Security of Smartcard Based Payment Protocol

Petr Hanáček

Department of Computer Science and Engineering,
Faculty of Electrical Engineering and Computer Science
Technical University of Brno
Božetěchova 2, 612 66 Brno
e-mail: hanacek@dcse.fee.vutbr.cz

ABSTRACT: *The article deals with the problematics of electronic payment systems and electronic money. Recently a new payment instrument has emerged: the multipurpose prepaid card or "electronic purse". It is a plastic card which contains real purchasing power, for which the customer has paid in advance. Although developments in the field of electronic purses are only at an early stage, the possibility of proliferation of such cards is a real one. In the future, if electronic purses were used in a great number of retail outlets, they would become a direct competitor not only to cashless payment instruments already in existence, but also to notes and coins issued by central banks and national authorities.*

Keywords: electronic payment protocols, retail banking, home banking, electronic purse, SEPP, STT, SET

Introduction

The term "electronic money" (according to [SEM96]) has been used in different settings to describe a wide variety of payment systems and technologies. "Stored-value" products are generally prepaid payment instruments in which a record of funds owned by or available to the consumer is stored on an electronic device in the consumer's possession, and the amount of stored "value" is increased or decreased, as appropriate, whenever the consumer uses the device to make a purchase or other transaction. By contrast, "access" products are those typically involving a standard personal computer, together with appropriate software, that allow a consumer to access conventional payment and banking products and services, such as credit cards or electronic funds transfers, through computer networks such as the Internet or through other telecommunications links.

The problematics of electronic money is tightly coupled with the problematics of information system security and mainly with the problematics of cryptography. The design of functional electronic payment system is not so difficult. The design of functional and secure payment system is quite difficult and security mechanisms are usually the most important part of the payment system.

Basic principles of electronic money

This section provides a general overview of the electronic payment systems products which we are interested in. Figure 1. illustrates the general structural model common to most electronic money systems, including participants and their interactions.

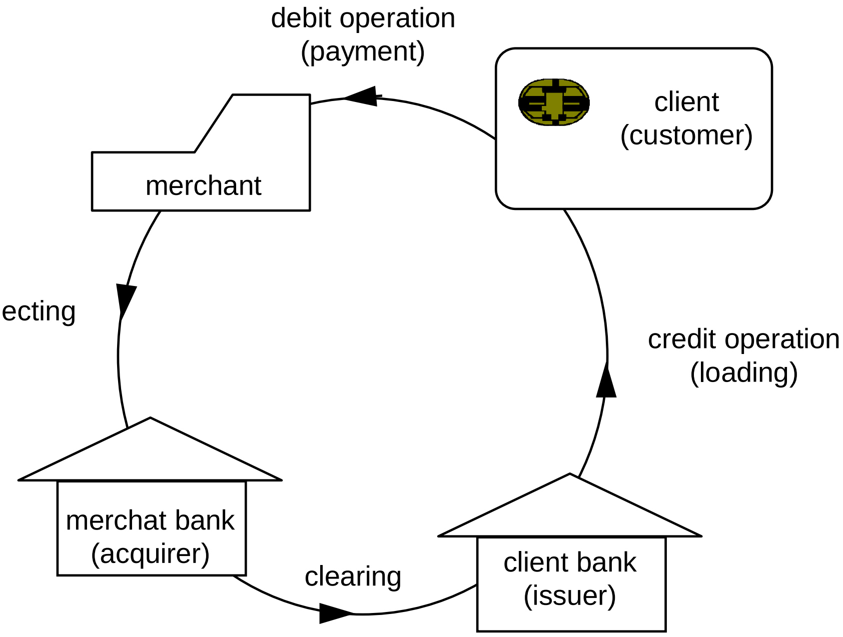

Fig. 1. General structure of electronic payment system

Electronic payment system contains following parties:

- *Client* (customer) - party that gets electronic money from client bank (issuer) and pays to the merchant.
- *Merchant* - party that gets electronic money from client and send these money (in the form of payment transactions) to the merchant bank (acquirer).
- *Acquirer* (usually the bank of merchant) - party that gets the transactions (i.e. electronic money) from its merchants and clears these payment transactions with appropriate issuer (client bank).
- *Issuer* (usually the client bank) - party that gives the electronic money to its clients and later receives these money from the acquirer.

The actions in this model are:

- *Credit* (loading) means transferring the monetary value from the issuer to the payment instrument (e.g. electronic purse) of client.
- *Debit* (payment) means transferring the monetary value from payment instrument of client to the payment instrument of merchant (which is usually payment terminal). In the terminal is then created payment transaction, that contains the electronic money and other payment details.
- *Transaction collecting* means transferring the payment transactions from the merchant to the acquirer.
- *Payment clearing* means clearing of payment request between acquirer and issuer.

