THOUGHTS ON TSN SECURITY

Contributed by

Philippe Klein, PhD (philippe@broadcom.com)
<table>
<thead>
<tr>
<th>Layer</th>
<th>Protocol</th>
<th>Description</th>
<th>Complexity</th>
<th>Performance</th>
</tr>
</thead>
</table>
| Layer 4..7| SSL / TLS,…    | ▪ Application layer encryption  
▪ Client server mode                                                             | ▪ Security built into the application  
▪ Phased deployment difficult  
▪ Client initiated  
▪ Uses TCP connection oriented protocol | ▪ Assumes medium to low performance                                           |
| Layer 3   | IPsec          | ▪ Layer 3 “Network” security  
▪ End to End "tunnels"  
▪ Peer to peer Protocol                                                       | ▪ Complex protocol suite, many options  
▪ Key management using IKE protocol and PKI for authentication               | ▪ Ranges from low to high  
▪ Significant header expansion                                                |
| Layer 2   | MACsec         | ▪ Layer 2 security  
▪ Hop by hop  
▪ Peer to peer protocol                                                       | ▪ Relatively simple to implement  
▪ Phased deployment possible  
▪ Key management (MKA via 802.1X-2010)                                        | ▪ Designed for high throughput  
▪ Minimal header expansion                                                    |
IEEE Std 802.1AE (aka MACsec) Media Access Control (MAC) Security

“MAC Security (MACsec) allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices.”

Relationship between IEEE Std 802.1AE and other IEEE 802 standards

- IEEE Std 802.1X specifies Port-based Network Access Control, and provides a means of authenticating and authorizing devices attached to a LAN.
WHAT IS MACsec?

- **Hop-to-hop Layer 2 Security**
  - Protects communication between trusted components of the network infrastructure
    - All frames exchanged between the two elements (called SecY) are authenticated and optionally encrypted
  - Controls access to the network when combined with 802.1X
  - Provides source authentication, integrity, and confidentiality using strong crypto (AES-GCM)

- **Secure LANs from attacks of:**
  - Wiretapping (confidentiality)
  - Impersonation (authentication)
  - Masquerading (MAC address spoofing)
  - Man-in-the-Middle attacks
  - Replay attack (authentication + anti-replay counter)
  - Denial-of-Service (DOS) attacks

- **Does not:**
  - Protect against attacks of trusted components themselves
  - Provide end-to-end security
  - Replace 802.11i
SECURE MAC SERVICE RELATIONSHIP

- **Connectivity Associations (CA)**
  - Set of stations that can securely communicate with each other using Secure Channels

- **Secure Channels (SC)**
  - An uni-directional channel identified by an SC Identifier in the packet header used to communicate between stations belonging to the same CA

- **Security Association (SA)**
  - An active key associated for each SC. Standard requires 2 active SAs per SC to support non-interrupting key swap

- **Usage Scenarios**
  - Point to Point LANs
  - Shared Media LANs
  - Provider Bridged Networks
2_STATION SC

Figure 7.1—Two stations connected by a point-to-point LAN

Figure 7.2—Two stations in a CA created by MACsec Key Agreement

Figure 7.3—Secure communication between two stations
3_STATION SC

Figure 7-4—Four stations attached to a shared media LAN

Figure 7-5—A CA including ports A, B, and C

Figure 7-6—Secure communication between three stations
MACsec - ENCRYPTION
• Cypher Suite: 128 or 256 AES-GCM (Galois/Counter Mode)
SecTAG
- 802.X authentication is used to authenticate end stations
- MKA (MACsec Key Agreement) Protocol is used to exchange session keys based on CA Key
IEEE Std 802.1X - PORT BASED NETWORK ACCESS CONTROL

Supplicant

Authenticator

Authentication Server

IEEE 802.1 Plenary Meeting, Berlin, March 2015
- Define a frameset to allow different Authentication METHODS
  - Pre shared keys,
  - Certificates,
  - Passwords,
  - SIM credentials,
  - Biometrics,…

- AEPoI/AEPoW : define container messages to carry the authentication protocol over wired and wireless links
IEEE 802.1X MKA KEY DISTRIBUTION

CAK Secure Connectivity Association Key
ICK Integrity Check Value Key
KEK Key Encrypting Key
SAK Secure Association Key

allows implementation of a policy of perfect forward security
MACsec - CHALLENGES
Examples of End to End Hybrid Networks for Service Providers

- CONTENTS
  - CO → OLT (PON) → ONU/GW (ETH) → Bridge → MoCA → Bridge → Wifi → End Point

- SERVICES
  - CO → CMTS (DOCSIS) → CM/GW (MoCA) → Bridge → ETH → Bridge → HPAV → End Point
HYBRID HOME NETWORK CONNECTIVITY

IEEE 802.1 Plenary Meeting, Berlin, March 2015
## Native L2 Security Schemes

<table>
<thead>
<tr>
<th>Technology</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet / IEEE 802.3</td>
<td>EAP</td>
<td>AES-128 GCM</td>
<td>IEEE 802.1AE (MACsec), 802.1X</td>
</tr>
<tr>
<td>MoCA</td>
<td>Proprietary (dynamic) PSKs</td>
<td>DES AES-128 CBC</td>
<td>The whole MPDU is encrypted in the PHY (including the Eth MAC header)</td>
</tr>
<tr>
<td>HomePlug AV2 / IEEE 1901</td>
<td>Proprietary (dynamic) PSKs</td>
<td>AES-128 CBC</td>
<td></td>
</tr>
<tr>
<td>WiFi / IEEE 802.11</td>
<td>EAP</td>
<td>AES-128 CCMP</td>
<td>802.1X, <strong>AES-GCM for 802.11ad</strong></td>
</tr>
<tr>
<td>EPON</td>
<td>EAP</td>
<td>AES-128 GCM</td>
<td>IEEE 802.1AE (MACsec), 802.1X</td>
</tr>
<tr>
<td>ADSL</td>
<td>PAP/CHAP</td>
<td>none</td>
<td>L3 encryption</td>
</tr>
</tbody>
</table>

EAP = Extendable Authentication Protocol (RFC 3748)
GCM = Galois/Counter Mode
PSK = Private Shared Key
DPoE = DOCSIS Provisioning of EPON Specifications
• Hop to hop “limitation”
  • Packet need to decrypted to access the inner VLAN tag
  • Key “explosion” – Let be realistic – Key management was and still is the main roadblock to security deployment…

• 802.1AEcg (aims to Provider bridges)
  • VLAN is copied outside the encrypted fields

• What if:
  • Same key could now be OPTIONALLY reused if the Authentication Method and credentials are the same on 2 links…
    • If the SA is the same on Ingress and Egress, could the encrypted packets be forwarded as is?
    • Better performance?
    • Better transit protection?
    • Retain network synchronization accuracy?
    • Optional link or path authentication

  Notice that this scheme was already presented at the Ethernet Summit in 2014 by Vitesse Semiconductors

• Q: What about IEEE 1588 Annex K?
IEEE 802.1AE (MACsec) is a robust solution for network wide security at the link layer but …

- More effort should be made to address the “low end” (SMB ? / SOHO / Home) market
- Hard to promote as many “customers” are foreseeing the need for security
- Seen as expensive and cumbersome
- Must be actively promoted beyond Ethernet Core Networks
- MUST BE INTEGRATED UP FRONT IN ARCHITECTURE DESIGN
Thank you