Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.3
Mark A. Trudelle
8 April 2002

Smart Talk

About

Smart Cards

Abstract:

In this paper, I will discuss the evolution and development of the "Smart" card. Included will be an overview outlining what a smart card is, the different categories of cards and it's uses in the past, present and the future development of the smart cards. I will also include statistics for the distribution and applications of smart cards. I have also included a graph that outlines worldwide distribution. I will also address the shortcoming of these cards in the area of security and some techniques that are used to protect these cards

Overview:

The official description (when loosely used) is any card with a capability to relate information to a particular application such as magnetic stripe, optical, memory and microprocessor cards. What the industry perceives as a "smart card," is the size of a credit card, it can store information on an integrated microprocessor chip located within the body of the card. Its contents also include memory, an operating system, and storage capabilities. These cards read this information when coupled with a card reader or contactless cards which use radio frequency signals to operate. These cards are used for such applications as credit card information, healthcare information, (Doctor – Patient information); banking and identity/access just to name a few.

History of Smart Card's

1950 – 1975:

The first plastic-based card was issued by Diners club in 1950. By the end of fifties two other firms joined the technology, American Express and Carte Blanche. These early

cards were only capable of storing names, numbers, and codes. The first cards with magnetic stripes were developed by the International Air Transportation Association (IATA). In 1970, Dr. Kunitaka Arimura of Japan filed the first and only patent on the smart card concept. The first smart card was developed in 1974 by a Frenchman named Roland Moreno. He developed a method of embedding an electronic memory in a plastic card. This was then loaded with currency onto the card to allow the user to spend it with merchants who had the necessary electronic payment equipment. These cards were also developed to unlock doors to government facilities. This was the precursor to one of today's uses of smart cards. Due to the immaturity of the semiconductor technology at this time, most of the work on this project was at the research and development stage

1975 – 1990:

In 1977, Motorola and Bull Corporation created the first microprocessor card but early design flaws made these types of cards impractical. In 1985, the French government was undergoing a complete overhaul of its technology infrastructure and undertook a major involvement in smart card applications by issuing an order for 16 million cards. These were to be used for Frances banks as a Visa debt card. In 1986, the prompting of security and vandalism of its pay telephone across the nation, France Telecom ordered 7 million cards for its customers. Also in that year, 14,000 smart cards were issued to clients of the Bank of Virginia and the Maryland National Bank. During this same period, 50,000 Casio cards were distributed to clients of the First National Palm Beach Bank and the Mall bank to be used with the new Automated Teller Machines (ATM). These were the first wide spread use in the United States. Several other U.S cities conducted smart-card trials, but the cards failed to win consumer confidence. This was due to the fact that Americans had been using the magnetic-stripe cards and were not ready to transition to the new technology that smart cards afforded.

1990 – Present:

As the 1980's ended, technological break throughs and increased reliability of the smart cards and practical applications of the card gained wider acceptance in the world especially Europe. In 1992, a nationwide prepaid card project (DANMONT) was started in Denmark. In 1994, the German government began issuing 80 million serial memory chip cards as citizen health cards. Also in this year, the French government initiated a field test of "multi-functional" smart cards. In 1995 Europay, MasterCard, and Visa published joint specifications for global microchip-based bankcards. In 1996 during the summer Olympics in Atlanta, GA 1.5 million VISA cash stored value smart cards were issued. During this same time period, MasterCard and Visa each began working on solving the problem of interoperability. Two different card solutions were developed; the JavaCard by Visa and the Multi-application Operating System (MULTOS) backed by MasterCard. In 1998 the U.S. Government's General Service Administration (GSA) began reviewing the smart card concept and looking at practical solutions for the Federal Government. This led to the development of the Smart Card Technology Center in Washington, DC. In September of that year, Microsoft joined the smart card bandwagon and introduced, it's new Windows smart card operating system. In 1999, GSA announced

that it would start to field approximately 4.3 million Common Access Cards (CAC) to military personnel and DOD personnel starting in FY 2001.

