Message Authentication in EPON

I.e. why to encrypt full MAC frame (DA - FCS) in upstream

Olli-Pekka Hiironen, Nokia

Message authentication

- Message authentication (data origin authentication)
  - a type of authentication whereby a party which receives a message have assurance of the identity of the party which originated the message
- PON is multi-point-to-point in upstream
  - OLT have no means to verify that the message received and presumably created by ONU A did indeed originate from ONU A.
- Threats
  - **Masquerading (authentication)**: The attacker could masquerade as another ONU by assuming the identity of a valid ONU.
  - **Unauthorized access (authentication)**: The attacker could gain access to privileged data and resources in the network by assuming the identity of a valid ONU.
  - **Detecting attacks (denial of service prevention)**: Attacker can actively try to attack to the OLT using valid LLIDs. OLT would not detect that without message authentication.

Message authentication mechanisms

- Message Authentication Code (encryption not needed)
  - Code calculated from message using a shared secret key is added to the end of message. Code is re-calculated at receiver and compared to received code.
  - Protect against data integrity threats (e.g. man-in-the-middle).
  - Used in WLAN.
- Encryption with decryption-error detection
  - Message (including error detection code, e.g. CRC) is encrypted with authenticated key. Message is decrypted at receiver. Correctness of decryption is checked with error detection code, e.g. CRC. Correct detection indicates that message was originated from the authenticated user.
  - Requires that key is traceable to authentication.
  - Usable if no data integrity threats (e.g. man-in-the-middle). We may assume this for PON.

Proposal for EPON: Message Authentication using CRC

- Authentication process makes also the initial key exchange
  - Encryption key should be traceable to authentication.
- Following key exchanges should maintain the traceability
  - Key exchange use secure and authenticated messages, or
  - Key derived from previous authenticated key (as in 802.11i).
- Frame including CRC is encrypted (Encrypt function)
- At receiving end frame including CRC is decrypted (Decrypt function)
- CRC is re-calculated as usually in MAC
  - Correctness of CRC indicates that message was originated from authenticated user because it is not possible to create data with correct CRC without knowledge of the encryption key.
  - Note that it is possible to modify data and CRC without knowledge of the encryption key. This is not a problem in PON if we assume that there is no man-in-the-middle possibility.

Conclusion

- Message authentication is as natural in upstream as encryption is in downstream
- Message authentication code guarantees message authentication if man-in-the-middle threat exists
- Encryption with decryption error detection using CRC guarantees message authentication in PON if
  - No man-in-the-middle threat
  - Encryption keys are traceable to authentication
  - Frame including CRC is encrypted
- **Requirements for 802.3ah:**
  - **Upstream should have encryption**
  - **Full MAC frame (DA - FCS) is encrypted**
- Requirements for EPON:
  - Initial encryption keys are derived from authentication
  - Re-keying maintains traceability to authentication