From the security point of view the most sensitive operations are credit and debit. The main threats are concentrated in these two operations. These threats include using of fake payment instrument, modifying communications of payment instrument, and illegal crediting.

Other two operations are less sensitive and the probability of security incident during these operations is much smaller.

Physical devices, such as smart cards or personal computers, are held by clients and by merchants. Merchants interact with clients and with their acquiring bank or other collection point, such as a third-party payment processor. Issuers receive funds in exchange for prepaid balances distributed to clients and manage the "float" in the system that provides financial backing for the "value" issued to consumers. In some cases, other intermediaries, such as banks, retailers or service providers, distribute stored-value devices and balances directly to consumers. The system may include a central clearing house or system operator.

Taxonomy of electronic payment systems

Generally there are two kinds of electronic payment systems - on-line systems and off-line systems. *On-line* systems require direct communication connection with the electronic money issuer (usually the bank) during every transaction (credit or debit). *Off-line* systems allow to perform payment transaction without such on-line connection with the issuer.

From privacy point of view the payment systems are divided to *identifiable* and *anonymous*. Identifiable payment system allows the issuer of electronic money to identify the participants of every transaction and gives him the possibility to trace the path of electronic money. Anonymous payment system preserves one of the property of real metal coins - the anonymity and untraceability. The issuer has no possibility to follow the path of electronic money. The anonymity of the payment system is, especially in past, quite desirable property of the payment system.

We also distinguish whether the payment system uses the intelligent token - *smart card* (sometimes called also *electronic purse* or *electronic wallet*) or it uses only non-intelligent payment instrument.

Next criterion is whether the payment instrument (magnetic card, smart card, personal digital assistant, personal computer) carries in itself an electronic monetary value (systems *with electronic money*) or it does not carries any value (systems *without electronic money*).

If the system uses the electronic money, we consider the implementation of value in the payment instrument. The value can be implemented using a *counter* (counter based systems) or using *electronic coins*.

According to the cryptographic mechanisms that are used, the electronic payment systems are based on *secret-key cryptography* or on *public-key cryptography*.

The taxonomy of electronic payment systems is shown at the following figure:

- Electronic payment systems (EPS)
    - EPS without electronic money
        - electronic banking (e.g. any home banking)
        - magnetic payment card (e.g. credit card)
        - payment smartcard (e.g. VISA Easy Entry)
        - network system without electronic money (e.g. SET)
    - EPS with counters
        - prepaid smartcard card (e.g. telephone card)
        - electronic purse with electronic cheques (e.g. UEPS)
    - EPS with electronic coins
        - electronic purse with electronic coins (e.g. CAFE)
        - network payment system with electronic coins (e.g. e-cash)

Fig. 2. Taxonomy of electronic payment systems

Proposed system of smart card based electronic purse

In following sections we will describe the proposed payment system, that is developed on the Department of Computer Science and Engineering, TU Brno. This payment system is developed in the framework of development the student smart card, that except other functions should have a property of electronic purse for closed payment system. The proposed system according the previously defined taxonomy is an *electronic purse with electronic cheques*, i.e. the system with counters.

The payment instrument contains inside a counter. The value of the counter is equivalent to the monetary value, that is stored in the payment instrument. The value of the counter can be changed using two operations - debit and credit. These two operations are equivalent to the two commands of payment instrument and have following semantics:

Operation **CREDIT (VALUE)** increments the COUNTER by value VALUE. Input parameter of this operation is a credit value VALUE. The operation has no output parameters - returned is only the status that indicates successful performing the operation.

Operation **DEBIT (VALUE)** checks whether value of the COUNTER is greater or equal than VALUE. If this is not the case, operation immediately quits with status that indicates not successful performing of operation. Otherwise the operation decrements the COUNTER by value VALUE. Input parameter of this operation is a credit value VALUE. The operation has no output parameters - returned is only the status that indicates successful or unsuccessful performing the operation.

From the functionality point of view are these operations correct. From the security point of view are operations with such semantics not suitable, because they do not prevent against following attacks:

- Tampering with the payment instrument. The value of counter can be modified (of course, increased) not only by performing the credit operation, but also using direct logical or physical manipulation with the payment instrument. These manipulations include patching in the case of software payment instrument or electrical tampering (e.g. using a microprobes injecting electrical signals) in the case of hardware payment instrument.

- Using of fake payment instrument. This instrument emulates the behaviour of debit operation and gives to the client infinite amount of money without any crediting.

- Modifying the communication between payment instrument and payment terminal. The communication could be modified in such way, that negative status code from unsuccessful debit operation is changed to positive status, although the payment instrument does not contain enough money to perform paymemt.

- Illegal crediting of genuine payment instrument. This attack can be done simply by performing the credit command on the payment instrument.

In the following text we would like to describe the security concept of these two most sensitive operations - debit and credit - that prevents above attacks. The first attack is prevented by using the tamper resistant hardware and next three attacks are prevented by using cryptographic protocols.

