U.S. Customs and Border Protection

Attachment L

Identification and Authentication – Password Management

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release is based on the merging of existing DHS 4300A, Version 6.1.1 attachment with existing 1400-05C, Version 2.1 appendix to create a baseline attachment that includes both DHS as well as CBP specific policy and guidance.
2.0	December 21, 2010	No changes.

CONTENTS

1.0 INTRODUCTION

CBP information systems are designed and operated with technical functions to positively identify users of those systems. It is the duty of the System Administrators (SA)/Network Administrator/LAN Administrator/Field Technology Officer (FTO) and ISSOs to ensure that the technical controls requiring proper identification and authorization of users operate as intended and are audited on a regular basis.

1.1 Purpose

The development of strong passwords is a critical aspect of the Identification and Authentication (I&A) element of IT security. The purpose of this document is to provide CBP users and IT security personnel additional guidance concerning password management in compliance with existing CBP IT security policies regarding I&A. This document discusses the importance of well-constructed passwords, describes applicable DHS password guidelines, and includes responsibilities of users and system administrators. Where appropriate, best practices for password and account protection have been included.

1.2 Password Management Policy

CBP IT security policy states that system ISSOs shall ensure strong passwords are used and passwords are changed at least every 90 days, users shall not share personal passwords, and use of group passwords is limited to situations of operational necessity, with DAA approval.

CBP has developed a set of password guidelines that must be followed by system users and system administrators to ensure adequate protection of user accounts and passwords.

1.3 Definition

Identification is the process of telling a system the identity of a subject. Users generally enter their name or a User ID created by the System Administrator. A smartcard or token can be presented to the system as additional or alternate means of identification. The identity of each user must be established prior to authorizing system access and each system user must have his or her own unique User ID. Group accounts are not permitted.

Authentication is the process of proving that a subject is who the subject claims to be. Authentication is a measure used to verify the eligibility of a subject and the ability of that subject to access certain information. There are three ways of authenticating oneself:

1. Something you know (e.g., password)
2. Something you have (e.g., a smartcard, token, USB key fob)
3. Something you are (e.g., a biometric such as a fingerprint, iris scan).

CBP systems are designed to ensure that each user is authenticated before access is permitted.

Passwords are a sequence of characters that are used for authentication purposes. Passwords are often used to authenticate the identity of a system user and, in some instances, to grant or deny access to private or shared data. Passwords are important because they are often the first line of

defense against hackers or insiders who may try to obtain unauthorized access to a computer system. Passwords provide a reasonable degree of certainty that you are the authorized user of the User ID, username, or logon ID. They are one of the most common methods used for controlling system access.

2.0 USER RESPONSIBILITIES

Users are responsible for their own passwords and any network activity conducted under their User-IDs. The rules listed below will help you to select a password and also protect your password from improper disclosure. Guidance on how to change passwords for a variety of CBP systems and guidance on how to configure various CBP systems to enforce the password policy are discussed later in this guide.

Required Action	Benefit Gained
Passwords shall be changed when directed by the System Administrator (SA) or expire in 90 days or less.	Reduces likelihood of unauthorized penetration by limiting password life.
System parameters must be set to prohibit reuse of passwords for at least six generations – users may not reuse the same password for at least six generations of password change.	Reduces likelihood of unauthorized penetrations by increasing password variability.
Passwords shall— —Be at least 8 characters in length. —Contain a combination of alphabetic, numeric, and special characters. —Combine words, numbers, and upper and lower case characters such as 1roBot4a. —Not be the same as the previous 6 passwords.	These requirements make it more difficult for a password guesser to obtain passwords. They increase the set of combinations that must be guessed and provide a mixture to defeat a dictionary attack.
Select a password that can be remembered without writing it down.	Reduces reliance on writing down passwords and therefore also reduces likelihood of unauthorized access.
Passwords shall not contain any dictionary word in any language.	Prevents dictionary type of attacks.
Passwords shall not contain any proper noun or the name or initials of any person, pet, child, or fictional character. Passwords shall not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password.	Helps prevent a password guess based on a hacker's personal knowledge of the user.
Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty", or "xyz123". Passwords should also avoid substiution of characters by switching ones (1) for "ells" (1) or zeroes for "ohs" (O).	These passwords are favorites a hacker might try early in a dictionary type of attack.

