Global Information Assurance Certification Paper

Smart Cards: How Secure Are They?

By John Abbott
GSEC Practical v1.3
Submitted March 1, 2002

Introduction

Some people believe that the small, tamper resistant nature of smart cards make them an ideal solution to many of today's computer security problems. Others believe that smart cards dependence on external systems for communication and the large number of different parties involved in smart card systems makes them vulnerable to attacks. Who is right?

To understand these arguments, we will look at the history, types and uses of smart cards and how they may be vulnerable. Since smart cards were never designed to be stand-alone systems, we will look at some of the applications that have incorporated smart cards into their design to see how they work, potential motivation for why they might be threatened, and review some of the documented attacks. Next we will look at the how to do the cost/benefit analysis of incorporating smart cards. At the end we will determine how secure smart cards really are based on the analysis in the rest of this paper.

Short History

Integrated circuit cards (ICCs) have patents dating back to 1968 in Germany, but they were not widely used until 1984 when the French PTT (Postal and Telecommunications services) successfully carried out a field trial with "telephone smartcards"[1]. Since then, they have become widely accepted in Europe. Recently they have started to break onto the scene in America with the American Express "Blue Card"[2], Visa[3] and MasterCard's[4] initiatives and most recently with the United States Department of Defense (DOD) committing to issue 4.3 million[5] cards over the next year for physical and on-line access control.

Types of Smart Cards[1]

Smart cards are tamper resistant, credit card size devices that include an integrated circuit chip to provide data storage and processing. Most smart cards require an external interface to provide communications, power, and clock cycles.

There are many different types of cards and card characteristics by which they can be distinguished. In this paper, the cards will be broken up into two major categories: memory cards and microprocessor cards. We will mention contactless smart cards and USB tokens in this section to explain their differences, but these differences will not be

covered in the rest of the paper.

Memory Cards
Memory cards are ICCs designed to store and protect information on the card. The cards can hold considerably more data than the magnetic stripes currently on credit cards and provide enough logic to protect that data from unauthorized read and/or write access.

Microprocessor Cards
Microprocessor cards contain a true CPU and RAM to allow for data processing other than just the protection of the data from unauthorized access. Some of these cards specialize in the math calculations required for cryptography functions, others are made to support specific programming languages such as Java cards, and others are made to do both.

USB Tokens[6]
According to Rainbow Technologies, USB tokens are "technologically identical to Smart Cards, with the exception of their form factor and interface". These tokens often contain the same type of ICCs that are in Smart Cards, but interface through a USB port instead of requiring a separate reader. These physical and interface differences provide both pros and cons in terms of the security of these devices, but these differences go beyond the scope of this paper.

Contact vs. Contactless Smart Cards
The main difference between contact and contactless Smart Cards is that contact Smart Cards must have a physical connection to a reader in order to work. Contactless Smart Cards communicates with the reader and derives its power from radio frequencies[7]. Contactless Smart Cards normally need to be within 10cm of the reader to operate and communicate.

The cost of the contactless Smart Cards has prevented them from becoming widely popular. Since these do not represent a significant market share and most of the security implications are the same as contact smart cards. They will not be discussed in this paper.

Card Uses

The potential for Smart Cards is enormous, but for the most part the uses can broken down into three main functions: information storage, stored value, and access tokens. Microprocessor cards have enabled a single card to handle any combination of these functions. This paper will discuss each of these categories, provide examples, and then explain how these functions may be integrated into multi-function cards.

Information Storage Cards
Information Storage Cards are cards that are used to store information that generally

needs to be kept with a person. Control over who can write this information is critical to its integrity. In some cases, control over who can access this information is just as critical due to the need for privacy.

In the wake of the September 11th tragedy, there has been some talk about a national ID card or using smart cards to help track legal aliens in this country. Airlines have even proposed using these cards for their frequent fliers and as an additional security measure to help verify that a person is not a terrorist[8].

Other countries have either implemented or discussed implementing a medical records card. This would keep a person's medical history on a card so that the information, including their current medication would be readily available in case of an emergency[9].

