INSIDE:
Password Composition, Length, Lifetime, Source, Ownership, Distribution, Storage, Entry, Transmission, Authentication Period

Auditing Password Usage

Dennis K. Branstad
Frederick Gallegos

PAYOFF IDEA. Passwords are often used to authenticate a system user's identity and to grant or deny access to data. The National Bureau of Standards' recently published Password Usage Standard *outlines effective password implementation and control rules. Using this standard as a guide, the EDP auditor can assess the adequacy of password controls and can audit conformance to password usage rules.*

PROBLEMS ADDRESSED

Although access is the most widely used and easily implemented method of personal authentication, a password-protected system can be penetrated accidentally or intentionally—when the password system is poorly implemented.

When written down, recorded, or displayed during input, passwords can be found out easily by one or more unauthorized users. Once a password is broken, it provides access for as long as it is valid.

Careless password control (e.g., users lending their passwords, using familiar and obvious passwords, or reusing passwords) is common and sometimes difficult to regulate. The EDP auditor assessing conformance to and adequacy of password usage rules must be familiar with such password use guidelines as the federal Password Usage Standard (Federal Information Processing Standard 112) and must know the best methods for auditing adherence to rules for password usage.

When auditing password usage, the EDP auditor must identify both management and user functions that can be implemented to satisfy the information systems and user environments. For example, What technical features can be implemented to support a password system? Some of the requirements can be satisfied by either user management or technical features. In such a system, if the security administrator specifies that each personal password must be changed at least every six months, user man-

agement can issue a directive to this effect, or the system can be programmed to make the changes automatically.

THE PASSWORD USAGE STANDARD

Passwords are the most common form of personal identification used with remote terminals to deter unauthorized access to computer systems and networks. Although the effectiveness of passwords has often been questioned, primarily because they can be easily forgotten or disclosed to others, passwords can provide effective deterrence to unauthorized access when they are well thought out and safeguarded by authorized personnel and secured in the password verification system.

The Password Usage Standard was developed to ensure safe storage and processing of passwords. This standard is one in a series of computer security standards and guidelines issued by the National Bureau of Standard (NBS). Another standard in this series, *Guidelines on Evaluation of Techniques for Automated Personal Identification* (FIPS Pub 48), describes various techniques for verifying identity and provides a set of criteria for the evaluation of automated identification systems employing these techniques. Shortly after issuing FIPS Pub 48, the NBS published Special Publication 500-9, *The Use of Passwords for Controlled Access to Computer Resources.* This publication concerns the generation of passwords and their effective application to the problem of controlling access to computer resources.

EVALUATING PASSWORD USAGE

There are ten fundamentals that must be considered, specified, and controlled in the design and operation of a password system. Descriptions of these fundamentals and the minimum acceptable criteria for passwords are provided in the following sections. In addition, recommendations and alternatives are provided.

Composition

A password is a sequence of characters generated or selected from a set of acceptable passwords. A good password system has a very large set of acceptable passwords. The larger the set, the more difficult it is for an unauthorized person to guess a valid password. The set of acceptable passwords should be large enough to support the value of the resources that are being protected. Allowable passwords must be simple to specify, select, remember, store, and enter.

Composition is defined as the set of all characters that may constitute a valid password. The composition of a password depends in part on the device from which the password is going to be entered. It also depends on how and where the password is going to be stored and how the stored password will be compared with the entered password. Although backspaces can be used effectively to mask printed passwords, the backspace has a special use in many computer systems and this masking technique should not be allowed.

The minimum composition of a password is 10 characters because some systems (e.g., financial transaction systems) use a 10-digit entry pad. The pad resembles the dial pad of a push-button telephone. Some banking systems use the push-button telephone for data entry and retrieval. A more complex composition is 16 characters—the 10 digits plus the letters *A* through *F*. This set can represent hexadecimal characters, each of which is a four-bit (binary digit) code. Many password compositions comprise only the 26 letters of the Roman alphabet, lowercase or uppercase. However, these sets encourage users to select words easily associated with themselves. Even allowing all possible four-letter, five-letter, or six-letter English words provides for a very limited number of passwords compared with the number of possible random-character passwords of the same length, range, and composition.

Length

Length is closely associated with composition in determining the potential security of a password system against an intruder willing to try all possible passwords. A password length of one character reduces the potential number of valid passwords to the number of characters in the composition set. A length of two characters squares this number; a length of three cubes this number; a composition set of ten and a password length of four provides for 10^4, or 10,000, possible passwords. The length should be allowed to vary within a specified range, probably from five to eight characters.

Personal identification numbers (PINs) are typically four digits long because of the low security requirements of the systems in which they are used. A PIN verification system generally prevents a person from quickly trying all 10,000 possible PINs for a particular financial account in order to find the valid PIN. But if the trial-and-error process can be automated, even on a small home computer, the valid PIN can be found in a few minutes. A length of four to six characters increases the possible number of PINs to 1,110,000 ($10^4+10^5+10^6$).

If all other factors are temporarily ignored, the security provided by a password is directly proportional to the allowed length of the password—longer passwords are more secure. However, other factors cannot be ignored in practical password systems. Long passwords take longer to enter. They are more likely to be entered incorrectly, and they are generally more difficult to remember (especially if the password consists of random characters). Sixteen random hexadecimal characters are very difficult to remember and enter quickly and accurately. Long passphrases can be transformed to virtual passwords of exactly 64 bits (or 56 bits with the other 8 bits recomputed to be parity bits). Long passphrases can be easy to remember, but they still take longer to enter.

A passphrase is an understandable sequence of words that can be transformed and stored as 64 bits and used as a password. A passphrase is generally easy to remember and therefore is allowed on some systems. Because there are considerably fewer understandable passphrases than ran-

dom sequences of characters of the same length, a longer passphrase is preferable to a shorter one. For example, the number of understandable 64-character passphrases composed with the 27-character set (*A* to *Z* and space) is considerably less than 27^{64}, which is the number of possibilities if the characters are selected randomly.

A passphrase can be transformed into a virtual password through a transformation method, such as a hashing or cryptographic function. The transformation function should use the entire passphrase as input to compute a unique value, so that any change in the entered passphrase results in a different computed value, within some probability. The resulting value is the virtual password and must be 64 bits, as specified in the standard. This allows all password systems to allocate a maximum of 64 bits for the storage of each password, and therefore permits up to 2^{64} possible passwords (many thousands of years of security against exhaustive searching attacks). Passphrases thus provide the benefit of being easily remembered, at the cost of the additional time needed to enter the longer passphrase and compute the virtual password.

Lifetime

The security provided by a password depends on its composition, length, and protection from disclosure and substitution. Frequent change can minimize the risk associated with undetected compromise of a password. If a password has been compromised in some way and a new password is created that is totally independent of the old password, the continued risk associated with the old password is reduced to zero. Passwords should therefore be changed periodically.

The useful life of a password depends on several variables, including:

- The cost of replacing the password.
- The risk associated with compromise.
- The risk associated with distribution.
- The probability of guessing the password.
- The number of times the password has been used.
- How easily the password can be discovered with exhaustive trial-and-error methods.

Password systems should enable the user or the security officer to replace a password quickly. Passwords should be changed periodically, with a maximum interval selected by the security administrator, and should be changed voluntarily by the owner whenever compromise is suspected. The interval can be a certain length of time or can depend on the number of uses. The password system itself can have automated features that enforce the change schedule and all security criteria for the installation. The system should check that the new password is not the same as the previous password. Very sensitive applications might require that a new password not be the same as the previous two, three, or more passwords. The system should not require that the password for each user be unique; rejection of a new password for this reason confirms that another user has the password.

Source

Passwords should be selected at random from the acceptable set of passwords by the owner or the password generator. Sometimes, however, this guidance is not possible or even desirable. The security administrator often selects first-access passwords for new users. The system can then require that the user immediately replace this password with a new one that only the user knows. The automated password system should check passwords that are created or selected by users to ensure that they meet all criteria of the password system, and it should reject passwords that do not. Some automated systems record attempts to select unacceptable passwords.

