SMART CARDS - UTILITY, APPLICATIONS AND VULNERABILITIES

Ana Maria Mihaela Tudorache, Mihai Tiberiu Iordache
Romanian American University, IMSAT, Bucharest, Romania
tudorache_ana_maria@yahoo.com, mihai.iordache@imsat.ro

Key words: smart cards, e-payment, vulnerabilities, security

Abstract

The Internet has taken its place beside the telephone and television as an important part of people's lives. Consumers use the Internet to shop, bank and invest online. Most consumers use credit or debit cards to pay for online purchases, but other payment methods, like "e-wallets," are becoming more common. But not all the payments are safe there are a lot of fake sites, hackers, viruses.

1. Introduction

For some industries the internet has already become an important distribution channel with very high growth rates (e.g. travel, books, tickets, software). Traditional retailer segments along with the media and other industries have been experiencing increasing competitive challenges stemming from the new electronic distribution channels.

In recent years, national retail champions in many European countries have chosen to expand their business spectrum and have started to introduce multi-channel strategies. Hence it comes as no surprise that national online shopping statistics identify high market shares concentrated on online merchants with very popular local brands that are often based on/have in parallel a physical presence as "bricks and mortar" stores.

Most online shoppers use credit cards to pay for their online purchases. But debit cards — which authorize merchants to debit your bank account electronically — are increasing in use. Your debit card may be an automated teller machine (ATM) card that can be used for retail purchases. To complete a debit card transaction, you may have to use a personal identification number (PIN), some form of a signature or other identification, or a combination of these identifiers. Some cards have both credit and debit features: You select the payment option at the point-of-sale. But remember, although a debit card may look like a credit card, the money for debit purchases is transferred almost immediately from your bank account to the merchant's account. In addition, your liability limits for a lost or stolen debit card and unauthorized use are different from your liability if your credit card is lost, stolen or used without your authorization.

Other electronic payment systems — sometimes referred to as "electronic money" or "e-money" — also are now common. Their goal is to make purchasing simpler.

Some Internet-based payment systems allow value to be transmitted through computers, sometimes called "e-wallets." You can use "e-wallets" to make "micro-payments" — very small online or offline payments for things like a magazine or fast food. "E-wallets" may work by using some form of stored value or by automatically accessing an account you've set up through a computer system connected to your credit or debit card account.[1]

2. E-payments and smart cards

E-payments are payments that are initiated, processed and received electronically. The electronification of payment services started many years ago and has reached a high level of maturity in many European countries. The first stage of innovation, process innovation, changed the way interbank payments are processed but went almost unnoticed by the public. Further stages of innovation were more visible, since they affected the way that customers interacted with their banks.

Most notable was the product innovation of electronic banking, e.g. ATMs, card payments and remote banking facilities. The banking industry was the main driving force behind these developments, which were primarily aimed at cost-saving and gains in efficiency (see Figure 1).

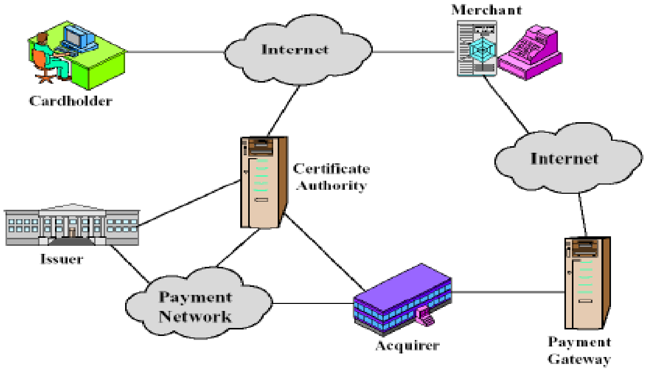

Figure 1 Secure Electronic Transaction Components

In practice, monetary claims used for e-payments constitute either claims held with commercial or central banks (deposit balances), or electronic money (e-money). New Community legislation permits e-money as a new means of payment.[3] Recently, where the regulations have permitted this, liabilities of non-banks have also been used as acceptable claims (see Table 1).[4]

