IDENTIFICATION AND AUTHENTICATION

NIST Computer Security Handbook

* * * * * * * * * * * * * NOTE * * * * * * * * * * * * * * * *

This file is a DRAFT chapter intended to be part of the NIST Computer Security Handbook. The chapters were prepared by different parties and, in some cases, have not been reviewed by NIST. The next iteration of a chapter could be SUBSTANTIALLY different than the current version. If you wish to provide comments on the chapters, please email them to roback@ecf.ncsl.gov or mail them to Ed Roback/Room B154, Bldg 225/NIST/Gaithersburg, MD 20899.

* *

DRAFT DRAFT DRAFT DRAFT DRAFT

Introduction

Information technology (IT) systems and the data they store and process are valuable resources which need to be protected. One of the first steps toward securing an IT system is the ability to verify the identity of its users. The process of verifying a user's identity is typically referred to as user identification and authentication. Passwords are the method used most often for authenticating computer users, but this approach has often proven inadequate in preventing unauthorized access to computer resources when used as the sole means of authentication.

New technology is emerging that can significantly improve the protection afforded by password-only authentication. This chapter will discuss the elements involved in authenticating users as well as technological advances that can be used with or instead of passwords to help ensure that only authorized users can access an organization's IT resources.

Overview

Determining if a user is authorized to use an IT system includes the distinct steps of identification and authentication. Identification concerns the manner in which a user provides his unique identity to the IT system. The identity may be a name (e.g., first or last) or a number (e.g., account number). The identity must be unique so that the system can distinguish among different users. Depending on operational requirements, one "identity" may actually describe one individual, more than one individual, or one (or more) individuals only part of the time.

For example, an identity could be "system security officer," which could denote any of several individuals, but only when those individuals are performing security officer duties and not using the system as an ordinary user. The identity should also be non-forgible so that one person cannot impersonate another. Additional characteristics, such as the role a user is assuming (for example, the role of database administrator), may also be specified along with an identity.

Authentication is the process of associating an individual with his unique identity, that is, the manner in which the individual establishes the validity of his claimed identity. There are three basic authentication means by which an individual may authenticate his identity.

- a. Something an individual KNOWS (e.g., a password, Personal ID Number (PIN), the combination to a lock, a set of facts from a person's background).
- b. Something an individual POSSESSES (e.g., a token or card, a physical key to a lock).
- c. Something an individual IS (e.g., personal characteristics or "biometrics" such as a fingerprint or voice pattern).

These basic methods may be employed individually, but many user login systems employ various combinations of the basic authentication methods. An important distinction between identification and authentication is that identities are public whereas authentication information is kept secret and thus becomes the means by which an individual proves that he actually is who he claims to be. In addition, identification and authentication provides the basis for future access control.

Technical Approaches

The use of passwords for authentication is widespread, and a certain amount of expense and time is required to upgrade to more sophisticated techniques. In the near-term, one approach to increasing the security of IT systems is to improve the use and management of passwords, while exploring the use of alternate technologies over time.

Passwords

Security Considerations

The security of a password scheme is dependent upon the ability to keep passwords secret. Therefore, a discussion of increasing password security should begin with the task of choosing a password. A password should be chosen such that it is easy to remember, yet difficult to guess. There are a few approaches to guessing passwords which we will discuss, along with methods of countering these attacks.

Most operating systems, as well as large applications such as Database Management Systems, are shipped with administrative accounts that have preset passwords. Because these passwords are standard, outside attackers have used them to break into IT systems. It is a simple, but important, measure to change the passwords on administrative accounts as soon as an IT system is received.

A second approach to discovering passwords is to guess them, based on information about the individual who created the password. Using such information as the name of the individual, spouse, pet or street address or other information such as a birth date or birthplace can frequently yield an individual's password. Users should be cautioned against using information that is easily associated with them for a password.

There are several brute force attacks on passwords that involve either the use of an on-line dictionary or an exhaustive attempt at different character combinations. There are several tactics that may be used to prevent a dictionary attack. They include deliberately misspelling words, combining two or more words together, or including numbers and punctuation in a password. Ensuring that passwords meet a minimum length requirement also helps make them less susceptible to brute force attacks.