If passwords are generated by the system, the method of generation should be unpredictable. Commonly used random-number generators available in computer systems for statistical purposes should be avoided because the sequences of random numbers that they generate are predictable. The DES algorithm, together with a nondeterministic parameter, can be used. The results of a random-number generator are then combined with password selection rules to obtain a password that meets mandatory and desirable criteria.

Ownership

Individual accountability within a computer system is provided when personal passwords are owned individually rather than by groups of individuals. This is desirable even when a group of individuals have common access privileges to the same resources or data. Individual ownership of personal passwords is required for the following functions:

- Determining who accesses what resources and for what purposes.
- Determining illicit use or loss of a password.
- Auditing user activities.

Individual ownership also prevents the need to change the password of an entire group when a single member of the group leaves or loses authorization privileges.

Distribution

The initial password is often distributed differently from subsequent replacement passwords. The initial password is created and issued directly, either orally or in writing, during the meeting at which a user is initially authorized to use the computer system or access a set of data. This password can be a one-time password that must be changed after the initial access request is granted. The changing of a password by a user generally requires that the user supply the old password and then the replacement password. The replacement is checked to ensure that it meets the security requirements of the system and that it differs from the old password; it is then entered into the storage location of the old password. An audit file should be generated that records the date and time of the change but does not record the new password. If a password is forgotten, a new password should be issued in a similar manner.

Passwords that are distributed in writing should be sealed inside envelopes marked "To be opened by addressee only." The user should be instructed to destroy the written password after memorizing it or to return the written password to the security administrator after signing the receipt and sealing it in a return mailer. The user should also be instructed to use the password as soon as possible.

Some systems distribute passwords in a sealed mailer that is printed by a computer and designed so that it cannot be resealed. The password is printed only on the inside of the mailer on the second page through carbon paper attached to the back of the mailer's front page. The mailer contains instructions to remove the front of the mailer (which shows the name of the intended recipient), destroy the front, and save the password in a protected place accessible only to the intended recipient. The part of the mailer that has the password has no other identification that would associate the password with either the system or the owner. Thus, anyone finding a lost password would usually not be able to use it. Although not as desirable as memorizing the password and destroying the distribution medium, this method is useful when passwords are not routinely used and would otherwise be written in a location more easily associated with the owner.

Receipt of a password distributed in a secure mailer can be validated either by positive response or on an exception basis. When passwords are distributed on an unscheduled basis, positive response of receipt is required. When passwords are distributed regularly, the user should be expecting a new password and should only report failure to obtain a new password. In either case, records must be kept when new passwords are issued.

During the transition period, it is often uncertain whether an old password or its replacement is valid. Some systems allow either password to be valid during the transition period, which requires that both passwords be stored and compared with an entered password. Some systems have no transition period (e.g., a password becomes valid at 8:06 PM exactly) and record attempts at using the old password in an audit file. A report of such attempts should be sent to the password owner, who should verify that the use was accidental rather than unauthorized.

Storage

Passwords should be secured in the authentication system. Several methods have been used to protect passwords in storage. Most systems have a password file that can be legitimately read only by the log-on program. The file is protected by a file-access mechanism that checks a protection bit in a file-access table. Only the privileged log-on program has access to read the file, and only the password program has access to write to the file. Some systems separate the password file from the authorized user file. An index file is used to establish correspondence between the user and the user's password. Some systems encrypt the passwords, either reversibly (two ways) or irreversibly (one way), by using a data encryption key or the password itself as a key. Of course, any key retained in storage would also need protection by encryption through a key encryption key. The type of

protection provided to the passwords should be commensurate with the protection desired for the system or data.