Basic payment instruments	**Means of payment**
Banknotes and coins	Claims against the central bank (central bank money)
Credit transfers	Claims against commercial banks (commercial bank money)
Debit instruments, including credit and debit cards	Claims against commercial banks (commercial bank money)
New payment instruments and related services	**Means of payment**
Electronic money and pre-funded payment schemes	Claims against e-money institutions (e-money), against commercial banks (e-money) or against companies (“company money”)
Cumulative collection services	Claims against commercial banks, e-money institutions or companies
Payment portals and integrated payment solutions	Claims against commercial banks, e-money institutions or companies
Mobile payments (m-payments)	Claims against commercial banks, e-money institutions or companies

Table 1 Classification of payment instruments and means of payment

In the European Union, the provision of bank deposits and electronic money is restricted to credit institutions. According to Directive 2000/28/EC of the European Parliament and the Council, credit institutions are either undertakings whose business it is to receive deposits/other repayable funds from the public and to grant credits for its own account, or that are e-money institutions.[2]

A smart card, chip card, or integrated circuit card (ICC), is in any pocket-sized card with embedded integrated circuits which can process data. This implies that it can receive input which is processed — by way of the ICC applications — and delivered as an output.

A "smart card" is also characterized as follows:

- Dimensions are normally credit card size. The ID-1 of ISO/IEC 7810 standard defines them as 85.60 × 53.98 mm. Another popular size is ID-000 which is 25 × 15 mm (commonly used in SIM cards). Both are 0.76 mm thick.

- Contains a security system with tamper-resistant properties (e.g. a secure crypto-processor, secure file system, human-readable features) and is capable of providing security services (e.g. confidentiality of information in the memory).

- Asset managed by way of a central administration system which interchanges information and configuration settings with the card through the security system. The latter includes card hot-listing, updates for application data.

- Card data is transferred to the central administration system through card reading devices, such as ticket readers, ATMs etc.

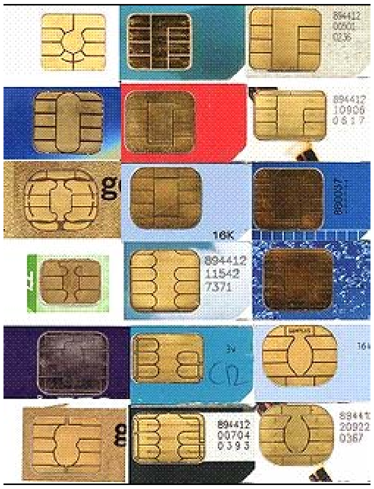

Figure 2. Many different pad layouts
can be found on a contact Smart card

3. Smart cards applications

Smart Cards provide a new set of technologies with a great deal of promise. Smart Cards provide a secure, portable platform for "any time, anywhere" computing that can carry and manipulate substantial amounts of data, especially an individual's personal digital identity. Java's portability allows Smart Cards to become a general-purpose computing platform and creates a potentially huge market for application software and development. Whether this market will diversify in the way personal computing has remains to be seen.

Still, there are some clearly defined markets that will adopt Smart Cards in the next few years. The most immediate areas in which Smart Cards have been establishing their positions include (see Figure 3):

- Financial services - Financial institutions are looking to use Smart Cards to deliver higher value-added services to businesses and consumers at a lower cost per transaction. These services include money on a card, corporate card programs, and targeted marketing programs based on analysis of consumers' buying patterns. Smart cards may also be used as electronic wallets. The smart card chip can be loaded with funds which can be spent in parking meters and vending machines or at various merchants. Cryptographic protocols protect the exchange of money between the smart card and the accepting machine. There is no connection to the issuing bank necessary, so the holder of the card can use it regardless of him being the owner.

- Affinity programs - Airlines, retailers, and other companies that offer a range of ancillary services and loyalty programs along with their basic product want to use Smart Cards to deliver these programs with a higher level of service, improved ease of use, and at a lower cost. For example, airlines want to use Smart Cards not only as a vehicle for issuing and carrying tickets - even though the single benefit of being able to securely order/provide a ticket directly to chip cards via the Internet is substantial. Airlines also want to use the cards to provide tie-ins to their frequent-flyer programs and to cross-marketing deals with auto rentals and hotels, as well as to provide simplified access to private airline lounges.