Required Action	Benefit Gained
Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, such as 98xyz123.	The dictionaries used by hackers are huge, and the Crack 5.0 algorithms are clever and thorough.
Pass phrases, if used in addition to or instead of passwords, should follow the same guidelines.	Consistent application of guidelines.
Passwords will not be shared with anyone else. Use of another person's password is prohibited.	Reduces likelihood of unauthorized access and accountability issues.
Protect your User-ID and password. Change your password immediately if you suspect it has been compromised.	Reduces likelihood of unauthorized access and accountability issues.
Do not allow anyone to access information through your computer once you have logged on using your password.	Reduces likelihood of social engineering.
Password-protect all files containing any data needing special handling or protection.	Provides added security to sensitive files.
Use a unique password on each system to which you have access.	Reduces likelihood of unauthorized penetrations by increasing password variability.
Passwords shall not be the same as the user ID or the system/server name.	Reduces likelihood of unauthorized penetrations by increasing password variability.

3.0 SYSTEM ADMINISTRATOR RESPONSIBILITIES

The following guidelines are to be followed by system administrators to ensure that password policies and settings are in compliance with CBP requirements.

Required Action	Benefit Gained
Do not store passwords in a clear text file. Do not configure any machine to automatically log on a particular UserID and password when system is booted.	Avoids situation where convenience and speedy login are achieved at the expense of security.
Passwords shall be changed when directed by the System Administrator (SA) or expire in 90 days or less.	Reduces likelihood of unauthorized penetration by limiting password life.
System parameters must be set to prohibit reuse of passwords for at least six generations – users may not reuse the same password for at least six generations of password change.	Reduces likelihood of unauthorized penetrations by increasing password variability.
Allow only one user per account; never share userIDs or passwords.	Provides user accountability.
Never assign a login account a password that is the same string as the UserID or that contains the UserID.	Eliminates this possibility, which is the very first thing any hacker tries once he/she gets a telnet prompt.

Required Action	Benefit Gained
Never install a guest/guest account. Rename or delete all default passwords provided by the vendor.	Prevents penetration via certain well-known vulnerabilities.
Inform the SA if you are leaving your work area for more than 60 days so that all your access privileges can be suspended.	Reduces likelihood of unauthorized penetration by active access management.
Deactivate unused accounts monthly. Consider an account unused if no login has occurred in 90 days.	Prevents a formerly authorized user from continuing to use the host.
No accounts will be named anonymous, ftp, telnet, www, host, user, bin, nobody, etc.	Avoids accounts commonly attacked via the password guessing method: e.g., ftp/ftp.
The manager or owner of the host shall revalidate all userIDs at least annually.	Best security practice to clean out userIDs of ex-employees and to verify which userIDs are valid.
Never set any password equal to the null string, which is equivalent to no password at all.	Follows best security practices.
Passwords will not be included in programs or scripts.	Increased security based on non-automated identification and authentication.
Passwords must be masked on the monitor/terminal as they are entered.	Reduces likelihood of unauthorized access by unseen observer.

3.1 Creating/Distributing Initial and Reset Passwords

The following are recommended guidelines for distributing initial and reset passwords:

Required Action	Benefit Gained
As suggested by DHS Security Policy, whenever possible initial and reset passwords should be distributed in person.	Reduces likelihood of unauthorized penetrations by decreasing opportunities for social engineering.
Vendor default passwords should never be used as initial and reset passwords.	These passwords are favorites a hacker might try early in a attack.
Initial password and reset should be programmed to expire after a 72 hour period.	Reduces likelihood of unauthorized penetration by limiting password life.
Initial password and reset should be designed as a one-time only password that automatically triggers the user to update by creating a new password.	Reduces likelihood of unauthorized penetration by limiting password life.
As with all passwords, the initial and reset password must be encrypted if transmitted to the user via email.	Reduces likelihood of unauthorized penetrations by password being captured and compromised during transit.
If the initial and reset password must be provided over the telephone, the system administrator or help desk analyst must seek to authenticate the user identity by	Reduces likelihood of unauthorized penetrations by decreasing opportunities for social engineering.

requiring either the verification of the user's identify by the user's supervisor or manager OR by having the user successfully answer two questions based on their profile.	

3.2 Implementing Strong Password Policies

Information Systems Security Officers (ISSO) can enforce strong passwords by using various password-cracking tools to test the strength of user passwords. Password crackers are programs that can determine whether a password is easy to guess, and therefore unacceptable. System security personnel should do a sampling periodically to identify weak passwords. If the operating system or other software application can be used to enforce the password policy then the use of a password-cracking tool is not necessary. Any use of password-cracking software must be approved and authorized in writing by the DAA and CBP CISO, or system owner. http://www.us-cert.gov contains useful information pertaining to cracking tools.

