Global Information Assurance Certification Paper

Smart Card - An Alternative to Password Authentication

Ahmad Ismadi Yazid B. Sukaimi
SANS Security Essentials
GSEC Practical Assignment Version 1.2d.

Purpose

This paper is intended to describe the benefits of smart card implementation and it combination with Public Key infrastructure (PKI) as a dual factor authentication to assist organization in seeking alternatives to conventional password base system (single factor authentication).

Introduction

Impersonation, in which somebody claims to be somebody else, is one of the most dangerous security threats. The security services that counter these threats are identification and authentication. The goal of authentication is to protect a system against unauthorized use. Therefore, a trusted user needs to be verified before any transaction can be done. Mainly, authentication method is based on the following approaches or combination of them: -

- **Proof By knowledge**
  The known information regarding the claimed identity that can only be known or produced by principal with that identity. (E.g. password, personal Identification Number (PIN).

- **Proof by Possession**
  The claimant is authorized by possession of an object (e.g. magnetic card, smart cards, passport, and optical card).

- **Proof by Property**
  Authorization comes from direct measurement of certain claimant properties using unique human characteristic (e.g. Biometric such as fingerprint, retina scanning, voice, DNA).

Although biometric authentication provides the most secure environment, but incompatibility among these methods has been major reason for the slow adoption of it. Interoperability among different vendor's products is a necessary requirement to enable broad consumer acceptance of authentication methods. Therefore, the need for security and enhanced privacy is growing. The emergence of the Internet and expansion of the corporate network have accelerated the demand for secure and practical solution.

Why use smart card?

Any system is only as strong as its weakest link. Therefore, it is necessary to look at all of the value-added components in any smart card system. Chips and card suppliers are more than willing to let you know why their chip is most secure. Reader and point-of-sale terminal manufacturers are constantly implementing higher levels of security in to their equipment. In addition, the

entire industry is constantly being audited by governments and the financial institutions to ensure that its products and processes meet stringent industry and government standards. Smart cards actually offer more security and confidentiality than a user ID and password system, making it a perfect solution for e-commerce transactions and other Internet connection activity. A smart card is a safe place to store valuable information such as private keys, account numbers, passwords, or personal information. Smart cards have computational or processing power to provide greater security, allowing verification of the cardholder. The benefit of a smart card is that you can verify the Personnel Identification Number or biometric authentication such as fingerprint securely, off-line.

A smart card is a credit card sized plastic card with a microprocessor chip embedded in the card that makes it smart. Depending on the type of embedded chip, smart cards can be Java Cards, memory cards or processor cards.

- Java card - these card specifications enable Java technology to run on smarts card and other devices with limited memory. Most of telecommunication providers use this type of card for their cellular phone system.
- Memory Cards - The chip acts as a memory storage device. Most usage of this card type is for phone card and ticket. The card stored rechargeable value and can be used many times.
- Processor cards - Smart cards with a full-fledged microprocessor on board can function as a processor device that offer multiple functions, such as encryption, advanced security mechanism, local data processing, complex calculation and other interactive process.

The information or application stored in the IC Chip is transferred through an electronic module that interconnects with a terminal or card reader. The card is "smart" since it contains its own processor, memory and operating system. The smart card has considerably more abilities than 'regular tokens' because of the microchip embedded in the card. For strong security implementation, i.e. using PKI solution via a smart card medium, it is highly recommended to use cryptographic card with strong encryption.

What are the major benefits that smart cards offer consumers?