Stored Value Cards[10]

Stored value cards allow for small value transactions to take place without the need for immediate verification from a remote resource. Stored value cards, in the form of phone cards, were the first large market for smart cards. This was because the phone companies in Europe because the phone companies needed a more reliable to get their payment

Basically what happens is an issuer, like a bank or credit card company, will take a person's money, either from their bank account, credit card, or as cash, and give them a card with a specified amount of money "stored" on it. That person can then use the card by inserting it into a pay phone, vending machine, subway turnstile, or other machine that will accept it as payment. The machine accepting the payment will decrement the value in the card and keep track of the card number and transaction amount. At some regularly scheduled interval (Hourly, daily, weekly, monthly), the information from the machines accepting the payments are collected, transmitted, and reconciled with the company that issued the smart cards. The issuing company will then reimburse the company that collected the payments.

As mentioned above, the three most popular uses of stored value cards are cash cards for vending machines, pre-paid phone cards, and mass transit tokens.

Access Token Cards

Access tokens can be used for many things and implemented in many ways. They can be used to generate tokens to provide either physical or electronic access. Physical access may be to a specific set of buildings, rooms, or machines each of which can be further restricted by time of day, day of the week, or other specific parameters. Electronic access may include not only the initial authorization, but also on-going secure communications to various types of accounts (banking accounts, credit card accounts, computer accounts, networking accounts, cell phone accounts, etc.). These cards normally will have built-in cryptography functions to provide hashing, digital signature, and encryption capabilities

on the cards

Depending on the type of access and the required controls, the card can be used in different ways. The simplest case is when card itself provides the access. This is becoming more common with hotels. A PIN number might also be used with the card to enable an application to access a password or other information stored on the card. This implementation is sometimes used to help reduce the number of passwords a user has to remember. Multiple passwords can be stored on the card and unlocked with a single PIN number. The card can also store public and/or private encryption keys that it will use to digitally sign and/or encrypt messages.

Multi-Function Card

Multi-Function Cards allow the same card to be used for multiple applications. These cards normally have a processor that includes not only the basic security provided for storage and retrieval of information, but also the ability to support customer defined applications. Most cards also provide support for built in cryptography functionality. There are several multiple application operating systems currently available. These include Windows for Smart Cards[11], MULTOS[12], and Java Card[13].

These cards are becoming fairly common on college campuses where they are used for identification cards, physical access control, network access control, cafeteria cards, etc. The common access card (CAC) being issued by the DoD is also a multi-function card.

Potential Smart Card Vulnerabilities

Although smart cards are supposed to be "hacker resistant", they are not "hacker proof". There have been several types of smart card vulnerabilities that could have, or potentially be, exploited. Some of these attacks are explained below:

Differential Power Analysis[14]

Differential Power Analysis (DPA) uses statistical analysis of the power used by a smart card during cryptographic functions to determine the secret keys stored on the card.

Timing Attacks[15]

A timing attack precisely times private key operations on a smart card and analyzes this information to determine important cryptographic information. Kocher has shown that it can be used to determine fixed Diffie-Hellman exponents and factor RSA keys.

DPA, Timing, and some other types of attacks[16] can be done with a relatively limited amount of equipment and access to the card, but a significant technical expertise in several areas is required.

Reverse Engineering of the Chips[17]

Reverse engineering is the ability to figure out how something works, in this case a computer chip, by examining and taking apart the item to see how it was put together and functions. In the case of computer chips, this is normally a destructive process and often needs to be done on more than one chip.

The technical ability and equipment needed to do this is quite extensive and costly. Generally this expertise is limited to governments, corporations, and other institutions that have large research and development budgets geared toward this type of research.

Flaws in Design/Implementation

By far, the most serious problem for smart cards are the attacks that exploit vulnerabilities caused by poor design or implementation of a card or system. These vulnerabilities tend to be easier to exploit, replicate[18], and therefore share among the hacker community.

