GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Smartcards: Understanding Smart Technology

Ahmed Qurram Baig, CISSP

Jan 13, 2003

Abstract

Smart cards are part of most of our lives and most of us use them in some or the other way for our everyday transaction, to start with I wanted to check my own wallet to see how many smart cards did I have myself, to my surprise I found most of the cards I had like credit card, ATM card, ID Card, Health Card and shopping rewards/points cards were all smart cards. This made me very inquisitive to do more research and understand this technology.

The purposes of this paper is to understand the smart card technology, security issues, pro and cons of implementing smart cards and learn more about the various areas of applications for this technology.

Introduction

Smartcards are credit card sized cards with an embedded microprocessor chip with internal memory or just memory chip with non-programming logic. The contact between the smartcard and the detection systems is via direct (physical contact) or contactless using radio frequency. Smartcards not only allow storage of information but also have the capability to process information (Microprocessor cards); Infact a smartcard could also be considered as world's smallest computer.

Evolution of Smartcard

The initial research and development on smartcards started in early 70's in France, Germany and Japan, Dr. Kunitaka Arimura filed the first patent on smartcard concept in 1970 and Roland Moreno of France filed the original patent for the IC card in 1974 which was later named Smartcard and Bull CP8, SGS Thomson and Schlumberge were one of the first manufacturers of Smartcard in 1977,

Why Smartcard

Passwords and biometrics are widely used to authenticate the user identity and are vulnerable to various attacks like keylogging and dictionary attacks. Biometrics solutions like fingerprint or retina scan are nothing more than a large mathematical number derived from unique, immutable biological characteristics that make for a strong password. Yet it's subjected to the same replay-attack that a password is. If a hacker were to intercept this transmission and obtain this "password/template information" it could be used in the future with malicious intent. While a biometric solution is a strong way to prove "who you are", it does not address the "what you have" criteria like smart cards. Let's also understand that the comparison biometric data is either stored on the reading device itself or a central database, which could be a bigger threat if compromised, risking individual's privacy.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Because the biometric data of every individual would be unique to himself always and once this is compromised it would be a lifelong threat. I hope this give us a general idea about the risk of biometrics.

Data stored in a smartcard is protected by secure and sophisticated mechanism making it difficult for an attacker to compromise information on it. It also works on multiple applications (Access control, Banking, Health care, Transportation) allowing cross compatibility with various devices like PC's, PDA, Mobile phones, ATM's, Digital receivers and many more devices.

Smartcards with higher memory capacity are ideal for keeping the Secret keys private in a secure environment. For instance the threats we understood earlier related to biometrics could be resolved by storing the biometric template of an individual on his Smartcard rather than the reader or central database, this allows him to get authenticated with applications by using biometric template data stored on his smart card and also the complete computation happens on the smart card itself without any template information being exported outside the card.

Certain obstacles to accept/implement smartcards

There are many advantages of smart cards but it faces the similar problems like most of the technology products and that is the lack of standards which leads to failure of interoperability among different vendors and platforms.

Though the smart cards are standard the applications accessing the smart card are different and companies involved in smartcards applications offer various benefits with company specific COS (Chip Operating System) which again leads to failure of standardization and leads to consumer difficulties to select the right solutions and above all is lack of infrastructure to accept smartcards in most part of the world which is a prime reason which took Smartcard such a long time to get popular.

Similar benefits and application support is available with cheaper cost, Ex: iButton , iKey (Works on USB interface which is available on most the Personal Computers) and it's much easier to install and configure than Smartcards, Installation of smartcard reader and application at times is difficult on various operating systems unless you have proper instructions and drivers available. But these USB tokens are easily to install, configure and use with same level of security. The greatest challenge of acceptance device of these USB token is solved as most of the PC's today have USB connector built-in and USB also adds reliability and ease of carrying around these tokens which are a part of your key chains.

During the period of writing this paper I installed and tested USB, Built-in and PCMCIA readers. Installing these on Windows 98™ and Windows ME™ was very easy while Windows 2000™ needed an update to be downloaded, but the real problem was when it was installed on Windows XP. It required vendor specific drivers and proper version of DLL files. Some vendors also provide tools which could help you diagnose and install smartcard system files like the one here http://www.cardwerk.com/devsupport/devtools.aspx

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Types of Smartcards, ISO standards, Access specifications and it's applications

Now let's look at various types of readers, Smartcards, Smartcard technology and its applications.

