Survey of Cryptographic Smart Card
Capabilities and Vulnerabilities

by Ronald Ward
Secure Telecommunications, ECE 636

May 5, 2001
Table of Contents

1. Introduction ........................................................................................................................................... 1
2. Smart Card Interface and Readers ........................................................................................................ 1
3. Smart Card Applications ....................................................................................................................... 2
   3.1. General Applications ...................................................................................................................... 2
   3.2. Multiple Application Smart Cards ................................................................................................. 3
   3.3. Future Applications ....................................................................................................................... 4
4. Smart Card Markets ............................................................................................................................... 5
5. Smart Card Vendors ............................................................................................................................... 6
6. Smart Card Reliability ........................................................................................................................... 7
7. Smart Card Cryptographic Co-Processors ............................................................................................... 8
   7.1. Manufactures of Cryptographic Co-Processors ............................................................................... 8
   7.2. Comparison of Cryptographic Co-Processors ............................................................................... 9
   7.3. RSA, DSA and ECC ...................................................................................................................... 12
8. Smart Card Security Attacks .................................................................................................................. 13
   8.1. Non-invasive Attacks ................................................................................................................... 13
   8.2. Invasive Attacks .......................................................................................................................... 14
   8.3. Smart Cards and Trust Splits ...................................................................................................... 16
9. Conclusions .......................................................................................................................................... 17
10. References ............................................................................................................................................ 19

Table of Figures and Tables

Figure 1: ISO 7816-2 Smart Card Physical Interface ............................................................................... 2
Figure 2: Millions of Smart Card Shipments per Market Sector in 1999 [ES99a] ....................................... 5
Figure 3: Geographic Distribution of Smart Card Shipments [ES99b] ....................................................... 6
Table 1: Smart Card Vendors .................................................................................................................... 6
Figure 4: Percentage of cards returned over time ....................................................................................... 8
Figure 5: Comparison of Characteristics of Crypto Co-Processors 1996 vs 1998 ................................. 9
Figure 6: Time of Cryptographic Operations in Siemens Chips 1996 vs 1998 ........................................ 10
Figure 7: Time of Cryptographic Operations in Philips Chips 1996 vs 1998 .......................................... 10
Figure 8: Time of Cryptographic Operations in Thomson's Chips 1996 vs 1998 ................................. 11
Figure 9: Average Time of Cryptographic Operations 1996 vs 1998 ................................. 11
Table 2: Projections for Cryptographic Co-Processors Available in 2000 ................................................. 12
Figure 10: Shamir's Countermeasures for Power Analysis [Sh00] ......................................................... 14
Figure 11: Hot fuming nitric acid dissolves the package [KK99] ............................................................... 15
Figure 12: The chip is glued to a test package using a manual bonding machine [KK99] ......................... 15
Figure 13: Smart card processor ready for microprobing experiments. [KA96] ........................................ 15
1. Introduction

In "The dawn of time" (La nuit des temps) the science fiction writer René Barjavel wrote about the Gondas- a civilization thousands of years old, but highly advanced,-using a magic ring endowed with the power of memorization and telecommunication. "Every time a Gonda wanted something new, some clothes, a trip, some objects, he would pay with his key. He would bend his middle finger, would enter his key and his account at the central computer would immediately be reduced by the value of the merchandise or the requested service." [Ugo01]

Smart cards made their debut in the 1970s. They are practically ubiquitous in certain parts of the world now, and the concept of embedding computer chips in other portable devices has really caught on in the last decade. Sun Microsystems, for instance, advertises iButton, which can be used for data storage, encryption and temperature measurements. It can be mounted on almost anything including a “magic” ring as conceptualized by Barjavel. Over the last few decades the demand for smart cards and similar devices has steadily increased. The demand has mostly come from large organizations such as mobile telephone companies, national administrations and insurance companies. More recently, demand for smart cards and their innovative capabilities has come from the growing e-commerce and home-networking industries. The capabilities and processing speeds of smart cards have also increased to meet the demand.

A recent article in Scientific American reported that cryptographic smart cards range in price from less than $1 to about $20 [Fa96]. Another source indicates that a cryptographic smart card generally costs $12 to $15 [Kin99]. By comparison, a typical magnetic stripe card costs 10 to 50 cents. A smart card reader generally costs $500 [Kin99].

