Smart card, security system, read permission, write permission, key follow-up permission

 wowocpp Posted on 2018-04-18 17:00:15 Reading: 1k Collection 4 Likes

Category Column: smart card

FMCOS has a unique security system

The security system of FMCOS can be conceptually divided into security state, security attributes, security mechanism and cryptographic algorithm .

5.1. Security Status

The security status refers to the level of security that the card is currently in.

The root directory and application directory of FMCOS have 16 different security statuses. **That is, 0 – F**

FMCOS can be a security level represented by a security status register inside the card; A value between 0 and F for the register.

The value of the security status register of the current directory is set to 0 after the reset or when the command to select a directory file is successfully executed, for example, it is set to 0 when a subordinate subdirectory is selected, and the value of the status register changes after the password verification or external authentication in the current directory is passed.

5.2. Security Attributes

A security attribute is a condition that must be met when an operation is performed on a file, that is, what is the value of the security status register required for an operation to be performed.

The security attribute is also known as the access permission, which is specified by a byte when the file is created,
which is XY, XY is hexadecimal, and the value of X is 0 – F, and the value of Y is 0 – F.

FMCOS access is different from any other operating system's access rights in that it uses a compartment to strictly restrict other unauthorized access.

Case 1: (when x is equal to 0)

If the access permission is 0Y, the value of the security status register of the MF is required to be greater than or equal to Y.
For example, if the read permission of a file is 05, the value of the MF security status register must be greater than or equal to 5 before the file can be read.

Case 2: (when X is not 0)

Case 2_1: X > Y

```
When the access permission is XY (X is not 0), it means that the value of the
security status register of the current directory must be greater than or equal
to Y and less than or equal to X.
```

Case 2_2: X = Y

```
If X equals Y, it means that the value of the security status register
of the current directory must be equal to X.
```

Case 2_3: X < Y

```
"If X is less than Y, it means that the operation is not allowed.
```

If a file has a write permission of 53,
it means that the value of the security status register of the current directory must be 3, 4, or 5 before the file can be written.
For example, if the read permission of a file is F0 and the write permission is F1, it means that it
can be read arbitrarily, and the value of the security status register of the current directory must be greater than or equal to 1 when writing.

> Execution Command: 80E0 00 04 07 28 00 0F F4 F0 FF 02
> Description:
> 80 E0: Command type and command code; Create file
> 00 04 : file ID;
> 07: length;
> 28: File type binary
> 00 0F: space size, that is, the number of bytes written to the binary;

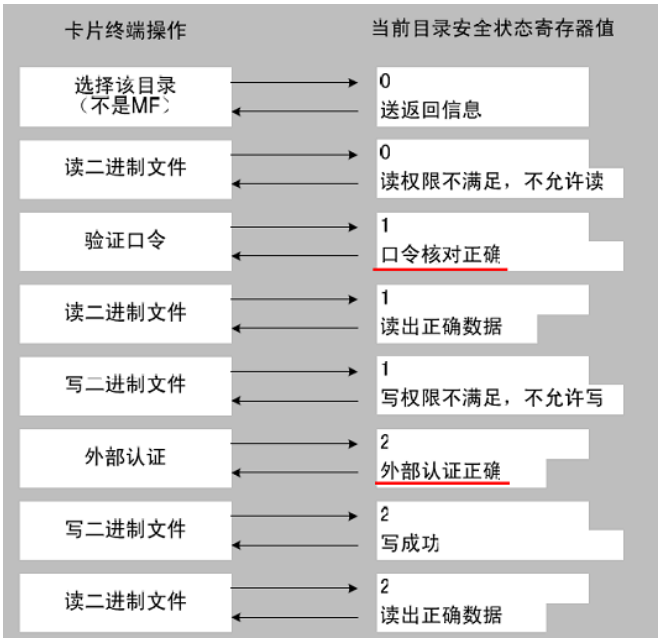
> F4: Read permission;
> F0: write permission;
> Note: The read permission here is F4, which means that the read permission can only be read when the read permission is greater than or equal to 4, that is
> , it can be read only after verifying the password, because the subsequent state of the password is 4
> and write, you can write it at will, there is no limit, that is, the security state value 0~F can write two-system data

5.3. Security Mechanisms

Security mechanism refers to the methods and means used to transfer one security state to another.
FMCOS changes the value of the security status register by **checking the password** and **external authentication**.
When the authentication is in MF, the value of the security status register of the MF and the current directory is changed at the same time,
and if it is not in MF, only the value of the security status register of the current directory is changed after the authentication is passed.
When a password or external authentication key is created, the subsequent status of the parameter indicates that the value of the security status register of the current directory is set to the subsequent state after
the password is successfully verified or the external authentication is successful.

> Example: Add the password key to the key file in the DF directory Execute the command: 80D4 0101 08 3AF0EF 44 55 12 34 56
> Description:
> 80D4: Command type and command code;
> 0101: File identification;
> 08: length;
> 3A: file type, i.e. password key
> F0: read permission;
> EF: write permission;
> 44: Follow-up status;
> 55: error count;
> 12 34 56: 3-byte PIN password

For example, if the subsequent status of a password key is 01, it means that after the password is successfully checked, the value of the security status register of the current directory is 1.
When a power-on reset is performed or a parent directory is moved from a parent directory to a child directory, or when it is returned to the parent directory, the value of the safety status register of the current directory is automatically set to 0.
In order to better understand the security mechanism of FMCOS, the following is an example:
If there is a binary file in a directory in the card, the
read permission of the binary file is defined as F1 and the
permission for write binary file is F2.
There is a password key in this directory, and the subsequent status after the password verification is 1 There is an external authentication key in the card, the use right is 11, and the subsequent status of the external authentication is 2



Reference from: "New FMCOS2.0 User Manual .pdf"