One-way encryption of passwords can be used for stored password protection. One-way encryption systems transform the password in such a way that the original password cannot be recovered. This restricts the original password from everyone, including the security administrator and system programmers. When a user logs on to such a system, the password entered by the user is encrypted one way and compared in encrypted form with the stored encrypted password. The same encryption method and key must be used to encrypt both the valid password before storage and the entered password before comparison.

As for auditing the use of two-way encryption of passwords, given the correct key, the original password can be determined from the encrypted password. A user-entered password can be compared with the decrypted form of the stored password or encrypted and compared with the stored password, as is done with one-way encrypted passwords.

Entry

Guaranteeing secure entry of a password into an automated authentication system is often difficult. Observers often can detect part or all of a password while a user enters it, especially if the user is not a skilled typist and enters the password slowly. A long, random password that is difficult to enter is more vulnerable to observation than a short, easily entered password. The following paragraphs describe some techniques that users and systems operation staff may find helpful in achieving this goal.

The computer terminal, keyboard, push buttons, and other password entry devices should provide a means for minimizing the exposure of the password during entry. The password should not be printed on the terminal during the entry process. If the keyboard and the terminal display or printer are directly coupled, the password should be masked. The password can be masked by overstriking the area after password entry. Computer-generated masks used during password entry to disguise the entered password should not always be the same so that the security of all passwords does not depend on one masking program. In any case, no printed or displayed copy of the password should exist after password entry.

On video display terminals that use half-duplex communications, the password can overwrite the understriking and remain visible on the display. In such systems, the display should be immediately cleared by the password program after password entry. Users should be instructed to clear the display manually following password entry if the password program cannot clear the screen.

When submitted as part of a remote-entry batch processing request, a password should be added to the request at the last possible moment and physically protected. Batch processing requests submitted in punched cards should require that the user add the password card just before submission. The computer operations staff should maintain the card decks in a protected area and remove and destroy the password card after the deck has been

read by the system. The password should never be printed on output media. One-time password lists that are securely delivered to the owner to be used for sequential batch processing requests are acceptable, but only if they are physically protected by the owner.

To allow for inadvertent errors, the system should permit only a limited number of unsuccessful attempts. A maximum of three attempts is considered adequate for typical users. The system should also prevent rapid retries when a password is entered incorrectly. Several seconds should elapse before another password is requested. This reduces the effectiveness of an automated, high-speed, trial-and-error attack on the password system. A security record of the attempted use of incorrect passwords should be maintained, but the incorrect passwords themselves should not be recorded. A security alarm should be generated, and the terminal should be disabled if one of the following parameters is exceeded:

- The maximum number of allowed password retries.
- The maximum number of allowed failed log-ons for one terminal.
- The maximum number of allowed failed log-ons for a certain time period.

These parameters must be set according to the sensitivity of the data being protected, the profile of the typical system user, and the policy of the organization. Some organizations are willing to set the parameters high to prevent user dissatisfaction, whereas other organizations set the parameters low to prevent security compromises. Only the security administrator should be able to restore service to the user following any of these events.

Following a successful log-on procedure, the system should inform the user of the last successful access by the user and any intervening unsuccessful access attempts. This will aid in uncovering any unauthorized or attempted accesses that have occurred between successful accesses.

Users can take several actions to prevent observers from learning passwords during the password entry process. First, entry of the password can be practiced so that it can be done quickly with several fingers. Second, users can block the view of the keyboard by leaning over it while typing the password. Third, users can request that guests not watch the password entry process. Fourth, users can enter passwords before demonstrating use of the system.

Transmission

Passwords are typically used to authenticate the identity of a user attempting to gain access to a shared computer system or network from a terminal. To be authenticated, the password is transmitted from the terminal to the computer via communications lines. Unless the communications line is physically protected or encrypted, the password is vulnerable to disclosure during transmission. Most communications lines between terminals and computers are not afforded this protection. Users should therefore be aware that their passwords can very easily be disclosed through passive wiretapping.

