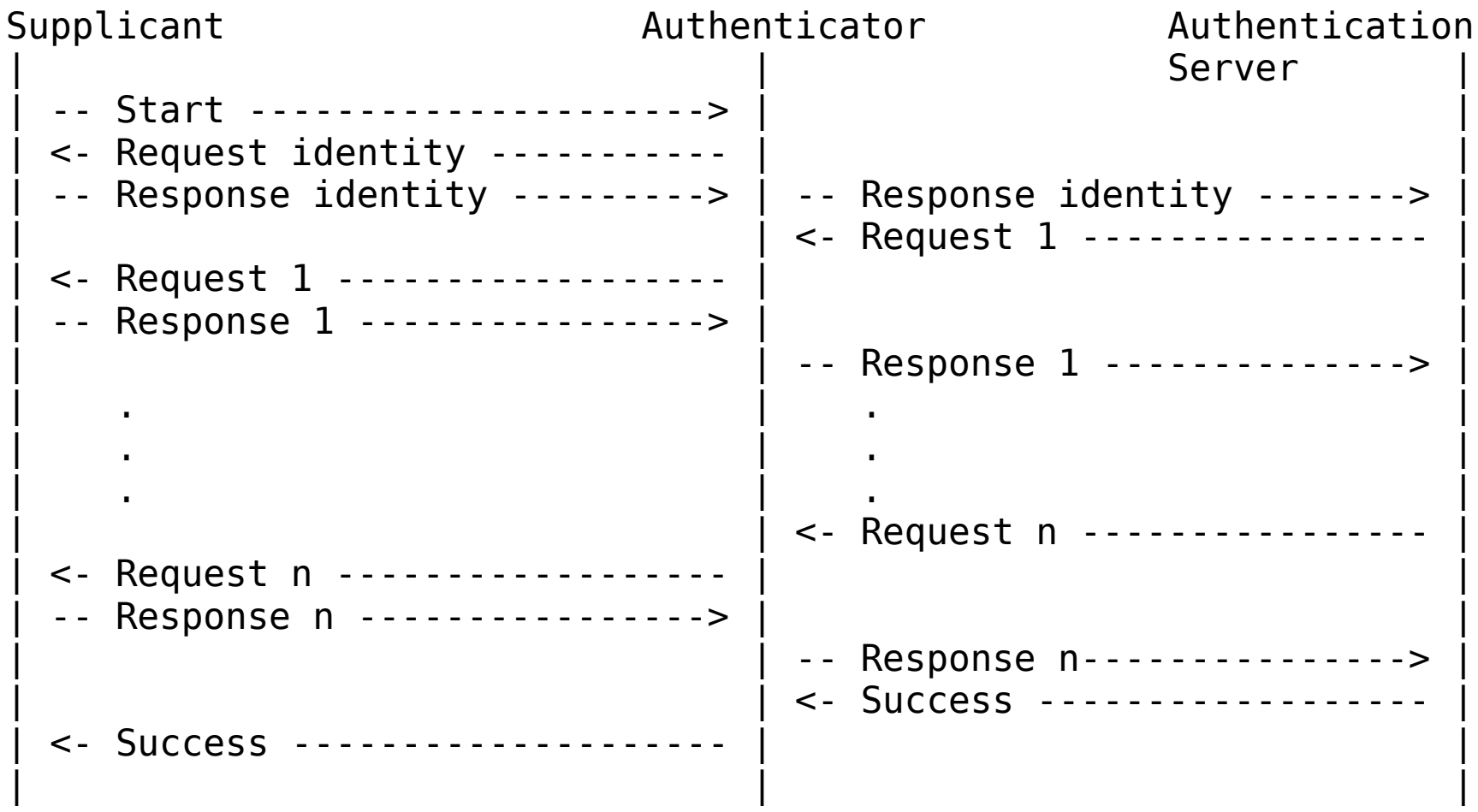
HIP BEX


Initiator
Responder
I1: trigger exchange
select precomputed R1
R1: puzzle, D-H, key, sig
check sig
remain stateless
solve puzzle
I2: solution, D-H, {key}, sig
compute D-H
check puzzle
check sig
R2: sig
check sig
compute D-H