Most systems involve a tradeoff between security and convenience to the users. An advances security system is worthless if it is so convenience the user finds ways around it. For example, many users have so many password to remember today that they write them down near their workstation or choose an easily guess password. Smart cards can help in most security system, because they can perform security tasks (like remembering difficult password) that user find burdensome. Smart cards contain unique features that bring many benefits to both consumers and issuing organizations. Amongst others, the advantages of using smart card are: -

- Smart cards provide a portable, easy to use form factor that many are familiar with using.
- Capable of processing, not just storing information.
- The processing power of a smart card makes it ideal to mix multiple functions thereby enabling ability to carry out offline, online and peer - to-peer transactions.
- Secret key information is stored tamperproof on the card. Secret key operation is performed directly on the card; therefore, no Trojan horses can spy the secret key on the PC.
- High security when running cryptographic operations.
- Rights, profiles and keys are stored with the user (better support of traveling users).
- Smart cards can enable multi -authentication by accepting biometric authentication such as a thumbprint on the surface of the card.
- Mobility and portability -The certificate and private key are portable, In addition, it can be used on multiple workstations, whether they are at work, at home, or on the road. If the lower level software layers support it, they can be used by different software programs from different vendors, on different platforms, such as Windows, UNIX, and Mac
- Non-Repudiation - The ability to deny, after the fact, that your private key performed a digital signature is called repudiation. If, however, your private signing key exists only on a single smart card and only you know the PIN to that smart card, it is very difficult for others to impersonate your digital signature by using your private key.

Smart card implementation is not without some issues that need to be resolved. Some of those issues are -

- Central administration - Central update of rights profiles on smart cards needs to be maintained.
- Establishment of Administration/issuing authority is necessary to ensure that this system works efficiently.
- Costs - Price of implementing and maintaining this type of system compared to that of other token alternatives is expensive. Lost/forgotten smart card replacement costs also need to be taken into consideration.
- User operability - User operability of token authentication requires that the end user must maintain a piece of hardware.
- Social acceptance - Since the smart card operates virtually identically to the credit card, the user perceives this token authentication device as just another piece of plastic. Users are more comfortable with associating ownership with and protecting physical objects through experience with campus ID cards, etc.
- Extensive Implementation - The process of implementing a smart card system requires setting up the server, issuing a card to each user, training the user on how to employ the authentication process, and setting up the database to maintain the smart cards.
- Special reading hardware is necessary for users.

- Liability issues if lost or stolen, potential for too much data on one card if lost or stolen.
- Vulnerable to static electricity, magnetic field, temperature, ultraviolet lamp.

Design and implementation of Smart card -based security system

If you decide to implement smart card -based security in a system you are designing, it wise to think about how your design choices will affect the security of the whole system, especially cryptographic keys. The Important question to keep in mind is, how can I make it easy and transparent for users of this system to protect their cryptographic key in the smart card?

The smart card application consists of a package that establishes secure Internet access and secures connections for transactions over the Internet. By using Public Key Infrastructure (PKI) technology, it protects the integrity and confidentiality of transactions. A public key infrastructure (PKI) is the set of components that manages certificates and keys used by encryption and digital signature services. A good PKI must provide services for cryptographic operations, certificate enrollment and renewal, certificate distribution and validation, certificate revocation, plus administrative tools and services for managing all of the above. Mostly, the smart card system design will use either shared cryptographic system or public cryptographic system.

In the shared cryptographic key system it is inherently more difficult to complete protect the cryptographic key, because it must known at least in two places. The private key from smart card client must know it and the server must know it to verify the client. The public cryptographic keys system can be inherently more secure, but it is possible to make them insecure with the wrong system design choices. The following question relates to design choices on obtaining the cryptographic key in a security system. The designer should be seriously considered this before designing and implementing smart card application. Roughly, they are listed in order of increasing difficulty to get the cryptographic key. Furthermore, the following question must be asked:

- Does the private cryptographic key exist only on a smart card, where the user does not even know about it? This would imply that the smart card has the ability to generate cryptographic keys.
- Is the cryptographic key PIN protected on the smart card?
- Does the cryptographic key always perform its duty on the smart card or must it come into the computer for action, where it might sniffed by a malicious program?
- Is the private cryptographic key stored unprotected on the smart card?
- Is the private cryptographic key always protected on the smart card and never leaves? : This would imply that the smart card cans perform the algorithm (e.g. RSA, DSA) for which the cryptographic key is intended
- Is the cryptographic key from the smart card transmitted in clear text across the network?
- Is the private cryptographic key from the smart card stored in the workstation, wrapped by weak choosing password ?