Smart Card Applications:

Smart cards are becoming more attractive as the price of microcomputing power and storage continues to drop. There are three main benefits over magnetic-stripe cards. First, they can carry up to 100 times as much information. Second, they can execute complex tasks in conjunction with a terminal. Third and most importantly is that they are secure. This is due to fact that most cards use some type of encipherment system, such as the Data Encryption Standard (DES) or a highly secure Public-Key Infrastructure (PKI) scheme. Today Europe and Asia still hold the world share of the smart card market as this graph indicates. Smart cards are most prominent in Western Europe, which holds 70% of the market. Worldwide distribution is: **

Region	1996	2000
North America	3%	12%
South America	11%	10%
Western Europe	70%	40%
Asia	10%	30%
Rest of World	6%	8%

**Source: Phoenix Planning & Evaluation
Source:http://www.scia.org/knowledgebase/aboutsmartcards/faqs.htm
(12)

As you can tell from these statistics, the U.S. is lagging far behind. This is because of the significant investment in an extensive magnetic stripe-based infrastructure, and the availability of reliable and low cost on-line telecommunications services and the lack of smart card applications that have been implemented. Another limiting factor is the lack of smart card readers for the individual users p.c. Most smart cards require the existence of one of these devices. Although relatively inexpensive (About $20), most people do not have a reason for the smart cards use. The following graph also represents some other import statistics about smart cards:

In 1996, approximately 805 million smart cards were issued, with an estimated 2.8 billion to be distributed in 2000. The distribution is:**
*In millions

Card Application	1996*	2000*	Average Annual Growth
Pay Phone	605	1,500	29%
GSM	20	45	25%
Health Care	70	120	14%
Banking	40	250	105%
Identity/Access	20	300	280%
Transportation	15	200	247%
Pay TV	15	75	80%
Gaming	5	200	780%
Metering/Vending	10	80	140%
Retail/Loyalty	5	75	280%

Source: http://www.scia.org/knowledgebase/aboutsmartcards/faqs.htm

(13)

This graph only represent figures up the year 2000. However, what about figures after 2000? The forecast predicts smart card shipments in North America will grow to 58 million this year and 85 million in 2003.

The U.S. Federal Government has taken a massive step by announcing that starting in FY 2001, that it would start issuing 4.3 million Common Access Cards (CAC) to all DOD military personnel. This process is being accelerated because of the Sept 11 attacks. These cards will be used to access buildings, including the Pentagon, and to logon to networks, including access to encrypted e-mail and online transactions. They will also carry the individuals medical and personnel data. These cards use PKI for authentication. These will be used for encryption, and digital signing certificates. Department Of Defense (DOD) is planning to issue 23 million cards to Military dependents, Civilian contractors and retirees. The proposed price is approximately $35 million dollars based on the average of $8-$9 a card. Other countries in Europe and Asia have expressed interest for their military using this concept. Other agencies inside the U.S. Federal Government are or have been in the planning states of issuing smart cards with features similar to those of the CAC's.

Meanwhile, there is been a flood of interest from governments and the airline industry worldwide ever since the September 11 attacks and then recent surge of security hacks into government and civilian corporations. This will ultimately lead to increased orders for smart cards and the need to improve upon smart card applications and security. This is going to be a boom for smart card manufactures and associated software vendors such as Gemplus, and SchlumbegerSema. Sales from these two giants that together own about 85 percent of the market have been down following a yearlong slump for mobile telephones and the slow take-off of chip-based bankcards in the United States. Most smart cards applications rely on revenue from the financial industry and Government. In France, every Visa Debit card (over 25 million) has a chip on it.