Types of Smartcards

- Magnetic Stripe Cards - Also known as memory cards because it only stores the private information without any internal processing capability, normally used as credit/debit cards, these cards are normally contact cards which needs a device to read the information from the magnetic stripe.
  Magnetic cards are prone to skimming attacks where in, any person who gets hold of the cards physically could swipe the cards through an illegal card reader called "Skimmer" and copy the data encoded on the cards to counterfeit cards which rack up illegal charges/ transactions.

- Proximity cards (Contactless card) – These cards are embedded with a computer chip and an aerial/antenna to emit signal to the cards accessing device, once the card is within the proximity of few centimeters the access device pick up the signal and verifies the user against the access control and allows him access to a particular area or device.
  Proximity cards are ideal substitute to allow legitimate user to different work areas in an organization without him needing many different keys to open locks. It is also difficult to monitor user access time and duration with conventional CCTV or other older mechanism but with contactless cards, report can be easily generated to check information related to user access.

- Microprocessor Chip Card - These cards have an inbuilt processor (Integrated Circuit - Chip) capable of processing information apart from storing private information. This chip is similar to the processor we find in a personal computer and it also runs on a COS (Chip Operating System) which manages data via organized file structure/ File System.
  Chip cards are ideal solutions for card based authentication on computing devices to check user's identity with digital certificates/ stored cryptographic information on the card. Chip cards allow users to encrypt the personal content like files, worksheets dataset or any file on their laptops/home folders, allowing only a card holder to decrypt the file for viewing or modification; this solves the problem of user botheration against administrators of the network having full control over user files.
  Remote access and VPN are most widely used technologies which require secure authentication and it's clear by now that most of the security practitioners recommend using dual factor authentication for this, like password and smart card/Token ID apart from other security measures. Though these cards store data securely if

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

somebody gets the pin code using Trojans or keyloggers and card itself from the victims system. The smart card can be misused easily.

- Combi Cards – Various combinations of security are available along with smartcards and these are proved to be better than just smartcard or any single security mechanism.
    1. Combination of a biometric device with Smartcard, this could provide you with Two/three factor authentication i.e. biometric (Fingerprint, IRIS Scan), Smartcard and pin/password. This mechanism is one of the best among all the solutions because it check for who you are (Biometrics), what you have (Smart card) and what you know (Pin/Password) the chances of compromising this solution is difficult, even if one loses the card he cannot use it anyway as he does know the pin/password and he also doesn't have the similar fingerprint/ Iris.
    2. Combination of contact card (Microprocessor chip card) and contactless card (Proximity cards) is quiet commonly used in many organizations taking advantage of a single card used in multiple applications, using proximity card to get access to secure work areas and authenticating/ securing information with microprocessor cards on the information network.
       This solution is not as secure as the previous one because one can steal and use the access card to enter secure work areas and if he knows the pin/password he can even access the information network.

ISO Standards

ISO standards have defined various specifications for Smartcards which include specification for physical structure, Application Programming Interface (API)/commands, Card Accepting devices (CAD) also know as Smartcard terminals, PC/SC (Personal Computer/Smartcard) reader specification for computing environment and EMV (Euro/Master/Visa) for financial applications like credit/debit cards.

Cards claiming to meet International Standards Organization (ISO) specifications must achieve set test results covering drop, flexing, abrasion, concentrated load, temperature, humidity, static electricity, chemical attack, and ultra-violet, X-ray, and magnetic field tests.

Access Specifications:

Access specification is the mechanism in which the smart card applications would access its hardware and cards; there are various specifications from different vendors and groups, some are given below.

- PKCS#11 specifies API to devices which hold cryptographic information and perform cryptographic function. It uses a simple object based approach allowing various devices to access the cryptographic token from various applications like web browsers and devices like

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

PDA's and mobiles. The biggest challenge here is to secure the digital certificates itself as it available in an importable file format for mail clients and web browsers.

- OpenCard aims at having an open architecture for card terminal vendors, card OS and cards issuers applications (Embedded Applications) using Java, thus allowing total interpretability between various applications, though this seems very interesting with advantages like enabling **card issuers** to select from a broader range of solutions to offer and allowing card reader manufacturers to get into various markets to sell their products which are currently dominated by key players.
  But I strongly feel this kind of framework is very risky and if the card is compromised on can get affected by different means.

- JavaCard™ as per the name is based on Java programming and has one advantage of inherent security of Java programming language. The open process for design and development of Java Card and it's proven deployments and security evaluations are one of the key reasons for the success of this specification. Vendors like SchlumbergeSEMA market various Java Cards named as the CyberFlex series for various applications.

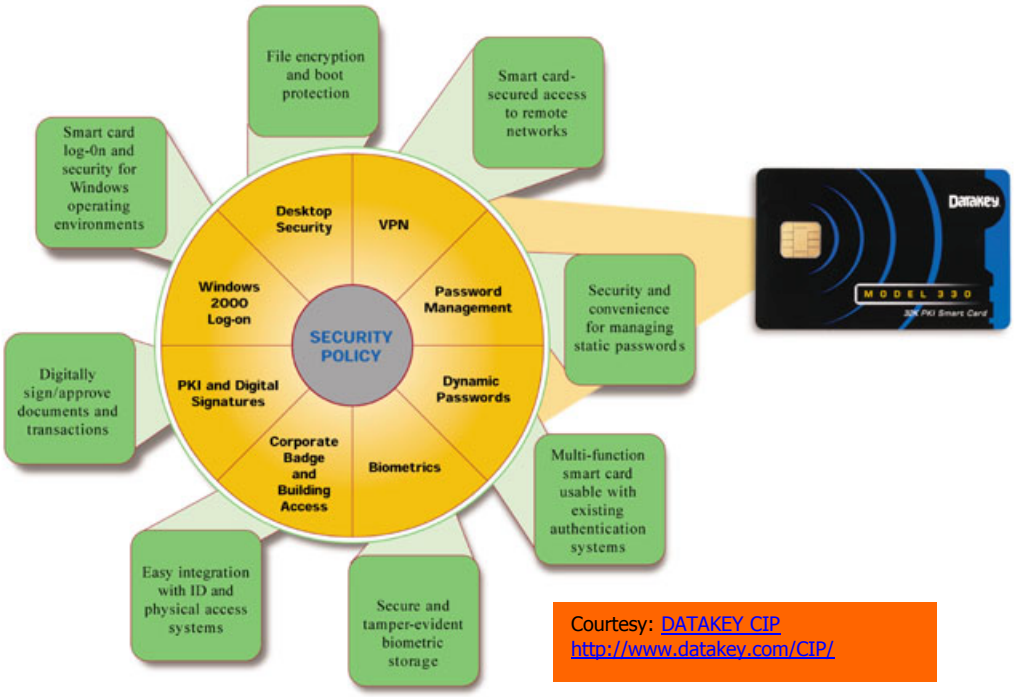
Applications of Smartcards

Shown below are examples of smartcard applications.

Financial Applications

- Electronic Purse to replace coins for small purchases in vending machines and over-the-counter transactions. VISA CashCard issued during Olympics 1996 were the best example for this and Singapore's Net CashCard system is a Smartcard which acts like electronic purse and holds the money; the money can be spent for Payment in Parking Lots, museums, telephones, fast food joints, vending machines, transportations and many more places.
  Ref: http://www.nets.com.sg/services/benefits.php?prodID=8

© SANS Institute 2003, Author retains full rights.



Common Applications of a single Smart Card

Communications & Entertainment Applications

- Subscriber Identification Module (SIM) providing secure initiation of calls and identification of caller (for billing purposes) on any Global System Mobile Communications (GSM) Mobile Phones. According to the survey don't by GSM World around 763 million cards used worldwide, this is one of the biggest applications of smartcards in the world after payphone cards,
- Subscriber activation for various programmes on Pay-TV like Showtime and others is a big market for smart cards.

Government Applications

- Smart card National ID: Smart Card based National ID's project have started to take of in many countries among which Sultanate of Oman is first middle east country to deploy 1.2 million National ID cards to it's residents. Gemplus, one of the leading providers of smart cards is behind this project with their solution called ResIDent for this purpose. Smart Card is one of the most secure mechanism today compared to any other type of ID cards, but when applications start to be deployed in such large scales it must taken care to make sure the whole system of such a project is secure rather than just the information on the smart card, failing to do so will result for high threats and failure of such systems.
- Health Cards: This solution is popular and can be found available for citizens of countries like France, Germany, Slovenia, Belgium, it was estimated that in Europe alone 32 million smart card were shipped for government and healthcare systems

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Driving license: The citizens of Argentina, El Salvador don't need to carry dumb cards/ license booklets as a proof of eligibility to drive; they are allotted smart cards with their complete information on it. This almost reduces the license fraud to none with a secure mechanism which is difficult to be faked.

Information Security

- PC cards: Chip cards are used today by majority of the corporations like Microsoft, Oracle to access their networks, chip cards can be incorporated with technologies like Active Directory to store the PKI certificates for authentications makes it dual factor (Digital Certificate + User password) and the it also allows the users to encrypt the files and digitally sign the emails. The advantage of this mechanism is that in case of any damage to smart card due to tampering/usage the user data is still secure to be decrypted by issuing a new card with the same original Digital Certificate. Incase the smart card is lost or if company decided no to reissue the same digital certificate to avoid any kind security breach, they can reissue the smart card with a new private key (Digital Certificate) and the data can be decrypted for the user by an special key. Giving access to the user in a decrypted form which could be encrypted again with his new smart card encryption.

Physical Access

- Employee access card are used in most of the organizations today and millions of cards are being distributed every year catering this market, this mechanism replaces the conventional lock and key security, employees today don't need to carry different keys to different locks for the secure office areas and access can be given or terminated at given point with just a click on the access software without any management of conventional keys , with the older mechanism of lock and key any disgruntled employee could make a fake key of the original while it was in his possession and misuse it later but in the case of smart cards this is almost impossible and if higher security is needed then biometrics can be combined to protect physical access to facilities.

Retail and Loyalty

- Consumer reward/redemption tracking on a smart loyalty card, that is marketed to specific consumer profiles and linked to one or more specific retailers serving that profile set. Most of the places in Europe and Middle East have Air Miles card which is an existing example which allows shoppers to gather points in common outlets and redeem these points for gifts.

University ID's

- Student ID card, containing a variety of applications such as electronic purse (for vending and laundry machines), library card, meal card and transportation are used and University of Nottingham is one them

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Additional Information on security and Reliability
We also need to understand that smartcards are tamper resistant and not tamper proof.

Security Considerations
Smartcards are one of the most economical and secure way to protect information and resources in most of the environments, Smartcards are renewable security elements in total security design, they requires correct pin code to be entered to any kind of access, failing to do so can block the access to the card after specific tries, which requires to be unblocked by a unblocking code, if the unblocking code is entered incorrectly after few tries it will permanently block the card making it unusable.

Like any other technology smartcard has to be used in a secure computing environment and avoid sharing with other users, the systems on which smartcard are installed have to be secured by other threats like key loggers or sniffers, which could cause a threat to the security otherwise.

Security threats to smartcard technology can be seen in the document published by Bruce Schneier and Adam Shostack on counterpane website, the common attacks on the smartcard are like

- Power attacks/ Non-invasive attacks: Information is trapped by raising or dropping the supplied voltage to microcontroller,
- Differential Power Analysis : A statistical attack on a cryptographic algorithm which compares an hypothesis with a measured outcome and is often capable of extracting an encryption key from a smart card or other computing device
- Simple Power Analysis: This attacks records the data and does direct analysis of the recorded power data to determine actions and data.
- Physical attacks: These attacks are normally done of the card's microprocessor chip to either erase/reverse engineer the information stored on the card techniques like erasing the security lock bit by focusing UV light on the EPROM, probing the operation of the circuit by using microprobing needles, or using laser cutter microscopes to explore the chip.

Reliability:
Smartcard reliability is one of the complex issues that most of the organizations face today; there are multiple issues to be taken care of for a reliable environment.

Tips to protect the smartcard environment:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Smartcards and Smartcard readers have to be protected from physical damage and ensure that Smartcard terminals which are damaging the smartcards have to be either replaced or taken out of the system to stop any further damage, Smartcard users needs to be educated about card care to avoid any kind of physical damage to the card which could be caused by bending the card or punching hole on the card on wrong location which results in complete damage to the card, reporting of lost cards and replacement card issuing policies have to be in place for business continuity purpose and to avoid any kind of misuse, most Smartcard vendors guarantee at least 10,000 inserts for contact based smartcards,

Conclusion

Smartcard is an excellent technology to secure storage and authentication, if an organization can deploy this technology selecting the right type of solutions which is cross platform compatible and supports the standards required, it would be economical as well as secure.

This technology has to be standardized and used in various applications in an organization not just for physical access or information access. Imagine having an Employee ID cards which acts an access card to secure work areas, login to various systems on the network and also allows you to pay the bill at the office food court. This is no more a wish list solution; it is already available from various vendors like SchlumbergeSEMA and Datakey Smartcard is a big hit with the consumer industry (Pay TV, Pay Phone) and a huge growth is now happening in the smartcard access/authentication applications. Various developments are happening in the smartcard industry with respect to higher memory capacities and stronger encryption algorithms which could provide us with much tougher security. But we need to understand that we will achieve better security only if we have users educated to use these technology with at most care.

Smartcard Exhibitions and show worldwide

OMNICARD – Conference ideal for bankers, government ministries, public institutions etc... To meet and discuss requirements with chip and card manufacturers,
http://www.cartes.com – Smartcard to Secure applications and Transactions
http://www.advancedcardawards.com/ - Smartcard awards to innovations and improvements in the smartcard products
http://www.ctst.com/conferences/CTST/CTST2002/index.htm - Smartcard and secure Technologies event held in North America.

Reference:

1. Smart cards "What's so smart about smart cards", 2002 Gemplus CA http://www.gemplus.com/basics/index.html (11 Jan, 2003)

2. "Contactless Technology for Secure Physical Access: Technology and Standards Choices", Smart card Alliance, 2002

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://www.smartcardalliance.org/alliance_activities/Contactless_Technology_whitepaper.cfm (11 Jan, 2003)

3. Cardwerk – Smart Card Solutions, "Smart Cards", Copyright 1999 – 2003, Jacquinot Consulting, Inc. http://www.cardwerk.com/smartcards/smartcard_overview.aspx (11 Jan, 2003)

4. Biocentric Solutions, "Why Use a Biometric and a Card in the Same Device?", 2002 http://www.bitpipe.com/data/bizcard?res_id=994763535_930 (11 Jan, 2003)

5. "Securing VPN with Smartcards", Datakey http://www.datakey.com/cardpage/documentDownloads/vpn.shtml (11 Jan 2003)

6. "Hypercom Launches Attack on Credit Card Skimming" 6/7/01, Hypercom corp. http://www.hypercom.com/web/news/display.asp?releaseID=346

7. Bruce Schneier and Adam Shostack "Smart Card threats", Counterpane systems and Netect, Inc. Oct 19, 1999 http://www.counterpane.com/smart-card-threats.pdf (11 Jan, 2003)

8. Ross Anderson, Markus Kuhn "Tamper Resistance - a Cautionary Note" Cambridge University http://www.cl.cam.ac.uk/users/rja14/tamper.html (11 Jan 2003)

9. RSA Security "PKCS #11 - Cryptographic Token Interface Standard", © 2002 http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/ (11 Jan, 2003)

10. "Java Card™ Platform Security" technical White paper, Sun Microsystems © 2002 http://java.sun.com/products/javacard/JavaCardSecurityWhitePaper.pdf

11. Smart card Alliance "Gemplus Introduces `ResIDent' - A Secure ID Solution for E-Government Programs", 13 Nov 2002 http://www.smartcardalliance.org/industry_news/industry_news_item.cfm?id=264

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.