Other Vulnerabilities

Other known vulnerabilities obviously exist that have not been covered. The vulnerabilities mentioned above are intended to give a flavor of some of the attacks that can be made against smart cards. There have been recommendations made on how to protect against most of these attacks and the smart card community is working hard to address known issues. But like all other areas of computer (and physical for that matter) security, there are people looking for and finding holes nearly as fast as they can be filled[19].

Smart Card Systems

In the last section we discussed how smart cards themselves might be vulnerable to an attack. But even if we magically came up with a solution to make smart cards truly hacker proof, we still have not solved the problem. Smart cards are only one component of an overall system. Attacks may exploit vulnerabilities in one or more components of a system, but the ultimate goal of most attacks on smart card based systems is to get unauthorized use of the system, not the smart card.

Attacks are always initiated, at some level, by a person. In the paper "Breaking Up Is Hard To Do: Modeling Security",[20] Bruce Schneier and Adam Shostack point out that different components of a smart card system are generally controlled by different people. Schneier and Shostack argue that this split in control opens up the system to attacks that are unique to smart card based systems.

The last statement is only true to the extent that 1) systems with split controls are opened up to a unique set of attacks, regardless of whether or not they use smart cards, and 2) every component in any system provides a set of unique vulnerabilities that are subject to attack.

The concept of a system splitting up control of a system is by no means unique to smart cards. Credit cards, ATM cards, and the entire banking system have been based on having split control long before smart cards ever existed. It can be argued that smart cards were designed as a way to better deal with this split in the electronic world.

Smart card systems can be broken up into two categories: systems that would not exist without the functionality of a smart card; and systems where smart cards provide an additional level of security.

Cash value card systems and satellite TV systems are examples of systems that would probably not exist without the security features offered by smart cards. These systems tend to be more prone to attack because they are "open" systems. Open systems are system where the card issuer does not know, and cannot control, when the card is being used.

Credit cards, mobile phones and computer authentication systems have all existed without the integration of smart cards, but smart cards can provide another layer of protection to each of these systems that make the attacks more difficult and less cost effective. These systems were able to exist before smart cards, because they are inherently "closed" systems. Closed systems have real time, two-way communications between the customer (or customer device), and the primary system.

Every system, whether or not they incorporates smart cards, needs to evaluate the overall system and determine if it is using the proper design and technology to effectively secure that system against all possible threats.

In the following sections we will look at a number of systems that can or do incorporate smart card technology into their systems, review the interaction of the different components, and discuss some of the more likely threats that may exploit the smart card component of the systems.

Cash Value Card Systems

Cash value cards are designed to allow a person to make small value purchases without having to carry around cash.

The process is started with banks, credit card companies, phone companies, transit authorities, or other large entities issuing cash value cards. These cards are then sold either directly, or through a third party retailer, to a customer. The initial cash value is stored on the card. The customer can use the card by inserting it into a machine (phone, vending, mass transit, etc) that is designed to accept it. After the purchase is completed, the value of the purchase is immediately deducted from the card. The vendor will keep track of the cash value card purchases, including the amount and card number, and report

them to the issuing company at a later time for reimbursement. The cardholder can continue using the card until the value is down to zero.

The most likely threat to this system is either a cardholder or an outside party modifying an existing card to add additional value to it or creating new cards that work like legitimate cards.[21] Since the system does not verify every transaction with the issuer at the time of the transaction, the machine that accepts the card is put into a position of trusting what is on the card at the time of the transaction. This is done because the cost of implementing the infrastructure to verify every small value transaction in real time would be more prohibitive than the potential loss caused by this type of attack.

Some of these attacks have been very costly. One reported case [18] cost Deutsche Telekom an estimated $34 million dollars. Companies that issue these types of cards expect a certain amount of loss. Since Deutsche Telekom brought in revenues of over $38 billion dollars that year, they could certainly cover this loss, but as the company looks towards the future, they have an incentive to spend millions or even tens of millions of dollars on research and development to create better cards or a more innovative system that can reduce this type of attack.

Another type of attack in a stored value card system is having a vendor over charge the smart card for the services provided. Since the card does not contain any user interface, the vendor's machine can tell the cardholder that a service cost $1 dollar and actually deduct $2 dollars from the card. Assuming the card is used multiple times with multiple vendors, it will be difficult to track how much each vendor actually deducted.

This attack can be easily countered by having each machine show the current balance of the card. The vendor that did the attack can show the modified displayed balance, but when the person uses the card at a different vendor, the discrepancy will be more apparent.

For most vendors, the additional short term revenue generated from this type of attack would not justify the loss of customer good will, the risk of losing the contract to be able to accept stored value card transactions, and the potential criminal prosecution.

Satellite TV Systems

Satellite TV Systems allow people to receive selected packages of TV programming as it is broadcast off satellites. Smart cards help limit the channels that can be clearly viewed based on the type of programming purchased with the subscriptions.

This system starts with a company that has access to a satellite that can receive and re-broadcast TV signals to Earth. These signals are generally encrypted before they are re-broadcasted. The company is responsible for purchasing the broadcast rights to the

stations or shows that it wants to broadcast, send to broadcast to the satellite and have the satellite re-broadcast the show back to Earth. The company also works with resellers to sell the equipment, installation, and programming to customers. Once the customer has the equipment installed and a subscription, the satellite company will start sending an encrypted signal indicating an equipment id and programming that the customer has valid access to. The equipment will receive that information, decrypt it, and use it to determine which broadcast signals should be decrypted and viewed clearly. The smart card is inserted into the equipment and used in the decryption process and to store the equipment id.

The primary attack on satellite TV systems involves getting free and clear broadcasts that would normally need to be purchased. The most common attack involves using "Test Cards" that emulate the real smart cards that are provided with a subscription. Like stored value cards, these attacks are possible because there is no communication from the components of the system at the customers site back to the service provider. Certain decisions made by, or forced upon, the satellite TV companies have provided additional motivation for these attacks.

One European hacker site that is no longer in existence claimed that in the early days, the satellite broadcasting companies actually caused a lot of their own problems. Apparently the company provided a 24-hour Star Trek station and made it a premium channel. For some reason, there seems to be a high correlation between hackers and Trekkies. Add to that, the encryption and scrambling methods initially used were not very sophisticated and what you end up with is a relatively weak system with highly motivated, capable people wanting to compromise it.

In North America, the satellite companies failed to reach an agreement with the Canadian government that would allow them to sell subscriptions for satellite broadcasts. However, there were no laws preventing Canadians from buying the equipment. Generally the smart cards are issued as part of the subscription. This provided the motivation for an entire country of hackers to want to compromise the smart cards used in these systems. In both Europe and North America, there continues to be an on-going battle between hackers and satellite TV broadcasters on both the technical and legal fronts[22].

Credit Card Systems

Credit cards allow people to make purchases and pay for those items at a later date.

The system starts with a credit card company setting up an agreement allowing banks or other financial institution to issue credit cards to its customers. The bank or other financial institution then issue credit cards to their customers and give the credit card company the required information. The cardholder can then go to a vendor, provide the credit card information, and make a purchase. The vendor normally has the ability to

verify with the credit card company that the card is valid and the customer has enough available credit to cover the purchase. After the purchase is made, the credit card company will reduce the amount of credit available on the card by the amount of the purchase and add that value to the vendor's account (less the transaction fee).

On a regular basis, the credit card company will give the bank an accounting of all the transactions made by the bank's customers. The bank will give the credit card company the money to cover any credit that the bank's customers have used. The credit card company will then use that money to pay the vendors. The bank will send the customer a statement accounting for all of the transactions made during a given period and expect some or all of the money to be paid. If all of the money is not paid, interest will accrue and be added to the next statement.

This system has been around for decades without smart chips on the card. Why do we need them? It has been shown that card fraud in France was reduced by 75% over a five-year period after smart chip enable credit cards were implemented.[23] The smart chip can provide better protection for the information on the card and more secure communications between the card and the credit card company during verification. The American Express Blue card allows a customer to create a one-time use transaction number to be used in place of the actual credit card number when making purchases over the Internet. This prevents someone from making multiple purchases on your credit card if they are able to steal this number on the net.