In Germany, about 40 million bankcards have been issued. The countries with national health care such as Germany have issued cards to every citizen (80 million) . Commercial applications include small dish TV satellite receivers. These devices use a smart card as its removable security element and subscription information. The telecommunications world up which up to last year was biggest user of smart cards. The transportation community especially mass transits and now some U.S. airlines are starting to use and benefit from smart card technology. The use of Biometrics for smart cards application in now being pursued. This will mean that an individual will be identified by his/her hand or finger print, retinal scanning and voice recognition. Although it is still in its infancy, some experts have expressed concerns that this type of application has moral implications such as individuals privacy.

Smart Card Features and Characteristics:

The world of smart card's technology and it's terms remains and mystery to most people. It concepts and verbiage are totally misused. The modern smart card is essentially a stand-alone computer, but without a screen or keyboard. Smart cards are composed of an Operating System (OS), Memory, and file storage all on one or two Integrated Chip (IC). This is in contrast to the magnetic stripe cards (sometimes confused as smart cards) that many of us carry today such as ATM and prepaid telephone cards. These cards are have information such as PIN's or have numbers that are decremented when used and have no of the attributes that are found in truly smart cards. Listed below are some of the terms and concepts associated with smart cards. Smart cards today generally fall into one of these categories and depending on the type of card perform different functions:

Contact Interface:

This type of card requires insertion into a smart card reader. These cards are imbedded with a microprocessor and a contact pad. When the pads come in contact with sensors on the card reader data, commands from the IC instruction set are set in motion, and information processing takes place. This category of card is the most common.

Contactless Interface:

Contactless smart cards also called "Fast Cards" have an antenna that uses low frequency radio waves and an IC embedded inside the card that communications with a reader without making physical contact with the reader. The user has to be about four to six inches from the reader in order for it to work. These cards are generally used for transportation where the customer can just wave the card near the reader instead of inserting and removing the card.

Hybrid Interface:

The hybrid card has two ICs, each with its own contact and contactless interfaces. The two chips are not connected. It is also fitted with a conventional magnetic stripe. This type of card can be used as a credit and debit card but also provides smart chip-card capabilities. In September 1999; American Express introduced its "Blue Card." Marketed towards younger people it can be used as the traditional credit card and take advantage of the smart chip capabilities for shopping on-line.

Combination Interfaces:

This type of card has only one IC that has both a contact and contactless interfaces, either of which can communicate between chip and reader. The mass transit and banking industries are expected to be the first to take advantage of this technology.

Magnetic Stripe:

I have added this category as a comparison to true smart cards. This type of card has no IC electronic components. This is a "Read Only" card. It has storage capability of only 200 characters, about two lines of code. It has numbers that are imbedded on to the magnetic stripe during manufacturing or activation. This type of card requires some sort of card reader. There are some five million devices in the U.S. that can read this type of card compared to 13,000 smart card readers. Although cheaper to manufacture at about 30 cents, they are easier to tamper with and the magnetic stripe can be come damaged.

Card Readers:

All of the above items require some sort of card reader or Card Acceptance Device (CAD) to interpret the data from smart cards. As sales of smart cards are expected to increase more that two dozen companies are working on smart-card readers. The average price for corporate or industry type devices range from $100 - $250 dollars. Prices are expected to drop when the volume increases. Most personal computer manufactures today offer these as an option for as little as $20 dollars. However, consumers have been slow to react, as there does not seem to be a demand for them they're yet.

Integrated Components:

The chips used in smart cards fall into two catagories as well. Listed below are some of the major components of smart cards:

IC - Microprocessor chips:

These cards are referred to as chip cards by the industry. These types of cards can add, delete and process information in its memory. Their ability to not only download data but applications as well is being used by Sun with JavaCard Technology. It is comprised of the following components:

Central Processing Unit (CPU) – These come in 8, 16, 32 bit architectures. And usually use an RISC processor running at 25 to 32 MHz.

I/O Controller – This manages the flow of data between the Card Acceptance Device (CAD) and the processor.

