Global Information Assurance Certification Paper

SMART CARDS – READY FOR PRIME TIME?

Carol Stettler

July 10, 2000

Introduction

This purpose of this paper is to provide some basic information on smart card technology. Smart cards and their uses are described as well as some implementation and security issues that should be considered.

What is a Smart Card

Smart cards resemble the many credit cards we carry in our wallets, but instead of the magnetic stripe they have an electronic microchip embedded in them. This microchip allows for the storage and retrieval of information as well as for data manipulation, depending on the type of chip used. A memory chip allows for storage and retrieval only while the microprocessor chip can also manipulate the data in its memory.

In addition to the two basic types of microchips, smart cards fall into two basic categories – contact and contactless. Contact cards must be inserted into a smart card reader which makes contact with electrical connectors that transfer data to and from the chip. Contactless cards are passed near an antenna to carry out a transaction. These cards have an antenna embedded inside the microchip that allows the card to communicate with an antenna coupler unit without physical contact. The contactless cards are powered by the microwave frequencies from the source card reader and need to come within 2 to 3 inches of the source to be powered.

Most smart cards today contain an 8-bit microcontroller and hold 16 KB of information. Expectations are that cards will soon hold 32K.

The international standards organization has developed standards for the size of the card (ISO 7810), as well as the physical characteristics of the plastic including the temperature range and flexibility, position of the electrical contacts, and how the microchip communicates with the outside world (ISO 7816). A number of standards have also been developed to address specific card applications such as electronic purses and credit card functions.

Smart Card Uses

Smart cards, particularly those with microprocessor chips, have a seemingly infinite number of uses. Because the microprocessor chip has processing capabilities, it can add or subtract values. Applications and data can be downloaded to provide a variety of functions. The capability exists for smart cards to replace the multitude of credit, id, and access cards we carry around today – one card that does it all.

Smart cards are widely used throughout the world, particularly in Europe. The first real applications appeared in France in 1985, where the cards have been used heavily by banking industry. In fact, French banks claim to have reduced fraud by 92% within 5 years by moving away from magnetic stripe cards.

The US has been slow to adopt smart cards. American Express released its Blue Card in October, 1999. But Harvey Golub, American Express CEO, claims that rival firms Visa and MasterCard have stifled smart card development by arguing that moving from magnetic stripe cards to smart cards would be too expensive.

One of the most successful smart card applications in the US has been campus cards which are used for student ID, parking, ATM access, library check out, dorm access, vending machine payment, etc. Also, there are about 3 million subscribers in the US with smart card-secured mobile phones. The US Government uses smart cards in Armed Services and Health and Welfare agencies for ID. And the gas keys many consumers are waving in front of gas pumps are actually smart cards.

Other potential uses include storing data, such as personal information – address, birthdate, medical history, insurance policy information, bank accounts. Smart cards can be used as authentication and authorization security devices for portable and desktop computers, as well as for the increasingly popular personal digital assistants (PDAs). They can be used for building access, transportation fare cards, ground transport transactions, electronic purses (similar to bank debit cards), and merchant loyalty card (give points for purchasing goods and services, card discounts, special offers). In the situation where the data to be accessed isn't on the card itself, a smart card can also do certification.

Many industry analysts believe that the explosive growth of e-commerce applications will be the driving force for smart card adoption in the US. PKI is key in securing these transactions,

and smart cards afford one of the more secure methods of storing and allowing access to certificates associated with PKI proceedings. The recent passage of the E-signature bill will most likely also fuel the use of smart cards.

Third generation wireless handsets look likely to include a smart card reader to access Internet data networks securely. It is also likely that the day is not far off when every PC will be shipped with a smart card reader. The European smart card market could very well drive this, as well as the roll out of Windows 2000 and Windows Smart Cards.

Studies have shown that the number one help desk call is forgotten passwords. It is estimated that many companies could realize up to a 40% reduction in help desk calls if they were to eliminate passwords through the use of smart cards for computer authentication and authorization.

Implementation Issues

Interoperability and standards are the key issues to adopting smart cards. Making sure that different cards from different manufacturers as well as the applications that go with them work together is a critical factor. We need the ability to operate multi-application cards while not being limited to a particular card issuer or a system integrator's proprietary software. The cards need to be expandable to accommodate the inclusion of new applications. Plus they need forward compatibility to accommodate new features as technology matures.

The smart card implementer must consider the time, expertise, and expense of implementing this technology. Smart cards cannot operate without the readers, servers, customization systems, and encryption key management systems that provide them with their functionality. This whole environment requires extensive know how in terms of system architecture, methodology, and security. The cards themselves can be costly ranging anywhere from about $15 a card for Java or Multos cards to $2-$4 for the new Windows Smart Cards. The costs associated with implementing smart cards must be weighed against the potential benefits and savings that can be realized.

Security Issues

Defining who can access the information can control card access. For example, information can be made accessible to anyone holding the card (requiring no authentication), to the card owner only (controlled through authentication such as passwords or PINs), or to the card issuer only (e.g. electronic purses).

Access can also be controlled by how the information can be accessed – read only, add to, modify, or erase.

Ideally a card system should include various security mechanisms for access such as passwords, PINs, biometrics, etc. When passwords or PINs are used, cards should be set to lock after 3 unsuccessful attempts.

Some smart cards are capable of ciphering and deciphering so that stored information can be transmitted without compromising confidentiality.

Other security benefits include portability -- users can carry the cards with them providing more secure authentication from home. Also, since smart cards are tangible objects, missing or stolen cards are more likely to be noticed versus stolen/compromised passwords. And smart cards used for authentication can eliminate the need to memorize multiple passwords so that different passwords can be easily employed for every application.

In the PKI arena, certificates stored on smart cards are not vulnerable to drive crashes and viruses and cannot be copied unlike when stored on disk. Also, smart cards allow greater mobility for PKI.

Can smart cards be compromised? Like any other security product you can think of, the answer is yes. Compromise methods include reverse engineering of the chip, trying to crack the algorithms that secure the data on the chip, and even tracking the radio waves that are generated between the card and reader. Various invasive and non-invasive attacks along with suggested countermeasures are detailed in a paper titled "Design Principles for Tamper-Resistant Smartcard Processors" by Oliver Kommerling and Markus G. Kuhn. Reverse engineering techniques are described which are designed to access information stored on the cards, bypass built-in security mechanisms, and build duplicate cards.

One thing to keep in mind is that the reverse engineering techniques described in the Kommerling/Kuhn paper are expensive, which tends to eliminate the script kiddie variety of crackers. It is probably safe to say that smart cards are much more difficult and costly to compromise than passwords. Like any other security device, the potential threats must be weighed against the benefits. Smart card vendors should be questioned

as to what steps have been taken to impede the reverse engineering of their cards.

Other Considerations

Another topic frequently discussed with smart cards is the issue of privacy. Would privacy be at stake if a single smart card would ever become a person's solitary identifier? Privacy is a strong concern in the US. People are concerned that big brother is watching and with a card that does everything, it would be easy for the government to keep an eye on people. For this reason, a single identification chip is probably the wrong direction to go in. The flip side to this argument is that people and actions can already be tracked through regular credit card purchases, etc. Also, people often voluntarily give out social security numbers and other personal information.

Smart cards are currently further along on the maturity curve than biometrics. Biometrics are still viewed as being somewhat exotic and an invasion of privacy. People seem to be more comfortable with card security.

Some believe it is only a matter of when, not if, smart card technology will be fully realized. According to Gemplus, a major international player in the smart card industry, the Gartner Group's Dataquest predicts that there will be a $6.8 billion worldwide market for chip cards in 2002. Dataquest further states that the applications for smart cards will expand to perform identification and security functions in computing and Internet access.

Conclusion

It appears highly likely that the use of smart cards will become the norm over the next few years. The only questions are the extent of their use and how many we will have to carry around. This, of course, will depend on how well they are accepted by the general public. Security professionals may find it prudent to investigate smart card technology and its security implications to determine the best fit in their corporate environments.

References

"A Token Gesture." SC Magazine. February 2000.
URL: http://www.scmagazine.com/scmagazine/2000_02/testc/testc.html (28 June 2000).

Armstrong, Illena. "Shunned or Supported Smartcards Abound." SC Magazine. March 2000.
URL: http://www.scmagazine.com/scmagazine/2000_03/feature.html (28 June 2000).

Cagliostro, Charles. "Rosy Outlook Predicted for US Smart Card Market." Nov/Dec 1999.

Leung, Amy. "Smart Cards Seem a Sure Bet."
URL: http://www.americanpacific.net/html/wp1.htm (28 June 2000).

Oliver Kommerling, Markus G. Kuhn. "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 (28 June 2000)

Terence Goggin, Eric Carr, Steven Vaughan-Nichols. "Security Smart Cards: Back from the Dead?" 12 Dec 1999.
URL: http://www.zdnet.com/sr/stories/issue/0,4537,2409604-3,00.html (28 June 2000).

"The Smart Card Market Opportunity." 04 Feb 2000.
URL: http://www.microsoft.com/windowsce/smartcard/start/background.asp (28 June 2000).

Trott, Bob. "Credit Card Duopoly Attracts Antitrust Fire." Infoworld. 19 June 2000.

"What is a Smart Card." 29 May 2000.
URL: http://www.gemplus.com/basics/what.htm (28 June 2000).

"Why is a Smart Card Secure." 29 May 2000. URL:
http://www.gemplus.com/basics/why.htm (28 June 2000).

Last Updated: July 25th, 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
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
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS