Global Information Assurance Certification Paper

GIAC Security Essentials Certification Practical
Bill Altmire
Version 1.4b

SMART CARDS

ABSTRACT

Smart cards have the technology base to revolutionize the storage and use of your personal information in a handy, centralized location. Many companies today embrace smart card technology as a state of the art resource used for system access and identity management. Who would have thought that your first credit card with that magnetic strip would evolve into one day having it's own microprocessor on it?

In this article I'll try to illustrate the different types of smart cards and show the reader some of the many ways these little cards are or can be used today for a variety of applications or as information stores about you.

WHAT IS A SMART CARD?

Webopedia defines a smart card as follows:
(http://webopedia.internet.com/TERM/s/smart_card.html)

'A small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit. Smart cards containing an IC are sometimes called Integrated Circuit Cards'.[1]

HISTORY of the SMART CARD

The first patent for a smart card was given to the Frenchman Roland Moreno in 1974. The original patent mentioned portable and protected data storage but didn't say how the data would actually be stored. The first applications for them were as telephone and payment cards. A chip on the card itself stores the information. and tracks changes, like deducting purchases from the amount originally entered on the card.

TYPES of SMART CARDS

There are two basic types of smart cards; contact cards and contactless cards. The difference between the two types of cards are that contact smart cards are inserted into a smart card reader, thus actually making physical contact with a smart card reader. The contactless smart cards have an embedded antenna inside the card that enables communication with the reader without physical contact. Smart cards themselves have no power source and depend on the smart card reader to power them. There are also cards being developed today

that can function as either a contact or contactless type cards, and these are generally referred to as combi cards.

Contact or contactless cards can be smart cards that have an Integrated Circuit Microprocessor. These cards are programmable; you can add, delete or manipulate the information in memory, allowing for a variety of applications and dynamic read/write capabilities. The non-programmable cards just store data and are not as useful as the cards with the integrated microprocessors. These are generally known as memory cards. These are like magnetic strip cards used around the world by banks, grocery stores, and even subway systems. They are definitely not as sophisticated as the newer smart cards. They are basically used to store information and have no real processing capabilities. The programmable smart cards can also hold a significantly larger amount of data than the old magnetic strip cards. But the biggest advantage is the processor itself. It has an operating system (Card Operating system or COS) embedded in the Integrated Circuit Microprocessor. It can actually manipulate the data on the card using many different types of application languages or commands. Someday smart cards will be everywhere, they may not all look like your basic credit card but in general they will use the same technology.

SMART CARD STANDARDS

A lack of any one type of, or standard smart card is a current limitation for its use. I've covered these in more detail in the sections that follow. These deal more with the software that runs on the card than the physical specifications of the card. The physical characteristics of the card are defined using a standard developed by the ISO. From the RSA laboratories web site: (http://www.rsasecurity.com/rsalabs/faq/5-3-4.html) The International Organization for Standardization, (ISO), is a non-governmental body promoting global standardization development. Altogether, ISO is broken down into about 2700 technical committees, subcommittees and working groups. ISO/IEC (International Electrotechnical Commission) is the joint technical committee developing the standards for information technology including smart card technology. [2]

During my research and using my experience with smart card technology I have not seen a smart card offered that didn't conform to the ISO standard for smart cards, ISO7816.

PC/SC

Microsoft was one of the founders of the PC/SC Workgroup, which was formed in 1996 by computer and smart card companies (This working group includes Microsoft, Apple, Schlumberger, and Gemplus) to develop specifications that address the issues concerning interoperability with different vendor's readers and smart cards. The PC/SC (PC/Smart card) application interface initially was only

compatible with Windows32 type computer systems. The PC/SC standard is currently being embraced by M.U.S.C.L.E (Movement for Use of Smart Card in a LINUX environment) to the LINUX platform as well as other flavors of UNIX. PC/SC is also ISO 7816 compliant.