To assist users in choosing passwords that are unlikely to be guessed, some operating systems provide randomly generated passwords. While these passwords are often described as pronounceable, they are frequently difficult to remember, especially if a user has more than one of them, and so are prone to being written down. In general, it is better for users to choose their own passwords, but with the considerations outlined above in mind.

Management Issues

Password length and the frequency with which passwords are changed in an organization should be defined by the organization's security policy and procedures and implemented by the organization's IT system administrator(s). The frequency with which passwords should be changed should depend on the sensitivity of the data. Periodic changing of passwords can prevent the damage done by stolen passwords, and make "brute force" attempts to break into system more difficult. Too frequent changes, however, can be irritating to users and can lead to security breaches such as users writing down passwords or using too-obvious passwords in an attempt to keep track of a large number of changing passwords. This is inevitable when users have access to a large number of machines. Security policy and procedures should strive for consistent, livable rules across an organization.

Some mainframe operating systems and many PC applications use passwords as a means of access control, not just authentication. Instead of using mechanisms such as access control lists (ACLs), access is granted by entering a

password. The result is a proliferation of passwords that can significantly reduce the overall security of an IT system. While the use of passwords as a means of access control is common, it is an approach that is less than optimal and not cost-effective.

Memory Card

There is a very wide variety of memory card systems with applications for user identification and authentication. Such systems authenticate a user's identity based on a unique card, i.e., something the user possesses, sometimes in conjunction with a PIN (Personal Identification Number), i.e., something a user knows. The use of a physical object or token, in this case a card, has prompted memory card systems to be referred to as token systems. Other examples of token systems are optical storage cards and integrated circuit (IC) keys.

Memory cards store, but do not process, information.

Special reader/writer devices control the writing and reading of data to and from the cards. The most common type of memory card is a magnetic stripe card. These cards use a film of magnetic material, similar or identical to audio and computer magnetic tape and disk equipment, in which a thin strip, or stripe, of magnetic material affixed to the surface of a card. A magnetic stripe card is inexpensive, easy to produce and has a high storage capacity.

The most common forms of a memory card are the telephone calling card, credit card, and ATM card. The number on a telephone calling card serves as both identification and authentication for the user of a long distance carrier and so must remain secret. The card can be used directly in phones that read cards or the number may be entered manually in a touch tone phone or verbally to an operator. Possession of the card or knowledge of the number is sufficient to authenticate the user.

Possession of a credit card, specifically the card holder's name, card number and expiration date, is sufficient for both identification and authentication for purchases made over the telephone. The inclusion of a signature and occasionally a photograph provide additional security when the card is used for purchases made in person.

The ATM card employs a more sophisticated use of a memory card, involving not only something the user possesses, namely the card, but also something the user knows, viz. the PIN. A lost or stolen card is not sufficient to gain access; the PIN is required as well. This paradigm of use seems best suited to IT authentication applications.

While there are some sophisticated technical attacks that can be made against memory cards, they can provide a marked increase in security over password-

only systems. It is important that users be cautioned against writing their PIN on the card itself or there will be no increase in security over a simple password system.

Memory cards can and are widely used to perform authentication of users in a variety of circumstances from banking to physical access. It is important that the considerations mentioned above for password selection are followed for PIN selection and that the PIN is never carried with the card to gain the most from this hybrid authentication system.

Smart Card

A smart card is a device typically the size and shape of a credit card and contains one or more integrated chips that perform the functions of a computer with a microprocessor, memory, and input/output. Smart cards may be used to provide increased functionality as well as an increased level of security over memory cards when used for identification and authentication.

A smart card can process, as well as store, data through its microprocessor; therefore, the smart card itself (as opposed to the reader/writer device), can control access to the information stored on the card. This can be especially useful for applications such as user authentication in which security of the information must be maintained. The smart card can actually perform the password or PIN comparisons inside the card.

As an authentication method, the smart card is something the user possesses. With recent advances, a password or PIN (something a user knows) can be added for additional security and a fingerprint or photo (something the user is) for even further security. As contrasted with memory cards, an important and useful feature of a smart card is that it can be manufactured to ensure the security of its own memory, thus reducing the risk of lost or stolen cards.