In general, the smart chip helps to prevent many types of attacks. However, the ability of the smart card to store and process information provides another mechanism for vendors and the credit card company to store and track additional information about you. Some vendors will use the card for frequent buyer or other programs. Many people consider these types of programs and the collection of other information as an attack on your privacy.

GSM Digital Mobile Phone Systems

The GSM (Global System for Mobile communications) mobile phone system is a network of secure digital communications. Many companies in countries all over the world support the infrastructure and standards required to make this system work. The system has a large network of communication towers and satellites that allow mobile phones to communicate with each other and land based phone systems all over the world.

Smart cards used in these phones, call SIMs (Subscriber Identity Modules), are used to store information about the phone number and subscriber, store private encryption keys, and support the encryption process. A customer can take a SIM card from one phone, put it into another phone and use it without any further changes. The secure communications is broken up into two parts; the first part allows the phone to

communicate with the network to identify itself and establish the connection; the second part that allows the communication between the phones to be encrypted.

The primary attacks against a GSM phone system would allow the attacker to make calls without having to pay for them. The GSM phone system is being used as an example because it is designed to work with smart cards.

Although the Smartcard Developers Association has shown that these cards can be cloned[24], the attack requires the hacker to gain access to a legitimate card and will only be successful until the legitimate owner recognizes the problem either because they find out that their card is already in use, or see the unrecognized charges on their bills. Imitations of the card cannot be used because the legitimacy of the card is verified, in real time, each time it is used.

Two Factor Authentication Logon

Authentication systems can be based on something you know (PIN or password), something you have (smart card or other physical token), or something you are (finger print, iris scan, voice recognition, etc). Two-factor authentication requires that a person meet two of these three criteria. When using smart cards, the authentication is based on something you have (smart card) and something you know (PIN).

The primary reason to attack a computer or network authentication system would be to gain unauthorized access to the computer or network. These attacks have been occurring since computers were invented and will continue as long as computers contain any valuable information.

When smart cards are incorporated into a two-factor authentication process, a process to issue the smart cards must be setup and the authentication system must be modified to recognize and deal with the smart cards. After a user is issued a card and wants to logon to a system, they put the card into the reader and enter their PIN number. The card uses the PIN number to verify the user. At this point, the system will issue a challenge to the card based on the card's public key. The card will respond to the challenge using its private key, allowing the system to authenticate the card and user.

Anybody who has dealt with computer security for any length of time can come up with any number of possible scenarios on how this system might be cracked, and some of them might even work. But none of those attacks are going to be less time consuming, complex, or costly than an attack on a normal password only authentication system.

Multi-Function Smart Card Applications

When a single card contains multiple applications, the single biggest concern would be the interaction of the multiple organizations that have applications on the card. Who

would be the issuer of the card? What would happen to the other applications if the issuer's application was cancelled or no longer needed? Could the applications legally or illegally share information on the card? What if the organizations became hostile to each other, could they set up the applications to attack each other? What about a denial of service attack?

To date, these problems haven't been major because in most cases the card issuer has owned the applications loaded on multi-function cards, but these concerns could become major problems if governments start issuing or encouraging the issuance of cards across multiple organizations[25].

Any organization planning on loading an application on smart cards issued by another organization (or allowing another organization to load an application on smart cards that they are issuing) should seriously consider the full impact of that decision. Unfortunately, this issue is about more than the security of smart cards and into organizational partnerships, trust and integration, which is beyond the scope of this paper.

Why Are They Considered "Secure"

The last couple of sections of this paper covered smart card vulnerabilities along with how and why smart card systems have been attacked. Given this, it is now time to discuss why smart cards are considered secure.

First, the cards have been designed from the inside out to be secure and tamper resistant. Since these cards were designed to be part of a split system, the system had to be designed with security in mind. Everything from the physical design, to the circuit logic, to the encryption schemes incorporated security in the design.