OCF

Another of the card standards in use today is the Open Card Framework or OCF. It is an entirely different standard than the PC/SC standard. It is based on using Java as the language instead of an independently developed Card Operating System. SUN Microsystems has done extensive work on its Java Card. This technology lets Java based applications execute on smart cards. It uses Java 2 Platform Micro Edition from SUN Microsystems in place of a Card Operating System. The Java card conforms to the ISO 7816 standard for smart cards and thus they claim will run on any Java card technology smart card. The Java card is comprised of standard classes and API's that let Java applets run directly on the standard ISO 7816 compliant card. The OCF standard is also ISO 7816 complaint. [3], [4]

EMV

Credit card companies have been big backers of the smart card technology. Visa offers smart card programs to different banks, as does Mastercard. The two companies have also joined forces with Europay to create a set of standards for chip card transactions. The standards apply to the chips as well as the hardware through which the transaction is conducted. The chip standards are refered to as the EMV Integrated Circuit Card Specifications for Payment Systems. They've actually created a company called EMVCo, LLC. Each of the three companies has an equal share of the EMVCo, LLC. All actions of EMVCo require acceptance by all members of the group. The current EMV standard for chip card transactions is EMV 2000 version 4.0.

SMART CARD Features

Smart cards today have many features. Persistent storage is one. Most smart cards contain at least 4k of available storage but depending on the manufacturer that can be much higher. The norm seems to be 32k of memory. ISO 7816 Part One contains standards for the physical characteristics of the cards.

SMART CARD Hacks

Are smart card hackers out there waiting to crack your codes? You bet there are. One of the largest groups of hack prone cards is the ones that come from your digital satellite vendors. One recent federal arrest of a man stated that the cards he sold (over 6000) had a market value of almost $15 million. I've had a dish for years and have read many other stories about these cards. It seems that

when the codes are changed on the cards it only takes the hackers a small amount of time to actually figure out the new encryption codes and crack the cards again allowing free unlimited access to the satellite signal.

Smart card manufacturers continue today to incorporate things like phantom transistors in cards to make examination more difficult. Also upper and lower limits of the cards clock frequency also hinder examination of the circuitry.

PKI and SMART CARDS

Another use of smart cards will be to store a users PKI certificates and digital signatures. PKI or Public Key Infrastructure was developed in 1976 by Whitfield Diffie and Martin Hellman. This technology uses cryptography to store an individual's key. A user gives his public key out as an authentication method. Someone returns something to the user like e-mail or the public key is registered as access to a web site. When a user wants to read the e-mail or access that web site he can't do that until he verifies his identity. He does that with his private key. The private key is only stored on his smart card and thus is nearly impossible to replicate or forge.

A working group founded by RSA Laboratories put the public key standards used with devices such as smart cards and other token type devices together. It has other major industry representatives also. The specific standard used for PKI is PKCS #11. These standards are relegated to the software access of the smart cards with PKI and shouldn't be confused with the physical standards for smart cards defined by ISO 7816.

SMART CARD Benefits or marketing talk?

Three of the benefits that Gemplus talks about on their web site are security, intelligence and convenience. [5]

For security, they state that their chip is tamper proof. What else would a smart card manufacturer want you to think? I've seen numerous smart card discussions and web sites mentioning that certain types of acids can dissolve the protective coating on a smart card. Other sources talk about a pocketknife to dig out the integrated circuit. Varying the voltage applied, the cards can also be manipulated in that manner. The bottom line is anyone and everything will eventually be hacked, some things just take longer than others to break. The amount of resources you have at hand can also make compromising something much easier. It doesn't matter if it's a smart card, password hash, control algorithm or what. If someone has the time and patience to crack it they will!!! Smart card manufacturers continue today to incorporate things like phantom transistors in cards today to make examination more difficult. Also upper and lower limits of the card's clock frequency also hinder the examination of the circuitry. [5]