A typical smart card today has an 8-bit microprocessor operating at 5 MHz, 256 to 1024 bytes of RAM, 6 to 24 KB of ROM, 1 to 16 KB of EEPROM, and sometimes an on-board encryption module. The typical rate of data communications is 9600 bits per second, with some that achieve 115,200 bits per second (e.g. GemClub-Micro card).

Although smart cards are becoming more and more widespread and offer incomparable convenience they are still vulnerable to attacks. In particular they are vulnerable to side channel attacks and physical attacks, such as microprobing.

2. Smart Card Interface and Readers

Most smart cards adhere to the International Standards Organization (ISO) 7816 standard physical interface, which is featured in Figure 1, below. Card terminals include readers attached to personal computer, vending machines, ATM machines, GSM mobile phones, and hand-held readers. OpenCard Framework, developed by IBM, Netscape, NCI and Sun Microsystems supplies standardized Application Programming Interfaces,
allowing applications to be written which are independent of card terminal vendor, card operating system, card provider, or card issuer. [Gr99]

Figure 1: ISO 7816-2 Smart Card Physical Interface

Some smart cards are contactless, meaning the reader interfaces with the card through a small inductive “antenna,” which is embedded in the card. This way a card need only be in close proximity to a reader in order to perform a data transfer or operation. The most versatile contactless smart cards also include the standard contacts for interfacing with conventional readers. Contactless, or proximity smart card readers are especially useful for mass transit or building access applications because the reader must perform its function very quickly while the card holder briefly pauses, then moves on.

Many smart card alternatives, which do not adhere to the ISO 7816 standard, are emerging in the market place. The iButton, from Sun Microsystems, has a unique “1-wire” interface. The reader, only available from Sun Microsystems, can interface with a standard serial port, parallel port or Universal Serial Bus (USB) port. Spyrus offers a product called Rosetta USB, which has the features of a smart card but can interface directly with a USB port. Many other smart card manufactures are also offering smart cards and similar devices with USB interface capabilities.

3. Smart Card Applications

3.1. General Applications

There are myriads of applications in which Smart Cards are used, with innovative applications being discovered continuously. The following is a list of merely a few general applications of Smart Cards:
• Authentication Card - These may include functions such as digital signatures, Personal Identification Number (PIN) encryption to verify identity. Depending on the sophistication they may or may not include a processor. According to Gemplus, a European smart card vendor, technical support calls for companies implementing authentication smart cards have been reduced by 40 percent by automatically performing the error-prone authentication process for users.
• Stored Value Card – These cards may be used for prepaid purchases such as prepaid telephone calls or ecommerce. If a processor is included it may also be used to store private keys and provide a secure computing environment for private key operations.
• Multiple Application or Multifunctional Card – The multiple application cards are especially interesting and versatile because they can be used to provide all the functions of multiple smart cards in one single smart card. Typically there is an operating system stored in the ROM of a multiple application smart card.

3.2. Multiple Application Smart Cards
JavaCards (produced by JavaSoft, a division of Sun MicroSystems) is a specification for a type of multiple application smart card, not an operating system. JavaCard uses an interpreter (called a JavaCard “virtual machine interface”) that is in ROM along with the operating system. It is the interface between an application or “applet” and the card’s operating system. The advantage of JavaCards is that applications that are programmed on them can run on different platforms and operating systems. A disadvantage is that expensive smart cards, with fast processors and high memory, are required for use with JavaCard technology. The Java Card 2.0 specification has a minimum system requirement of 16 kB of ROM, 8 kB of EEPROM and 256 bytes of RAM. Patrice Peyret, CEO of Integrity Arts, claims that the JavaCard is eventually going to be the largest deployed computing platform in the world [Pey97].

A typical Java Card could include the following functions in one card:

• GSM cellular telephone access
• Financial transactions, both online and off line
• Campus access card
• Logical access control to enterprise IT systems

SIMagine 2001 recently announced the winners of a JavaCard application development contest at the GSM World Congress in Cannes. The contestants were asked to develop applications in Java and integrate them on to GSM SIM cards. Some of the interesting and innovative applications included the following: [SIM01]

• First Prize and €25,000 euros were awarded to French start-up Ofye for its “Ofye” middleware. This enables a user to receive personalized information (such as promotions) in the form of an icon (connected to a URL). Clicking on the icon activates the over-the-air download of the application.
• Eurecom Institute based in Sophia-Antipolis, France, received an award for their “Zebra” platform enabling advertisement messages to be filtered according to the user’s profile.