The role of tamper resistant hardware

The concept of tamper resistant hardware is tightly coupled with the concept of reference monitor. The reference monitor was defined in [AND72] and was standardized in [TCSEC]. The reference monitor concept was found to be an essential element of any system that would provide multilevel secure computing facilities and controls. Reference monitor is also a heart of the most of cryptographic modules using secret-key cryptography. An usual implementation of reference monitor is a reference validation mechanism, so we will define the reference monitor in the this implementation (see [TCSEC]). Reference validation mechanism as "an implementation of the reference monitor concept that validates each reference to data or programs by any user (program) against a list of authorized types of reference for that user." Three design requirements that must be met by a reference validation mechanism are:

a. The reference validation mechanism must be tamper proof.

b. The reference validation mechanism must always be invoked.

c. The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured.

The implementation of this concept in described payment protocol is done by using the smart card as a payment instrument. The used smartcard has such physical and logical properties that it complies to the three above conditions. The conditions are met in following ways:

a. The reference validation mechanism is tamper proof because of physical properties of the used smartcard, that is designed as secure hardware, that is resistant against physical, electrical, electro-magnetic, and chemical tampering.

b. The reference validation mechanism is invoked because of communication protocol, that is the only way to communicate with the smartcard.

c. The reference validation mechanism is small enough to be subject to analysis and tests, because of simplicity and standardization of the communication protocol that is used.

Smart card used

The used smartcard is *AT card*, developed at Department of Computer Science and Engineering, TU Brno. AT card is an authentication smartcard, adapted to cryptographic and prepaid card applications. It incorporates the ISO 7816-4 standard commands and return codes. AT card operating system must fulfill two main functions:

i) Be a general purpose operating system for smart card applications.

ii) Provide security processing for authentication and prepaid applications

For the card user, the applications of AT card are many. Personal data such as medical history could be stored. It is possible to support financial applications such as EFTPOS, or to implement electronic wallet/cheque book functions all easily and securely from within the AT card system. In fact any application requiring the storage and retrieval of small to medium volumes of data with restricted or general access is possible from within the AT card structure. Use of recognized international standards where applicable makes the system acceptable across national boundaries making both the cards and the application developed for them internationally acceptable.

The communications protocol conforms to ISO/IEC 7816-3 in order to make the card readable from general purpose reading equipment. To achieve reliable and secure data transfer data encryption is based on the ANSI DES (X3.92-1981) algorithms, ANSI 3-DES algorithm and proprietary TEAX algorithm. Message authentication is based upon ANSI X9.9-1982.

The following list summarizes the AT card commands:

- VERIFY - Compares a card holder verification value (PIN) against a reference value.
- SETPIN - Changes the card holder verification value (PIN).
- READ BINARY - Reads data from a data file.
- UPDATE BINARY - Updates data in a data file.
- GET CHALLENGE - Generates an eight byte challenge and provides it to the external world.
- PUT RANDOM - Initiates the computation of the session key, based on supplied random number sent from the reader.
- INTERNAL AUTHENTICATE - Allows an external application to verify whether the card or an application on the card is authentic.
- EXTERNAL AUTHENTICATE - Authentication of the external world based on a previously generated random number and a secret key.
- DECREASE (DEBIT) - Decreases the value in a purse file by a specified amount and returns the new value.
- INCREASE (CREDIT) - Increases the value in a purse file by a specified amount and returns the new value.

Cryptographic protocol for credit and debit operations

Operations credit and debit are cryptographically secured using so called MAC (Message Authentication Code). MAC is a way how to ensure authentication (i.e. proof of origin) of the secured message and the integrity (i.e. prevention against modification) of the message.

$MAC_K(M)$ is a fixed length value, usually 32 or 64 bit long, that is the function of message M and secret cryptographic key K. This value is computed by the creator (sender) of the message and is appended to the message. The recipient of the message which knows the same secret key K as creator can compute independently the MAC value according to received message M and his key K and then compare the value of received MAC and computed MAC. If both values are equal, the recipient can be sure, that:

a) The message was created by the creator that knows the secret key K, and

b) The message was not changed during the transmission.

Unfortunately MAC is not enough to protect the messages that contain the credit and debit commands because of replay attack. Replay attack allows attacker to capture a legal message with its MAC and send it later to the recipient. It is clear that e.g. replay of message with credit command means illegaly increasing the value of payment instrument which is highly undesirable.