On the intelligence issue I would have to agree with the fact that smart cards are intelligent. Anything with a microprocessor chip, operating system, and some amount of memory is going to be intelligent, It's the human side of things that make all computers un-intelligent (How many people do you know who write down their pin umbers and passwords on a piece of paper and keep them someplace like a wallet!!! What a security issue that is!!). The great thing about the evolution of smart cards is the fact that you can write an application that uses or manipulates information on that smart card. Previous magnetic strip cards had no logic whatsoever included. They were just basic storage devices. Not much security on those babies! Ever get your credit cards zapped when you got too close to a magnet!! I have!!! About 10 years ago I lived in Alexandria, Virginia. They had a giveaway day for riders of the local bus service. They gave away refrigerator magnets. Oh my!!!! You should have seen the people who put them in their wallets near a metro card standing at the reader wondering why they didn't work anymore. I had already been burned before that so I knew not to do that.

The convenience of the smart card will no doubt be a selling point for it. Logical and physical access via one device would make a lot of systems integration work much simpler. There is an underlying cost with smart cards. You'll need to buy the actual cards first. The more features you have on the card the more it will cost. You'll need some sort of reader obviously to read the card. That's another cost item.

A few SMART CARD Applications

Windows for Smart cards: Microsoft has embraced the smart card technology as a way to authenticate users logging into a Windows network. The cards can be used to log on to a PC or to one or more networks and to perform remote logons. They claim it can "enhance protection, improve productivity, increase profit, and facilitate promotion". To log on to a computer with a smart card, users do not need to press CTRL+ALT+DEL. They simply insert the smart card into the smart card reader, and they are prompted for their personal identification number (PIN) instead of their user name and password (and domain, if applicable). [6]

Smart Cards can also be used to:

Store a user's key pair.
Store an associated public key certificate.
Retrieve the public key certificate.
Complete private key operations on behalf of the user.

Other Smart Card Uses

Smart cards are being deployed almost everywhere these days. You can find them used in phone cards, credit cards, debit cards, supermarkets, and security access cards. Mass transit and parking application are also another example of smart card usage. The majority of these are antiquated implementations of smart card technology.

In my mind someday we will have one standard smart card that will be used for every electronic function we do everyday. Will it be a Java card or PC/SC cars? That question I believe can't be answered today. If you loose that card or it gets stolen it will be like loosing every credit, metro, supermarket, phone, and all your major documents you have all at once.

Biometric smart cards are also beginning to become available on the market today. Biometric smart cards can use things like your fingerprint to verify your identity. Other biometric type cards can use things such as facial and voice recognition to verify your identity.

Personal information about you can also be stored on the smart card. Thing like you medical information and other similar type information are finding their way onto these cards. The defense department today uses smart cards in this way.

SMART CARDS in the Federal Arena

The federal government is also embracing the use of smart cards. I don't want people to think and I don't mean to say in the last section that the federal government does not use or hasn't embraced the use of smart cards. That's definitely not the case. The National Institute of Standards publishes a web site, which contains a link to the Government Smart Card Interoperability specifications document. This document contains very specific technical documentation on the use of smart cards for the federal government. It also lists in the forward a short history of smart card deployment in the federal government. NIST works in conjunction with the General Services Administration on the smart card initiative. The GSA web site has a list of the many government projects (and a few commercial) that have successfully used a smart card deployment and a short description on what this technology was deployed to do. Upon review of that list you'll see that the Department of Defense has a large number of smart card related projects. One in particular is the CAC (Common Access Card) project. DOD has distributed 2.4 million smart cards to date. These are based on the JAVA card technology. The Office of Management and Budget has recently taken on the Smart Card/PKI issues. OMB has created a group named the Federal Identity and Credentialing Committee. It has combined two former federal working groups the Federal PKI Steering Committee and Smart Card Interagency Advisory Board to create the FICC. It will operate under the guidance of the E-Authentication E-Government Initiative. It hopes to

standardize how all Federal agencies will someday interoperate for physical and logical resource access. Another benefit of this group will be its ability to do procurements in bulk rather than have each agency do individual procurements. This should save the government substantial money. [7], [8], [9], [10], [11]

CONCLUSIONS and FINAL THOUGHTS.

I believe Smart cards will eventually be used to access every type of computer system we use today. Smart cards can add convenience and security to any transaction of value and data. Security will be a major driving force behind the use of smart cards. When used with a PKI based scenario with digital signatures they are some of the most cost effective solutions to manage network login. Soon every PC in every major company and government institution will have some sort of card reader attached to their workstation. Eventually your smart card will hold all the information and access keys you will need at work.

I can see how my job working in a large network environment could use some sort of smart card deployment already! Today we are only using proximity cards as an access method for facility access. They are basically everyone's identification badges. For access to our computer systems we still use the standard userid/password login scheme. Physical and logical access controls used with one smart card would be a great benefit and would save considerable amounts of resources, both human and capital.

If I were to have an input on how the smart cards would be deployed I'd like to focus it on a single sign on solution for access to our systems and among other things would include it as a facility access management solution. It could also be used as the underlying base for an Identity management solution, which could include resource access, role based computing, single sign on for applications and probably the biggest benefit of smart cards would be the main storage and management of user account information. Of course you would have to implement an underlying directory/meta-directory service for the storage of this information. An Identity management product would also be needed to accomplish the role based computing goal. PKI and digital signatures would be a big part of this environment.

The problems with hacking of smart cards will always be a factor. The major players who offer services that use smart cards will always be at risk. Anything that people can do to make an easy buck will always attract some element of society with the brains and resources to exploit that system. The bigger problem with smart card will happen when your life is contained on the card. With the infancy of the smart card today for logical access to systems I can also see there will be many issues forthcoming. Today we haven't even cracked the possibility for many uses of the smart card. Once more and more applications

are written using smart cards more people will become interested in fining ways to exploit their use.

Biometric smart cards will be the safest toll we could use against hacking. Storing a fingerprint image on the card and then verifying it at the card reader will give us a touch more security than a pin based smart card system.

A couple of other conclusions I'd like to make are from doing research on smart cards it seems to me that Europe has embraced the smart card technology more aggressively than the United States. I think over the next few years that will change especially in the Federal government community.

Another thought is that smart cards seem to be heading the same direction of operating systems. Basically two flavors, the Microsoft flavor which would be to embrace the PC/SC smart card standards, and the open systems type of card supported by the OCF standard. Looks sort of like windows vs. UNIX/java all over again. The M.U.S.C.L.E group with their port to Linux may fix that issue depending on how it is embraced by the user community. I would say that competition in any industry is good and drives each side to make a better product.

REFERENCES:

1. “Smart card”, Febrauary 25 2002,

URL : http://webopedia.internet.com/TERM/s/smart_card.html

2. “What are ISO Standards?” , Cryptography Standards,

URL: http://www.rsasecurity.com/rsalabs/faq/5-3-4.html

3. “What is OpenCard and the OpenCard Framework”

URL: http://www.opencard.org/overview.shtml

4. “Java Card Platform”

URL: http://java.sun.com/products/javacard/

5. “Smat Card Basics”

URL: http://www.gemplus.com/basics/benefits.html

6. “Introduction to Windows for Smart Cards” ,Smart Card Deployment Cookbook, March 2001

URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/smrtcard/smrtcdcb/sec1/smartc01.asp

7. “Smart Card Standards and Research”, Smart Card Research and Development, February 13, 2003.

URL: http://smartcard.nist.gov

8. Dray, Jim. Goldfine, Alan. Iorga, Michaela. Scharwzoff, Teresa. Wack, John. “Government Smartcard Interoperability Specification”, Version 2.0, July 8, 2002

URL: http://smartcard.nist.gov/GSCISV2-0.pdf

9. “Smart Card Standards and Interoperability”

URL: http://www.smartcard.gov

10. “SmartData”

URL: http://estrategy.gov/scripts/sc_viewer.asp

11. Jackson, William. “BIG DEAL: DOD puts millions of smart cards into play”, Government Computer News, June 9, 2003

URL: http://www.gcn.com/22_14/cover/22332-1.html