• Indonesian start-up INTI received an award for their “CarGuard” application enabling on-site notification of the user’s insurance company of relevant user information in the case of an automobile accident.

• Russian start-up Novasoft received an award for their GSM home automation application. With this application, a user can remotely control or monitor various Internet-connected home appliances.

Smart cards with Windows for Smart Cards, by Microsoft, are another example of multiple application smart cards. Windows for Smart Cards is an operating system that is an extension of other Windows operating systems. Windows 2000 is optimized to work with Windows for Smart Cards. Existing applications include digital signatures, storage of keys, authentication, restriction of network access and permissions, key exchange encryption. Microsoft loads a blank smart card with Windows for Smart Cards and the user can download applications from the internet. Microsoft claims the cost will be 2-4$ compared to $15 for a typical JavaCard.

Another less known operating system for multiple application cards is Multos. Applications may be written in Multos Executable Language (MEL), an assembly language, or in C and then compiled into MEL. [Gr99]

3.3. Future Applications

Thierry Lamotte, a researcher at Gemplus, posits that IP smart cards are in the not so distant future [La01]. These IP smart cards would include not only layers 1 and 2 of the OSI model (physical layer and data link layer), but also layer 3, the network layer. The advantage of integrating IP in a smart card is greater interoperability of smart cards due to the use of a standard network layer. As an experiment, he and a group of researchers implemented a daisy chain network of smart cards connected to a host platform, which in turn was connected to a common IP network. Through this experiment they determined that an efficient communication peripheral in smart cards is lacking. The Maximum Transmission Unit (MTU) that can be implemented on a smart card and the lack of fast access memory are severe limitations. Lamotte claims that Gemplus research labs have overcome these difficulties, but not in a way that will allow cheap mass production of the implementation.

The future will also likely see greater integration of biometrics with smart cards for positive identification. For example, a reader could require a fingerprint or voice challenge response before allowing the user to perform any smart card operations. Implementation of biometrics today is somewhat cost prohibitive and is therefore only used in well-funded organizations such as government agencies.
4. Smart Card Markets

The majority of smart cards, by far, are used in the telecommunications sector, where Subscriber Identity Modules (SIMs) are the major applications. Smart Cards have been specified as the access medium to the digital European mobile phone system (GSM). They are ideal because they provide secure access to the network by verifying the subscriber's identity, and they allow separation of sale of mobile phones from that of services by the network operator and service provider. Thanks, in large part to smart cards, the GSM mobile phone system has spread quickly across Europe. Figure 2 shows the results of a survey done by the European Smart Card Industry Association (EUROSMART), which studied the distribution of smart cards used in different sectors of the market in 1999.

![Figure 2: Millions of Smart Card Shipments per Market Sector in 1999 [ES99a]](image)

There was a substantial increase over the amount of shipments made in 1998. There has been a strong increase in use of microprocessor cards (+60%) and a slight increase in use of memory cards (+14%). Participants in another survey done by Frost & Sullivan's reported a total of 14.1 million cryptographic smart cards shipped in 1999. The report projects this number to rise 114.7 million by 2006. It also states that the network security segment of the smart card market is projected to make up nearly half of all units shipped by 2006 [Ru00].
Figure 3 shows the geographic distribution of the smart card shipments included in the EUROSMART survey of 1999. The geographical breakdown between Europe, Middle East, Africa (EMEA) and Asia/Pacific (ASPAC) was the same as in 1998. There was a higher increase of Americas (+27%) than in ASPAC (+13.5%) due to a rapid growth of the Central and Southern American market.

![Figure 3: Geographic Distribution of Smart Card Shipments [ES99b]](image)

5. **Smart Card Vendors**

The major vendors of smart cards with encryption capabilities are listed in Table 1 below.