Some computer systems can also be easily spoofed. Spoofing is a method of fooling the system so that it behaves as if an authorized user were at the terminal when one is not. In reverse spoofing, a user is fooled into believing that he or she is communicating with the intended computer when another computer is operating in its place. An authorized user can be spoofed into providing the valid password to a simulated log-on request. After the password is obtained, the intruder informs the user that the requested service is temporarily unavailable. During this exchange, the intruder has obtained a valid password without the user's knowledge.

An intruder can spoof the system by inserting an active wiretap between a terminal and the computer. An active wiretap can be built for several hundred dollars by a home computer hobbyist. The wiretap, which can be built into a briefcase, consists of a personal computer with a receive/transmit communications chip that receives data from the terminal and computer and then retransmits modified data back to the computer and terminal. The active wiretap can replace one user's password with another, even if the passwords are encrypted at the terminal.

These threats can be prevented by one of two encryption methods. First, the communications lines can be protected by encrypting data in transit. Transmitted passwords are thus protected from disclosure. In addition, each transmission can be numbered so that a previous transmission cannot replace a later transmission (i.e., a previously used valid password cannot be saved and reused to replace an invalid password, even if both are encrypted). Passwords are thus protected to the same degree as the data they protect.

The password itself can be used as the encryption key or part of the encryption key. For example, a user can enter a password that will be used as an encryption key at the terminal but will never be transmitted to the computer. The stored version of the password is retrieved from the computer's memory, used as the encryption key at the computer, and never transmitted to the terminal. The terminal and the computer are mutually authenticated when communication is possible using the encryption and decryption keys (one at the terminal, one at the computer).

To prevent compromise of the security provided by the cryptographic mechanism, personal passwords used as keys must be selected at random from the set of possible encryption keys used by the cryptographic process. In addition, passwords used as data encryption keys should not be used as key encryption keys. This minimizes the possibility of discovering the key (and thus the password) through cryptoanalysis.

Authentication Period

Interactive sessions between a user and a computer by way of a remote terminal often last several hours. Although security policy should state that a terminal logged onto a computer should never be left unattended by the user, this policy is often ignored in practice. Many systems have a feature that automatically logs a user off the system if the terminal is left inactive for a certain period of time. Some access control systems require users to be reauthenticated on a periodic basis in addition to the initial authentication

process. These systems may antagonize users if reauthentication is required frequently. Reauthentication should be required only to satisfy high security requirements, and then requested only if the terminal has been inactive for a certain period of time. This should prevent the reauthentication process from occurring in the middle of important work.

EXAMPLES OF PASSWORD SYSTEMS

The following examples are provided to assist EDP auditors in evaluating password systems. These examples should not be considered the only suitable combinations of parameters for the 10 password system factors; they are presented simply to illustrate how systems can be designed to satisfy various security requirements and what auditors should look for from an operational and technical level.

A Password System for Low Protection Requirements

The following hypothetical password system meets the Password Usage Standard requirements for minimal protection. This system is similar to password systems found in many retail, customer-initiated financial transaction systems in which the maximum liability of the customer is $50 and the maximum liability of the bank is limited by the number of transactions allowed per day. It is typical of many government-owned and government-leased computer systems in which no sensitive applications are performed. Small scientific systems, special-purpose systems, and systems not making critical automated decisions fall into this category. Systems that require only accountability and control of computer use and cost can also be considered in this category.

A password system for low protection requirements might have the following specifications:

- Composition—Ten characters, digits (0 to 9).
- Length range—Four to six characters.
- Lifetime—One year.
- Source—User.
- Ownership—Individual (personal passwords), group (access passwords).
- Distribution—Unmarked envelope in US mail.
- Storage—Central computer online storage as plaintext.
- Entry—Nonprinting PIN pad.
- Transmission—Plaintext.
- Authentication period—Each transaction.