UNIX

Crack, by Alec Muffett, is a dictionary-based password cracker for UNIX passwords. It supports sophisticated permutation of each dictionary term and requires the UNIX password file with the password hashes included. If UNIX is running with a shadow password file, the hashes from the shadow file must be combined with the password file before *Crack* is run (*Crack* includes a utility to do this).

Most UNIX sites store encrypted passwords together with corresponding user accounts in a file called /etc/passwd. Should a hacker gain access to this file, he or she can simply run a password-cracking program such as *Crack*. *Crack* works by encrypting a standard dictionary with the same encryption algorithm used by UNIX systems (called crypt). Then it compares each encrypted dictionary word against the entries in the password file until it finds a match.

3.3 Enhancing Password Enforcement Capabilities

Microsoft Windows

Microsoft provides a number of resources that can assist an organization in strengthening its password policy and protecting the Security Access Manager (SAM) database. Introduced with NT 4.0 Service Pack 2 and included in all subsequent service packs, *passfilt.dll* allows for the enforcement of stronger passwords. Instructions on deploying this DLL file can be found on the Microsoft web site at http://support.microsoft.com/support/kb/articles/Q161/9/90.asp. The functionality described above for the *passfilt.dll* file for Windows NT 4.0 has been included in the operating system security components for Windows 2000. You can enable strong password enforcement in Windows 2000 by starting the Local Computer Policy snap-in utility and enabling the "Passwords must meet complexity requirements" setting in Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy.

Microsoft's *syskey* utility adds another level of encryption to the SAM database; thus, providing a greater degree of protection against employing *L0pht* or similar programs to "dump" the entire SAM database from the registry. *Syskey* uses a 128-bit cryptographically random key and can be used with both Windows NT 4.0 and Windows 2000. Issues involved in using the *syskey* utility and a link to the *syskey* hotfix software can be found at http://support.microsoft.com/support/kb/articles/Q143/4/75.asp.

Installing Microsoft's *NTLM v2* authentication provides an improved authentication method for Windows 9x products that brings their password encryption hashes closer in strength to the native Windows NT/2000 method. *NTLMv2* password hashes greatly increase the security of hashes traversing the network from Windows 9x machines and make it much more difficult to crack any intercepted passwords. *NTLMv2* has been available since NT 4.0 service pack 4 and is natively supported in Windows 2000. Information on installing and using this improved authentication method is provided at http://support.microsoft.com/support/kb/articles/Q239/8/69.ASP.

The Windows XP Professional authentication model protects network against malicious attacks:

- Masquerade attacks. Because a user must prove identity, it is difficult to pose as another user.
- Replay attacks. It is difficult to reuse stolen authentication information because Windows XP Professional authentication protocols use timestamps.
- Identity interception. Intercepted identities cannot be used to access the network, because all exchanges are encrypted.

More information on Windows XP is provided at http://www.support.microsoft.com/support/kb/articles/Q239/8/69.ASP

NOVELL NETWARE

Novell's networking package is known as *NetWare*. Version 3 has cryptographic security. Version 4 security was enhanced to use public key cryptography. Version 4 simplifies management. Instead of having a database entry for each user separately managed at each server the user is authorized to use, *NetWare* Directory Service (NDS) stores the user's security information, and servers retrieve the information from NDS. Strong passwords can be enforced through the use of standard Novell features provided, or through add-on software from Novell or third parties. Detailed information on implementing strong passwords in an NDS environment can be found at http://support.novell.com/techcenter/articles/ana20000802.html.

UNIX

UNIX enforces strong passwords with utilities such as *npasswd* and *anlpasswd*. Use replacement for UNIX passwd command that enforces good password choices. [Set password aging command using passwd command with the –n and –x options.]

Oracle's Enterprise Edition uses a GUI interface to check for strong passwords. With a basic SQL command, the database management can be set up to check passwords for such characteristics as age, alphanumeric characters, and reusability.

