CPU card e-wallet circle consumption debugging records

转载 deng214

Reference:
Fudan FMCOS (PBOC2.0 Part 2)

1. Key Mounting:
Trap Key Mounting: 80D40102153FF0F2000200112233445566778899aabbccddeeff

02 - Key identification

3F - Trap key

F0F2 - Use Permissions to Change Permissions

0002 - Key version algorithm identifier

2.
Circle deposit Select e-wallet: 00A4000002000200

Send Trap Initialization: 805000020b020000200000112233445510

0002-P1P2-e-wallet

02 - Key identification

00002000 - Quad byte transaction amount

001122334455 - Terminal number

10- Le

1.00 Trap key 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f 3f

2.01 Trap key 00112233445566778899aabbccddeeff

3.02 Trap key 00112233445566778899aabbccddeeff

Trap initialization command and return data:

=> 80 50 00 02 0B 02 00 00 20 00 00 11 22 33 44 55 10

<=00 00 00 00 00 00 00 02 39 48 bc 11 31 ba 0b cd 90 00

3DES Encryption Algorithm - ECB

Initialization vector: 00 00 00 00 00 00 00 00 00

Data processed: 39 48 bc 11 00 00 80 00

(4-byte random number + 2-byte online transaction number +8000)

Key: 00112233445566778899aabbccddeeff

Result: 3FF239BBDB26018A

MAC Encryption Algorithm-CBC (PBOC-MAC)

Initialization vector: 00 00 00 00 00 00 00 00 00

Data processed: 00 00 00 00 00 00 20 00 02 00 11 22 33 44 55

(4 bytes of original balance + 4 bytes of transaction amount + 1 byte of transaction type ID + 6 bytes of terminal number)

Key: 3FF239BBDB26018A

Result: C47312E9

The card returns 31 ba 0b cd

Trap key mounting:

80 D4 01 00 15 3F F0 F2 01 03 3F 3F3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F 3F

Trap initialization command and return data:

805000020b00000020000112233445510

<=00 00 00 00 00 00 01 03 ee 75 37 42 00 00 00 00 90 00

The algorithm ID is 03, and the MAC1 returned by the Circle Deposit Initialization Command Card is: 00 00 00 00

None of the above results are correct, and it should be verified that there is a problem with the key loading, and the key should be loaded from a new one and then stored

Load the captive key from the new

80D40101153FF0F2010000112233445566778899aabbccddeeff

80D40102153FF0F2000000112233445566778899aabbccddeeff

80D40103153FF0F0010000112233445566778899aabbccddeeff

TAC Key:

80D401001534F0F2010100112233445566778899aabbccddeeff

Consumption Key:

80D40100153EF0F2000000112233445566778899aabbccddeeff

Trap initialization command and return data:

=> 80 50 00 02 0B 02 00 00 20 00 00 11 22 33 44 55 10

<=00 00 00 00 00 00 00 00 e0 b8 47 48 ea 41 1f 90 90 00

Process key: 7C45FBFB5B3A68F5

MAC 1： EA411F90

Calculation process:

3DES Encryption Algorithm - ECB

Initialization vector: 00 00 00 00 00 00 00 00

Data processed: e0 b8 47 48 00 00 80 00

(4-byte random number + 2-byte online transaction number +8000)

Key: 00112233445566778899aabbccddeeff

Result: 7C45FBFB5B3A68F5

MAC Encryption Algorithm-CBC (PBOC-MAC)

Initialization vector: 00 0000 00 00 00 00 00

Data processed: 00 00 00 00 00 00 20 00 02 00 11 22 33 44 55

(4 bytes of original balance + 4 bytes of transaction amount + 1 byte of transaction type ID + 6 bytes of terminal number)

Key: 7C45FBFB5B3A68F5

Results: EA411F90

Card result: EA 41 1F90

The verification result is correct, and it is proved again that there is indeed a problem with the loading of the trap key, and because the card is taken out halfway, the trap initialization is done again.

The process key used by the card to calculate MAC2 in the captive command is the process key generated when MAC1 is calculated, so the captive initialization and capturing are a continuous process, and the card cannot be powered off in the middle of the process.