<table>
<thead>
<tr>
<th>Europe</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gemplus</td>
<td>Invincible Data Systems</td>
</tr>
<tr>
<td>ORGA</td>
<td>Litronic, Inc.</td>
</tr>
<tr>
<td>Schlumberger ET</td>
<td>Racal Security &amp; Payments</td>
</tr>
<tr>
<td>Bull - CP8</td>
<td>VASCO Data Security, Inc.</td>
</tr>
<tr>
<td>Gieseche &amp; Devrient</td>
<td>ActivCard, Inc.</td>
</tr>
<tr>
<td>BasicCard</td>
<td>Certicom</td>
</tr>
<tr>
<td>SCM Microsystems</td>
<td>HID Corporation</td>
</tr>
<tr>
<td>Omnikey</td>
<td>IBM Corporation</td>
</tr>
<tr>
<td>Advanced Card Systems</td>
<td>Information Resource</td>
</tr>
<tr>
<td>Athena SmartCard</td>
<td>Ankari</td>
</tr>
<tr>
<td>Solutions</td>
<td>Engineering, Inc.</td>
</tr>
<tr>
<td>Intertex IX</td>
<td>Okiok Data</td>
</tr>
</tbody>
</table>

Certicom’s smart cards store private keys and perform digital signatures. Certicom’s smart cards are unique in that they implement elliptic curve encryption, an algorithm that is recognized as a viable competitor with RSA for public key cryptography. An elliptic
curve encryption algorithm requires a shorter key than RSA for the same level of security. Their smart cards also provide optional user data, which can hold a full X.509 certification or other information, as required by an individual business. Certicom currently offers three smart cards, each built on standard smart card hardware. They use the following three hardware bases: Motorola MSC0208 IC, Siemens SLE44C80S IC, and Siemens SLE66C80s IC.

Gemplus, a company based in France, produces a wide variety of smart cards for almost every application. Their revenues include 18% generated in the Americas, 16% in Asia Pacific and 66% in Europe, the Middle East and Africa (EMEA). Gemplus had a 33% share of the smart card solutions market at the end of 1999 (source: International Data Corporation, 2000).

ActivCard is based in Paris, France. ActivCard smart cards are mainly for authentication of identity for e-business. ActivCard touts being a key enabler of business-to-business (B2B) and business-to-consumer (B2C) communication and commerce. Their top of the line product, ActivCard Gold, supports static password storage and protection, dynamic password generation for remote access, and other PKI services.

Schlumberger offers a range of smart cards, readers and development tools for implementing public key infrastructure (PKI) technologies. Typical applications include:

- Secure log-on
- Secure email/digital signatures
- Secure web access / remote access
- Virtual private networks
- Hard disk encryption
- Computer trust (Trusted Computer Platform Alliance Initiative)

6. Smart Card Reliability

Smart cards have steadily increased in reliability as the industry has been making billions of cards per year and has leveraged experience from traditional magnetic striped cards. Below is a card failure chart from one of the oldest and largest bank smart card projects in the world, the French GE Carte Bancaire project. This project has more than 22 million Visa Debit Smart Cards in use and more than a decade of experience.
Unfortunately, the failures of smart cards are often due to the tampering sensors implemented on them. If the sensors are too difficult to adjust correctly they are simply disabled. Using a narrow statistical analysis, it is conceivable for a vendor to purport that their smart cards are becoming more reliable, when in reality the overly sensitive tamper sensors are being disabled, thus making the smart cards vulnerable to attack.

7. **Smart Card Cryptographic Co-Processors**

7.1. **Manufactures of Cryptographic Co-Processors**

With the exception of Certicom’s elliptic curve based smart cards, the cryptographic operations of a smart card are performed on a cryptographic co-processor. Manufacturers of cryptographic co-processors for smart cards include:

- SGS Thomson
- Siemens
- Philips
- Motorola
- SEPT
- Cylink Corporation
- Atmel
- Fondazione Ugo Bordoni/Amtec
- Pijnenburg
- Hitachi
- Oki

The leading manufactures of cryptographic smart card chips are SGS Thomson, Philips and Siemens. Interestingly, they each use a different algorithm for modular
multiplication. Motorola’s and SGS Thomson’s chips use the Montgomery algorithm. Philips chips use the de Waleffe and Quisquater algorithm. Siemens chips use the Sedlak algorithm. [NM96]

7.2. Comparison of Cryptographic Co-Processors

The capabilities of cryptographic co-processors have increased rapidly in the last few years. Figure 5 shows a summary of the results of two studies done by Gemplus, one from 1996 the other from 1998 [NM96],[HP98]. The data presented is an average of all the chips that were included in the Gemplus studies. The chips improved a surprising amount in the short span of two years. Evidently, the clock speed has decreased, on average. Since the clock speed is directly proportional to current consumption, the newer smart cards actually do more while consuming less power.

