Analysis of fast-reauthentication alternatives in EAP-based wireless networks

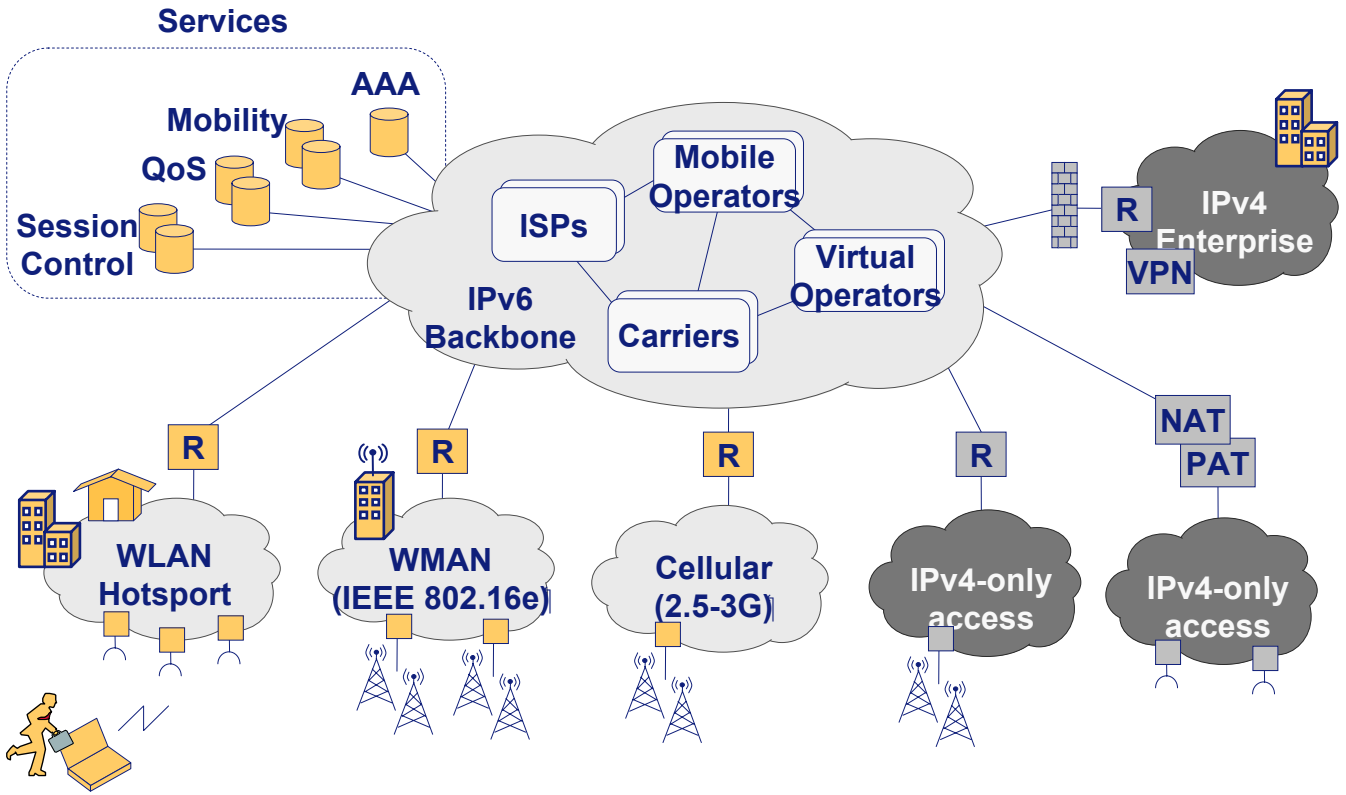
Rafael Marín López
Pedro García Segura
Antonio F. Gómez Skarmeta

University of Murcia

Introduction (1)