Read Only Memory (ROM) – This is where instructions are burned into memory during manufacturing. Manufacturers typically embed security features into this section. These instructions are then used by the Chip Operating System (COS). Its storage capability is about 16K.

Random Access Memory (RAM) – its purpose is to hold temporary information during processing by the CPU. Its storage capability is about 512 bytes. Its contents are lost when the card is not in use.

Electronic Erasable Programmable Read Only Memory (EEPROM) – Referred to as Application Memory. This data can be electronically erased and be rewritten. It used for permanent storage of information of about 16 – 128 K.

Chip Operating System (COS) – Or sometimes called the Mask. These take instructions from the ROM and execute routines based upon the application. There are two types of COS; the general purpose, which has a generic command set in which it will work with most applications and the dedicated which has specific commands, designed to work with a specific application.

IC – Memory Cards:

These types of cards have no CPU on board and require the card reader to process information. They are suitable for fixed operations. These are typically pre-paid phone cards and represent the bulk of smart card sales. They offer better security alternatives to magnetic stripe cards. The typical storage capacity in between 100 – 16,000 bits of data.

Optical Memory Cards:

These look like smart cards but have no microprocessor on them. They have an integrated Compact Disc (CD) installed and can store up to 4 MB of data on them. Once data is written this data cannot be modified or moved. These types of cards are used for record keeping applications such as medical files, and driving records. These offer little in terms of security but are better suited in this type of environment than magnetic stripe cards. Although comparable in price to smart cards, these type of card uses a non-standard protocol for its card readers and are expensive.

Chip Comparisons:

	Maximum Data Capacity	Processing Power	Cost of Card	Cost of Reader and Connection
Magnetic Stripe Cards	140 bytes	None	$0.20 - $0.75	$750
Integrated Circuit Memory Cards	1 Kbytes	None	$1 - $2.50	$500
Integrated Circuit Processor Cards	8 Kbytes	8-bit cpu, moving to 16- and 32-bit	$7-$15	$500
Optical Memory Cards	4.9 Mbytes	None	$7 - $12	$3,500 - $4,000

Source: Gartner Group http://java.sun.com/products/javacard/smartcards.html

(14)

Standards:

Like any organized industry, there are standards that vendors and manufactures agree upon to ensure interoperability and compatibility in their products. Smart cards are no different. They fall into the International Standards Organization (ISO) 7816 – Integrated Circuit Cards with Electrical connectors. This standard does not directly address smart card applications but deals with the physical, electrical, mechanical and application programming interface.

The ISO 7810 deals with the physical characteristics of the plastic such as temperature, tolerances, and flexibility. As of now, there are no standards in place to address the Chip Operating System. Each smart card vendor produces a unique product. Therefore, one of the drawbacks to smart cards is that they use a proprietary operating system. The Java Card technology or Java Card Application Environment (JACE) launched in 1996 by JavaSoft, allows applications written for the smart card enabled with this technology to be run on any other similar platforms. This technology allows interoperability with other vendors cards that use JCAE and is capable of running multi-applications in a secure environment.

Security:

So far, I have detailed the concepts, history, uses, features, and characteristics of smart cards. In this section, I will address security-related items. One of the primary benefits of using smart cards is that they provide a higher level of security than magnetic stripe cards.
These types of cards are relatively easy to alter, as they provide no level of security. Over the years, credit-card fraud and counterfeit magnetic-stripe cards have created huge losses for the financial industry. The demand for a more effective solution led to the development of the smart card. Smart card technology and manufacturing concepts make

it possible to integrate several security features onto the card. Philips Semiconductor is one of the main suppliers of IC components that have on-chip crypto system capable of computing public-key algorithms. This chip can also generate 512-bit key signatures. The Department Of Defense will be using these type chips when it issues the CAC to all military personnel. These cards will contain Public Key Infrastructure (PKI) certificates and digital keys. Security algorithms and built-in individual card Ids mean that each card in unique. Smart card readers are also being used to provide an extra level of security for smart cards.