3.4 Storing Encrypted Passwords

Passwords shall not be stored in clear text (unencrypted). Password-only mechanisms, especially those that transmit the password in the clear, can be monitored and captured. Several standard protocols (e.g. FTP, Telnet[1]) transmit all data in the clear, unless tunneled through an encrypted channel. Encryption converts data into unintelligible code. This process causes data to be

[1] FTP and Telnet protocols are prohibited within CBP.

unreadable to anyone who does not have the key to decrypt it. The data will remain private and confidential, regardless of whether it is being transmitted or stored on a computer. Those without authorization will need to invest significant effort to decrypt the encrypted passwords. Shadow passwords are to be used on all systems to eliminate world-read access to encrypted passwords.

When a password is typed, the system must determine whether it is valid. If the system stores the passwords unencrypted, anyone with access to the system storage or backup tapes can steal passwords. In some cases, the password is stored in memory while or after it is verified. A user who can access the memory (directly or through a program deliberately installed for this purpose) can extract the password for later unauthorized use.

It is not necessary for the system to know a password to verify if it is correct. Instead of storing the password, the system can store a hash of the password. When a password is supplied, it computes the password's hash and compares it with the stored value. If they match, the password is found correct. If an attacker obtains the hashed password file, it is not immediately useful because the passwords cannot be derived from the hashes. Historically, some systems made the password file publicly readable, an expression of confidence in the security of the hash. Even if there are no cryptographic flaws in the hash, it is possible to guess passwords and hash them to see if they match. If a user is careless and chooses a password that can be guessed (a word that would appear in a 50,000-word dictionary or book of common names), an exhaustive search would "crack" the password even if the encryption were sound. For this reason, it is a good practice to hide the hashed password list.

4.0 BEST PRACTICES FOR PASSWORD AND ACCOUNT PROTECTION

In addition to the DHS password guidelines, the following "best practices" have been included in this guide. These "best practices" may be imposed by the DAA or other authority.

USER

- **Use different passwords**. The same password should not be used to access multiple systems or applications. Once a hacker has one password, he or she will quite likely try to use it to get into other systems or applications.
- **If a user has reason to believe that his or her password has been compromised, it is imperative that this be IMMEDIATELY REPORTED TO THE INFORMATION SYSTEM SECURITY OFFICER (ISSO)**. Timely reporting allows for investigation for compromise and may minimize damage. This is important because if someone uses a valid UserID and password to access the system or compromise the system integrity, it will appear as if the user whose password and user ID was compromised was the person actually responsible for damaging the system.
- **Users must be alert to others who may be trying to obtain their password**. Hackers may pose as a system administrator. Hackers will randomly call a user and say that something is wrong on the system in order to get access to the system. The hacker will tell the user that they need his or her password in order to issue a new one. Remember that system administrators DO NOT need the old password in order to issue a new one. Users must NEVER give out their password over the phone.

- **Do not re-cycle passwords**. This refers to changing passwords at the required interval but using two, or a few passwords over and over in turn, or making minor changes to passwords by adding a number to the base password. (e.g., password is changed to password1, password1 is changed to password2). Many operating environments can be configured to enforce this policy.

ADMINISTRATOR

- **Replace passwords whenever a compromise is suspected**. User accounts should be deleted as quickly as possible from the time that the user is no longer authorized to access a system. Passwords forgotten by their owner should be replaced, not reissued. An automated password system should allow the administrator to delete or replace a password, and it should have the capability to maintain a record of when a password was created or changed.
- **Terminate user accounts when a user transfers or has been terminated**. System owners should review accounts semi-annually. The ISSO and System Administrators should be notified when a user transfers or has been terminated. The user account(s) should be disabled or deleted immediately.
- **Reset passwords**. When resetting passwords, system administrators need to verify the identity of the user

4.1 How to Change Your Password

Windows 98/Novell/Windows Screen Saver

1. Click *Start Menu.*
2. Select *Settings.*
3. Select *Control Panel.*
4. Select *Passwords.*
5. Select *Change Windows Password* (This allows you to change Novell and Screen Saver passwords at the same time) or *Change Other Passwords* (Novell, Screen Saver).
6. Select the password(s) you want to change and enter the new password(s).

Windows 2000

1. Press *CTRL-ALT-DELETE*
2. Select *Passwords*
3. Enter New Password

Windows NT

1. Press *CTRL-ALT-DELETE*
2. Select *Passwords*
3. Enter New Password

Windows XP

1. Press CTRL-ALT-DELETE
2. Select C*hange Password*
3. Enter New Password

Lotus Notes

1. Go into Lotus Notes
2. Click *File*
3. Click *Tools*
4. Click *UserID*
5. Enter Current Password
6. Click *Set Password*
7. Enter Current Password
8. Enter New Password

FedDesk

1. Enter FedDesk Website
2. Click the Door Knob
3. Enter New Password

4.2 Operating System Settings

MVS and VM

Listed below are the recommended settings for MVS and VM operating system using CA-TOP SECRET. Subsystem passwords, if used, shall comply with the provisions of this standard. Passwords shall be assigned to all user IDs.

- The NOPW option **shall not** be used.
- The CA-TOP SECRET PWVIEW (password view) option shall be **disabled**.
- New passwords shall be **user selected** or **randomly generated**.
- The CA-TOP SECRET MIN (minimum password length) parameter shall be set to **8** or higher.
- The CA-TOP SECRET MINDAYS (number of days before password can be changed - prevents user from re-using a password) parameter shall be set to **1** or higher.
- The CA-TOP SECRET WARN (interval in days to notify user that password will expire) parameter shall be set to **15**.
- The CA-TOP SECRET NR (number of repeating characters allowed in password) parameter shall be set to **1**.

- The CA-TOP SECRET RS (prevents a user from selecting a password on restricted list) parameter shall be set to **YES**.
- The CA-TOP SECRET ID (prevents a user from selecting a password that contains their ID or the first four characters equal to part of a UserID as part of a password) parameter shall be set to **YES**.
- The CA-TOP SECRET TS (user cannot use password similar to previous password) shall be parameter set to **YES**.
- The CA-TOP SECRET NM (password indicates numbers only) parameter shall be set to **NO.**
- The CA-TOP SECRET NU (prevents users from changing password) parameter shall be set to **NO.**
- The CA-TOP SECRET NV (no vowels allowed in password) parameter shall be set to **NO.**
- The CA-TOP SECRET RN (user can select random password if desired) parameter shall be set to **YES**.
- The CA-TOP SECRET SW (password contains a national character) parameter shall be set to **NO.**
- The CA-TOP SECRET MASK (types of characters that can be used for each position in a password) parameter shall be set to **????????** (any eight characters).
- The CA-TOP SECRET PWEXP (password lifetime) parameter shall be set to**180.**
- The CA-TOP SECRET PWHIST (number of passwords checked to prevent reuse) parameter shall be set to **8.**
- The CA-TOP SECRET NPWRTHRESH (number of times for new password re-verification) parameter shall be set to **1.**
- The CA-TOP SECRET INACTIVE (number of inactive days allowed before password is suspended) parameter shall be set to **30.**

UNIX

Where possible UNIX systems shall implement random password generation via modification of the PASSWD routine to reduce the vulnerability from dictionary attacks. Where possible a shadow password file shall be used. NOTE: This option is not supported by some UNIX systems. Many UNIX systems, when first installed, do not have a root password. All operational systems must have passwords assigned to all user IDs.

AS400

- The QMAXSIGN parameter should be set to **3** to limit maximum sign-on attempts.
- The QPWDEXPITV parameter should be set to **180** or less to limit the password lifetime.
- The QPWDMINLEN value should be set to **8** to specify the password minimum length.
- The QPWDRQDDIF option should be used to prevent the reuse of passwords.

NOVELL NETWARE (3.x)

The following options are recommended using *Account Restrictions* in the SYSCON *User Information* menu.

- Allow user to change password = **Y**.
- Require Password = **Y**.
- Minimum password length = **8**.
- Force periodic password changes = **Y**.
- Days between forced changes =**180.**
- Limit grace logins = **Y** (a grace login allows a user to sign on with an expired password).
- Grace logins = **1.**
- Require unique password = **Y** (prevents password reuse up to 8 passwords).

Microsoft Windows NT (4.0.x)

The following options are specified using the Policy Account window in the User Manager or User Manager for Domains.

- In the *Policy Accoun*t window, select the *At Least* radio button under *Minimum Password Length*. Type in **8** for the number of characters.
- Set the *Maximum Password Age* to expire every **180** days.
- In the *Minimum Password Age* area, select the radio button *Allow Changes In* to **1** day. In the *Password Uniqueness* area, select the radio button *Remember* and type **8** for the number of Passwords.
- *No Account Lockout* option shall be set to **3** bad logon attempts. Manual action by a security administrator is required to reactivate the ID.

5.0 REFERENCES

- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources
- Department of Homeland Security (DHS) Sensitive Systems Policy Publication 4300A
- Department of Homeland Security (DHS) 4300A Sensitive Systems Handbook