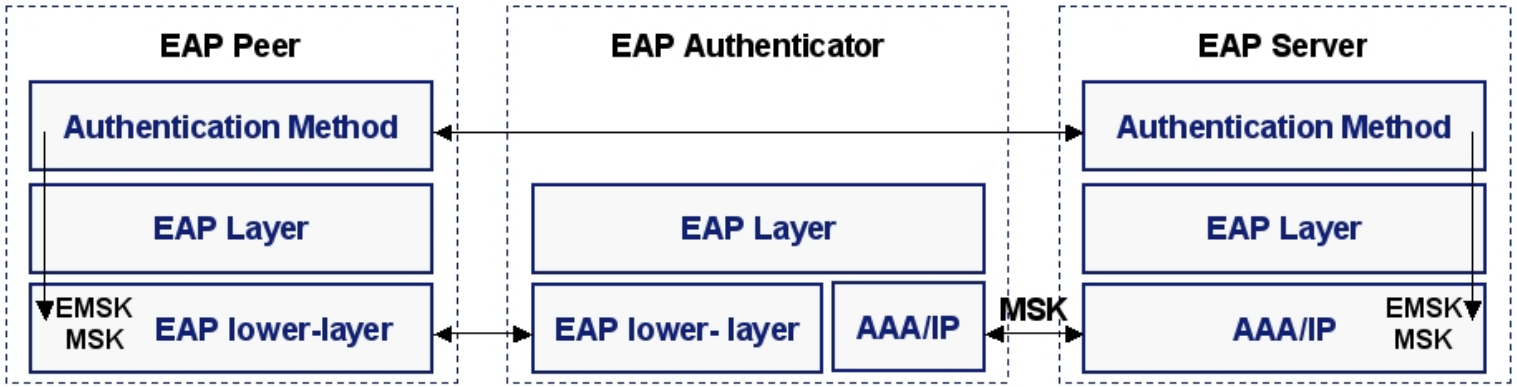
- The EU-funded project **ENABLE** (Enabling Efficient and Operational Mobility in Large Scale Heterogeneous IPv6 Networks) aims to enable efficient and operational mobility in large heterogeneous IP networks.
- This also comprises the enrichment of the basic mobility service provided by Mobile IPv6 with a set of additional features, enabling the on-demand activation and auto-configuration of specific "premium" network features (e.g., multi-homing, fast handovers) based on the operator policies and customers profiles.
- But these features require an authentication process in order to provide access service (in particular network access service)

Introduction (2)



Introduction (3)

- The Extensible Authentication Protocol (EAP) : flexible way of authentication.



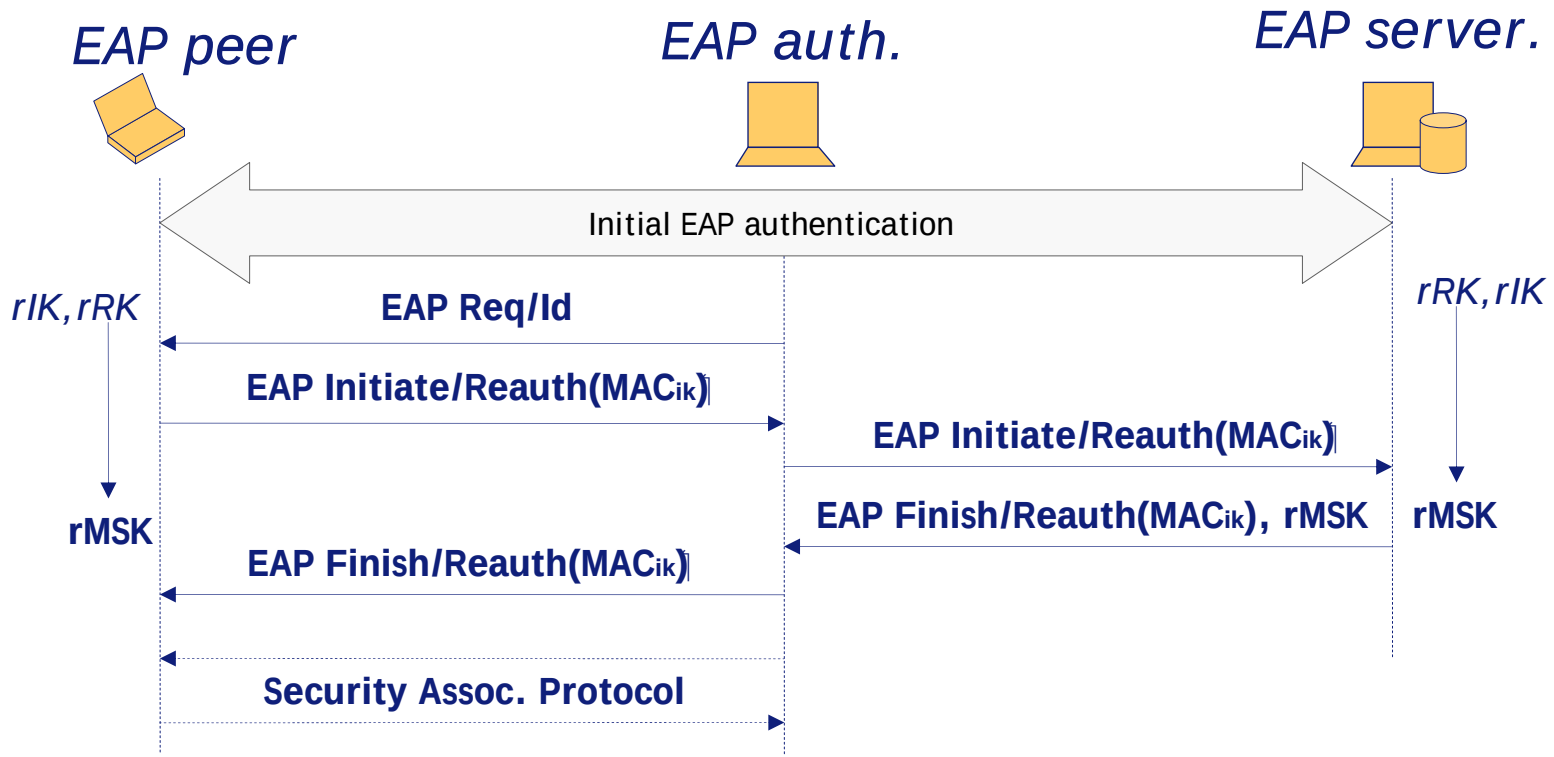
Introduction (4)

- The HOKEY WG addresses these problems with two main objectives
  - Specify a method-independent and efficient re-authentication protocol
  - Allow the peer to use a locally reachable server with efficient EAP re-authentication capability support, in order to avoid contacting the original EAP server for each re-authentication

EAP-ER Overview

- **EAP Extensions for Efficient Re-authentication**
- Supports EAP method independent re-authentication for a peer that has valid, unexpired keying material from a previous EAP authentication
- Introduces two new EAP messages
  - EAP Initiate Re-auth message
  - EAP Finish Re-auth message
- Since the transport is based on EAP, it requires support for the protocol on the authenticators

EAP-ER Message Flow



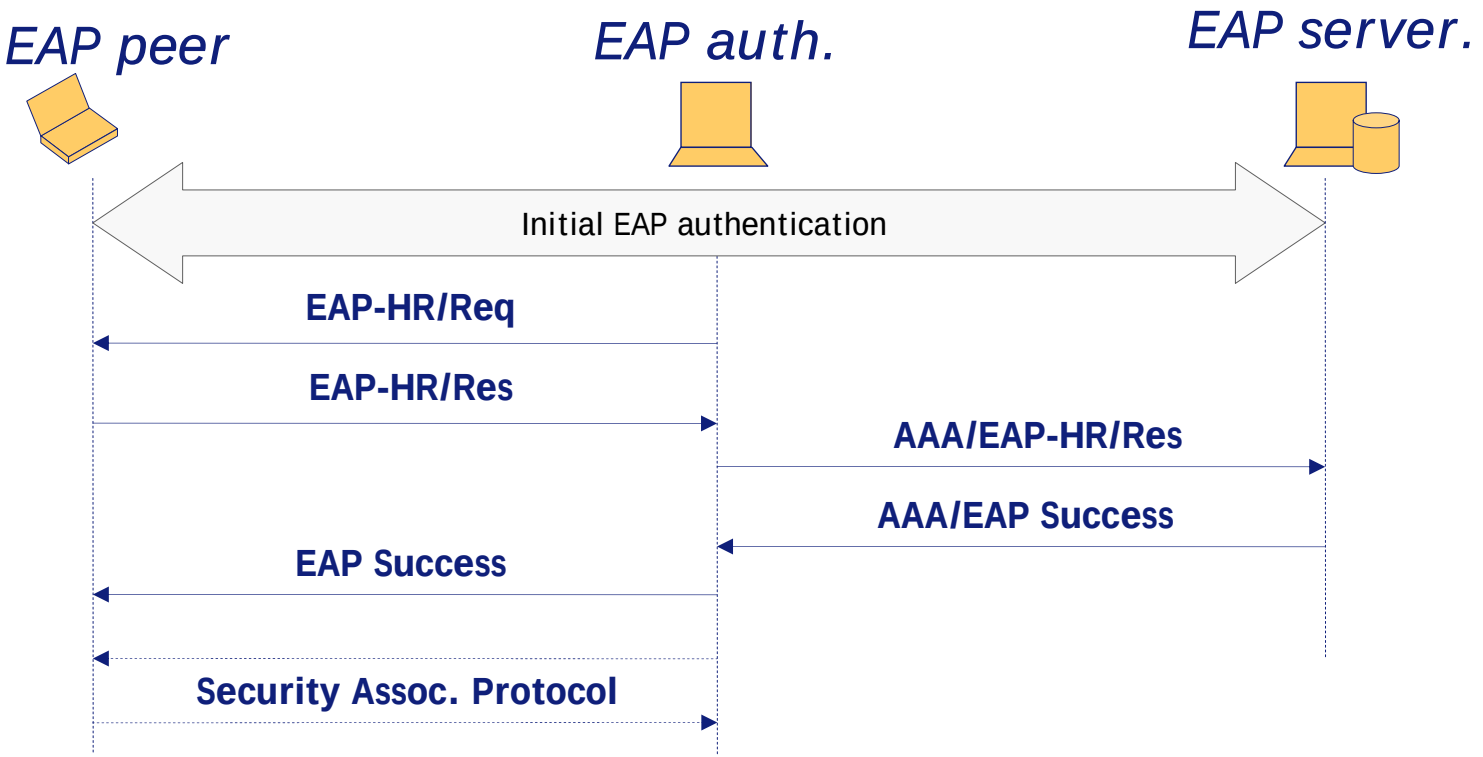
EAP-ER Conclusions

- Pros
  - Supports method-independent re-authentication
  - Can perform the re-authentication in a single roundtrip
  - Supports explicit bootstrapping, which can be used by the peer to obtain a server ID at the end of a successful full EAP exchange
- Cons
  - Involvers major changes in the EAP state machines, modifying flows and adding new states, as well as new EAP messages
  - Requires support for the protocol on the authenticators. This implies that every NAS deployed in the network must be modified to support EAP-ER, unless some fallback mechanism is defined

EAP-HR Overview

- **Keying and signaling for wireless access and handover using EAP**
- Very similar to EAP-ER but using new EAP types.
- That is, a new EAP method called EAP Handover and Re-authentication (EAP-HR)
- It seems it may affect less to current EAP implementations
- Reality is it implies modification also in authenticators, peers and servers.
- The proposed signaling completes a re-authentication in a single roundtrip

EAP-HR Message Flow (re-authentication)