![Comparison of Common Characteristics of Crypto Co-Processors 1996 vs 1998](image)

**Figure 5: Comparison of Characteristics of Crypto Co-Processors 1996 vs 1998**

The speeds of encryption and decryption have been reduced significantly over the last half-decade. Figure 6, Figure 7, and Figure 8 present a comparison of the speed of different cryptographic operations on Siemens, Philips and SGS Thomson’s chips, respectively. The data for the following figures was adapted from [NM96],[HP98]. It is difficult to find any data on cryptographic smart card chips that is more recent than that of the Gemplus survey of 1998 and even that data is sparse.
Figure 6: Time of Cryptographic Operations in Siemens Chips 1996 vs 1998

Figure 7: Time of Cryptographic Operations in Philips Chips 1996 vs 1998
Figure 8: Time of Cryptographic Operations in Thomson's Chips 1996 vs 1998

Figure 9 presents the average amount of time taken for different cryptographic operations in chips available in 1996 versus chips available in 1998. The data is adapted from the sources [NM96] and [HP98].
The decrease in speed is remarkable, especially considering the fact that the chips in 1998 have slower clock speeds on average than the chips in 1996. The only explanation for this is that the implementations in 1998 were much more optimized than those of 1996. The manufacturers of crypto co-processors are wary of revealing the details of their implementation due to the security risk it poses, therefore an explanation for this remarkable optimization requires a thorough and costly analysis of the chips.

A linear projection of the data presented in Figure 8 would indicate that cryptographic co-processors chips available in 2000 should be able to perform operations in tens of milliseconds. The data available from the Philips, SGS Thomsons, and Siemens web sites do not provide information on any chips that perform better than those in that were included in the 1998 Gemplus survey. If the web sites are indeed current, then perhaps the demand for speed of cryptographic operations on smart cards may have reached a plateau. Another, more plausible, explanation is that the next release of chips has not yet been advertised. Table 2, below, provides a rough linear estimate of the speeds of several operations for chips available in 2000 if the trend from 1996 to 1998 were to continue.

<table>
<thead>
<tr>
<th>Cryptographic Operation</th>
<th>Average Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA 512 sign with CRT</td>
<td>7 ms</td>
</tr>
<tr>
<td>RSA 512 sign without CRT</td>
<td>16 ms</td>
</tr>
<tr>
<td>RSA 512 verify</td>
<td>1 ms</td>
</tr>
<tr>
<td>RSA 1024 sign with CRT</td>
<td>27 ms</td>
</tr>
<tr>
<td>RSA 1024 sign without CRT</td>
<td>91 ms</td>
</tr>
<tr>
<td>DSA 512 sign</td>
<td>16 ms</td>
</tr>
<tr>
<td>DSA 512 verify</td>
<td>21 ms</td>
</tr>
</tbody>
</table>

7.3. **RSA, DSA and ECC**

Although the digital signature algorithm (DSA) was based on the Schnorr signature, which was first announced as a smart card application, most smart card’s cryptographic co-processors implement RSA signatures as opposed to DSA. RSA is actually more effective if implemented with the Chinese Remainder Theorem.

Many chips are beginning to include elliptic curve signature algorithms, also. [Gr99] Certicom claims that “other public-key systems involve so much computation that a dedicated hardware device known as a crypto coprocessor is required. The crypto coprocessors not only take up precious space – they add about 20 to 30 percent to the cost of the chip, and about three to five dollars to the cost of each card. With Elliptic Curve Cryptography (ECC), the algorithm can be implemented in available ROM, so no additional hardware is required to perform strong, fast authentication.” [Cert]

Bruce Schneier, a world-renowned expert in cryptology, recommends ECC for smart cards because of the small key size, but recommends RSA for applications where performance and key size is not a factor. According to Schneier, ECC has not been
studied long enough and there may be a loophole in its mathematical properties that have not been discovered. [Sc99]

8. Smart Card Security Attacks

8.1. Non-invasive Attacks

Non-invasive attacks, also known as side channel attacks or eavesdropping attacks, are difficult to prevent in smart cards. A non-invasive attack takes advantage of the analog characteristics of the power supply and interface connections, or any other electromagnetic radiation produced during normal operation of the card.

