Global Information Assurance Certification Paper

Authentication mechanisms – which is best?

Introduction

The foundation of commerce is built on trust and security incorporating principles of confidentiality, authentication, integrity and non-repudiation. Trust and security are fundamental requirements and business success factors for electronic commerce applications over the Internet.

As businesses place massive investment in their information and computer/network infrastructure, effective arrangements are needed to identify individual users of system resources and to confirm that they are who they purport to be and that they are entitled to use the resources required.

The purpose of this paper is to present information on various methods of authentication. The information will consist of a summary of the pros and cons of the alternative solutions. Also introduced are key decision factors that should be considered.

Scope

The following types of authentication mechanisms were assessed:

- Passwords
- Tokens
- Smart cards
- Digital Signatures
- Biometrics

Each authentication technology has been addressed as follows:

- Overview of the technology
- Advantages
- Disadvantages
- Issues relating to the particular technology

Key requirements in authenticating users across networks

Business managers expect to keep out unauthorised parties and hold legitimate users accountable for their actions. Moreover, they expect to achieve these objectives without unnecessary expense.

In order to satisfy these expectations, authentication of users across a network should fulfil the following six inter-related requirements (according to the European Security Forum):

- Users should only be registered once, no matter how many systems they may need to use in order to perform their function;
- Registrations should be conducted promptly and efficiently;

- In gaining access to the system(s), they are entitled to use, users should only have to log-on and have their identity confirmed once per session;
- Identification/confirmation processes should be effective (i.e. able to determine accurately whether prospective users are registered and, if so, whether they are who they say they are);
- Identification/confirmation processes should be efficient in terms of cost and time taken per user;
- Identification/confirmation processes should be appropriate to the circumstances of the users.

PASSWORDS

Overview

Many of today's authentication schemes are based upon what the individual knows - their ID and password.

Passwords along with a user-identification code have been the predominant method of authentication in the client/server environment.

Advantages

- They can be implemented entirely within software, avoiding the need for peripheral hardware.
- ID/password carried over SSL encryption is feasible and deployable.

Disadvantages

- Ids and passwords travelling over the network are becoming increasingly prone to "eavesdropping"
- Subject to replay attacks
- Subject to password guessing
- Ineffective password management and controls (i.e. re-issue, unlocking, etc.)
- Lack of user awareness and training
- Trojan horses can capture ids and passwords under false pretences
- Can be stolen or observed

Issues

- *Lifetime* – passwords need to be changed at reasonable intervals to prevent password guessing.
- *Ownership* -- passwords need to be used and owned by a single individual, not shared by a group.
- *Distribution* –Whether distributed in hardcopy or electronically, the distribution process should provide for protection against disclosure.
- *Storage* –Passwords can be stored encrypted or in a physically separate area which is only accessible by authorised system components.
- *Entry* –The computer terminal should not display the user's password as it is being entered.
- *Transmission* -- Encryption should be considered to scramble passwords crossing the network.
- *Cost* - It is cheap and easy to implement. Costs rise when the number of users begins to generate a significant amount of administrative work in

issuing/registering users and when special software is required to handle the authentication process efficiently.

- *User operability* – The entire solution is implemented in software and the user does not need to worry about any peripheral hardware devices.
- *Social acceptance* - Users are already familiar with passwords and are comfortable with this authentication process.
- *Ease of installation* – Most systems already have userid and password facilities built in by the manufacturer to handle this type of authentication.

TOKENS – CHALLENGE RESPONSE

Overview

Hardware-based "challenge-response" authentication (in which the server challenges the user to demonstrate that he *possesses* a specific hardware token and *knows* a PIN or passphrase by combining them to generate a response that is valid, but only once) has been a popular method of enhancing the authentication of remote access users.

Advantages/benefits

- Ease of use for users as they only need to remember a single PIN to access the token.
- Ease of management as there is only one token instead of multiple passwords.
- Enhanced security as the attacker requires both the PIN and the token to masquerade as the user.
- Better accountability as tokens are tangible.
- They are mobile in comparison to digital signatures
- Mature solutions that have gained widespread market acceptance and deployment
- Consistent with Thin Client approach, no client side software component
- Mobility and portability, since security is not tied to the specific machine, users have access with any browser based Internet connection
- Browser independent

Disadvantages

- Client required to carry a token card in order to use Internet banking facilities.
- Tokens need to be replaced every 4 years.
- Ongoing operations costs to keep track of token cards.
- Possible barrier to customer acquisition since client cannot use service until he receives the token card.
- Longer time to authenticate the identity of the user as numerous steps are required to authenticate the client.