EAP

- Lock-step protocol
- No fragmentation support
- Initiated by the authenticator
- Both peers may be authenticators simultaneously

EAP negotiation



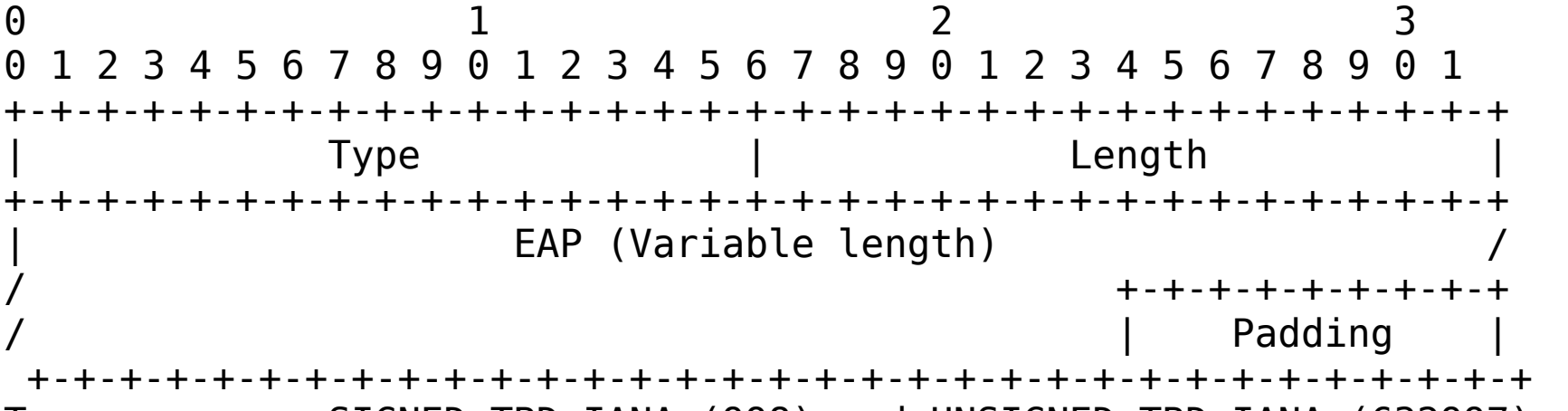
Road to here...

- Extending BEX:

  - Reuse control packets → dirty / state machine
  - Hiccups in front → logical / state machine
  - Hiccups in the middle → dirty / state machine
  - Hiccups after bex → just wrong