- Is the cryptographic key shared between users ?

Many securities companies are enabling the ubiquity of smart card on desktop computer by defining necessary standard and deploying tools and reference implementations. The power of smart cards is becoming available to millions programmer who use development environment. When designing a program that can benefit from smart card, take step back and carefully consider the security aspects of the design. Smart cards can be used to enhance security and portability in a range of application limited only by imagination.

Standard and protocol involved in Smart Card -based system

To ensure interoperability among smart card and reader, it follows the International Standard Organization (ISO) ISO 7816 standards for integrated circuits cards with contact. This standard defines the physical dimensions of smart cards and their resistance to static electricity, electromagnetic radiation and bending forces , which are the common treat of smart card.

The Public-Key Cryptography Standards (PKCS)
This specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for accelerating the deployment of public -key cryptography. First published in 1991 because of meetings with a small group of early adopters of public-key technology, the PKCS documents have become widely referenced and implemented.

Some of the PKCS related to smart card applications and implementations are as follows :-

- **PKCS #11 Cryptographic Token Interface Standard**
  Most smart cards use PKCS #11 -. PKCS #11 defines a standard architecture for cryptographic hardware tokens, such as PCMCIA or smart cards that enable the highest level of data security available. This standard specifies an API, called Cryptoki, to devices that hold cryptograp hic information and perform cryptographic functions. Cryptoki, pronounced crypto-key and short for cryptographic token interface, follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sha ring (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a cryptographic token.

- **PKCS #15: Cryptographic Token Information Format Standard**
  PKCS #15 is intended at establishing a stand ard which ensure that users in fact will be able to use cryptographic tokens such as smart card to identify themselves to multiple, standards -aware applications, regardless of the application's cryptoki (or other token interface) provider.

- **PKCS #7 - Cryptographic Message Syntax Standard**
  This standard describes general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes

X.509 Standard

This popular PKI standard needs to be considered when implementing smart card authentication scheme in an enterprise environment. This standard defines what information can go into a certificate, and describes how to write it down (the data format), which is the best-known public-key certificate format.

Conclusion

Claiming that any system and technology is hundred percent secure would be irresponsible. Any system can be compromised if given the appropriate amount of resources. The main consideration for any system is whether the level of security meets with the level of effort that an entity would be willing to expand in order to compromise the security. Even though smart card is not the total solution, for the present situation, the current security platform provides more functionality, scalability, combination of many authentication methods (ID, password, biometric, PKI) and the practical solution. Implementation issues also need to be considered when dealing with smart card security. Choosing smart card as a part of authentication method will enhance the security and trust of people in transacting on the net. It may not be the best in all scenarios but better than just password authentication.

Reference

1. Internet Security Advisor - February 2000 -Enhance Security with smart card - John R.Vacca pg 18-24

2. Ivest - The smart card application -
URL : http://www.ivest.com.my/UserGuide/index.html

3. Understanding the Public Key Infrastructure
URL : http://www.developer.ibm.com/library/articles/sinn1.html

4. Smart Card Technical - Internet & Smart Cards
URL:
http://www.smartcardcentral.com/technical/articles/jsource/jsource_080999.asp

5. CRYPTO Card Network Security: More Secure... More Cost Effective
URL : http://www.cryptocard.com/Content/publicity/2001/article_apr1.cfm

6. RSA Laboratories Public Key Cryptography Standards (PKCS)
URL : http://www.rsasecurity.com/rsalabs/pkcs/index.html

7. Smart cards and smart card technology - CompInfo Directory
URL: http://www.compinfo-center.com/smart_cards.htm

Last Updated: July 28th, 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
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 Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	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
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
Community SANS Sacramento SEC401	Sacramento, CA	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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event