Issues

- *Vendor dependency* - Dependant on vendor to supply physical token cards causes risk of future hardware support.
- *Scalability* - This solution does not scale well beyond 100,000 users.
- *Distribution* - Distribution of tokens to customers needs to be considered.

- *Cost* - Cost of implementing a token system has to be considered. One of the additional costs for using token authentication systems is the token itself. It is important to note that there are many instances where user's report lost tokens which lead to additional replacement costs. The costs of the tokens themselves needs be a critical component in a company's evaluation process. Consideration of both the application software implementation costs as well as the token hardware need to be taken into consideration.
- *Accuracy* - The accuracy of tokens is considered high as the methodology and logic incorporated into this method has provided excellent reliability in authenticating their users.
- *User operability* - User operability of token authentication requires that the end user must maintain a piece of hardware. This additional hardware requirement can become inconvenient.
- *Social acceptance* - One disadvantage of the token is that some individuals will not accept the token as a means for authentication due to their fear of losing the device. If the user needs to pay for replacement and replacement cost is high, then the acceptance of such a device will be diminished.
- *Product lifecycle* - Two factors need to be taken into account to assess the lifecycle of token authentication. First, the token itself is usually portable. As such, the replacement cost for lost, stolen or misplaced tokens tend to reduce the lifecycle of any such token. Second, token authentication systems are still evolving. New technology consisting of lower transaction costs and increased features is being developed continuously. Companies must consider their strategy and how this fits in with token authentication. If the company desires to have the latest and greatest token authentication scheme available, then the lifecycle of a token scheme is drastically shortened.
- *Ease of installation* - The process of implementing a token authentication system into the existing computer environment can be time consuming. The process requires setting up the server, issuing a token to each user, training the user on how to employ the authentication process, and setting up the database to maintain the tokens.
- *Non-repudiation* - The token scheme possesses a medium level of non-repudiation. By design, it cannot give absolute assurance on who initiated the transaction since tokens and their passwords can be stolen.

TOKENS - SMARTCARDS

Overview

A smartcard is a credit card sized plastic card with a micro processor chip embedded in the card. The smartcard reader makes electrical contact with various connectors, to feed data in and out of the chip. The card is "smart" since it contains its own processor, memory and operating system. The smartcard has considerably more abilities than 'regular tokens' because of the microchip embedded in the card.

The smartcard is generally used as a substitute for user ID / password systems. A much higher level of security can be achieved with a secure communication protocol between the smartcard and reader and between the reader and PC.

Advantages

- "Single sign on". Instead of having to enter passwords or token codes for every new service, the user can just insert the card and enter the pin to activate the card.
- Key features of the smartcard are digital signatures, where the smart card can prove that a particular user signed a given document.
- A smart card contains all the data needed to personalize networking.
- Versatility of combining credit, debit and stored value cards in one convenient platform
- Multifunctional use possible (access card, time recording ...) Smart cards may carry multiple applications which may, in principle, be added or removed during the card's lifecycle. This can considerably aid the business case for the introduction of card technology, since a single card can be used for multiple functions by multiple organisations.
- The processing power of a smart card makes it ideal to mix multiple functions thereby enabling banks to manage and improve their operations at lower costs and offer innovative services
- 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 travelling users).
- Public Key Infrastructure systems are more secure than password based systems because there is no shared knowledge of the secret. The private key need only be known in one place, rather than two or more. If the one place is on a smartcard, and the private key never leaves the smartcard, the crucial secret for the system is never in a situation where it is easily compromised. A smartcard allows for the private key to be usable and yet never appear on a network or in the host computer system.
- Smartcards can enable multi-authentication by accepting a thumbprint on the surface of the card in addition to the PIN in order to unlock the services of the card. Alternatively, a thumbprint template, retina template, or other biometric information can be stored on the card, only to be checked against data obtained from a separate biometric input device.

