SMART CARD SECURITY & SMART CARD APPLICATION SECURITY

By Mr. Tan Keng Boon, Executive Director Advanced Card Systems Ltd.

Introduction

No security in this world is perfect. Security is always about the cost of implementing and enforcing the security versus the cost of the fraudster to break the security and the cost to be paid for the security breach. Depending on the type of the system, the cost may or may not be limited to just monetary cost but include the reputation damages, live lost but also national security. Certainly if human live and national security is concerned then the system cost may not be the most important consideration factor. However for many commercial smart card applications, which is the subject of discussion in this paper, it must be able to bring real benefits to all parties – the application operator, cardholders and other service providers in the application. It must be able to help to make more money, lower cost and / or bring benefits to all parties in the application. Last but not least, smart card technology must be the most cost effective technology to be used.

Security in smart card applications

In any smart card application, a basic requirement is that it must be secured. The axiom for smart card application security is that the cost of enforcing the security must be much smaller than the effort to break the security and the cost to break the security must be less than the potential rewards that can be obtained after breaking the security. In an efficiently designed smart card application, the cost of the system implementation must be minimized but the security not compromised. A smart card application is a distributed system. It compromises of a number of subsystems with each subsystem doing part of the system function. The security of the system comprises of the front-end enforcement, front-end and back-end verification, backend audit and system fraud damage control. The system design always assumed a scenario of a fraud and how it can be controlled.

Security must be addressed at the system level and not to be focused on just a small subsystem or component in the system. It can still make sense to use a lower cost card which is seemingly less secured in a smart card application but it does not mean that security will be compromised. Security can still be implemented in other subsystems so that the application remains secured and meanwhile lowering the entire system cost.

To illustrate my argument, let me take a real application example of using the I2C free access memory card (e.g. 24C02) as a prepaid electricity meter card! This card is freely read and update and is therefore easily cloned. However I will show that a cloned card will not be accepted by the system. This is done as follows:

The prepaid electricity meter is installed in the house and that it shall only accept one or a limited number of prepaid cards, using 24C02 free access memory card. A prepaid card is only acceptable to the meter if the card is authorized by the authority staff card for the first time, which his authorization system will ensure that the card is not being registered with another meter. The staff card can be inserted into the meter, followed by the prepaid card so that the card is registered by the meter. The card contains a serial number, a transaction counter and a stored value. These data is MAC-ed so that it cannot be tampered with being detected. During topping up of value into the meter, the meter shall first verify that the card serial number is registered in the meter and that the transaction counter is one higher than the previous transaction. Also the MAC indicates that the data has not been tampered. Then the transaction counter inside the meter is incremented and value is transferred to the meter. The fraudster will not know the MAC of the next transaction counter since he does not have the MAC key. He needs to pay for the topup before he becomes aware of the MAC. He cannot tamper with the stored value as it will be detected. A cloned card cannot be used as the meter expects the counter to be incremented in the card! This illustrate that even with a free access memory card, security can be achieved if the system security design is done correctly.

Is smart card really secure?

There has been some publicity in the smart card industry about how Mifare card can be cloned. People without good understanding about smart card application security design tend to focus only on the smart card and its algorithm. Cryptographic algorithm in memory smart card such as Mifare certainly cannot be compared to CPU smart card. Competent smart card application designer using such type of card must implement other security measures in the card mapping design and in other subsystems to strengthen the application security, which will be discussed shortly. On the other hand, an incompetent designer, even if he uses the most secured card in the world there can still be a security loophole that can be fraud by any one. Take this simple example:

1. Clone a multi-services prepaid card such as an Automatic Fare Collection card graphically, including the card number printed on the card.
2. Topup the genuine card to the maximum limit.
3. Destroy the cloned card chip by putting into a microwave oven to kill to fake card.
4. Report that the clone card is not working and wait for the refund.
5. After getting the refund, use the genuine card.

Here you can see that many application designers may not think about blacklisting a dead card, and if so there is a security loophole. The same technique can be used to steal control / management smart card in the application system by replacing the genuine card with a dead fake card and nobody will suspect a potential fraud! A good system designer is able to avoid a fraud or even if there is a fraud, the system design is able to quickly spot it and then control and then stop the fraud.

How to increase the security of smart card?

There are a number of design measures that can increase the security of smart card.

1. MAC-ing of the Unique Identification number (UID)

Smart card like Mifare comes with a unique chip number (UID), guaranteed by the manufacturer. The designer can attached a MAC or message authentication code to the UID, possibly also including some other data like a customer ID. A MAC is an encryption of a block of data with a secret key. This MAC is verified by the application terminal, and to be more precise the SAM (Security Application Module) in the terminal. This is a first level to block out any un-authorized cloning of the card as someone trying to clone a card will have a different UID.

2. Key Diversification

Key diversification ensures that the cryptographic key in each card is unique. This is typically achieved by encrypting a master key with the card UID. Security is further increased by requiring the SAM to do the key diversification if and only if the MAC of the UID is correct.

3. Transaction Counter

Transaction counter can be an incrementing or decrementing counter. It changes with each transaction. The counter can be used to generate unique per transaction certificate. The certificate is verify before a transaction takes place, and is updated after the transaction using the new counter. Of course anti-tearing measures to prevent data corruption is required. A value block of the Mifare card is deal for this purpose.

4. Data Certificate

From a security point of view, it may not be sufficient to just rely on the stored value in the value block of the Mifare card. A certificate computed using the transaction counter, balance and say triple DES can be used to protect the stored value.

5. Debit Certificate

An good electronic purse smart card must be able to return a debit certificate to prove that the card has indeed the transaction amount. Some CPU smart card is unable to do that. Mifare card is also not capable to doing that. A good system security designer must understand the application requirements and exploit the card capabilities. On the other hand if the chosen card does not have such a capability, he will need to design the equivalent capability such as using the SAM to compute the certificate.

6. Credit Certificate

A reloading terminal capable of reloading an electronic purse without remote authorization and control is an electronic cash money printing factory ! It must also ensure that reloading transaction cannot be replayed. The security issue would be much higher than the possible cloning of individual cards. The concept of protecting stored value of the Mifare card with a certificate can also achieve this purpose.

7. Host Back-end Auditing

Host backend auditing ensures that in an unlikely event that there is a fraud, it will be detected. A fraud is only meaningful if the illegally created money outside the system is used inside the system. If it is used inside the system, it will be detected. Fraudulent card will then be blacklisted.

"Technically Mifare card can be emulated. However if the system security design is correct, fraud is only possible with a colluding cardholder or a merchant."

Conclusion

Technically Mifare card can be emulated. However if the system security design is correct, fraud is only possible with a colluding cardholder or a merchant. One cannot expect a merchant to accept a payment with the cardholder carrying a big emulator to pay for the transaction. We will need to invest in the semiconductor design, then manufacture into wafe and then make it into a contactless card to fraud and have the card blacklisted the next day.

The above design measures will improve the security of the smart card application even if a low cost card like Mifare is used. Mifare is attractive because the price difference compared to a CPU contactless card is at least double! There can be tremendous cost saving by using a cheaper card but with a good system security design.

Security is never perfect. It is always about the cost of enforcing the security must be much smaller than the effort to break the security and the cost to break the security must be less than the potential rewards that can be obtained after breaking the security.

● This article was authored by Mr. Tan Keng Boon, Executive Director, Advanced Card Systems Ltd.
Email: kengboon@acs.com.hk