MACSec Security Service FIPS Validation

Richard Wang
May 19, 2017
International Crypto Module Conference
Topics

- MACSec Overview
- MACSec Authentication Mechanisms
- MACSec with FIPS
- Draft IG A.5
- References
- Q&A
MACSec Overview

• What is MACSec?
  • Media Access Control Security (aka MACSec) is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices.

• Why MACSec?
  • Layer 2 (not layer 3) data encryption (AES-128/256 GCM)
  • Integrity Check
  • Denial of service (DoS) attack isolation
  • Others
MACSec Overview (Cont.)

- MACSec Components
  - Suppliant
  - Authenticator
  - Authentication Server
    - EAP Authentication Mode: Authentication is done via the RADIUS Server if Extensible Authentication Protocol (EAP) is used
    - PSK Authentication Mode: Authentication is done in the Authenticator locally if Pre-Shared Key (PSK) is used
MACSec Authentication

- Authentication using EAP method
  - EAP-TLS Authentication
  - RADIUS Server
  - TLS or IPSec tunnel

Supplicant
Hello, can I join in?

Authenticator
Wait! Let me ask Mr. RADIUS

Authentication Server
Yep!

Traffic Protection by SAK

MACSec Key Agreement (MKA)

SAK Transfer

CAK Transfer

IPSec/TLS
MACSec Authentication (Cont.)

- Authentication using PSK method
  - Pre-shared Key (PSK) Authentication
  - No RADIUS Server

Supplicant

Hello, can I join in?

Wait! Let me check my database.

Authenticator/Authentication Server

MACSec Key Agreement (MKA)

SAK Transfer

Traffic Protection by SAK
So is my MACSec Okay for FIPS?

MACSec Cryptographic Keys
- PSK – Pre-shared Key (in PSK Mode)
- MSK - Master Session Key (in EAP Mode)
- CAK - Connectivity Association Key
- CKN - Connectivity Association Key Name (used to identifies the CAK).
- KEK – Key encryption key
- ICK - Integrity Check Key
- SAK – MACSec Secure Association Key

So many keys!
MACSec for FIPS (Cont.)

- **MACSec Keys Establishment**
  - **PSK – Pre-shared Key (PSK Mode)**
    - Entered by Admin/Crypto Officer
  - **MSK - Master Session Key (EAP Mode)**
    - Derived from EAP session (802.1x-2010)
  - **CAK - Connectivity Association Key**
    - $CAK = KDF(\text{Key, Label, mac1 | mac2, CAK length})$
    - Derived from MSK
    - IEEE 802.1x-2010, Section 6.2.2
MACSec for FIPS (Cont.)

- **MACSec Keys Establishment**
  - **CKN - Connectivity Association Key Name (used to identifies the CAK)**
    - $\text{CKN} = \text{KDF}(\text{Key}, \text{Label}, \text{ID} | \text{mac1} | \text{mac2}, \text{CKN length})$
    - Derived from MSK
    - **KDF:** SP800-108 KDF (NIST Approved)
    - IEEE 802.1x-2010, Section 6.2.2

- **KEK – Key Encryption Key**
  - $\text{KEK} = \text{KDF}(\text{Key}, \text{Label}, \text{Keyid}, \text{KEK Length})$
  - Derived from CAK
  - **KDF:** SP800-108 KDF (NIST Approved)
  - IEEE 802.1x-2010, Section 9.3.3
MACSec for FIPS (Cont.)

- MACSec Keys Establishment
  - ICK – Integrity Check Key
    - ICK = KDF(Key, Label, Keyid, ICKLength)
    - Derived from CAK
    - KDF: SP800-108 KDF (NIST Approved)
    - IEEE 802.1x-2010, Section 9.3.3

- SAK - MACSec Secure Association Key
  - SAK Establishment
    - Option 1: Generated by the Authenticator (SP800-133 Key Generation)
    - Option 2: Derived from CAK
    - IEEE 802.1x-2010, Section 9.8.1
MACSec for FIPS (Cont.)

• SAK Key Transfer

  • FIPS Approved Key Transport Method
    ➢ RSA-based key transport scheme, as specified in SP 800-56B.
    ➢ Approved key wrapping algorithms are specified in SP 800-38F.

  • FIPS Approved Key Transport Method (before Dec. 31, 2017):
    ➢ Any key encapsulation scheme employing an RSA-based key methodology that uses an RSA modulus that is at least 2048 bits long.
    ➢ A key wrapping using any approved mode of AES or three-key Triple-DES
Draft A.5 Requirements for MACSec

- Still in Draft since last modified (5/13/2016)
- EAP Mode
  - IPSec/TLS secure tunnel in MACSec deployment
  - IV generation method in IPSec/TLS meets the A.5 requirements.
- PSK Mode
  - PSK can be used as CAK
  - PSK shall not be directly used as SAK
- IV Generation requirement in MACSec???
- SP800-108 KDF
- Check the lab for the A.5 update status.
References

- IEEE 802.1x-2010
- SP800-38D
- SP800-108 KDF
- FIPS Implementation Guidance (IG)/A.5
Questions and Answer
Contact Information

- Richard Wang – FIPS 140-2 Lab Manager
  - RichardWang@gossamersec.com

- Ed Morris – FIPS 140-2 Lab Director
  - EdMorris@gossamersec.com