The smart card can replace conventional password security with something better, a PIN, which is verified by the card versus the computer system, which may not have as sophisticated a means for user identification and authentication. The card can be programmed to limit the number of login attempts as well as ask biographic questions, or make a biometric check to ensure that only the smart card's owner can use it. In addition, non-repeating challenges can be used to foil a scenario in which an attacker tries to login using a password or PIN he observed from a previous login. In addition, the complexities of smart card manufacturing makes forgery of the card's contents virtually impossible.

Use of smart devices means the added expense of the card itself, as well as the special reader devices. Careful decisions as to what systems warrant the use of a smart card must be made. The cost of manufacturing smart cards is higher than that of memory cards but the disparity will get less and less as more and

more manufacturers switch to this technology. On the other hand, it should be remembered that smart cards, as opposed to memory only cards, can effectively communicate with relatively 'dumb', inexpensive reader devices.

The proper management and administration of smart cards will be a more difficult task than with typical password administration. It is extremely important that responsibilities and procedures for smart card administration be carefully implemented. Smart card issuance can be easily achieved in a distributed fashion, which is well suited to a large organizational environment. However, just as with password systems, care should be taken to implement consistent procedures across all involved systems.

Hand-Held Password Generators

Hand-held password generators are a state-of-the-art type of smart token. They provide a hybrid authentication, using both something a user possesses (i.e., the device itself) and something a user knows (e.g., a 4 to 8 digit PIN). The device is the size of a shirt-pocket calculator, and does not require a special reader/writer device. One of the main forms of password generators is a challenge-response calculator.

When using a challenge-response calculator, a user first types his user name into the IT system. The system then presents a random challenge, for example, in the form of a 7-digit number. The user is required to type his PIN into the calculator and then enter the challenge generated by the IT system into the calculator. The generator then provides a corresponding response, which he then types into the IT system. If the response is valid, the login is permitted and the user is granted access to the system.

When a password generator is used for access to a computer system in place of the traditional user name and password combination, an extra level of security is gained. With the challenge response calculator, each user is given a device that has been uniquely keyed; he cannot use someone else's device for access. The host system must have a process or a processor to generate a challenge response pair for each login attempt, based on the initially supplied user name. Each challenge is different, so observing a successful challenge-response exchange gives no information for a subsequent login. Of course, with this system the user must memorize a PIN.

The hand-held password generator can be a low-cost addition to security, but the process is slightly complicated for the user. He must type two separate entries into the calculator, and then correctly read the response and type it into the computer. This process increases the chance for making a mistake.

Overall, this technology can be a useful addition to security, but users may find some inconvenience. Management, if they decide to use this approach, will have

to establish a plan for integrating the technology into their IT systems. There will also be the administrative challenge for keying and issuing the cards, and keeping the user database up-to-date.

Biometrics

Biometric authentication systems employ unique physical characteristics (or attributes) of an individual person in order to authenticate the person's identity. Physical attributes employed in biometric authentication systems include fingerprints, hand geometry, hand-written signatures, retina patterns and voice patterns. Biometric authentication systems based upon these physical attributes have been developed for computer login applications.

Biometric authentication systems generally operate in the following manner:

Prior to any authentication attempts, a user is "enrolled" by creating a reference profile (or template) based on the desired physical attribute. The reference profile is usually based on the combination of several measurements. The resulting template is associated with the identity of the user and stored for later use.

When attempting to authenticate themselves, the user enters his login name or, alternatively, the user may provide a card/token containing identification information.

The user's physical attribute is then measured.

The previously stored reference profile of the physical attribute is then compared with the measured profile of the attribute taken from the user. The result of the comparison is then used to either accept or reject the user.

Biometric systems can provide an increased level of security for IT systems, but the technology is still less mature than memory or smart cards. Imperfections in biometric authentication devices arise from technical difficulties in measuring and profiling physical attributes as well as from the somewhat variable nature of physical attributes. Many physical attributes change depending on various conditions. For example, a person's speech pattern may change under stressful conditions or when suffering from a sore throat or cold.