Trap initialization command and return data:

=>80 50 00 02 0B 01 00 00 20 00 00 11 22 33 44 55 10

<= 00 00 00 00 00 00 01 00 c9 03 81 4d 03 97 6c 22 90 00

Process key: 11FDF264E8AEEFA3

MAC1：03976C22

Entrapment commands and return data:

805200000B201612161058008AFA5718

<= fa 00 06 6d 90 00

MAC2 COMPUTE:

MAC Encryption Algorithm-CBC (PBOC-MAC)

Initialization vector: 00 0000 00 00 00 00 00

Data processed: 0000200002001122334455201612161058 00

(4 bytes of transaction amount + 1 byte of transaction ID + 6 bytes of terminal number + 7 bytes of terminal transaction date and time)

Key: 11FDF264E8AEEFA3

Results: 8AFA5718

TAC Calculation:

MAC Encryption Algorithm-CBC (PBOC-MAC)

Key: 8888888888888888

(8 bytes of XOR left and right of the internal key)

Data processed: 0000200000000000200002001122334455201612161058 00

(4 bytes of new balance + 2 bytes of old online serial number + 4 bytes of transaction amount + 1 byte of transaction type + 6 bytes of terminal number + 4 bytes of terminal transaction date + 3 bytes of terminal transaction time)

Result: FA 0006 6D

Card: FA 0006 6D

The deposit is successful, and the e-wallet balance is updated to 00002000

3. Consumption
Consumption initialization command

805001020b00000000001001122334455

8050-CLA and INS

0102-P1 and P2

00 - Key identification

00000001 - the amount of the transaction

001122334455 - Terminal number

Consumption initialization command and return data

805001020b00000000001001122334455

<= 00 00 20 00 00 00 00 00 00 00 00 58 46 33 c9 90 00

MAC1 Computing:

3DES Encryption Algorithm - ECB

Initialization vector: 00 00 00 00 00 00 00 00

Data processed: 58 46 33 c9 00 00 0000

(4-byte random number + 2-byte offline transaction number + rightmost two bytes of transaction number)

Key: 00112233445566778899aabbccddeeff

Result: C08346DF9F1D457A

MAC Encryption Algorithm-CBC (PBOC-MAC)

Initialization vector: 00 0000 00 00 00 00 00

Data processed: 00 00 00 01 06 0011 22 33 44 55 20161216134600

(4 bytes of transaction amount + 1 byte of transaction type ID + 6 bytes of terminal number + 4 bytes of terminal transaction date + 3 bytes of terminal transaction time)

Key: C08346DF9F1D457A

Results: D45737C5

Consumption Command:

805401000F00000000201612161346000D45737C508

8054-CLA and INS

0100-P1 and P2

00000000 - Terminal transaction serial number

20161216 - the date of the terminal transaction

134600 - terminal trading hours

D45737C5-MAC1

Consumption commands and return data:

805401000F00000000201612161346000D45737C508

<= 8a f2 70 dc 66 b5 4a 6b 90 00

TAC Calculation:

MAC Encryption Algorithm-CBC (PBOC-MAC)

Key:

8888888888888888

(8 bytes of XOR left and right of the internal key)

Processed data:

000000010600112233445500000000020161216134600

(4 bytes of transaction balance + 1 byte of transaction type ID + 6 bytes of terminal number + 4 bytes of terminal transaction serial number + 4 bytes of terminal transaction date + 3 bytes of terminal transaction time)

Results: 8AF270DC

Card: 8A F270 DC

MAC2 COMPUTE:

MAC Encryption Algorithm-CBC (PBOC-MAC)

Initialization vector: 00 0000 00 00 00 00 00

Data processed: 00000001 (4 bytes of transaction amount)

Key: C08346DF9F1D457A

Results: 66B54A6B

Card: 66b54a6b

4. Summary:
1. The calculation of MAC1 in captive initialization is incorrect, because the algorithm identification is incorrect when the captive key is loaded

00-3DES

01-DES

03-255 reserved

2. The process key calculation uses the ECB mode 3DES algorithm, and the MAC algorithm of the CBC mode des is used
for MAC 3. For general consumption or storage, the CPU card is loaded with a dispersed key, and the SAM card is loaded with an undistributed key

4. In this case, no SAM card is used, and the stored consumer keys are not distributed
---