Possibly, the simplest attack to mount is to block the reader’s access to a particular contact on the card. This type of attack was successful on pay-TV systems in which broadcast signals were used to instruct the card to block channels that had not been paid for. Blocking the programming contact with tape or clamping it off with a diode prevented that signal from ever reaching the card, which in turn allowed the viewer to have free channels. A similar approach has been used on public telephone systems. If the contact that is used to decrement the card’s value is dirty or bent, the card’s value would remain the same. Few smart cards today are vulnerable to this simple type of attack. [KA96]

Timing analysis exploits the execution time of operations on a smart card. If an attacker has access to the card and can make a series of measurements of the time required for partial operations, this data can be used to determine the key. Paul Kocher discovered timing analysis to the public in December 1995 [Ko95]. An effective and efficient method of counteracting timing analysis is to use nonlinear key updating.

Simple Power Analysis, Differential Power Analysis and High Order Differential Power Analysis attacks exploit the power consumption characteristics of the smart card and can be used to expose the secret key and the protocols and algorithms used on it. A more detailed description of these techniques can be found in the publications of the inventor of the technique, Paul Kocher [Ko98].

Since power analysis attacks were discovered, at least to the public, only a few years ago there are not many practical solutions for preventing them. And of the few methods that have been proposed for preventing power analysis attacks they have yet to be implemented in the majority of smart cards. The most promising method, proposed by Shamir in [Sh00], is to include a diode and capacitor network at the power supply input to the smart card, as shown in Figure 10, below.
Glitch attacks, software protocol attacks, fault generation attacks all take advantage of abnormalities in the chip. These attacks often require detailed analysis or trial and error methods to determine how a chip will react to certain environmental conditions such as fast or slow clock speeds, power fluctuations or other “glitches.” These techniques can be used to change the states of flip-flops, for example.

Using a random clock signal or randomized multithreading of operations will prevent an attacker from predicting the time at which certain instructions will execute. Many chips come with sensors that will disable the chip if, for example, an out of range clock speed, temperature or voltage is detected. Unfortunately, these sensors are often disabled because they are not very robust.

8.2. **Invasive Attacks**

The marketing director of Gemplus, P Maes, was recently quoted as saying that there was no demand from their users for anything really sophisticated in preventing access to the smart card’s embedded chip [Mae94]. However, mounting an invasive physical attack against most smart cards is surprisingly easy and can reveal the smart card’s most protected secrets. In addition, several publications are publicly available on the internet that describe physical attacks that can be mounted against smart cards.

An attacker may analyze and probe a smart card’s chip in a standard test bed by removing the processor from the card. A sharp knife can be used to cut away the plastic behind the chip module until the epoxy resin becomes visible. The resin may be dissolved by applying a few drops of fuming nitric acid (>98% HNO3). Heating up the acid with an infrared radiator will accelerate the process.
Figure 11: Hot fuming nitric acid dissolves the package [KK99]

Then, shaking the card in acetone will expose the silicon surface. The chip may be removed and attached to a test package.

Figure 12: The chip is glued to a test package using a manual bonding machine [KK99]

Figure 13: Smart card processor ready for microprobing experiments. [KA96]
Finally, the chip can be examined and attacked directly. Kuhn and Anderson claim that all the tools necessary for this preparation were obtained for $30 in a pharmacy.

After preparing the chip as described, on chip signals may be read using electron beam testers or microprobing needles. The functionality of the card may be altered with lasers, ultrasonics or focused ion beams. Several undergraduate students have reported on the successful application of this method. More detailed descriptions of these and other unpackaging techniques may be found in [B98], [LP93], [KA97].

After unpackaging the chip, the chip’s test pads may easily be identified with a confocal microscope. Occasionally, the test fuses are left intact after the card’s test cycle. Even if they are not, Bovenlander has described a repair method using two microprobe needles to bridge the blown fuse. Then the re-enabled test routine may be used to read out the memory contents. [Bo97]

Anderson and Kuhn report several other low-cost attacks in their paper, Low Cost Attacks on Tamper Resistant Devices. Once the chip is exposed, the contents of memory may be read or altered using focused ion beam editing. They claim to be able to overwrite single bits in ROM using a laser cutter microscope. If the DES implementation is well known, one bit, or a relatively small number of bits, can be changed which will then allow the key to be easily extracted. They report other ROM attacks for implementations that are not as well known. Similar attacks for keys and algorithms stored in EEPROM are also described. [KA97]

One method used to prevent tampering is often a capacitive sensor to detect the continued presence of the passivation layer. Alternatively, an optical sensor under an opaque coating may detect tampering and disable the chip. Unfortunately, these sensors are often disabled or not used because they are not very robust.

