CS381 Exercise 21

Name: Zhang Yupeng

Student ID: 5130309468

1. Is it possible to clone a smartcard ?

Solution:

Generally, an EMV chip is a small microprocessor. It runs a specific application. You can't just read what it knows, but you can 'ask' it 'questions' by issuing commands from the EMV set, and see what it returns. Unlike Magstripe, it's interactive, and is capable of both answering and more importantly, refusing to answer queries.

EMV isn't unclonable, but it is significantly more difficult because now that the algorithm used in the microprocessor is unknown to the attacker and the behavior cannot be replicated. However, as the time being, there'll be a possible way.

2. What kind of properties of EEPROM are used to provide security for smartcard?

Solution:

EEPROM provides nonvolatile storage so that it can provides secure and unmodified secure logic sector for different users.

EEPROM is used for data storage, it will be seperated into different part, each has different functions in order to ensure the safety of the smart card. If the attacker want to access the data, it cannot bypass the secure logic that is around the data.

3. Describe the similarities and differences of PKCS15 and PKCS11?

Solution:

Both of PKCS15 and PKCS11 is a kind of standard. PKCS11 refers to the API to cryptographic tokens as well as the standard that defines it. PKCS 15 defines the cryptographic token information format standard.

Their usage is different. Most commercial certificate authority software uses PKCS11 to access the CA signing key or to enroll user certificate. PKCS15 allows users of cryptographic tokens to identify themselves to applications, independent of the implementation. PKCS11 emphasizes on API and PKCS15 emphasizes on the standard.

4. How is TPM used to provide security for computers?

Solution:

TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the computer. These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.

TPM can store pre-run time configuration parameters, but it is other applications that determine and implement policies associated with this information. Processes that need to secure secrets, such as digital signing, can be made more secure with a TPM. And mission critical applications requiring greater security, such as secure email or secure document management, can offer a greater level of protection when using a TPM.

By establishing the trust chain together with the BIOS, TPM is used to detect changes to previous configurations and derive decisions how to proceed. It can assure platform integrity which means behaving as intended. TPM is also used for disk encryption and password protection. Encryption-enabled applications can use TPM for digital rights management, protection and enforcement of software license, and prevention of cheating in online games.