A Password System for Medium Protection Requirements

Government systems that process limited sensitive applications fall into this category. Included here are applications that process data leading or directly related to monetary payments or that process data subject to the Privacy Act of 1974 or electronic communication and that fall under the provision of the Electronic Communication Privacy Act of 1986. Agency management may determine that additional applications should be designated as sensitive. Computer systems that are subject to fraud, theft, erroneous payments, or other loss of sensitive information may also fall

into this category. Government systems that make payments (e.g., Social Security, Treasury), keep inventories (e.g., armed forces), or process personal information (e.g., Internal Revenue Service, Department of Education) are examples of systems whose requirements would probably be satisfied by this type of password system.

A password system with medium protection requirements might have the following specifications:

- Composition—Sixty-two-character set, uppercase letters (*A* to *Z*), lowercase letters (*a* to *z*), and digits (0 to 9).
- Length range—Four to eight characters.
- Lifetime—Six months.
- Source—System generated and user selected.
- Ownership—Individual.
- Distribution—Terminal and special mailer.
- Storage—Encrypted passwords.
- Entry—Nonprinting or masked-printing keyboard.
- Transmission—Plaintext.
- Authentication period—At log-in and after 10 minutes of terminal inactivity.

A Password System for High Protection Requirements

Systems with high protection requirements include those that have unusually high potential for fraud or theft, offer great economic benefit to a system intruder, and have a substantial impact on the safety or well-being of society. Some computer systems of the Department of Defense or the Federal Reserve Communication System fall into this category. Systems with very high security requirements may require methods of personal identification based on physical characteristics (signature, voice, fingerprint) or a combination of badges, ID cards, and passwords. Once a risk analysis is performed to determine the system's security requirements, a personal indentification system that best satisfies these requirements should be selected.

Computer systems that process sensitive information and rely on passwords to provide personal identification may have high processing requirements that can be satisifed by a password system having the following characteristics:

- Composition—A full 95-character set.
- Length range—Six to eight characters.
- Lifetime—One month.
- Source—Automated password generator within the authentication system.
- Ownership—Individual.
- Distribution—Registered mail, receipt required; personal delivery, affidavit required.
- Storage—Encrypted passwords.
- Entry—Nonprinting keyboard.
- Transmission—Encrypted communication with message numbering.

- Authentication period—At log-in and after five minutes of terminal inactivity.

RECOMMENDED COURSE OF ACTION

The need for good planning in performing an audit of password usage and controls is extremely critical. This article provides the auditor with a guide to evaluating the effectiveness and level of security provided by password security controls.

An auditor undertaking password security evaluation should be familiar with Password Usage Standard (FIPS Pub 112) and how it can be adapted for a specific system. Though the Password Usage Standard applies to federal departments and agencies that use passwords to authenticate users or to authorize access to data, it is intended to provide a common foundation for password systems and to specify basic security and internal control criteria for the use of such systems. It should not be interpreted as satisfying all security and control requirements in all applications.

Dennis Branstad is manager of the Computer Integrity, Security, and Speech Input/Output group in the Institute for Computer Sciences and Technology at NBS. He is responsible for the development of Federal Information Processing Standards and Guidelines in the technical areas of computer security and speech processing and has played a major role in the development of security standards in the areas of password usage, data encryption, data communications, and data storage. Branstad holds a BS in mathematics and an MS and a PhD in computer science, all from Iowa State University. He has been an adjunct professor of computer science at the University of Maryland and has taught computer security courses at George Washington University and for the IEEE. He received the Department of Commerce Silver Medal in 1975 and the Department of Commerce Gold Medal in 1980 for his work in computer security.

Frederick Gallegos, CISA, CDE, is manager of the Management Science Group, US General Accounting Office, Los Angeles Region, and a Lecturer for the Computer Information Systems Department, California State Polytechnic University, Pomona, CA.

Recommended Reading

US Department of Commerce, "Federal Information Processing Standard 112—Password Usage Standard" (September 1985).

——"Federal Information Processing Standard 48—Guidelines on Evaluation of Techniques for Automated Personal Identification" (April 1977).

——"NBS Special Publication 500-9, The Use of Passwords for Controlled Access to Computer Resources" (May 1977).

——"Federal Information Processing Standard 102—Guideline for Computer Security Accreditation and Certification" (October 1983).