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

Smart Card Authentication
Added Security for Systems and Network Access

Lawrence Thompson
GSEC Practical Assignment
Version 1.4b
Option 1

© SANS Institute 2003, Author retains full rights.

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

Introduction

As security professionals one of our major objectives is ensuring that a person accessing a resource has the authority to do so. In order for users to access a resource it must be determined if this individual is whom they claim, if they have the necessary credentials, and they have been given the necessary rights and privileges to perform the actions requested. For most organizations user authentication is accomplished through a combination of username and password. Passwords are the foundation on which much of information security is built and an enterprise's first line of defense against unauthorized access. Smart cards can provide added security to help bolster that defense.

This paper will provide some background information on smart cards, identify some issues with traditional password security, focus on the added security of using smart cards for user authentication, as well as some practical uses for controlling system and network access. Smart card technology can also be deployed for physical access control but it is beyond the scope of this paper and therefore will not be discussed.

What is a smart card?

Smart cards are not a new technology. Roland Moreno invented and developed the first smart card in 1974.[1] They have been used in Europe for many years in healthcare, banking and telephone long distance services. Many people in the U.S. have no idea what smart cards are or how they can be used. Even those seasoned security professionals who have heard of smart cards, many have little or no experience with their use.

Identification is one of the important uses of the smart card technology. It is the motivation behind its development. Identifying a user can be accomplished in three ways; "something you know", "something you possess", or "something you are". Combining at least two of these methods is considered to be strong authentication. The use of smart cards can offer an added layer of security by combining these methods to provide multi-factor authentication.

The term "smart card" has been used to describe a class of credit card sized devices with varying capabilities: contact cards, proximity cards, stored value cards, and Integrated Circuit Cards (ICC).

Contact: A contact card has an imbedded integrated circuit and an electronic "contact" module. This module makes a physical connection to a smart card reader in order for a system to receive power and transfer information. Most commonly these types of cards follow the ISO 7816 standard for communication between the card and it's reader. Smart card readers are available in a variety of form-factors and can be connected to a computer using an RS-232, PCMCIA or USB interface.

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

Proximity (contactless): A proximity smart card receives its power from a radio frequency transmitter. It has an antenna coil embedded inside that communicates with an external receiving antenna. These cards conform to the ISO 14443 communication standard. They are known as “contactless” cards because the reader and card do not need to make direct contact but must be in the same proximity to work, generally about 10cm.

Stored Value: A stored value card has an EEPROM (Electrically Erasable Programmable Read-Only Memory) chip for storage. These cards tend to be the least expensive and are generally used when the data stored rarely changes.

Integrated Circuit: Integrated Circuit Cards (ICC) have an embedded microchip that is a combination of a microprocessor and an EEPROM memory chip. These cards also tend to be contact type cards due to the power requirements of the processor.

All of these cards differ in functionality from each other and from the more familiar magnetic stripe cards used by standard credit, debit, and ATM cards. Smart cards can store several hundred times more data than the conventional magnetic stripe card.

It is the ICC contact card that is of most interest to the computer industry over stored-value cards because it contains an operating system (OS) and is able to perform more sophisticated operations, including cryptographic functions. The two most common OS used are JavaCard and MULTOS (Multiple Operating System). Older smart cards have 32K bytes of memory, roughly the computing power of a Commodore 64.[2] Newer smart cards have more processing power that can perform cryptographic functions directly on the card.

Problems with passwords

Passwords are the enterprise’s first line of defense. They are the most widely used form of authentication method but they are far from adequate for ensuring a high level of security. According to the FBI’s list of five common mistakes that leave company and employee data vulnerable, weak passwords ranked #2. Some 40 percent of user’s passwords are “password”.[3]

A password policy is the basis for strong password enforcement. An example of a strong password policy from the SANS Security Essentials Manual:

- Passwords must change every 60 days.
- Accounts are locked after 3 failed attempts.
- All passwords must contain at least one alpha, one numeric, and one special character.
- Cannot reuse previous 5 passwords.