All this security may sound impressive but in an article in the *New York Times of June 10, 1998,* states that a team of San Francisco-based computer scientists has successfully breached the security system in tamper-resistant smart cards. The technique used on the tamper-resistant card involves the use of electrons that the IC uses to do the calculations. By hooking up an oscilloscope to the card, the scientists were able to determine the "secret key" by watching the power surges as the keys scramble the data. This technique was a blow to the smart card industry that thought these cards were untouchable by hackers. One analyst stated "we've changed our mindset" he said. "We write software in a different way now."

Conclusion:

Before I did research on this project had no idea of what a smart card was. Although I own a credit card, pre-paid telephone calling card and an ATM, I never thought of these cards as being smart or intelligent. These were everyday devices that would make my life much easier. Could I live without these cards? Yes, do I worry that these cards may be lost or stolen and be used without my consent? Yes, and they have been.

As of this writing, Common Access Cards are now being issued to members of the New Hampshire Army National Guard of which I'm a member. When I receive mine, I will now understand and appreciate the importance aspect such as the convenience and security that these cards will afford me. Most members of the armed forces I assume, will have know idea how these cards will affect their day-to-day activities while serving in the military. If I had been living in Europe for the past fifteen years, I probably could have provided more personnel experiences with smart cards. Europeans have embraced these cards and has become an everyday facet of their lives. Citizens in the U.S. through no fault of their own are totally ignorant when it comes to smart cards. This is do to the fact that we do not want or cannot give up our alliance to our magnetic stripe cards that we have been using all these years. The events on September 11, 2001 have had a severe impact on our society and how we think about security

The U.S. government is the very near future is going to try to change that way of thinking implement policy regarding smart cards to all U.S. citizens. Will having a national ID card system be effective in deterring terrorists and guarding our way of life? There are now raging debates and concerns about the enormous costs and complexity in implementing these systems. There is also the potential for the forging or stealing of a person's identity, not to mention the civil liberties abuses brought about by knowledge of

a persons medical or personnel history. Opposition would also arise from the fact that some people think that the government would infringe on their private lives by merging their financial affairs with their personnel affairs on to one of these cards. I hope that the U.S. will understand and embrace smart card technology for this purpose as did the Europeans and now Asia. It will also be up to Corporate America and retailers to develop and promote smart card technology and applications. Once the U.S. public sees the benefits of this concept, smart cards will find their niche in our society.

References:

1. Internet Week Website:
   http://www.internetweek.com/story/INW20011113S0003

2. InfoWorld.com Website:
   http://www.americanpacific.net/html/wp1.htm

3. Business2.0 Website:
   www.business2.com/articles/web/0,1653,11515,FF.html

4. U.S. General Service Administration (GSA) Website:
   http://egov.gov/smartgov/tutorial/smartcard_foyer.htm

5. Smart Card Industry Association Website- Overview:
   http://www.scia.org/aboutsmartcards/overview.html

6. Roger Clarke's Intro to Chip-Cards Website:
   http://www.anu.edu.au/pepole/Roger.Clarke/EC/ChipIntro.html

7. RedHerring Website:
   http://www.redherring.com/insider/2002/0130/1300.html

8. JavaWorld Website:
   http://www.javaworld.com/javaworld/jw-12-1997/jw-12-javadev_p.html

9. Scientific American Website:
   http://www.sciam.com/0896issue/0896fancherable.html

10. Gemplus Corporation Website.
    http://www.gemplus.com

11. Information Week Website:
    http://www.informationweek.com/829/smartcards.htm

12. Smart Card Industry Association Website- Overview:
    http://www.scia.org/knowledgebase/aboutsmartcards/faqs.htm

13. Smart Card Industry Association Website – Overview:
    http://www.scia.org/knowledgebase/aboutsmartcards/faqs.htm

14. Java.sun.com Website:
    http://java.sun.com/products/javacard/smartcards.html

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor