



# EAP-OTP: An Extensible Authentication Protocol (EAP) Method for OTP Algorithms

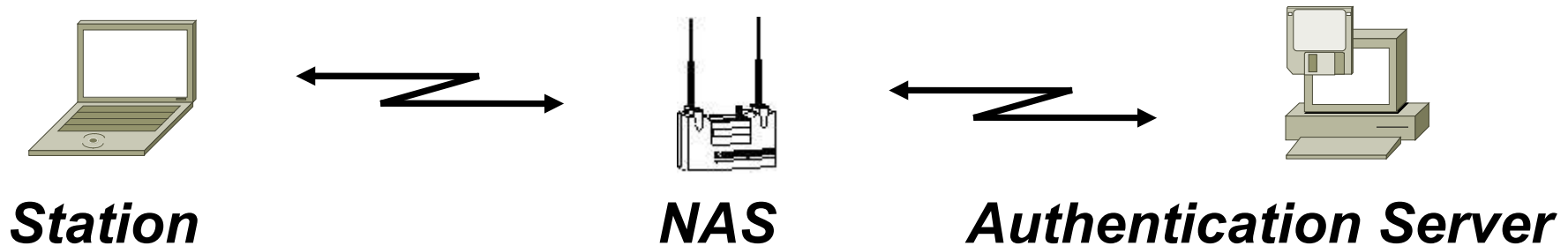
Tuesday, February 15, 2005

**RSA Conference 2005**

# EAP Primer



- EAP is the protocol used to authenticate peers in network access contexts such as WLAN, PPP remote access, and in IPSEC credential access
- EAP entities are usually the peer (or station), NAS (e.g. access point) and the authentication server:



- Usually, the peer authenticates to the NAS who forwards the credentials to the authentication server

# EAP Primer



- Even if the NAS “speaks” EAP, it probably does not know about all EAP methods or users
- To this end, NASes usually also “speak” some AAA protocol like RADIUS to back-end authentication servers who do know about a particular EAP method and users
- This allows for support of new EAP methods without replacing or upgrading NASes

# EAP and OTP Tokens 1 (3)



- As demand for strong user authentication grows, OTP-based authentication tend to become more common
- OTP tokens (devices) increasingly tend to support “connected” mode (e.g. USB)
- There is a desire to increase the security and performance of EAP methods
  - Strong user authentication
  - Protection of user credentials in transit
  - Mutual authentication
  - Generation of session keys
  - Session resumption

# EAP and OTP Tokens 2 (3)



- Current EAP support for OTP algorithms is poor
  - EAP Generic Token Card
    - Prompts sent from server to peer, intended for human consumption
    - Unilateral authentication
    - No generation of keying material, e.g. for protection of subsequent session
  - EAP OTP
    - Despite its name, a specialized method for a particular algorithm (S/KEY). No generation of keying material, no session resume
  - EAP-MS-CHAP
    - Challenge-response based
    - Requires MD4, DES, No features to slow down attacker

# EAP and OTP Tokens 3 (3)

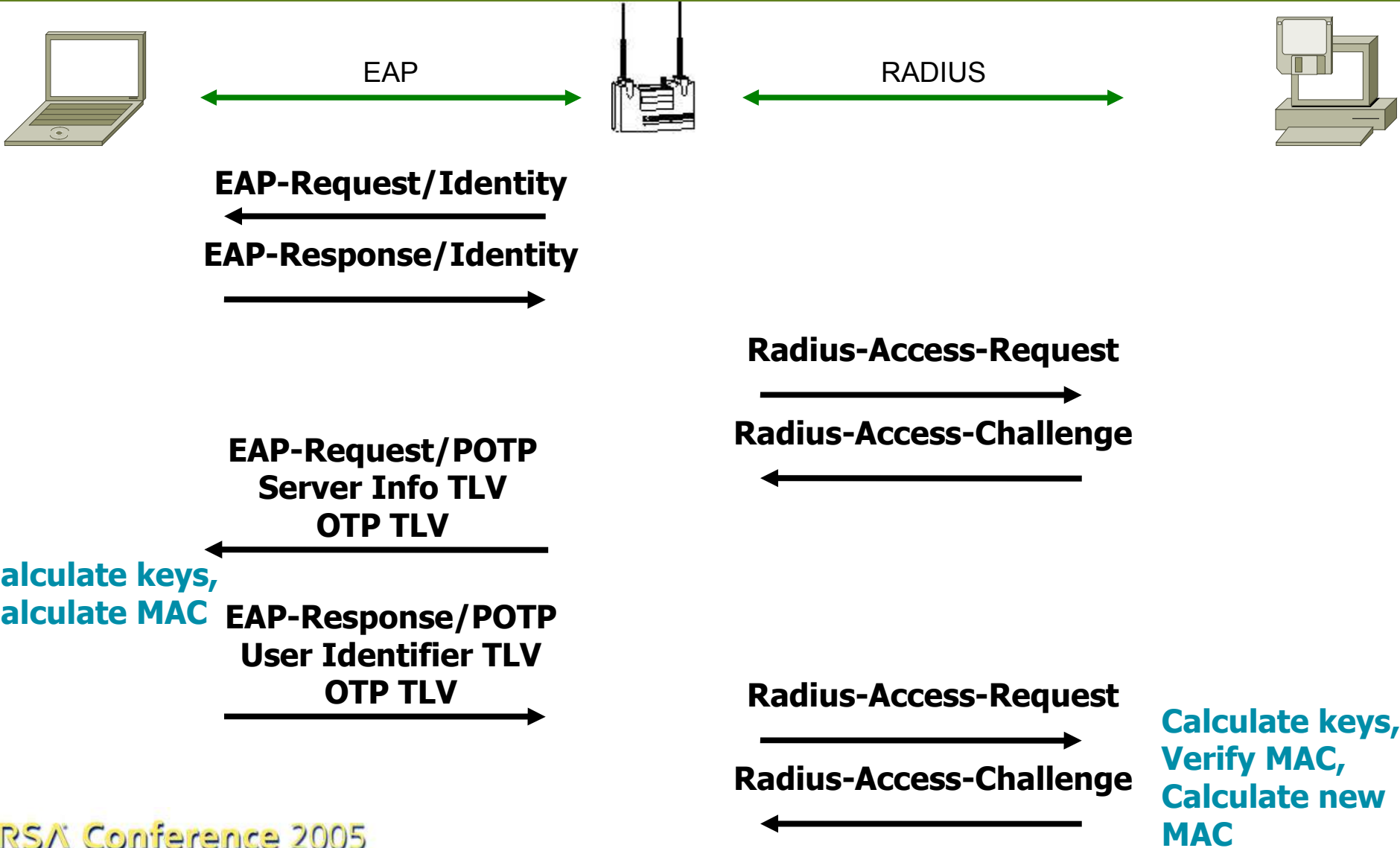


- The current state of affairs combined with EAP needs motivates a new EAP method oriented towards OTP tokens
  - Should be usable also for handheld OTP tokens and other forms of OTP systems)

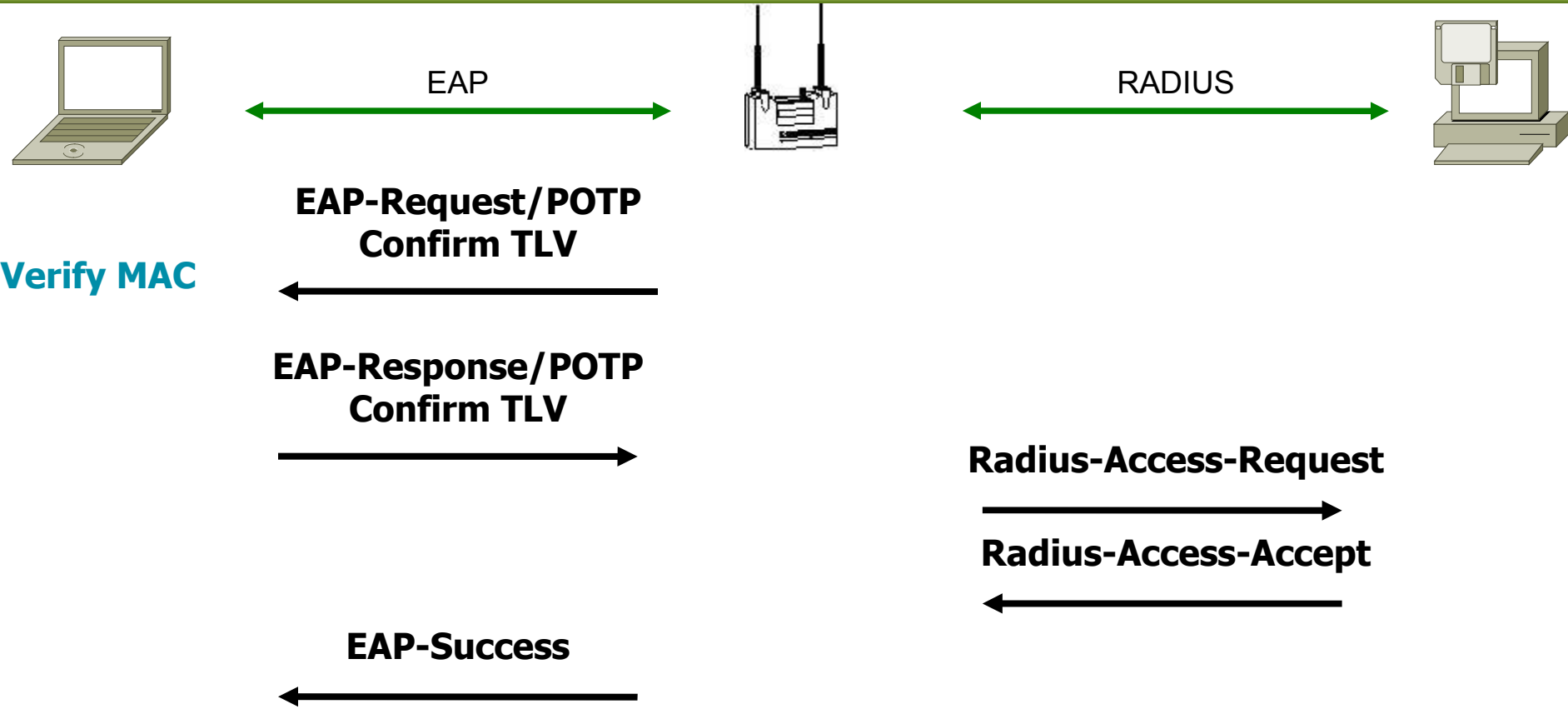


- Defines an EAP protocol that
  - Enables programmatic use of a connected OTP token
  - Provides mutual authentication
  - Generates keying material
  - Does not rely on tunneling (provides privacy for OTP values)
  - Provides fast session resumption
- EAP-POTP
  - Complements EAP-PEAP, EAP-TTLS, and EAP-FAST
  - May be used as a better alternative for an “inner” EAP method than EAP-GTC, PAP, CHAP, etc

# Principles of Operation



# Principles of Operation, Continued



**Start of encrypted and mutually authenticated session**

# Protection of OTP Values



- Both sides calculate:

$$K_{MAC} | K_{ENC} | MSK | EMSK =$$

PBKDF2-SHA256 (*otp*, *salt* | *pepper* | *auth\_addr*, *iteration\_count*, *kLen*)

where

$K_{MAC}$  is used to authenticate (MAC) the parties – MACs on PDUs

$K_{ENC}$  is used to protect sensitive data

$MSK$  is delivered to the EAP method caller (“Master Session Key”)

$EMSK$  is saved for future use

PBKDF2 is defined PKCS #5 v2.0 (Password-based KDF)

*otp* is the OTP value

*salt* and *pepper* are random nonces (only *salt* is sent in protocol)

*auth\_addr* the NAS address as seen by the peer

*iteration\_count* slows down an attacker (as does *pepper*), and

$kLen = |K_{MAC}| + |K_{ENC}| + |MSK| + |EMSK|$

# Pepper



- The use of pepper slows down an attacker without slowing down the peer
  - Peer just selects a random pepper
  - Does not disclose it to anyone
- Naïve implementation slows down server too
  - Needs to search for suitable pepper
- Therefore, server may select pepper and send (encrypted with  $K_{ENC}$ ) to peer for later use
  - Allows much longer (stronger) pepper values

# Extensibility



- The method is profiled for RSA SecurID – EAP-POTP RSA SecurID
- Designed to be easily and in a straightforward manner extensible to other OTP algorithms too
- May be used as a framework within a framework – OTPs within EAP

# Summary



- EAP-POTP provides a framework for OTP algorithms in EAP, which
  - Allows for mutual authentication
  - Establishes session keys
  - Offers fast session resumption
  - Never sends OTP values directly
  - Works well with connected OTP tokens
- EAP POTP has been submitted to the IETF for broader review

# Questions?



- Contact information:
  - OTPS: <http://www.rsasecurity.com/rsalabs/otps/>
  - OTPS editor: <mailto:otps-editor@rsasecurity.com>