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

The above requirements may make for stronger passwords but they create other problems. These types of passwords are not very user-friendly. They are difficult for us as humans to remember, so we tend to write them down, place them in a desk drawer, under the keyboard, or use a sticky note on our computer monitor. Forgotten passwords are the number one type of help desk call – and the average help desk call costs $50 - $150 in resources and lost productivity.[4]

These strong passwords are designed to make it more difficult for a hacker to discover a users password. Type the words “password hacking” into any Internet search engine and you will discover there are a wide variety of password attacks and discovery methods, including sniffing, dictionary, brute force, personal information gathering, and social engineering. The most common and easiest method that a hacker may use is through social engineering.

Social engineering is the ability to exploit human nature. Since humans are “social” beings by nature, we tend to be friendly and trusting of other humans, especially if they are nice to us. Hackers will use this to their advantage and could pretend to be computer personnel and offering to help with a problem. They may say that in order help you they would require your account and password. Many users have been known to reveal this information because someone is willing to “help” them. This is one way in which a hacker could trick a user into disclosing their information. Even the strongest password becomes weak if freely disclosed.

There are other methods by which a hacker could discover passwords. Password cracking programs like Crack for Unix and L0phtCrack for Windows can run dictionary and brute force attacks against the encrypted password file to discover the user’s password. This is accomplished by comparing word-character combinations and the associated one-way hash with the stored hash value in the password file. This of course requires the hacker to actually have a copy of the password file, but there have been Trojan programs such as “PWSteal.Coced240b.Tro” and “Unix.Penguin” that copy the file and distribute it to hacker undetected via email.

Potential intruders value a password far more than the single computer it's protecting. Hackers who can get the password list from a server or PC can use those passwords to gain access to other computers on the network, bypassing all the high-tech security erected to keep them out.

Advantages of smart cards over passwords

The more difficult and longer the password, the more time the cracking programs will take to discover it. However, there is no password that cannot be discovered, it is just a matter of how much time and effort it will it take. Strong passwords still

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

only offer one-factor authentication, “something you know”. Once a password is discovered, it can be used to freely access your system.
In a recent news story, 30,000 consumers were the victims of the largest identity-theft scam to date. A former employee of a credit reporting agency allegedly used stolen access codes and passwords to illegally obtain credit reports. These were then later sold to as many as 20 conspirators who used them to obtain loans and credit cards in the names of the victims. Fraud losses are said to be in the millions. “This highlights the vulnerability of password-only security”, says Randy Vanderhoof, executive director for the Smart Card Alliance.[5]

Smart cards offer much more security than using passwords alone by using two-factor authentication. Instead of just requiring “something you know” (password), you add the requirement of “something you possess” (smart card). A common example of two-factor authentication is your ATM card. This requires something you possess (ATM card) and something you know (your PIN). Having one without the other results in no access. A hacker could learn password or PIN but it would be of no use without the smart card and vise versa.

Smart cards also have added security built-in due to their design. A user’s credentials are stored in non-volatile memory and can only be accessed through the card reader, the corresponding software and by entering the proper PIN or passcode. When a user needs to access a system, the system’s software sends the user’s card a random number. The card’s processor does a computation using the stored private information and sends the answer back to the system. If the response is as expected, access is granted. As such, the user can be validated without having to reveal the user’s private information to the system.

The cards have been designed so that they can be permanently locked if the wrong PIN is entered a specified number of times in a row. This prevents the credentials from being discovered in a dictionary or brute force type of attack. Smart cards are more difficult to tamper with or clone than magnetic stripe cards.[6]

Many times a user will have multiple usernames and passwords for access to different systems within the enterprise network. This can often cause confusion as to which password is for which system. Smart cards have the ability to store multiple user credentials on a single card that can then be used to authenticate to each system. This creates the ability to have a network Single Sign-On (SSO), which is the capability to have users log on to multiple systems with only having to remember one passcode. The user only needs to insert the smart card into the reader and enter the PIN one time. The processor on the card will authenticate the user to each system based on the stored credentials as needed. This can aid in reducing the number of help desk calls for forgotten passwords.

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

Passwords can be discovered and used for system access without the user even knowing it has occurred. Another advantage of using smart cards is that they are "tangible", meaning they are discernible by touch. If a user's card was ever stolen or misplaced, it is no longer in their possession and would be discovered quickly so the appropriate personnel could be notified. The user's credentials on the card could then be canceled and a new set of credentials and smart card created. This would prevent unauthorized access by anyone using the misplaced smart card.

Practical uses within the Enterprise

Windows Network Logon

There are several practical uses for smart cards as a means of providing two-factor authentication for access control. The most common is probably the network logon. Microsoft has built smart card usage into its Windows NT/2000/XP operating systems for network and computer system access. The smart card interfaces with the Windows Graphical Identification and Authentication (GINA) module to create an alternative method for user authentication in place of the Windows default username and password mechanism. The smart card is automatically detected when inserted into the reader and can trigger the Secure Attention Sequence (SAS), normally Ctrl + Alt + Del for NT/2000/XP. The user is prompted for and then enters their corresponding PIN, the credentials on the card are read, a cryptographic comparison is made, and the authentication process is completed.

Microsoft Windows® 2000 Active Directory has the ability to use Kerberos based authentication for network access, which can be used in conjunction with the Windows 2000/XP GINA to interface to a smart card. The Novell Modular Authentication Service (NMAS) and even Linux now support the use of smart cards for network and system authentication.

Users inherently leave their workstations without logging off creating a security risk. Another bonus to using smart cards as authentication to a Windows workstation is that if the smart card were removed, it could trigger the SAS to lock the user's workstation or to force all sessions to be logged off and the credentials to be flushed from the local system's cache.[7]

Public Key Infrastructure

Today the most common use of smart card deployment for system access within an enterprise is the facilitation of a Public Key Infrastructure (PKI). PKI is a major component of the Microsoft Windows® 2000 Active Directory where a user's public and private keys are the basis for authentication to the system. The identification of a user is based on the premise that only that user has knowledge of the private key.

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

Certificates containing the public and private keys can be distributed to the user securely on a smart card. They are encrypted using the cards on-board processor and stored in the non-volatile memory. The credentials can only be accessed when the user has entered the proper PIN, which is generally delivered separately from the card. This is usually done via telephone or standard mail delivery.

The private key is also used to decrypt email messages or files encrypted with the corresponding public key. This is designed to prevent anyone from reading the contents except for the party for which it was intended. The private key is also used to electronically "sign" a file or message for non-repudiation. It would be checked with the corresponding public key as a means to prove it came from the proper entity. If the private key were to be stolen or compromised, a form of identity theft would occur since the hacker could impersonate the "electronic identity" of that user.

Without the use of smart cards, the public and private keys used on a Microsoft Windows® system are stored in the system's registry. Since the Windows registry consists of the system.dat and user.dat files on the hard drive, this makes the keys vulnerable to an intruder and subject to being copied, exported, or deleted.

In Windows NT/9x, user certificates are stored in the registry under:

HKCU\Software\Microsoft\SystemCertificates\MY

In Windows 2000/XP, user certificates are stored on the local drive under:

%SystemDrive%:\Documents and Settings\<username>\
Application Data\Microsoft\SystemCertificates\My\Certificates

Even worse, the key may be appear in a swap file that contains the intermediate state of a previous signing session; or it may appear in a backup file automatically created by the operating system at fixed intervals; or it may appear on the disk in a damaged sector that is not considered part of the file system.[8]

With the use of smart cards, the public and private keys are stored on the card instead of the PC and less vulnerable to tampering. The smart card's on-board processor can handle all of the cryptographic functions needed so the user's private key never leaves the card. Since the credentials are not stored on the PC itself, this makes them portable. The user is not bound to using a single machine where the keys would be located, but can use any machine within the organization just like they could if using only passwords.

© SANS Institute 2003, Author retains full rights.

VPN and Remote Access

Virtual Private Networks (VPN) and remote access have been typical uses for smart card authentication for some time now. Since access to network resources does not take place in a physically controlled environment, username and password systems were simply not enough to provide good security. The implementation of smart cards has been in use even before the beginnings of PKI. Symmetric encryption keys and usernames were stored on the smart card and could only be accessed by entering the proper PIN.

Disk Encryption

Disk encryption for the protection of sensitive data has been available for several years. This technology has been widely used for the protection of data on laptop computers. Every day thousands of laptops are stolen or forgotten in taxis, airports and hotels. Inside those laptops might be valuable customer data, financials, contracts, email or other sensitive information. Certain versions of this type of software required a password during the boot process to unlock the encrypted portion of the hard drive. This meant the password was stored in the unencrypted boot sector of the hard drive and was vulnerable to discovery. Newer laptops and software can now utilize a smart card as the authentication method to unlock the encrypted hard disk. Individual workstations can be booted from a smart card using the patented Boot Integrity Token System (BITS). BITS stores a computer's boot sector on a smart card and requires the smart card and a password to boot the machine.[9] Even if an attacker can gain physical access to the hardware, it is impossible to guarantee system integrity. With the frequency that laptops are stolen or lost, using disk encryption and smart cards can provide an extra layer of protection.

PDA

Personal Digital Assistants (PDAs) have become one of the most popular portable storage devices in use today. These devices are a security risk for corporations due to the ability to download and store files, email, and contact information from the user's PC attached to the corporate LAN. This is an important consideration since these smaller devices are easily stolen or misplaced. The newer PDA's also have wireless capabilities to further increase the risks. One way to help reduce risk when using these devices is with a smart card. The card's processor can be used to encrypt the stored information on the PDA, verify the user before allowing access, and also help to secure the wireless data transmission via encryption technology.

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

Since smart cards are so portable, new applications and uses are constantly being developed. We are beginning to see smart card authentication with thin client devices (terminal services) and stand-alone kiosks. This allows the user to access services from any connected terminal.

Biometric Smart Cards

Biometrics is defined as the method of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics. Biometrics can provide very secure authentication for an individual since they cannot be stolen or forgotten and are very difficult to forge.[10] Biometrics increases the validity of an individual by using a measurable physical characteristic of a person to prove their identity, such as a fingerprint or DNA.

Biometric smart cards have been developed in recent years that add an additional layer of authentication to the two-factor method smart cards already provide. Fingerprint readers have been added to the smart card body that interface with the on-board processor and memory to store the biometric data or template. Verification can now be based on "something you know" (PIN), "something you possess" (smart card) and "something you are" (fingerprint).

Biometrics adds to the security of the overall system and improves the accuracy and control of the cardholder authentication. The user must be present when the smart card is created to initially "copy" and store the fingerprint template. The biometric data is stored encrypted in the smart card's memory. When attempting to access a system, the smart card's processor performs the comparison of the current fingerprint and the stored biometric template and PIN information. If the comparison checks out, access is allowed.

Nothing for Free

Smart cards are not the "holy grail" of secure authentication. There are issues to contend with when using smart cards. Deployment, user training, system setup, and the loss of the cards themselves need to be considered.

Deployment of smart cards can be costly, not just in the price of the cards alone, which can be between $10 to $20 each ($100 if biometric) and the card readers (about $50 each), but the time of the IT or security staff. A separate card must be created for each user in the system. In the case of a biometric smart card, the user must be present at the time the card is created. Each computer system must be touched in order to add the card reader and configure it to use a smart card for network and system access. This may also require an upgrade to the computer's Operating System (OS) or system applications to support the usage of smart cards.

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

If a PKI is deployed, a public and private key for each user needs to be created and maintained. Certificate Revocation Lists (CRL), expiration times, and card replacement can tax an IT department. If a user loses a card or the certificate validity period has expired, the certificate must be revoked and a new set of public and private keys created and distributed on another smart card. If a user should leave their smart card at home, do you revoke the credentials and create a new one? Or do you create a temporary card with credentials that expire after that day? These types of scenarios need to be considered.

User training can be overwhelming to a corporation in both time and money. The addition of a new technology like smart cards requires end user and IT staff training. There can be an increased volume of help desk calls from confused users and result in lower productivity until users become comfortable with their usage. Users must remember to carry their cards to work every day, remove them from their computers and not store them in their laptop bag with the computer or desk drawer.

Smart Card Security

It should not be surprising that smart cards have their own set of risks. As stated earlier, smart cards are much harder to "clone" than other forms of credential storage. Though most current smart cards have the ability to send an electrical charge that resets the memory to zero at the slightest alteration of the card's body, there are other methods to extract information.[11]

Smart cards provide an isolated processing facility capable of using the stored information without having to expose it to the host computer where it could be at risk to viruses or Trojan programs. It provides a limited Application Program Interface (API) to the host computer for passing of needed information. Cryptographic smart cards interface with the host system through the Crypto API (CAPI) and it has been developed to integrate with all current OS platforms.

There have been a lot of publications about a smart card's vulnerability to a form of attack and the ability to extract data from a smart card through a process known as Differential Power Analysis, or DPA. A DPA attack enables a skilled hacker to obtain secure data on a cryptographic smart card by monitoring the electrical signals of the device, sample the data, and extract the information through statistical methods.[12] Though this method is extremely difficult to perform, it is still possible. New smart cards are being developed to prevent this type of attack.

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

Choosing an authentication method

Deciding which authentication method is best for your organization can be a daunting task. According to RSA Security, the criteria for choosing an authentication method can be divided into three categories, total cost of ownership, strategic fit for the end user, and strategic fit into your system.

10 criteria for choosing a method of user authentication[13]

Category	Criteria	Passwords	Smart Cards
Total Cost of Ownership	Acquisition Cost	Very Low	High
	Deployment Cost	Very Low	High
	Operating Cost	Medium (Help Desk)	Low
Strategic Fit (End User)	Ease of Use	Low (Hard to remember)	Medium
	Portability	High	High
	Multi-Purpose	No	Depends
Strategic Fit (System)	Relative Security	Very Low	High (Multi-factor)
	Interoperability/Integration	High	High
	Future Flexibility	Low	High
	Robustness/Scale	High	High

From the chart you can see that the total cost of ownership for smart cards is higher than using passwords. This includes the cost of the cards as well as the deployment, maintenance and training costs. However for this added cost the relative security for your systems, future flexibility and scalability becomes much higher.

© SANS Institute 2003, Author retains full rights.

Conclusion

Risk management and defensive design are the optimal security strategies. The goal as a security professional is to minimize risk to an acceptable level, because 100-percent security is unattainable. Since the tragedy of September 11, 2001, organizations have been investing in security measures to protect themselves and their data systems from unauthorized access.

Enterprises intent on improving authentication methods for access to applications and other IT resources are looking towards smart cards as a stronger form of authentication than mere username and password. Smart cards can help reduce the risk of unauthorized access by adding a multi-factor user authentication of "something you know" and "something you possess" or even perhaps "something you are" before allowing access to a system's critical data.

There is no perfect solution in the area of authentication. Organizations are left to do the best they can with what is available. Smart cards are gaining momentum. Computer hardware and operating systems are moving towards a more secure authentication mechanism and the current trend is to use the multi-factor capability of smart cards.

© SANS Institute 2003, Author retains full rights.

Cited resources

[1] Avolio, Fred. “Smart card smarts”. SearchSecurity.com. Sept 20, 2001. URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci771214,00.html (Dec 12, 2002)

[2] Hurley, Edward. “Smart cards have their advantages over passwords”. SearchSecurity.com. Nov 22, 2002. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci865191,00.html (Dec 3, 2002)

[3] Krishna, Arvind. “Five steps for keeping hackers at bay”. ZDNet.com. Sept 18, 2002. URL: http://zdnet.com.com/2100-1107-958397.html. (Dec 10, 2002)

[4] “Passwords have an insecurity complex!”. SecureComputing.com. URL: http://www.securecomputing.com/index.cfm?sKey=1091 (Dec 13, 2002)

[5] Hulme, George. “Lessons Learned”. InformationWeek. Dec 2, 2002. URL: http://www.informationweek.com/story/IWK20021127S0036 (Dec 20, 2002)

[6] Phillips, Andrew. “Planning for smart cards”. Tech Update. Jan 29, 2002. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2843255,00.html. (Dec 2, 2002)

[7] D, Narayanan. “Windows NT/2000 Login Security – Whitepaper”. California Software Laboratories. Mar 21, 2001. URL: http://www.cswl.com/whiteppr/white/gina.html. (Dec 23, 2002)

[8] Vacca, John R. “Encryption Keys: Randomness Is Key to Their Undoing”. Information Systems Security. Winter 2000 (Vol 8 No 4): p. 28 (5 pages).

[9] Clark, Dr. Paul C. “Secure Compartmented Data Access over an Untrusted Network Using a COTS-based Architecture”. SecureMethods, Inc. URL: http://www.acsac.org/2000/papers/71.pdf. (Dec 21, 2002)

[10] “Smart Cars and Biometrics in Privacy-Sensitive Secure Personal Identification Systems”. Smart Card Alliance Whitepaper. May 2002. URL: http://www.smartcardalliance.org/about_alliance/Smart_Card_Biometric_paper.cfm. (Dec 12, 2002)

[11] Evers, Liesbeth. “Smart cards still the smart choice”. Vnunet.com. Mar 19, 2002. URL: http://www.vnunet.com/News/1130248. (Dec 20, 2002)

[12] Chu, Francis. “New Test Tool Pins Down DPA Attacks”. Eweek. Nov 27, 2002. URL: http://www.eweek.com/print_article/0,3668,a=34259,00.asp. (Dec 18, 2002)

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

[13] "B2C Security Made Easy: Authenticate Your Customers Using Wireless Devices". Webcast Wed, Dec 4, 2002 02:00 PM ET. Archived URL: http://www.placewareforum.com/rsasecurity/page.cfm?p=event&eventid=18101&catid=11728. (Dec 16, 2002).

Other resources

Harris, Shon. All-in-One CISSP Certification Exam Guide. Berkeley: McGraw-Hill/Osborne, 2002.

Gilhooly, Kym. "Smart Cards, Smart Move?". Computerworld. May 21, 2001. URL: http://www.computerworld.com/printthis/2001/0,4814,60688,00.html. (Dec 2, 2002)

"Technical Introduction to Datakey CIP and Datakey cryptographic smart cards". Datakey Whitepaper. URL: http://www.datakey.com/resource/whitePapers/cip_whitepaper.shtml. (Dec 9, 2002)

Platform SDK: Security. Microsoft Developers Network. Microsoft Corporation. URL: http://msdn.microsoft.com/library/en-us/security/security/system_store_locations.asp. (Dec 12, 2002)

Hutz, Ben and Fink, Jack. "Essentials of Replacing the Microsoft Graphical Identification and Authentication Dynamic Link Library". Microsoft Corporation. June 2001. URL: http://www.microsoft.com/windows2000/docs/msgina.doc. (Dec 13, 2002)

"PKCS#15 – A standard for storing keys and certificates on smart cards". Smarttrust AB. 2002. URL: http://www.smarttrust.com/whitepapers/pkcs15.asp. (Dec 20, 2002)

Symantec Security Response Web Site. URL: http://securityresponse.symantec.com. (Dec 30, 2002)

© SANS Institute 2003, Author retains full rights.