EAP Identity Protection

draft-zcao-emu-id-protection-00.txt

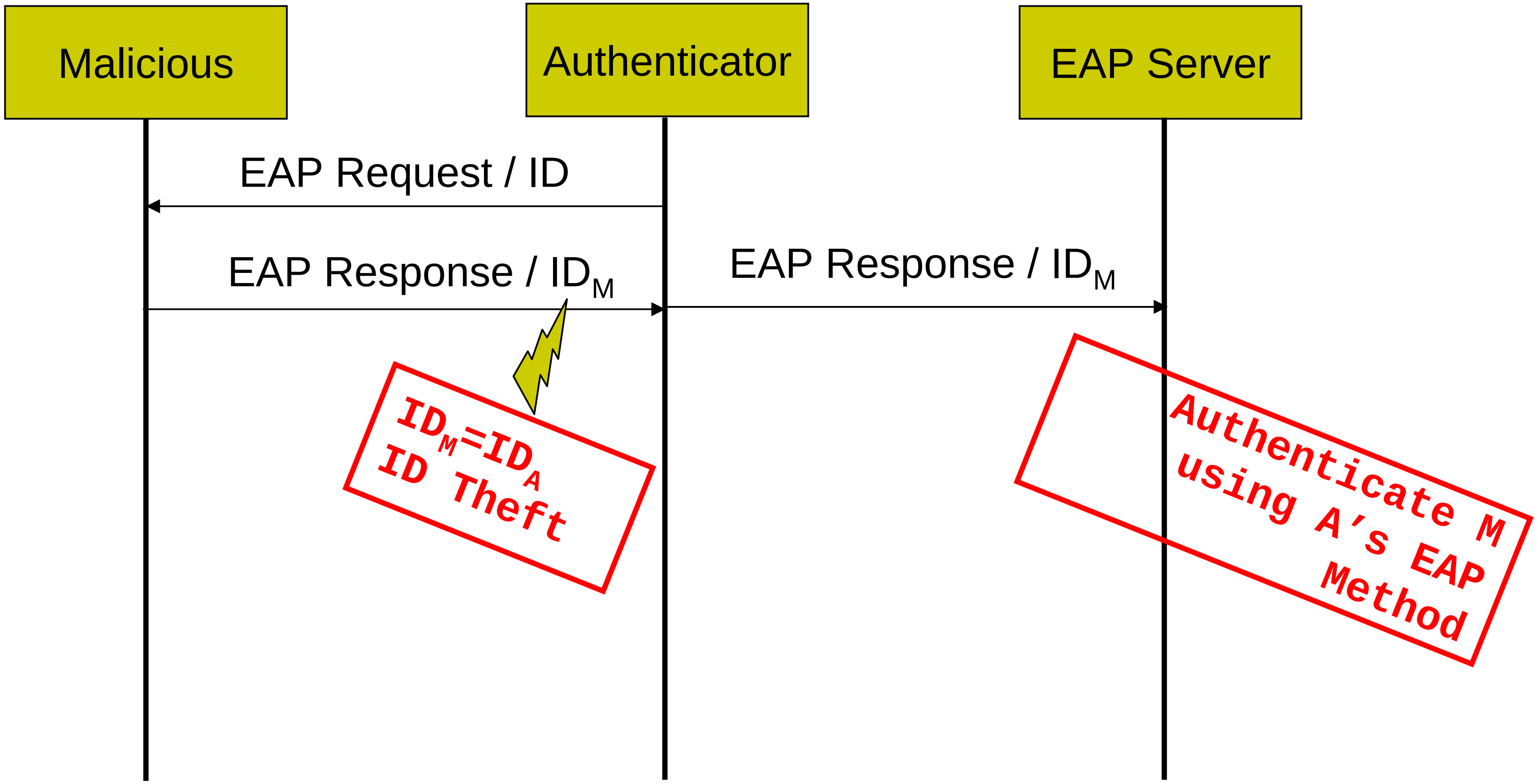
Zhen Cao, Dapeng Liu, Hui Deng
China Mobile

EMU WG Meeting @ IETF78
July 28, 2010
Maastricht, NL

The problem

- Upon receiving the authentication Identity provided by the peer, the EAP server determines which EAP method to start with
- The Identity can be easily forged, resulting into downward attacks
- We should protect the ID

An Example

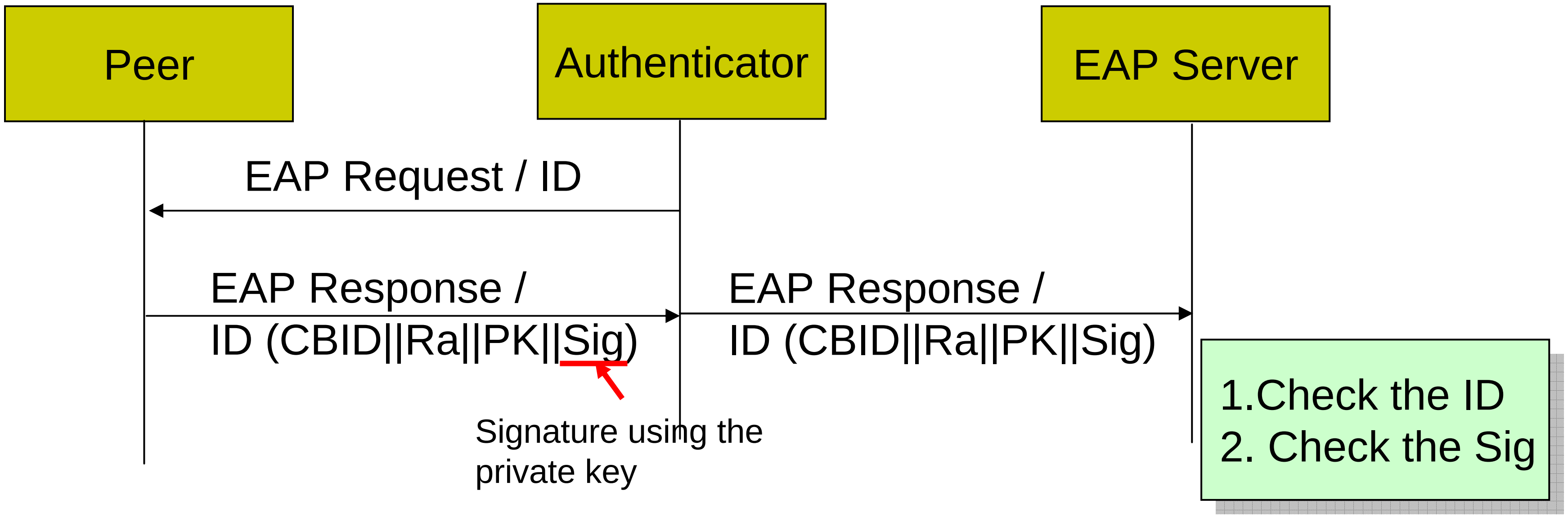

Malicious
Authenticator
EAP Server
EAP Request / ID
EAP Response / ID_M
EAP Response / ID_M
$ID_M=ID_A$
ID Theft
Authenticate M using A's EAP Method

Intuition of the Solution:

- Native IDs are easy to compromise
- What’s desired :
  - Identity ownership: EAP peer has a method to demonstrate its ownership of the Identity
  - Others cannot generate the correct message if they do not know the “secret”
- Crypto-binding Identity is the way we choose

The Solution

- ID generation
  - Public-private key pair: (PK, SK)
  - CBID = HASH (PK||OPTIONAL-CONTENT)
- ID exchange



Other considerations

- To avoid replay attack
  - We have used the random number Ra
  - The EAP server needs to keep the history of this random to avoid replay

The extended message

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+---------------+-----------------------------------------------+
|    Type=1     |                                               |
+---------------+                                               |
|                       CBID (160 bit)                          |
|                                                               |
|               +-----------------------------------------------|
|               |                 Random (24 bit)               |
|---------------+-----------------------------------------------|
|                                                               |
|                  Public Key (variable length)                 |
~                                                               ~
|---------------------------------------------------------------|
|                                                               |
~                  Signature (variable length)                  ~
|                                                               |
+---------------------------------------------------------------+
```

- Any interests to continue working on this direction?
- Adopt it as a work item?