Second, the added encryption capabilities built into many smart cards provide a means of securely storing private keys that never need to leave the card while providing the ability to digitally sign and encrypt messages.

Third there is significant incentive for the industry to address known vulnerabilities[26] and proactively look for ways to improve existing security. Smart cards are designed primarily to be a secure device. If the industry cannot earn and keep the public's trust in these cards, they will cease to be used. In many cases, a government or specific industry will specify that cards must be certified to meet strict, documented standards before the government or industry will use them[27]. This was the case with the Department of Defense (DoD) and their Common Access Card (CAC) initiative.

Companies that use open smart card systems like satellite TV and stored value cards are attacked on a daily basis by highly motivated, technically competent people. Security specialists, especially cryptographers, have long argued that open standards subject to

industry and public critic and analysis provides much better security in the long run than security through obscurity. Not only are these systems open to public critic, but the systems provide significant motivation to analyze them. This public review and improvement cycle will continue to reduce the probability of successful attacks and make those attacks less cost effective.

Closed systems, such as credit cards, mobile phones, and logon authentication, that have incorporated smart cards have made the attacks more costly, the probability of success less likely, and reduced the overall risk to the system. These systems have benefited greatly from the improvements required to make the open systems more secure.

Cost / Benefit Analysis

Organizations, either implicitly or explicitly, make decisions based whether the cost of that decision is justified by the benefit. This is true whether the organization is hiring a new employee or building a new plant. Sometimes the determination of the value of the cost and/or benefit is more subjective than objective, but this is the nature of business. The decision on whether to implement smart cards in a system in no different.

When evaluating smart cards or other security devices, if the cost of the new feature (C_f) is less than the value of the reduce risk (RR) plus any additional benefits provided by the card (B), then the device should be implemented.

If $C_f < RR + B$, then implement

Reduced risk is defined as the initial risk R_i – risk after implementation R_a.

$RR = R_i - R_a$

Risk is defined as the probability of a successful attack S times the expected loss if a successful attack occurs L

$R = S \times L$

Therefore, if

$C_f < ((S_i \times L_i) - (S_a \times L_a)) + B$ then the feature should be implemented.

Now let's take a look at each of these components to see what they include.

Costs (C_f): The obvious costs include the cost of the smart cards, readers, software, and people and infrastructure to implement and support the feature. But there could also be

hidden costs; loss of customer satisfaction because the feature is difficult to use; downtime for a customer if they lose their card, loss of other features; or additional training that may be required. If possible, the total cost over the expected life of the feature should be included.

Probability of a successful attack (S): This will indicate the likelihood of a successful attack over the time period being evaluated. This likelihood will be affected by the number of people who believe the value they can derive is less than the cost it would take from successfully attacking the system.

This value can be any whole or fractional number greater than or equal to zero. This should only be zero if there is no system in place to be attack. The probability could be above one if you expect more than one successful attack over the life of the feature. Since the probability will be affected by the amount of time being evaluated, you should use the same time period that was used to determine costs.

Expected Loss in a successful attack (L): This should be expressed in terms of dollars. It would include any loss of assets or revenues caused by the attack, any costs associated with responding to and/or recovering from the attack, and any loss of customer goodwill that resulted from the attack.

Benefits (B): Some security features, like smart cards, can actually provide additional benefits to the system. The most obvious benefit would be the ability to implement a new system, like stored value cards, which would not have been feasible without this feature. The benefit in this case would be the additional revenue stream or customer satisfaction derived from implementing the new system. Other benefits could include additional capabilities like easily changing mobile phones by moving the card, automatically tracking frequent buyer purchases, or only requiring a user to remember a single PIN number instead of multiple passwords.

The probability of a successful attack on a smart card system will vary greatly depending on the application. Smart cards on open systems that do not have an immediate feedback loop are much more likely to be attacked. There are two reasons for this; first, these systems are normally designed for very large markets. Since there are a large number of people using it, there is a greater likelihood that one or more people will have the ability and desire to attack it. Second, without the feedback loop, there is no way to detect if an unauthorized card is in use. This allows the attackers to make multiple copies, or even mass produce the cards once they have figured out how.