Philips offers some protection against physical attacks. They advertise a technique called glue logic. On their web site they claim that glue logic transfers the entire chip logic into a random layout. It can be compared to a ‘visual’ encryption of the IC layout, making identification of individual blocks as well as any navigation on the chip area nearly impossible. Another feature offered is memory protection. The location of data and its actual address location are de-correlated. This technique, however, only applies to dynamically updated memory (e.g. RAM).

8.3. Smart Cards and Trust Splits

Perhaps the most difficult security problem to overcome is trust splits, as described in [SS1]. A trust split occurs when one party in control of a portion of the smart card’s functionality attacks a party in control of another portion of the smart card’s functionality. For example, a smart card’s functionality is potentially split among the following parties:

- Cardholder
- Data owner
- Terminal
- Card issuer
- Card manufacturer
- Card software developer

One example of a trust split is a rogue terminal deducting the incorrect amount of money or steals private information such as PIN. Attacks similar to this have been and are done on ATMs, for example. [Per98] One way to prevent a terminal attack against a card, or a cardholder attack against a terminal, is to implement back-end processing systems that monitor transactions and flag for suspicious activity. Most of these attacks are not possible in a conventional computer system because they would take place within the security boundary of one computer. With smart cards, the functionality is split and therefore the security boundaries are split also.

The most versatile of smart cards, the multi-application smart cards are particularly vulnerable to a breach in security due to the various trust splits inherent in the systems they support. Any complex smart card based system, such as those that use multi-application smart cards, should always include means of authenticating the various system components and parties involved. The reader should authenticate the card’s validity and the cardholder’s identity. The card or cardholder should be capable of authenticating the card reader. The card reader should authenticate the interface it has with any other peripherals it is attached to.

One of the major drawbacks of smart cards is that they sorely lack in ability to communicate with the outside world. Schneier and Shostack recommend merging the data owner and cardholder into one party. This is the most simple and cheap method to prevent attacks that currently plague many smart card based systems [SS99]. Another, more expensive, way to reduce the number of trust splits is to simply add screen and input devices to the card.

Finally, Schneier and Shostack recommend that the best way to ensure the security of any system is to allow widespread public examination of it. This has proven effective on many systems in the past and tends to sway systems toward being simpler and having fewer trust splits. The Mondex system, for example, allows users to check certain parameters independent of the merchant’s terminal. This exposes and prevents a whole range of attacks from occurring. Using open source implementations and/or clear specifications could prevent an attack by a software developer.

9. Conclusions
If the main advantage of smart cards were to be summed up in one word, it would probably be “convenience.” Multi application cards are particularly convenient and versatile but are also vulnerable to various attacks. In order for JavaCard to become the most ubiquitous computing platform in the world, as Patrice Peyret predicts, the security issues must be overcome or at least mitigated first. Adi Shamir notes that “a general problem of protecting smart cards in a cost effective way against active probing and
microsurgery attacks seems to be currently unsolvable.” [Sh00]. Multi application smart card developers need to be careful about deploying a smart card based system with multiple trust splits. In particular, they should allow widespread public examination of it during the design process. Issuing small-scaled test cases of the system to uncover problems prior to mass production and distribution is highly recommended.

Both non-invasive and invasive attacks are a real problem for smart cards. Implementing effective tamper resistance is more difficult than it appears. One European signals intelligence agency declared that the Dallas DS5002FP Secure Microcontroller was the most secure processor available on general sale. However, R. Anderson and M. Kuhn were able to conceive of and perform a software protocol attack, which revealed all of the secrets stored in the chip. They did it in less than three months using equipment available in a student hardware laboratory at the University of Erlangen-Nurnberg. Details of the attack are given in [KA96]. Even if biometrics were used to prevent unauthorized users from gaining access to the card, microprobing and focused ion beam editing techniques could circumvent those security measures.

Smart cards may not be the magic bullet for digital data security. What they do offer, however, is a combination of features not found on any other device that is as cost effective, small, increasingly versatile and portable. The speed and cryptographic capabilities of smart cards are increasing rapidly. JavaCards and other multiple application smart cards are pushing the envelope on the capabilities of smart cards. If the trend continues smart cards will continue to find new niche markets, some of which have never been conceived of before.
10. References


[Bo97] E. Bovenlander, invited talk on smart card security, Eurocrypt 97


[MAE94] P Maes, marketing director, Gemplus, comment during a panel discussion at Cards 94