Biometric systems are typically used in conjunction with other authentication means in environments requiring high security.

Cryptography

Cryptography can play many different roles in user authentication. Cryptographic authentication systems provide authentication capabilities through the use of cryptographic keys known or possessed only by authorized entities.

Cryptography also supports authentication through its widespread use in other authentication systems. For example, password systems often employ cryptography to encrypt stored password files, card/token system often employ cryptography to protect sensitive stored information, and hand-held password generators often employ cryptography to generate random, dynamic passwords. Cryptography is frequently used in distributed applications to convey identification and authentication information from one system to another over a network.

Cryptographic authentication systems authenticate a user based on the knowledge or possession of a cryptographic key. Cryptographic authentication systems can be based on either private key cryptosystems or public key cryptosystems.

Private key cryptosystems use the same key for the functions of both encryption and decryption. Cryptographic authentication systems based upon private key cryptosystems rely upon a shared key between the user attempting access and the authentication system.

Public key cryptosystems separate the functions of encryption and decryption, typically using a separate key to control each function. Cryptographic authentication systems based upon public key cryptosystems rely upon a key known only to the user attempting access.

Issues

In addition to the actual choice of identification and authentication technology, there are a number of other issues that should be addressed to ensure the overall success and security of one's IT system.

Networks and Applications

With the increased use of networks connecting multiple hosts, an average IT user may find himself logging onto several different computers, some of them remotely through a network. This situation poses a number of options with respect to user identification and authentication. In one option, the user must authenticate himself to each computer separately, with a possibly different password each time. If there is a different password for each computer, then that user will have difficulty in remembering them. If one password is used for all systems, then the compromise of the password will have more far reaching effects.

A more desirable situation is one in which the user need only authenticate himself to the first computer he logs into and that computer passes the authentication data to each of the other computers the user then needs to access. This scheme requires that all of the computers on the network are

capable of reliably handling this authentication data. Standardization efforts such as Open System Environment (OSE), Portable Operating System Interface (POSIX) and Government Open Systems Interconnection Profile (GOSIP) can contribute to this goal of transparent authentication across networks.

Related to the issue of user authentication across different platforms is the issue of user authentication across different applications on the same platform. Large applications, such as database management systems (DBMS), frequently require that users login to them as well as to the underlying operating system. This second application login is considered an unnecessary burden by many users. As discussed in the network context above, if authentication data can be reliably shared between an operating system and the applications running on it, then the task of authenticating a user to a complex IT system becomes simpler.

Procurement Considerations

An organization must answer numerous questions when it decides to implement an advanced authentication system. The following discussion highlights many of the issues involved in evaluating, procuring, and integrating these systems.

Sources of information

A variety of sources should be used when evaluating authentication systems. Vendor product literature can be very helpful in describing specific details of product operation, and in understanding the range of products offered. There are several annual conferences devoted to computer security, network access control, and authentication technology. In addition to the papers presented at these conferences, there are usually large vendor exhibit halls and product forums. Many organizations, particularly those in the government sector, have published information on the selection and integration of advanced authentication technology. These publications are often the result of practical experience gained during the implementation of these systems, and so can be particularly useful.

Accuracy

The accuracy of an authentication system refers to the ability of that system to correctly identify authorized system users while rejecting unauthorized users. Since this is the primary function of an authentication system, accuracy is directly related to the level of security provided by the system. Vendors may not be objective about producing an interpreting the results of tests which quantify the accuracy of the authentication process with regard to the vendor's particular products. For these reasons, an organization may wish to run independent tests to determine the accuracy of an authentication system in terms which are relevant to the environment in which the system will be used.

Reliability

An authentication system should be capable of operating in its intended environment for a reasonable period of time. During this time, the system is expected to perform at or above a level which ensures an appropriate amount of protection for the host system. If the authentication system fails, the chances for unauthorized access during the failure should be minimized.

Maintainability

All hardware and software systems require some form of maintenance. The components of an authentication system should be evaluated to determine the level of maintenance which the system will require. One goal in the design of an authentication system should be to minimize the maintenance requirements within the constraints of system cost, performance, and available technology.

Commercial availability

Large-scale networking of computer systems and distributed computing are relatively recent developments, and are the driving forces behind the need for more effective methods for authenticating system users. Unfortunately, the market for advanced authentication technology is not fully developed and is somewhat unstable. Many commercially available authentication systems have not yet been sold in quantity. An organization that is considering the use of this technology should evaluate the vendor's ability to produce systems that meet specific quality control standards and in sufficient quantity to meet the user's requirements. Contracts written to procure authentication systems should provide some form of protection for the customer in the event that the vendor is unable to produce systems in the quantities required.

Upgradeability

Because the technology of advanced authentication systems is continually developing, any authentication system should be able to accommodate the replacement of outdated components with new ones. A modular approach to the design of an authentication system, with clearly defined interfaces between the system components, facilitates the process of upgrading to new technology.

System Integration

The integration of an authentication system into an existing computer environment can be very difficult. Most operating systems do not contain well-defined entry points for replacing the default authentication mechanism supplied with the operating system. This is partly because there is no widely accepted standard for the interface between an operating system and an authentication device. Until such a standard becomes available, there are three general options:

In some cases, the vendor who provides the authentication system may have already integrated it into certain operating systems. If the authentication system meets the requirements of the customer and the customer is using the specified operating system, then the system integration has already been accomplished.

Operating system vendors may select certain security architectures for incorporation into their systems. If these architectures include an authentication technology which the customer finds acceptable, then the operating system may be purchased with the appropriate authentication mechanism as part of the package.

It may be necessary to customize the authentication system and perhaps modify the host operating system so that the two can communicate. This will involve cooperation between the operating system vendor, the authentication system vendor, and the customer, unless the customer has sufficient expertise to perform the integration in-house. A prototyping approach is strongly recommended, due to the complexity of this type of project. Implementing such a system on a small scale first can be very helpful in determining what problems will be encountered in a full-scale implementation.

Cost

As in other aspects of IT security, the specific cost of enforcing Identification and Authentication should be balanced against the value of the information processed on an IT system and the vulnerability of that information to attack. In general, devices with a higher performance level will cost more, but individual cases should be evaluated carefully. The authentication systems described in this chapter provide a range of cost from password-only systems at the low end to biometrics at the high end. Token systems, such as memory cards and smart cards, fall inside the range.

In assessing the cost of an authentication system there are several issues to consider. The first is the actual cost to purchase and install the required equipment and software. In general there is no additional cost to purchase a password system because they are included with most IT systems. Programs that check for good passwords, an important part of using a password system, do cost additional money. The use of memory cards is quite extensive and the use of smart cards is increasing significantly so the costs associated with these technologies will decrease over time. The application of biometrics is not that extensive so costs are comparatively higher. Managers should keep in mind that similar products from different vendors may vary widely in cost, depending on the vendor's manufacturing and development techniques and marketing philosophies.

In addition to the cost of procuring authentication technology, there is the cost to the organization involved in using that technology. This includes on-going training

of staff in the correct use of the technology as well as the training and time of personnel to administer the authentication system.

While the relationship between cost and performance can appear complex for authentication technology, the general approach should be to procure the authentication system which provides the required level of security and other performance factors at a minimum cost.

Interdependencies

Security Management & Administration

The incorporation of a new or improved user authentication system will have a noticeable effect throughout an organization. To ensure the acceptance and success of such a program, careful management of the change should take place throughout the organization.

Cryptography

Cryptography plays a role in identification and authentication in two ways. The first is a supporting role for each of the other forms of authentication. Cryptography can provide for the security of authentication data both while it is stored in a computer as well as while it is being transmitted between. In addition, cryptography can be used itself as an authentication method.

Risk Management

A thorough analysis can be done to determine what parts of an organization's IT system are vulnerable to a login attack, and to prioritize these vulnerabilities in terms of severity and likelihood. The types of authentication technology used should be appropriate for the risk at hand. Not all systems may require identification and authentication, e.g., public access systems.

