FMCOS uses ciphertext with MAC to add/modify keys

FMCOS (FM1208-9, FM1208-10, FM1216, etc.) supports adding/modifying keys in common plaintext and ciphertext + MAC addresses.

Basic principles

FMCOS keys can be divided into two types: [common key] and [ciphertext + MAC key] according to the operation mode of adding/modifying the key. Thi classification has no effect on the type of key (e.g., external authentication key, line protection key, etc.) and how the key is used.

[Ciphertext + MAC Key] means that the maximum byte of the type of [Common Key] is set to "11" by up to 2 bits. For example, the type of [Normal] exter authentication key is 39 (0011 1001), and the type of [ciphertext + MAC] external authentication key is F9 (1111 1001).

The prerequisite for using ciphertext + MAC address to change the key is that the master key (an external key identified as 00) must exist in the current k The master key is used to encrypt data and compute MAC addresses. The master key can be of type 39 or F9. (However, you can only add the master k type 39 in plaintext first, and then use ciphertext + MAC to modify it to type F9.))

When do you need to use ciphertext + MAC operation key:

1. Add a [ciphertext + MAC key] (e.g. type F9);

2. Change [Common Key] to [Ciphertext + MAC Key] (for example, type 39 is changed to F9);

3. Modify [ciphertext + MAC key], including changing it to [normal key] (for example, change the value of the F9 key; or change Type F9 to 39).

Experimental environment

The following keys exist in the key file in MF:

1. Master key, key value FF FF.

2. External authentication key, ID 01, type 39.

Add a key (F9)

To use ciphertext with MAC address, add an external authentication key (type **F9**, not 39) with the identifier 02 under MF.

The right to use and modify the key is F0. Subsequent status A; Error counter F; Key value 11 22 33 44 55 66 77 88.

The data field of the command:

> **F9** F0 F0 AA FF 11 22 33 44 55 66 77 88

Note 39 (0011 1001) becomes **F9** (1111 1001).

Expand and populate the data field to obtain the plaintext data to be encrypted:

> *0D* F9 F0 F0 AA FF 11 22 33 44 55 66 77 88 *80 00*

Note: 0D is the LD byte, which indicates the length of the original data; 80 00 is the padding byte. (Please refer to the FMCOS 2.0 User Manual for speci implementation)

Use the master key to encrypt the plaintext data in DES to obtain the ciphertext.

> 7C 87 BC 23 14 00 21 B3 AF EA 67 E6 35 9D DC FE

Note: FMCOS uses DES-ECB encryption.

Command to add key:

> **84** D4 01 02 ***14*** 7C 87 BC 23 14 00 21 B3 AF EA 67 E6 35 9D DC FE

The actual length of the ciphertext is 0x10, but because it is followed by a 4-byte MAC, the LC is 0x14.

Because ciphertext + MAC (i.e., encrypted line protection) is used, the CLA becomes 84.

Request a nonce and use the master key to calculate the MAC:

> Random number: 4C 45 BA B9
> MAC：D7 C9 43 F6

Note: For the implementation of MAC calculation in FMCOS, please refer to the FMCOS 2.0 User Manual.

Full Command:

> 84 D4 01 02 14 7C 87 BC 23 14 00 21 B3 AF EA 67 E6 35 9D DC FE D7 C9 43 F6

Modify the key (39 to F9)

To use ciphertext with MAC address, change the external key identified as **01** in MF and change its key value and type (39 to F9).

The right to use and modify the key is F0. Subsequent status A; Error counter F; The new key value is 11 22 33 44 55 66 77 88.

The data field of the command:

> **F9** F0 F0 AA FF 11 22 33 44 55 66 77 88

The reason why 39 becomes F9 has already been shown above, so I will not repeat it.

Expand and populate the data field to obtain the plaintext data to be encrypted:

> 0D F9 F0 F0 AA FF 11 22 33 44 55 66 77 88 80 00

Use the master key to encrypt the plaintext data in DES to obtain the ciphertext.

> 7C 87 BC 23 14 00 21 B3 AF EA 67 E6 35 9D DC FE

Command to modify the key:

> 84 D4 39 01 14 7C 87 BC 23 14 00 21 B3 AF EA 67 E6 35 9D DC FE

Request a nonce and use the master key to calculate the MAC:

> Random number: EF 36 48 18
> MAC：90 95 E4 E1

Full Command:

> 84 D4 39 01 14 7C 87 BC 23 14 00 21 B3 AF EA 67 E6 35 9D DC FE 90 95 E4 E1

Change the key (F9 to 39)

To use ciphertext with MAC address, change the external authentication key type identified as 02 in MF (F9 to 39).

The data field of the command:

> 39 F0 F0 AA FF 11 22 33 44 55 66 77 88

Expand and populate the data field to obtain the plaintext data to be encrypted:

> 0D 39 F0 F0 AA FF 11 22 33 44 55 66 77 88 80 00

Use the master key to encrypt the plaintext data in DES to obtain the ciphertext.

> 7E 65 DE 14 2F 66 CA 41 AF EA 67 E6 35 9D DC FE

Command to modify the key:

> 84 D4 F9 02 14 7E 65 DE 14 2F 66 CA 41 AF EA 67 E6 35 9D DC FE

Request a nonce and use the master key to calculate the MAC:

> Random number: C0 B3 54 9C
> MAC：01 2E F5 F5

Full Command:

> 84 D4 F9 02 14 7E 65 DE 14 2F 66 CA 41 AF EA 67 E6 35 9D DC FE 01 2E F5 F5