SECURITY IN ELECTRONIC PAYMENT SYSTEMS

The number of private and corporate financial transactions that are done electronically is growing rapidly. From a user's point of view, efficiency and flexibility are clear advantages of existing and emerging electronic payment systems. Due to technical progress (*e.g.,* powerful smart cards) and new developments in cryptology, these systems offer also a high level of security.

The underlying model of an electronic payment system consists of three parties—a bank, a customer and a shop. There are three different types of transactions within the system withdrawal involving the bank and the customer, payment involving the customer and the shop and deposit involving the shop and the bank. The customer's account is debited during withdrawal and the shop is credited during deposit. The three transactions take place simultaneously or separately, depending on the payment system.

Customer, shop and bank have different security requirements. The shop, receiving a payment, wants to be sure that the bank will pay the amount into its account. The bank wants to prevent fraud, *e.g.*, that an individual can deposit more money than he or she has withdrawn from another account or received during a payment. Finally, the customer does not want unauthorized persons to make payments debiting his or her account, or to lose money because of theft. Furthermore, the customer may wish to have the possibility to pay anonymously.

Not all of these security requirements have the same priority prevention of forgery is essential, but there exist well-accepted payment systems that provide no protection against loss or theft, or that do not allow anonymous payments.

We now introduce two crypto logic concepts which will be used below.

A Digital Signature

A digital signature scheme is a public key algorithm that allows to au[illegible]ticate a message by means of a piece of information, called the signature. The generation of the sigr[illegible]e requires the knowledge of the signer's private key, while for the verification of the signatur[illegible] only the knowledge of the corresponding public key is necessary. If the public key is publicly acc[illegible]e, then everybody can verify the signature, while only the signer, who knows the private key, is able [illegible]n.

There are now two parties involved in the generation of the sigr[illegible]e a sender who chooses the message to be signed and the signer who provides the sender with in[illegible]nation allowing him or her to compute the signature. The main difference to ordinary digital signa[illegible]s is that the signer does not receive any information, neither on the message nor on the resul[illegible] signature. More formally, the signer's information and the resulting message signature pair are stat[illegible]ly independent.

The concept of blind signature which is an extension of the conc[illegible] of digital signatures. There are now two parties involved in the generation of the signature—a sende[illegible]r chooses the message to be signed and the signer who provides the sender with information alle[illegible]ng him or her to compute the signature. The main difference to ordinary digital signatures is that [illegible]he signer does not receive any information, neither on the message nor on the resulting signature. More formally, the signer's information and the resulting message signature pair are statistically ino[illegible]pendent.

Anonymous Electronic Payment Systems

Usually, the security of electronic payment systems is realized by a combination of physical measures and crypto logic methods. Physical security measures depend on the current technology; therefore, technological progress may threaten seriously the existing systems. It is therefore interesting to investigate systems whose security relies solely on cryptologic methods. In this section we propose an electronic payment system that provides payer's anonymity.

CREDIT CARD PROCESSING & SECURITY POLICY

Purpose : The purpose of this policy is to establish guidelines for processing charges/credits on Credit Cards to protect against expo sure and possible theft of account and personal cardholder information that has been provided to the University of Miami; and to comply with the Payment Card Industry's Data Security Standards (PCI) requirements for transferring, handling and storage of credit card information.

Definitions

Cardholder Information Security Program (CISP) : Visa's Cardholder Information Security Program (CISP) is designed to ensure that all merchants that store, process, or transmit Visa cardholder data, protect it properly. To achieve CISP compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard.

PCI : The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

Cardholder Data : Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Card member ID (Discover) or CID - Card Identification Number (American Express) (*e.g.,* three or four digit value printed on the front or back of a payment card.

SYSTEM ADMINISTRATOR / DATA CUSTODIAN

An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems or services. Only full-time and permanent part-time employees of the University and/or third party vendors approved by IT and/or Treasury Operations may function as system/network administrators and/or data custodians.