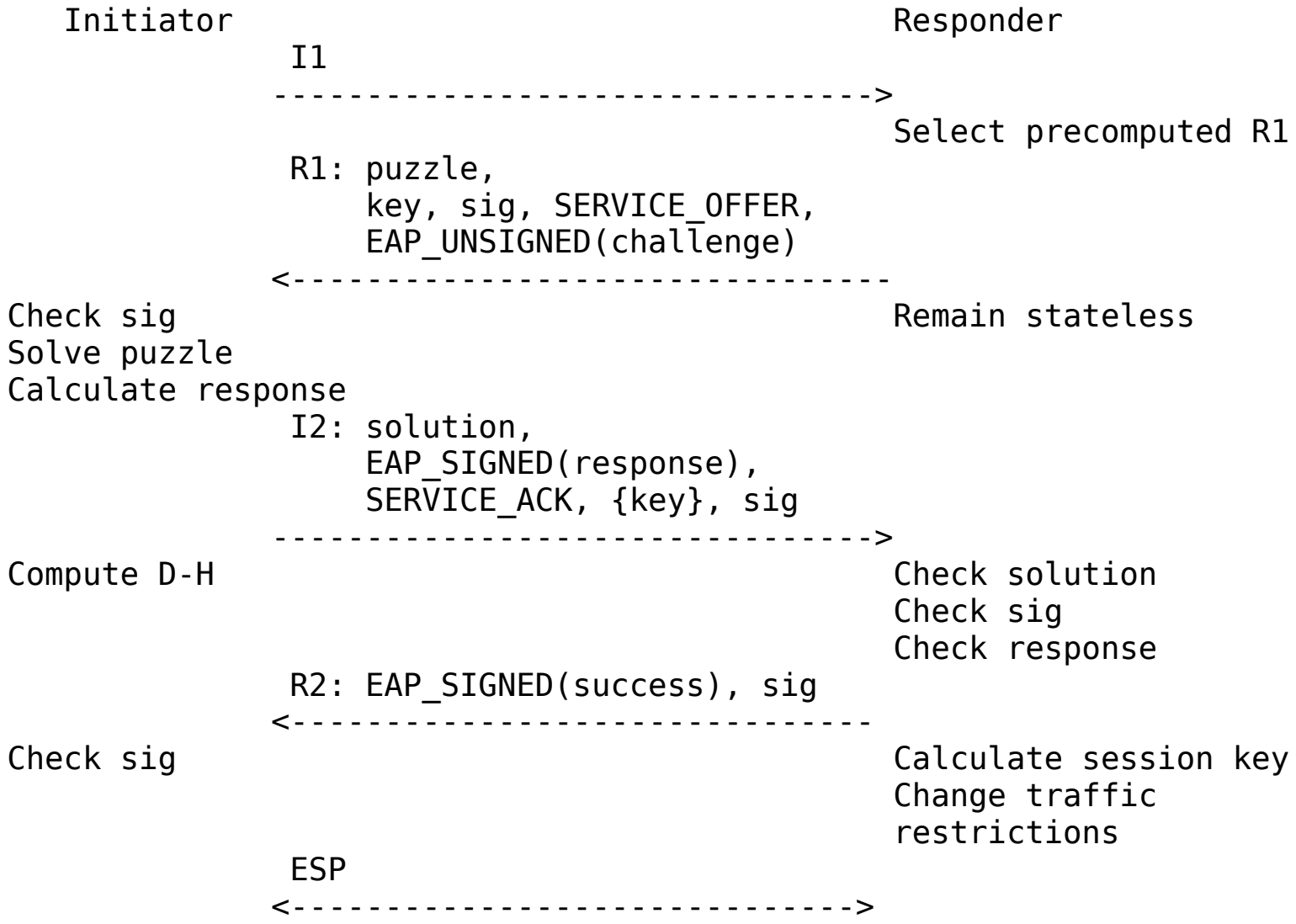
- Access control the SA and use UPDATEs

EAP_SIGNED / EAP_UNSIGNED parameters

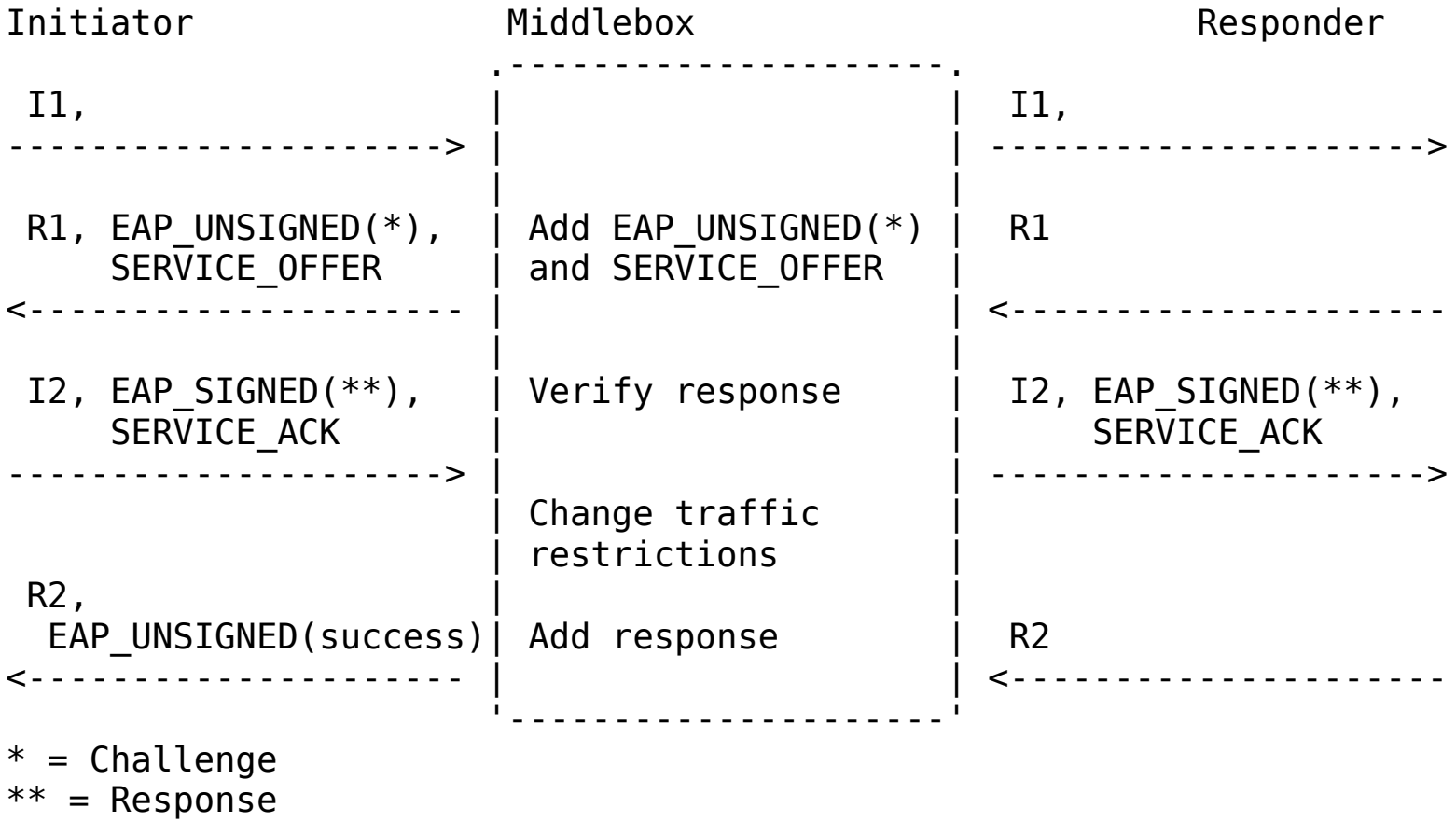


Type	SIGNED TBD-IANA (998) and UNSIGNED TBD-IANA (632997)
Length	Length in octets, excluding Type, Length, and Padding
EAP	EAP message, variable length.
Padding	Any Padding, if necessary, to make the parameter a multiple of 8 bytes as defined in [RFC5201] in section 5.2.1.