Personnel

The types of identification and authentication methods used by an organization should be chosen in a context that includes personnel considerations. This will help determine what measures will work best for an organization's employees. It is important to note that the cooperation of an organization's staff is very bit as important as the technology to provide identification and authentication.

Audit

Identification and authentication provide the basis for auditing in an IT system. By tying actions of a user to a unique identification, individuals may be held accountable for their actions.

References

CSC-STD-002-85, Department of Defense Password Management Guideline, April 12, 1985.

FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., April 1, 1977.

FIPS PUB 83, Guideline on User Authentication Techniques for Computer Network Access Control, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., September 29, 1980.

FIPS PUB 113, Computer Data Authentication, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., May 30, 1985.

Feldmeier, David C. and Philip R. Karn, UNIX Password Security - Ten Years Later, Crypto '89 Abstracts, Santa Barbara, CA, August 20-24, 1989.

FIPS PUB 112, Password Usage, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., May 30, 1985.

Haykin, Martha E., and Robert B. J. Warnar, Smart Card Technology: New Methods for Computer Access Control, NIST Special Publication 500-157, U.S. Department of Commerce, National Institute of Standards and Technology, Washington, D.C., September 1988.

R. Morris and K. Thompson, Password Security: A Case History, Communications of the ACM, Vol. 22, No. 11, November 1979, pp. 594-597.

R. M. Needham and M. D. Schroeder, Using Encryption for Authentication in Large Networks of Computers, Communications of the ACM, Vol. 21, No. 12, December 1978, pp. 993-999.

Smid, Miles, James Dray and Robert B. J. Warnar, A Token Based Access Control System for Computer Networks, Proceedings 12th National Computer Security Conference, October 1989.

Steiner, J.G., Neuman, C., and Schiller, J.I., Kerberos: An Authentication Service for Open Network Systems, Proceedings Winter USENIX, Dallas, Texas, February 1988, pp. 191-202.

Troy, Eugene F., Security for Dial-Up Lines, NBS Special Publication 500-137, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., May 1986.

CCITT Recommendation X.509, The Directory - Authentication Framework, November 1988, (Developed in collaboration, and technically aligned, with ISO 9594-8).

ANSI X9.26-1990, American National Standard for Financial Institution Sign-On Authentication for Wholesale Financial Transactions, American Bankers Association, Washington, D.C., Approved February 28, 1990.

Sidebar Notes

- (1) Sec. 1, para 1: The process of verifying the identity of an IT system user is referred to as identification and authentication.
- (2) Sec. 1, para 2: Many new technologies offer significant increases to the protection afforded by password-only systems.
- (3) Sec. 3.1.1, para 3: Passwords will be more difficult to guess or obtain illicitly when combined or misspelled words are used and when a minimum length requirements for passwords is met.
- (4) Sec. 3.1.1, para 2: The use of passwords as a means of access control to IT systems can result in a proliferation of passwords that reduces overall IT system security.
- (5) Sec 3.2, para 1: A memory card authenticates a user's identity based on a unique card used in conjunction with something known to the user, such as a PIN.
- (6) Sec. 3.2, para 3: Common types of memory cards are telephone calling cards, credit cards, and ATM cards.
- (7) Sec. 3.3, para 1: Smart cards, which contain one or more integrated chips, can provide increased functionality and increased security over memory cards.
- (8) Sec 3.4, para 1: A hand-held password generator is a state-of-the-art device about the size of a shirt-pocket calculator that is used to access an IT system in place of the traditional user name and password.
- (9) Sec. 3.5, para 1: Biometric authentication systems operate based on unique physical attributes of users, such as voice patterns, fingerprints, and hand geometry; however, the technology is less mature than that for memory and smart cards.
- (10) Sec. 3.6, para 1: Cryptography can be the basis for an authentication system; or it can be used in conjunction with other system discussed.
- (11) Sec. 4.2.1: In choosing an authentication system, managers should explore information provided by vendors, at IT security conferences and presentations, and in special publications.
- (12) Sec. 4.2.7: Important considerations in choosing an authentication system include accuracy, reliability, maintainability, commercial availability, upgradeability, and system integration.