EAP-HR Conclusions

- Pros
  - Can perform the re-authentication in a single roundtrip
  - Support for authentication of all parties
  - The protocol has been updated to support 3-party scenarios
- Cons
  - As EAP-ER, requires support for the protocol on the authenticators

Bootstrapping: EAP-EXT

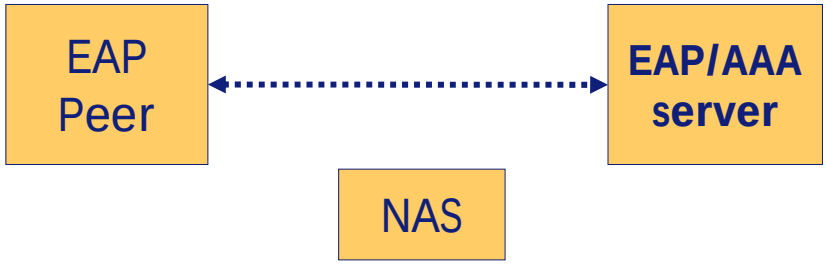
- **An EAP Method for EAP Extension**
  - draft-ohba-hokey-emu-eap-ext-01
- The document describes an EAP method that is used for extending EAP functionality
- The EAP-EXT method also allows sequencing of multiple EAP methods within itself
  - It can generate MSK and EMSK in cases where the inner EAP method(s) generate MSK but do not generate EMSK
- It is very useful to provide bootstrapping information related with Fast Re-authentication.

EAP-EXT (conclusions)

- Provides capabilities exchange
- No changes in the EAP state machines. Can reuse existing infrastructure
- Can use any key-deriving inner EAP method
- Useful for bootstrapping (initial step) in Fast Handover scenarios.

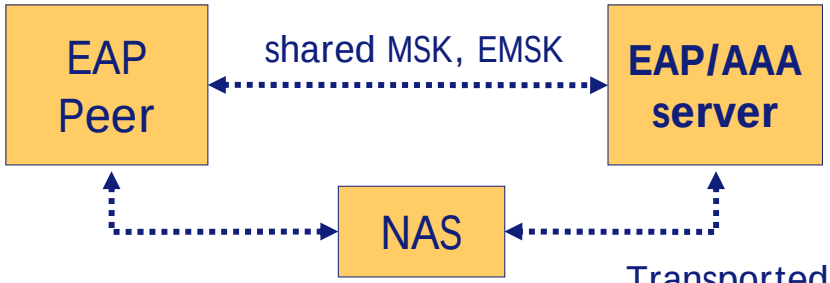
3-Party Key Distribution Problem (1)

- EAP-Based Network Access Authentication have been based on a 2-party trust model
- Eventually, Network Access Authentication was extended to be more scalable by separating the authentication engine from the NAS



3-Party Key Distribution Problem (2)

- After a successful mutual authentication EAP peer and EAP server has pre-shared keys (MSK,EMSK)
- But a key is required in the EAP authenticator (NAS) !!!
- Therefore, 3 parties are involved in the key distribution model.
- The EAP model based on 2 parties is no longer valid.
- This key distribution mechanism must be based on a *3-party* key distribution model.



3-Party Key Distribution Problem (3)

- In handover keying, there is a server named HOKEY server that distributes keys between the EAP authenticators
- When HOKEY server does not have a key (roaming scenario) three main parties are involved:
  - EAP peer
  - EAP server in the home domain
  - Handover keying (HOKEY) server in the visited domain
- Once the HOKEY server owns a key, the three main parties are:
  - EAP peer
  - HOKEY server
  - EAP authenticator

Conclusions & Future Work

- Reducing time spent on authentication (in particular EAP based) is very important for a smooth and seamless handover.
- IETF through HOKEY WG is working on a solution and several proposals are on the table: EAP-ER, EAP-HR
- Under security perspective, the tendence is leading solutions a 3-party model.
- In ENABLE, we are putting our effort on providing a secure 3-party protocol which is able to provide a secure key distribution in fast secure handover.

Questions?