The probability of an attack on a closed system, like a logon authentication system, tends to be much lower, but the potential loss, depending on what is stored on the computer or network, could be quite high. The probability is lower because the system will verify that

the card is a valid, registered card every time it is used. If an attacker did know how to crack the card, they would probably have to get a hold of a legitimate card and clone it before the legitimate cardholder knew it was missing. At this point, if both the legitimate card and cloned card were in use at the same time, the system and/or the legitimate cardholder would know it and could take an appropriate action. This eliminates the possibility of mass-producing clones of a legitimate card.

Conclusion

How secure are smart cards? They are very secure, and getting better everyday, but they are not perfect. There are some known vulnerabilities, but most of those required extensive technical expertise, access to one or more legitimate cards, and in some cases, very expensive specialized equipment.

This paper has discussed various applications that use smart cards including several documented cases of successful attacks, and some of them were very costly. How can they be "secure"? They are secure because they help reduce (not eliminate) the risk and/or cost of a successful attack to an acceptable level. Without the smart card component, many of these applications would not be financially viable; others would be more costly and/or less profitable.

Smart cards were designed from the inside out to be a secure component of systems with split functionality. As with any security component, the better they are integrated with the overall system, the more effective they will be. This is why closed systems, with a real time feedback loop, will always be more resistant to attacks than open systems, but smart cards have shown that they can reduce the risk in either case.

Many governments, corporations, and other large organizations in Europe have used and trusted smart cards for many years. American Express, Visa, and the DoD have all made major commitments to deploy smart cards in the United States. This level of commitment is only possible because these organizations believe that the cost of implementing smart cards systems will be significant less than the benefits, mostly in the form of reduced risks, derived from using the systems.

There has yet to be a physical or cyber security system that any security specialist would say is impenetrable or hacker-proof. Smart card systems are no exception. But smart cards can provide an additional level of security that will make some systems economically and technically feasible and provide additional protection to existing systems to help significantly reduce their overall risk.

[1] Petri, Steve – Litronic Inc. “An Introduction to Smart Cards” © 1998, 1999 URL: http://www.litronic.com/whitepaper/ (2/5/2002)

[2] American Express “Benefits of Blue from American Express” © 2001 URL: http://www25.americanexpress.com/cards/Fmacfservlet?38/1026/b/3/0/014154237369/0/n&from=88 (2/5/2002)

[3] Visa International Service Association “smart Visa Card - The Versatile Card With the Intelligence to Help Simplify Your Life” © 1996-2001 URL: http://usa.visa.com/personal/cards/visa_smart.html (2/5/2002)

[4] MasterCard International Incorporated “MasterCard Smart Card – The Card To Fit Your Lifestyle” © 1994-2001 URL: http://www.mastercardintl.com/newtechnology/smartcards/ (2/5/2002)

[5] Weisman, Robyn. "U.S. Orders Over 4 Million Digital ID Cards" NewsFactor Network, October 26, 2001 URL:http://www.newsfactor.com/perl/story/14429.html (2/5/2002)

[6] Rainbow Technologies "About USB Smart Tokens and Smart Cards" December 4,2001 URL: http://www.rainbow.com/ikey/index.html (2/5/2002)

[7] Gemplus Corporate “The contactless solution from Gemplus” © 2000 http://www.gemplus.fr/developers/products/gemeasy8000/index.htm (2/5/2002)

[8] Associated Press. "With security a sudden priority, 'smart card' technology gets a second look" SiliconValley.com October 14, 2001 URL: http://www.siliconvalley.com/docs/news/svfront/017046.htm (2/5/2002)

[9] Health Card Technologies, Inc. "Answers to Frequently Asked Questions About Medical Smart Cards" © 1997-1999 URL: http://www.hct.com/faq.htm (2/5/2002)