The solution to replay attack is to make every MAC unique by parametrizing it by the random value. The MAC value is computed over the message M and the random value Rnd that is unique for every command. Thus we need two new operations of payment instrument:

- ASK RANDOM (in AT card called GET CHALLENGE) that asks the payment instrument for random value that will be used by subsequent command
- PUT RANDOM that gives to the payment instrument the random value, created by the outside world that will be used by subsequent command

Now we can define the cryptographic requirements for the credit and debit operations:

Credit operation increases the value of counter, so the illegal performing of this command is highly undesirable and is against security policy. The command itself must be secured by the MAC to prevent illegal credits of payment instrument. Because payment instrument must prevent the outside world against fake credits, the random value for MAC must be generated by the payment instrument and retrieved by the ASK RANDOM command (in the opposite case the "fake" outside world will generate the same random value as previously and thus can perform replay attack).

Because this operation always succeeds (of course only when it is performed legally), it is not necessary to cryptographically secure the response (returned status) of this command.

Debit operation decreases the value of counter, so the illegal performing of this command is not dangerous and need not be prevented. An attacker cannot gain anything by performing of this operation. So the command itself need not be secured by the MAC.

The status of operation indicates the merchant whether the client is solvent, so the response message must be cryptographically secured against modification by MAC value. Correct MAC value indicates that the payment instrument is genuine (fake payment instrument does not know the secret key K and it is not able to compute correct MAC value). Correct MAC value also indicates that the response message was not modified, i.e. that the client had on its payment instrument enough money to pay and that his counter value was decreased. Because the outside world (in this case the merchant) must be assured that the message is authentic, the random value for MAC must be generated by the outside world and entered by the PUT RANDOM command.

The resulting protocol for the credit and debit operations is shown on the figure 3.

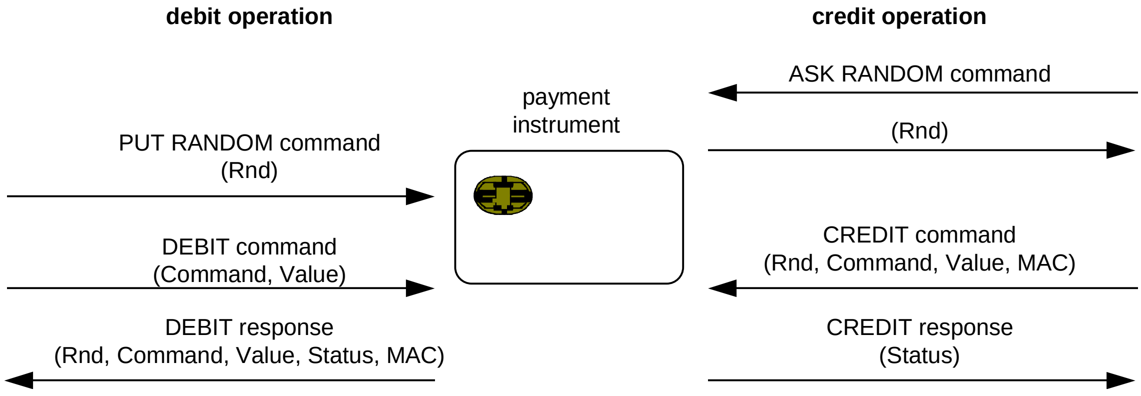
debit operation
credit operation
ASK RANDOM command
payment instrument
(Rnd)
PUT RANDOM command (Rnd)
DEBIT command (Command, Value)
CREDIT command (Rnd, Command, Value, MAC)
DEBIT response (Rnd, Command, Value, Status, MAC)
CREDIT response (Status)

Fig. 3. Credit and debit commands

Conclusion

Electronic money products have the potential to provide important benefits to payment systems if implemented with appropriate security. These systems can not be made fully secure against all types of attack. Determining the appropriate level of security for a particular system should involve consideration of the magnitude of potential risks, the cost of implementing varying levels of security, the impact on the functionality of the product and the implications for privacy.

References

[AND72] Anderson, J. P. Computer Security Technology Planning Study, ESD-TR-73-51, vol. I, ESD/AFSC, Hanscom AFB, Bedford, Mass., October 1972 (NTIS AD-758 206).

[TCSEC] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STDm December 1985, US Department of Defense, December 26, l985

[CHA90] Chaum, D. Fiat, A. Naor, M., Untraceable electronic cash. (Springer-Verlag, Berlin, West Germany, p. 319-27, 1990)(Conference: Advances in Cryptology - CRYPTO '88. Proceedings, Santa Barbara, CA, USA, 21-25 Aug. 1988)

[TUN87] Tunstall, J.S., Electronic currency. (North-Holland, Amsterdam, Netherlands, p. 47-8, 1989) (Conference: Smart Card 2000: The Future of IC Cards. Proceedings of the IFIP WG 11.6 International Conference, Laxenburg, Austria, 19-20 Oct. 1987)

[OO92] Okamoto, T., Ohta, K.: Universal Electronic Cash, Proceedings of Crypto 91, p. 324-337, 1992, Springer

[SEM96] Security of Electronic Money, Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries, Basle, August 1996