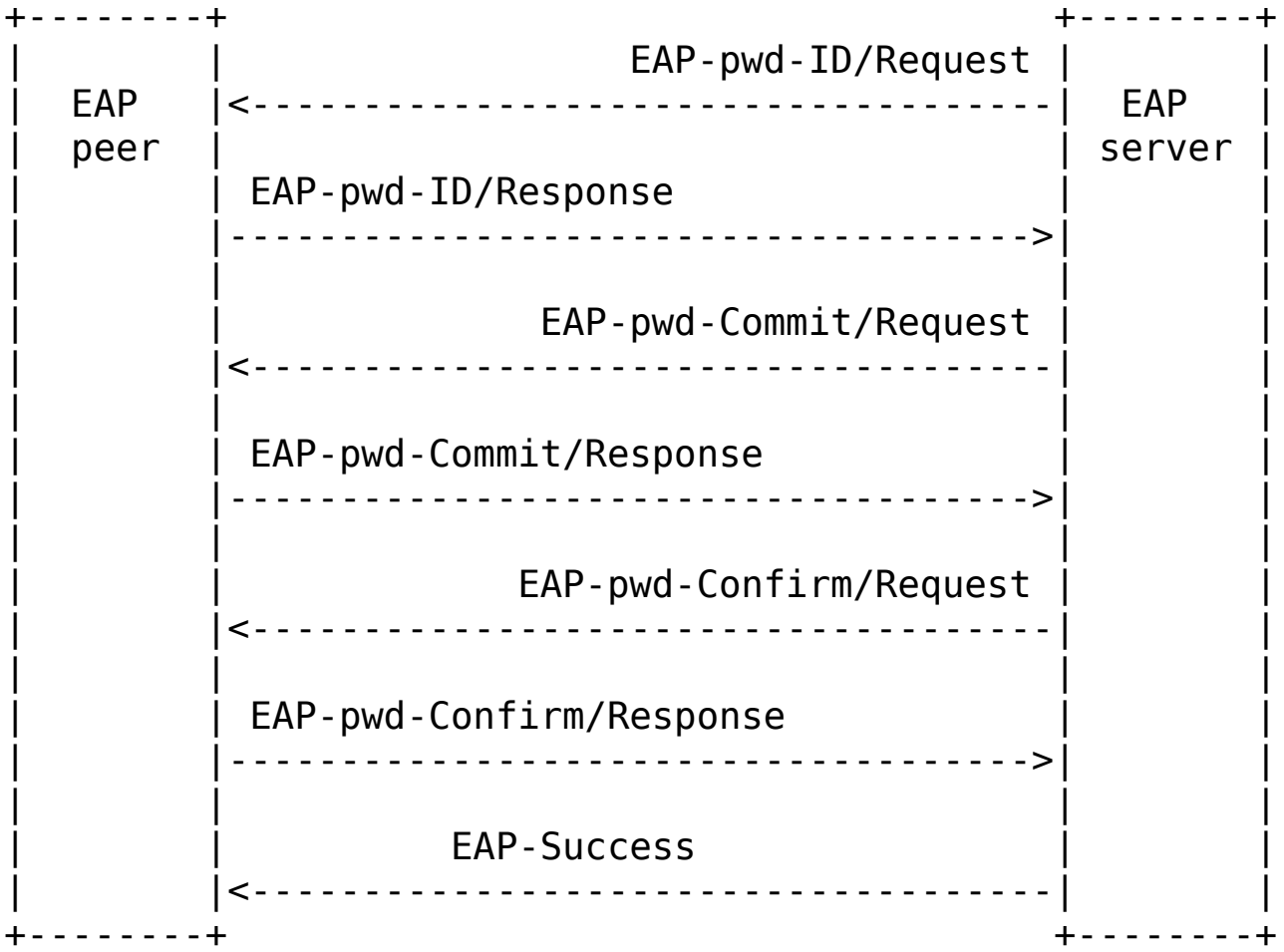
EAP Challenge/Response



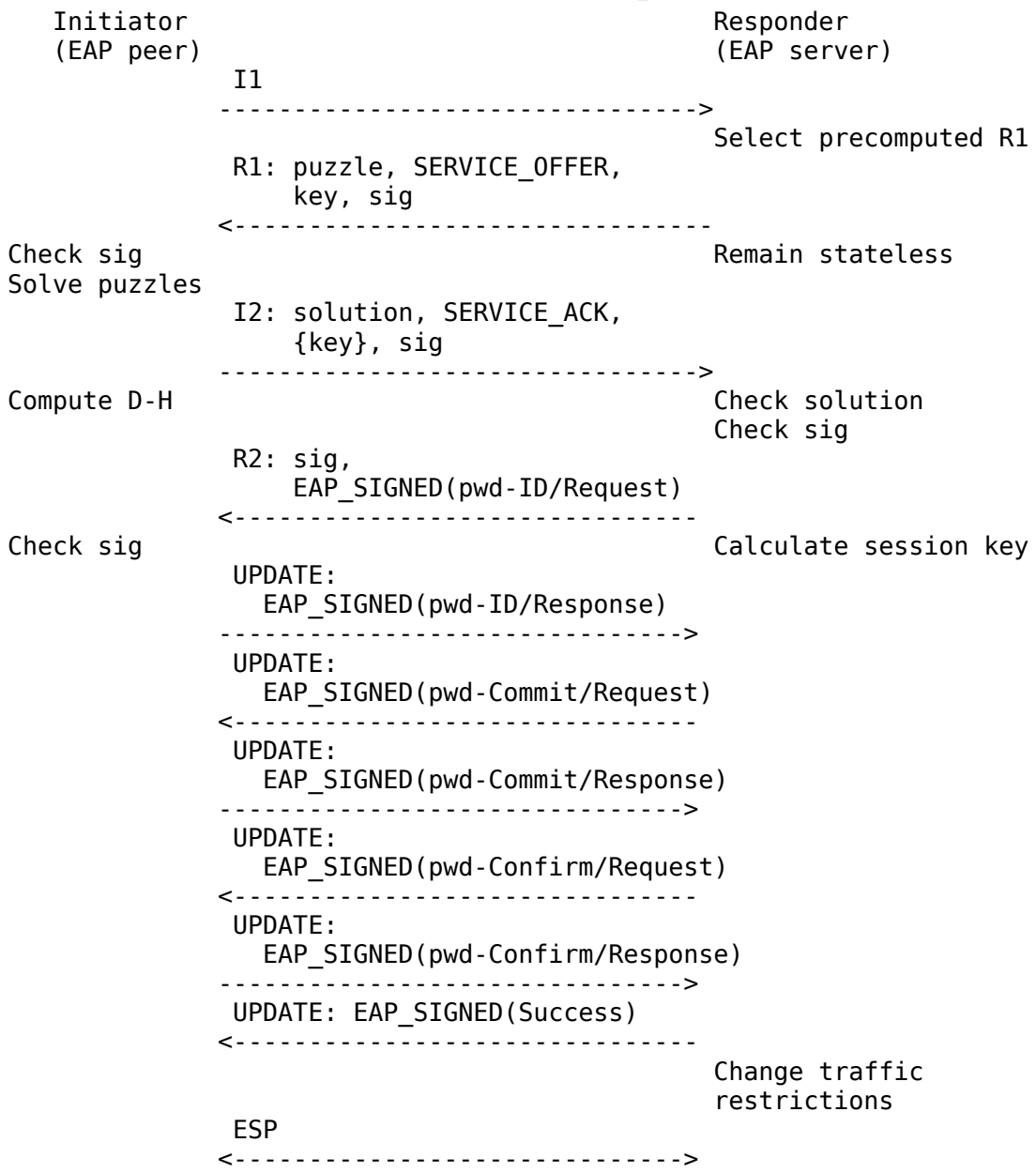
Middlebox in challenge/response



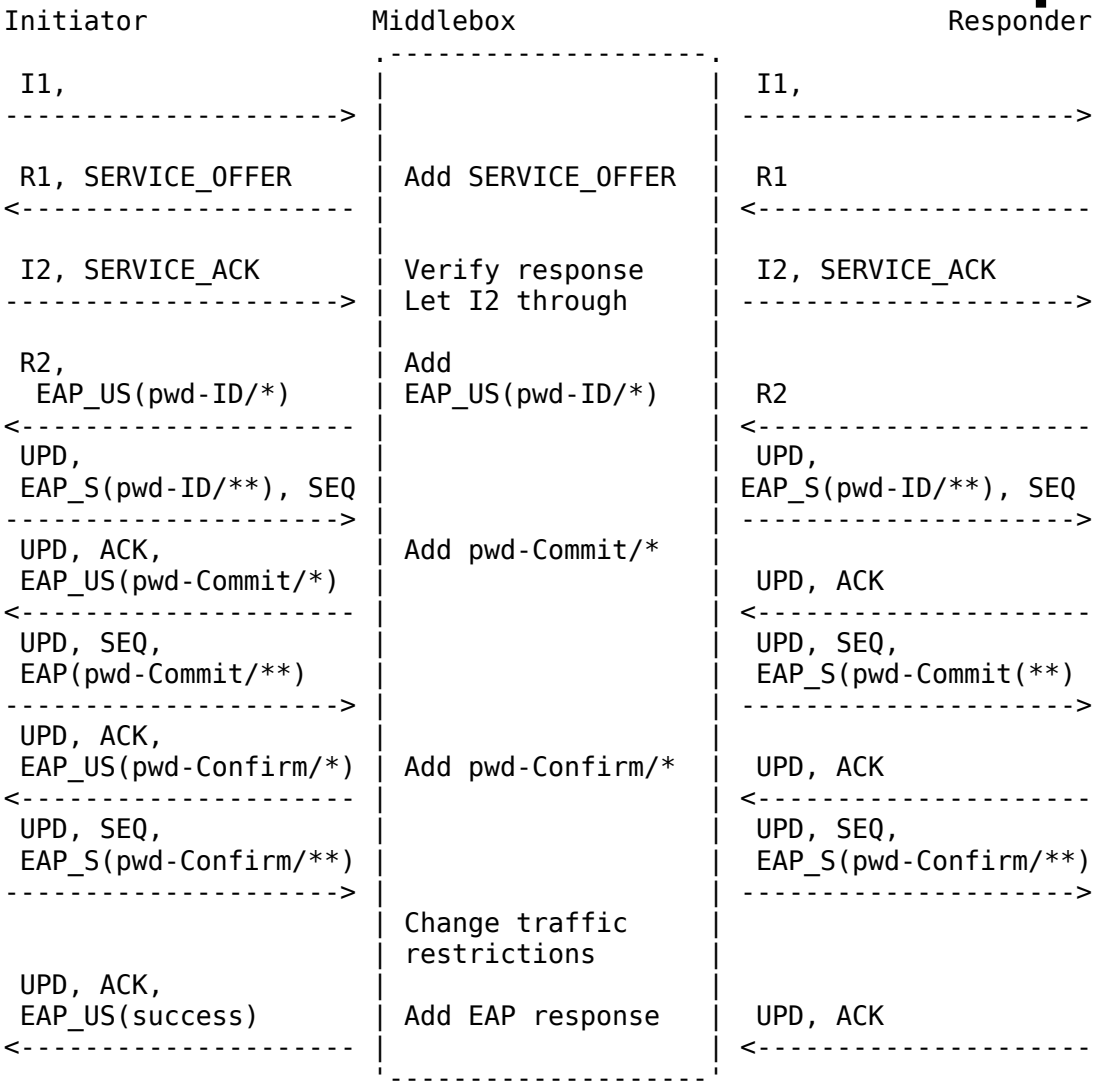
EAP-pwd Handshake



HIP-EAP-pwd


Initiator
(EAP peer)
Responder
(EAP server)
I1
Select precomputed R1
R1: puzzle, SERVICE_OFFER,
key, sig
Check sig
Remain stateless
Solve puzzles
I2: solution, SERVICE_ACK,
{key}, sig
Compute D-H
Check solution
Check sig
R2: sig,
EAP_SIGNED(pwd-ID/Request)
Check sig
Calculate session key
UPDATE:
EAP_SIGNED(pwd-ID/Response)
UPDATE:
EAP_SIGNED(pwd-Commit/Request)
UPDATE:
EAP_SIGNED(pwd-Commit/Response)
UPDATE:
EAP_SIGNED(pwd-Confirm/Request)
UPDATE:
EAP_SIGNED(pwd-Confirm/Response)
UPDATE: EAP_SIGNED(Success)
Change traffic
restrictions
ESP

Middlebox in HIP-EAP-pwd



Thanks

Questions ?