[10] Proton World “Smart Cards – What can smart cards be used to do?” URL: http://www.protonworld.com/smartcards/intro/smartcards_use.htm (2/5/2002)

[11] Microsoft Corporation “What Windows for Smart Cards Can Do for Your Business Today” © 2000 January 28, 2000 URL: http://www.microsoft.com/windowsce/smartcard/start/intro.asp (2/5/2002)

[12] MULTOS URL: http://www.multos.com/index.ihtml (2/5/2002)

[13] Sun Microsystems, Inc. “Java Card Technology” © 1995-2002 URL: http://java.sun.com/products/javacard/ (2/5/2002)

[14] Kocher, Paul; Jaffe, Joshua; Jun, Benjamin. - Cryptography Research, Inc "Cryptography Research Q&A on Differential Power Analysis" © 1998, 1999URL: http://www.cryptography.com/dpa/qa/index.html (2/5/2002)

[15] Kocher, Paul."Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems" December 1995 URL: http://www.cryptography.com/timingattack/ (2/5/2002)

[16] Ross Anderson, Markus Kuhn "Low Cost Attacks on Tamper Resistant Devices" Security Protocol Workshop. April 1997. M Lomas et al. (ed.), Security Protocols, 5th International Workshop, Paris, France, April 7{9, 1997, Proceedings, Springer LNCS 1361, pp 125{136, ISBN 3-540-64040-1. URL: http://www.cl.cam.ac.uk/~mgk25/tamper2.pdf (2/5/2002)

[17] Ross Anderson, Markus Kuhn "Tamper Resistance - a Cautionary Note" The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp 1-11, ISBN 1-880446-83-9. URL: http://www.cl.cam.ac.uk/users/rja14/tamper.html (2/5/2002)

[18] Glave, James "Pirates Cash In on Weak Chips" Wired News May 22, 1998 URL: http://www.wired.com/news/technology/0,1282,12459,00.html (2/5/2002)

[19] Anderson, Ross J. (Cambridge University Computer Laboratory) "Tamperproofing of Chip Card" URL: http://www.infowar.com/class_2/class2_091197a.html-ssi (2/5/2002)

[20] Schneier, B. and Shostack, A. "Breaking Up Is Hard To Do: Modeling Security" USENIX Workshop on Smart Card Technology, USENIX Press, 1999, pp. 175-185 URL: http://www.counterpane.com/smart-card-threats.html (2/5/2002)

[21] Pelé, Laurent "French banking smartcard cracked: the story!" February 25, 2000 URL: http://www.parodie.com/english/smartcard.htm (2/5/2002)

[22] "DSS HISTORY" Doc Debugs DSS Dealer and DVT Hacker Info (Donated to Doc 7/10/00) URL: http://64.246.7.185/dsshistory.htm (2/5/2002)

[23] MasterCard International Incorporated "Smart Cards: Ushering in a New Era of Opportunity for the Banks" © 1994-2001 URL: http://www.mastercardintl.com/newtechnology/smartcards/articles/article1.html (2/5/2002)

[24] Goldberg, Ian (ISAAC research group) and Marc Briceno (Director of the Smartcard Developers Association). "GSM Cloning" Orig. April 13, 1998 URL: http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html (2/5/2002)

[25] Foundation for Information Policy Research "Framework for Smart Card Use in Government - Consultation Response" March 2nd, 1998 URL: http://www.cl.cam.ac.uk/users/rja14/cards.html (2/5/2002)

[26] Kommerling, Oliver and Kuhn, Markus G. "Design Principles for Tamper-Resistant Smartcard Processors."
Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard'99), Chicago, Illinois, USA, 10-11 May 1999, USENIX Association, pp. 9-20,ISBN 1-880446-34-0.
URL: http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf (2/5/2002)

[27] SchlumbergerSema "SchlumbergerSema First to Market FIPS 140-1 Level 2 Certified Java™ Open Platform-Based Cryptographic Smart Card " Press Release October 29, 2001 URL: http://www.cyberflex.com/News/32K/32k.html (2/5/2002)