- Secure network access - Smart Cards can carry an individual's digital signature. With this ability, they provide a special mechanism to secure access to computer networks within a corporation, they help ensure that only individuals with the proper authority can get access to specific network resources, and they reduce the likelihood that hackers can break into a system.

- Computer security - The Mozilla Firefox web browser can use smart cards to store certificates for use in secure web browsing. [6] Some disk encryption systems, such as FreeOTFE or TrueCrypt, can use smart cards to securely hold encryption keys, and also to add another layer of encryption to critical parts of the secured disk [7]. martcards are also used for single sign-on to log on to computers.

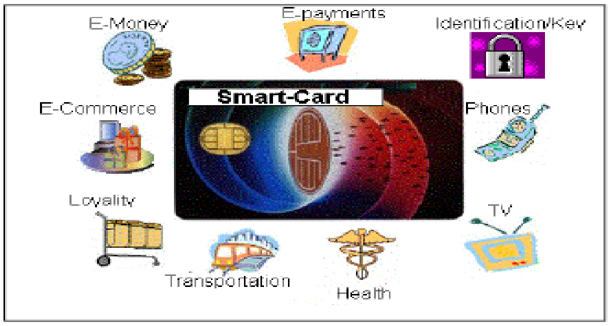

Figure 3 Smart cards applications

Other Applications of Smart Cards technology include: Government, Healthcare, Information Technology, Mobile Communication, Banking, Loyalty Programs, Mass Transit, Driving Licensing, Electronic Toll Collection, Telephone Cards, etc. [5]

4. Smart cards vulnerabilities

The security community has more or less a clear picture of what the side channel vulnerabilities of smart cards are, what the threat models are, and how to mitigate side-channel attacks on smart cards.

There are two main reasons why smart cards were the first type of devices that was analyzed extensively from the side-channel point of view. Smart cards store secret values inside the card and they are especially designed to protect and process these secret values. Therefore, there is a serious financial gain involved in cracking smart cards, as well as, analyzing them and developing more secure smart card technologies.[10]

While the flexibility of smart cards gives them many uses for businesses—access control, ecommerce, authentication, privacy protection—it can also be susceptible to attacks. Smart cards have the following vulnerabilities:

- Attacks by the cardholder: against the terminal, against the data owner, against the issuer, against the software manufacturer
- Attacks by the terminal owner against the issuer
- Attacks by the issuer against the cardholder
- Attacks by the manufacturer against the data owner [9]

5. Conclusion

Internet is the most important part of any e-payment, electronic payment being a very large area from global economic process. Banks did the first step into innovation, using more and more e-payments and online banking. Every electronic transaction must be secure.

Smart cards used for client-side identification and authentication are the most secure way for example internet banking applications, but the security is never 100% sure. In the example of internet banking, if the PC is infected with any kind of mal-ware, the security model is broken. Security is an important problem of digital economic, specially, on secure electronic transactions.

Security is the degree of protection against danger, loss, and criminals. Individuals or actions that encroach upon the condition of protection are responsible for a "breach of security." Smart cards have many forms and details, from a region to another.

Smart cards have a lot of application, being more popular in last 4-5 years. In the future, all industries would use this type of cards, and every human being would have a chip in its skin, a biometric chip. The information from this chip would be personal information.

References

[1] http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec01.shtm
[2] http://www.ecb.int/events/pdf/conferences/epayments2004/epaymentsconference-issues2004en.pdf
[3] Directive 2000/46/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions (E-money Directive)
[4] ECB, Electronification of payments in Europe, Monthly Bulletin, May 2003
[5] http://people.cs.uchicago.edu/~dinoj/smartcard/
[6] http://www.mozilla.org/projects/security/pki/pkcs11
[7] http://www.freeotfe.org/mobile_site/index.html
[8] http://www.smartcard.co.uk/tutorials/sct-itsc.pdf
[9]http://www.hackerz.ir/e-books/The.International.Handbook.of.Computer.Security.eBook-EEn.pdf
[10] http://ir.library.oregonstate.edu/jspui/bitstream/1957/3810/1/mythesis.pdf