Scope : This policy applies to all University of Miami employees, contractors, consultants, temporaries and other workers. This policy is applicable to any unit that processes, transmits, or handles card holder information in a physical or electronic format. Affiliated corporations are encouraged to comply.

have allowed debit cards issued in one country to be used in other countries and allowed their use for internet and phone purchases.

Unlike credit and charge cards, payments using a debit card are immediately transferred from the cardholder's designated bank account, instead of them paying the money back at a later date.

Debit cards usually also allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash. Merchants may also offer cash back facilities to customers, where a customer can withdraw cash along with their purchase.

Debit Card Processing

We offer flexible one-source debit/EFT processing options, including multiple authorization options, settlement and card management. Financial institutions may choose reliable and comprehensive client services support or opt for pass through processing in order to retain control and service on site.

Types of Debit Card Systems

There are currently three ways that debit card transactions are processed **EFTPOS** (also known as online debit or PIN debit), **offline debit** (also known as signature debit) and the **Electronic Purse Card System**. One physical card can include the functions of all three types, so that it can be used in a number of different circumstances.

Online debit system

Online debit cards require electronic authorization of every transaction and the debits are reflected in the user's account immediately. The transaction may be additionally secured with the personal identification number (PIN) authentication system; some online cards require such authentication for every transaction, essentially becoming enhanced automatic teller machine (ATM) cards.

One difficulty with using online debit cards is the necessity of an electronic authorization device at the point of sale (POS) and sometimes also a separate PINpad to enter the PIN, although this is becoming commonplace for all card transactions in many countries.

Offline debit system

Offline debit cards have the logos of major credit cards (for example, Visa or MasterCard) or major debit cards (for example, Maestro in the United Kingdom and other countries, but not the United States) and are used at the point of sale like a credit card (with payer's signature). This type of debit card may be subject to a daily limit and/or a maximum limit equal to the current/checking account balance from which it draws funds. Transactions conducted with offline debit cards require 2-3 days to be reflected on users' account balances.

In some countries and with some banks and merchant service organizations, a "credit" or offline debit transaction is without cost to the purchaser beyond the face value of the transaction, while a fee may be charged for a "debit" or online debit transaction (although it is often absorbed by the retailer). Other differences are that online debit purchasers may opt to withdraw cash in addition to the amount of the debit purchase (if the merchant supports that functionality); also, from the merchant's standpoint, the merchant pays lower fees on online debit transaction as compared to "credit" (offline).

WHO USES STORED VALUE CARDS?

Stored value cards are an attractive alternative for organizations that want to limit the circulation of cash and reduce the expense and administration of processing credit cards and checks. Federal Agencies currently using SVC applications include the Army, Air Force, Marines and Navy. SVC systems are installed on Army and Air Force bases in the U.S. wherever a basic training operation exists, overseas at several bases with deployed troops, as well as on ships at sea. SVC cards can be used as payment in post exchanges and post offices, ships stores, vending machines and used for MWR.

How does a stored value card work?

Typically SVC cards have no value until they are activated and have funds placed on them electronically. Value can be added to cards in a number of ways, including payroll or other financial file transfer, from a credit or debit card, or from cash or checks. A card is considered "active" once it has been assigned to an individual and loaded with financial value. Depending on the application, different types of cards can be issued. "Disposable" cards can be used to purchase goods and services up to the value remaining on the card and discarded when the value is fully expended. "Re-loadable" cards are issued with an initial value and are capable of having additional value added to them at the cardholder's direction. Some SVC cards have the added ability to also serve as a debit card, allowing cardholders access to ATM's and merchants around the world who accept debit and credit cards.

Both the SVC and the back-end financial system processor keep track of the balance on the card and systematically perform an accounting and control function.

How big is the stored value program?

Since the program's inception in 1997, approximately 4 million cards have been issued and placed into service representing over $3.9 billion in value. Annually, over 80 million retail transactions are performed with merchants on military bases and ships around the world.

How secure are stored value cards?

Security is one of the great advantages of Stored Value Cards. The cards use multi-layered, integrated chip circuitry to control access to funds. This technology is more secure than the mag-stripe technology used to authenticate credit and debit card transactions. Both the card and the user can be authenticated using a combination of encrypted security "keys" and user PINs.