Disadvantages

- Special reading hardware necessary for users
- Lack of a standard infrastructure for smartcard reader/writers is often cited as a complaint. The major computer manufactures haven't until very recently given much thought to offering a smartcard reader as a standard component. Many companies don't want to absorb the cost of outfitting computers with smartcard readers until the economies of scale drive down their cost.
- Concerns about different groups accessing the information on the card.

Issues

- *Administration* - Central update of rights profiles on smartcards needs to be maintained; Administration/issuing authority and secure logistics are necessary to ensure that this system works efficiently.
- *Mobility and portability* - Public key certificates and private keys can be utilized by web browsers and other popular software packages but they in some sense identify the workstation rather than the user. The key and certificate data is stored in a proprietary browser storage area and must be export/imported in order to be moved from one workstation to another. With smartcards, the certificate and private key are portable, and 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
- *Costs* - Price of implementing and maintaining this type of system compared to that of other token alternatives is expensive. Lost/forgotten smartcard 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 smartcard 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.
- *Product Lifecycle – A*s smartcards are usually portable, the replacement cost for lost, stolen or misplaced tokens tend to reduce the lifecycle of any such token.
- *Ease of installation* - The process of implementing a smartcard 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 smartcards.
- *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 smartcard and only you know the PIN to that smartcard, it is very difficult for others to impersonate your digital signature by using your private key.

DIGITAL KEYS AND CERTIFICATES

Overview

Digital Certificates are electronic documents that are issued generally by a trusted third party called a Certificate Authority (CA). These certificates contain information about the user that the CA has verified to be true. These certificates consist of a "Public Key" denoted by a series of characters which reside on a physical computer or a smartcard. When an electronic message is sent from the client to the bank it is signed using the digital certificate. This ensures that the user is who he says he is. Public Key cryptography is the enabling technology, a PKI (Public Key Infrastructure) is the infrastructure that manages the keys and certificates.

Advantages

- Validates the creation of a file by a sender. Recipients need to know that the sender created the file.
- Prevents the sender from denying involvement in the creation of a file.
- Ensures that only intended recipients are able to read the files.
- Guarantees that the file was not altered during transit.
- Customer centric solution to base personalization features from authentication.
- Wide application use for the future which achieves authentication and encryption using the same technology.
- Certificates can be stored on smartcards in the future which provides secure physical storage.
- Considered to be a reliable authentication method recognized by legal systems.
- Industry momentum is growing for digital certificates.
- Certificates are attractive because browsers and servers already have some support for them (designed for electronic commerce).
- Software components needed for X.509 public key infrastructure are already available on the marketplace.

Disadvantages

- Complicate for users to install.
- Must be installed on every computer user wishes to work on.
- Not feasible where users share machines.

Issues

- *Ease of use*. It will probably be quite complicated for the user to handle their certificates.
- *Problems with public work stations*. Certificate use is problematic with public workstations because certificates are not automatically flushed from browser after use.
- *Mobility & Portability*. Must move certificates from system to system for a particular user.
- *Multiple certificates*. Cannot deliver single sign on, as users are always likely to have to choose among a number of certificates.
- *Administration*. In order to manage certificates, the following needs to be considered:
- A certification authority that issues and manages certificates
- Routines to register individuals, and create their keys and certificates
- Routines to revoke certificates (due to key loss/compromise)
- A directory service to store and retrieve certificates and revocation lists
- *Legal issues*. The law about certificates has not been clarified e.g. should CAs have to provide Key escrow (back up of private keys) and whether digital signatures will come to be legally binding.

- *Legacy systems*. There will be legacy systems that cannot interact with certificates.
- *Storage of certificates*. How should certificates be stored for each client - smart cards are still expensive.
- *Cost*. Certificates themselves are quite expensive and the whole system of certification is quite complex. The cost of digital signatures is relatively low compared to the other schemes, since DS's are primarily a software -based solution to authentication. DS's can be from VeriSign. Ongoing maintenance is relatively inexpensive in schemes where users administer their own keys, ranging to more expensive if an entity wants to get a third party CA involved.
- *Accuracy* - The accuracy of digital signatures is considered high as the methodology and logic incorporated into both of these methods has provided excellent reliability in authenticating their users. The only way to compromise authentication is if someone learns a person's authorization code and has access to the computer holding the private key. This risk, while valid, is relatively low and therefore does not alter the overall accuracy of the authentication method. One final point is that digital signatures often utilize complex mathematical algorithms to ensure accuracy and reliability.
- *Operability* - Most technology today requires minimal effort on the part of the user. Once the DS capability is "turned on," DS's are applied automatically. Additionally, the speed of authentication using DS's is high due to the fact that the operation of attaching a DS to a message can be performed at the speed of transmission. DS's reside on the hard drive of the user's PC or servers on the network. Therefore, their physical size is not applicable, but their logical size can be significant and should be considered.
- *Social acceptance* - The general public is not very familiar with DS's nor does it understand how digital signatures work. Until society alters their present reliance on a paper signature, digital signatures will be slow to gain acceptance.
- *Product lifecycle* - Very similar to tokens, the digital signature product is in its infancy with constant enhancements being made. Therefore, depending upon a company's information security strategy, many systems could be implemented until the product reaches maturity. One advantage of using digital signatures is that there is no separate hardware required eliminating the need for hardware replacements. Also, the lifespan of an individual digital signature is high since once created, it is limited only by the user or the CA upon generating the keys. DS's can be configured to be valid for life.
- *Ease of installation* - Depending on the complexity of the DS authentication scheme, ease of installation can be relatively easy or difficult. If no Certification Authority is used, installation is relatively easy. However, the use of a CA introduces additional steps in the installation of DS software and creation of Public and Private keys which decreases the ease of installation.
- *Non repudiation* - DS schemes possess a medium level of non -repudiation. By design, it cannot give absolute assurance on who initiated the transaction since private keys and their passwords can be stolen.

BIOMETRICS

Overview

Biometric identification is based upon an individual's physical characteristics. Biometric devices use some measurable feature of an individual to authenticate their identity. The devices are built on the premise that physical human characteristics are unique and cannot be borrowed, misplaced, forged, stolen, duplicated, or forgotten.

There are a number of different human characteristics that can be used in biometric recognition, including the following:

- Fingerprints - involves a scan of the patterns on the surface of the skin on the finger;
- Hand geometry - involves a scan of the shape and characteristics of the entire hand;
- Facial recognition - compares a live facial image against a previously recorded facial image;
- Hand written signatures - involves a scan of the handwriting or signature patterns;
- Retinal Patterns - involves a scan of the blood vessel pattern on the retina;
- Voice patterns - involves a scan of the aural pattern of the voice; and
- Iris patterns - involves a scan of the iris (the colored part of the eye surrounding the pupil).

Advantages

- Offers the highest level of assurance in the authentication of users as it is difficult for one to fake the physical characteristics of another.
- Easy to use as the user only needs to present him/herself in person and need not remember data or carry tokens.

Disadvantages

- Most implementations require special hardware input devices at each workstation.
- If the physical reader can be bypassed, such that biometric data derived from the scanning can be entered, then the person can be impersonated.
- Biometric devices are not reliable under abnormal circumstances (i.e. dirty fingers may bar biometric authentication based on fingerprints).

Issues

- *Physical variance* -When using biometric devices some problems may occur due to technical difficulties in measuring and profiling physical characteristics as well as from the somewhat variable nature of physical attributes.
- *Vendor interoperability* - A number of different vendors exist currently and most of the hardware and software are incompatible.
- *Costs* - Biometric devices tend to be expensive. Biometric systems do not require much as far as future replacements or maintenance throughout the life of the

product, but they are relatively expensive initially. Other items adding to the cost of implementing a biometric system include the cost to train personnel to use the system, and the initial set-up cost to enroll authorized users in the system

- *Accuracy* - Because biometric technology is based on a unique physical trait of a human being, its accuracy to correctly identify authorized system users while rejecting unauthorized users does not always have to be precise. The level of accuracy of biometric systems is based on the setting of the comparison algorithm. The comparison algorithm compares how close the digital representation is to the stored template. For many systems, this threshold can be adjusted to ensure that virtually no impostors will be accepted or to ensure that virtually no users will be rejected.
- *Operability* – The biometric scheme is very convenient since the user does not need to remember to carry some form of token with them. This high level of convenience is offset by the speed of authentication as being in the lower range. Depending on the number of user templates stored in the database, it may take a while before a match can be placed, thereby decreasing the speed of authentication.
- *Social acceptance* – Biometrics is viewed as having a low level of social acceptance. This criterion depends on the type of biometric device used as some biometrics is viewed as intrusive.
- *Product lifecycle* –As some physical characteristics of a person change over time, routine updates would need to be made to the host server in order that proper levels of authentication are achieved. With respect to the life of the system, most biometric systems consist of the use of a scanner, a CPU, and other equipment such as video monitors and cameras. These items have a relatively long life span unless they are damaged. As such, biometric authentication systems generally have a longer life span.
- *Ease of installation* - These devices require enrolling each individual using the biometric authentication method into the system. Some vendors state that it takes two minutes to enroll a user into the application. If you are enrolling a significant amount of users, the process can take a significant amount of time.
- *Non-repudiation* - Biometric devices possess a high level of non-repudiation. As these devices are based on the unique characteristics of one's being, a user, for example, cannot deny that their fingerprint initiated a transaction.

Conclusions

Passwords

Authentication that relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons. If users are allowed to make up their own passwords, they tend to choose ones that are easy to remember and therefore easy to guess. Password systems can be effective if managed properly, but which is seldom the case. Advances in security technology provide alternative authentication mechanisms that can be used in combination with passwords to improve the overall authentication to a system.

Tokens – Challenge Response

The token based solution strength lies in the portable device that the user utilises to verify his/her identity with a password/PIN. Although this is an improvement on password based authentication, it is a costly solution which does not scale well. Token

solutions, such as SecurID, has been proven in the past and can be implemented in a timely fashion, however, it does not satisfy the fundamental security objectives such as confidentiality, integrity or non-repudiation. The user will have to carry a token card that could be lost and need replacement, leading the organization to incur a cost for replacing the card.

Tokens - Smartcards
The smartcard has considerably more abilities than 'regular tokens' because of the microchip embedded in the card. Key features of the smartcard are digital signatures, where the smartcard can prove that a particular user signed a given document. The only disadvantage of smartcards is the high price of implementing and maintaining this type of system compared to that of other token alternatives. However, expectations are that the use of smartcards will increase rapidly in the future. Especially since companies and organizations are trying to defend themselves against the unauthorized use and abuse of business critical resources and information. With the growing use of the Electronic Commerce to deliver goods and services, the network security requirements will become more and more important.

Digital certificates
Digital certificate technology is a large part of an electronic commerce solution on a global scale providing a common set of shared services and infrastructure standards between trading partners. Once established, the value proposition to the users will provide business facilitation through authentication of trading parties, confidentiality, data integrity and non-repudiation of transactions. Digital certificates issued and managed by certification authorities potentially provide a scaleable, flexible, and, above all, secure system by which to implement identity authentication procedures.

Biometrics
Biometric identity authentication systems combined with rigorous operating procedures have the potential to provide maximally secure identity authentication for electronic transactions. They are unlikely to be widely implemented for reasons of cost, data storage, processing time, and ergonomics. There are also serious ethical issues associated with biometric identification systems.

References and resources

1. Federal Information Processing Standards Publication 190 (FIPSPUB190). September 1994. "Guideline for the use of advanced authentication technology alternatives". URL: http://www.itl.nist.gov/fipspubs/fip190.htm (24 March 2001)

2. Lynch, Clifford. "A white paper on authentication and access management issues in cross organisational use of networked information resources". April 1998. URL:http://www.cni.org (26 March 2001)

3. Baker, Stewart & Yeo, Matthew. "Background paper on electronic authentication technologies and issues". June 1999. URL: http://www.nzcs.org.nz/nzpkaf/jointoecd.htm (22 March 2001)

4. Ford, Matthew D. "Identity authentication and 'E-Commerce'". October 1998. URL: http://www.law.warwick.ac.uk/jilt/98-3/ford.html (20 March 2001)

5. Choi, Soon Yong & Whinston, Andrew B. "Smart Cards - Enabling Smart Commerce in the Digital Age". May 1998. URL: http://www.cism.bus.utexas.edu/works/articles/smartcardswp.html (26 March 2001)

6. Lyons Burke, Kathy. "Federal agency use of public key technology for digital signatures and authentication". October 2000. URL: http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.doc (26 March 2001)

7. Smith, Danny. "Selected aspects of computer security in Open Systems". November 1993. URL: http://www.nsi.org/Library/Compsec/selected.txt (24 March 2001)

8. European security forum. State of the art review - Authenticating users across a network. May 1992.