VeriSign™

White Paper

The Security Risks of Using Passwords

Trusted Internet Services from the Sign of Trust on the 'net.

Using Passwords Can be Hazardous

As the need for information security continues to grow at an ever-increasing rate, secure transactions have become a necessity and great value to corporations. In this race to have the best that money can buy, authentication systems have received much less consideration. A time is fast approaching when passwords will not and cannot be an effective security mechanism for our enterprise environments.

When we consider what a password provides, our discussion must encompass a two-fold process. The First process is an identification phase (telling who you are), the second is an authentication phase (obtaining and validating the identification). Authentication should occur before any rights are granted to the identifying party. A simple authentication process usually contains a prompt for a secret password that only the identifying party knows. Identification is of very little value without authentication in place. Since identification should always be backed up with some type of credential to provide security, this process is one of the first and easiest to implement in today's information technology environments.

"Without authentication, user identification has no credibility."
DOD Password Management Guideline

What are the Problems of Passwords

We typically place the responsibility of creating strong passwords in the hands of the users. The end user is asked to create a password that they can remember, but others cannot guess, thereby developing a paradox—the user cannot remember the password in his quest to create an unguessable one. This, more often than not, leads to apathy of users, which is the leading factor working against the strength and efficiency of today's authentication systems today.

Password management years ago washed its hands of creating passwords for users ("let the users set their own passwords"). Letting the user set his or her own password nearly always leads to weak passwords. Once we force the setting of strong passwords, "Sticky Note" passwords become all too common.

If we consider current authentication or password systems, it is easy to determine that certain weaknesses can be traced back to specific components within the authentication system. The following discussion highlights the weaknesses of today's authentication system.

Password Input or Interface

In many cases, password input is easily compromised by the simple act of shoulder surfing—watching the hands on the keyboard. Even advanced programs are written to produce a list of passwords from possible letter combinations and the placement of the hands on the keyboard. KeyStroke recorders have been around since the keyboard; this provides an excellent way to obtain passwords and user names. In some cases, the software remembers the password; therefore, the application is provided with identification and authentication from the application, not from the individual.

Password Transport

Once a user enters the password was it transmitted to the authenticating device securely or insecurely? Unfortunately, the answer is insecurely, in most cases. How many times have you been asked for a password to login to a specific Web page and noticed your browser was not in a secure mode? Additionally, many vendors using encrypted transport, which is weak or has other limitations such as size. Transportation of the secret password is one of the most over-looked issues in modern authentication devices.

Password Verification

How are passwords verified and correlated to the identity of the user? Many times, passwords are cached, so the old or invalid password can be used instead of the correct password. In some cases, the software that is conducting the verification can be over written by access controls and permissions. The problem with this is the authentication mechanism is then bypassed, allowing a failed authentication attempt to succeed.

Password Storage

How are the passwords stored on the system? There are 4 levels of storage—Clear, Encrypted, Hidden-Clear, Hidden-Encrypted. Many software tools have adapted to poor storage issues in the past, but some are using trivial encryption or allowing the files to be obtained from the system. A simple brute force cracking program can easily bypass this encryption. Some of the more popular programs have been developed for most versions of Unix, Windows NT, Windows 95, and Windows 98, which allows for cracking of both user passwords and cached passwords. Other programs can reclaim passwords saved in browsers and applications such as Word, Excel and even Zip files.

Passwords

Passwords are indisputably the biggest risk area in the authentication arena, but they are also the item we have the most control over. If our users continue to use weak passwords, it makes no difference how strong we are with transport, storage, verification and input—we will be compromised!

"Hackers don't even need to know much about your particular operating system to try username/password combinations"
— *Hack FAQ*

Passwords are the most common form of authentication. One of the major problems is that the user is allowed to specify his or her password. On occasion a user may be assigned a machine- or administrator - generated password.

So why do we keep banging our heads against the "Password Brick Wall"? There are several explanations. Passwords are the most cost-effective security mechanism; they are usually free and built into almost all information technologies. Passwords are simple, easy to use; most users can understand them so there are no barriers to implementation.

Most password authentication systems work in much the same way, so management is uniform on a good number of authentication systems. Although passwords may not be the best security, they are better than nothing at all.

Problems associated with the password are security, brute forcible, common passwords, lifetime expiration, and disclosure. Brute Forcing of passwords is just guessing the password; in some cases, we use default passwords or common passwords that are built into applications and devices. These are all known and usually easily guessable. Brute forcing of strong passwords is also becoming faster and faster as technology continues to increase.

Lifetime expiration of passwords has increased the security of passwords by forcing a change of the passwords. But weak passwords are still weak, and some users often change their password back to previously used passwords. Some users often add a number to the front or the end of the same password. In worse cased, passwords are sometimes set to never expire, due to a single reason: the Information Technology Administrator does not want to change a password across the enterprise, or it is "hard" coded into some scripting applications.

Disclosure is very common in Enterprises. Users disclose their password, accidentally or purposefully, to a co-worker or even someone they may not know. Disclosure may be as simple as a note taped to the

monitor or giving another coworker a password "just this one time." Intruders often use a form of Social Engineering to acquire passwords that are given via innocent disclosure.

Passwords at the Simplest Level

Passwords can be made up of 4 Character sets

Numeric	Total Characters	10
Alphabetic	Total Characters	26
Upper/Lower	Total Characters	52
Keyboard/Extended	Total Characters	33
Maximum Characters	Total Characters	95

To find the total number of potential combinations of characters for a fixed length password, take the total number of possible characters(x) and raise to the power of the number of characters in a password (y). A six-character password using all uppercase letters has a total possible combination of 26^6=308,915,776

The total number of potential character combinations in a variable length password is found by taking the number of available characters (X) to the power of the lowest number of fields (Y) added incrementally to the power of the highest number of fields (Z). If you have a 1- to 6-character password consisting of all lowercase alphabet letters, the result is:
$X^Y + \ldots + X^Z$ is $26^1 + \ldots + 26^6 = 321,272,406$

1- to 6-character-length passwords yield these possibilities:

Alpha	321,272,406
Upper/lowercase alpha	20,158,268,676
Numeric	1,111,110
Upper/lowercase alpha + numeric	57,731,386,986
Extended	1,108,378,656
Upper/lowercase alpha + numeric + extended	742,912,017,120

1- to 8-character-length passwords yield these possibilities:

Alpha	217,180,147,158
Upper/lowercase alpha	54,507,958,502,660
Numeric	111,111,110
Upper/lowercase alpha + numeric	221,919,451,578,090
Extended	1,134,979,744,800
Upper/lowercase alpha + numeric + extended	6,704,780,954,517,120

Reusable Password Study:

Reusable Password Study

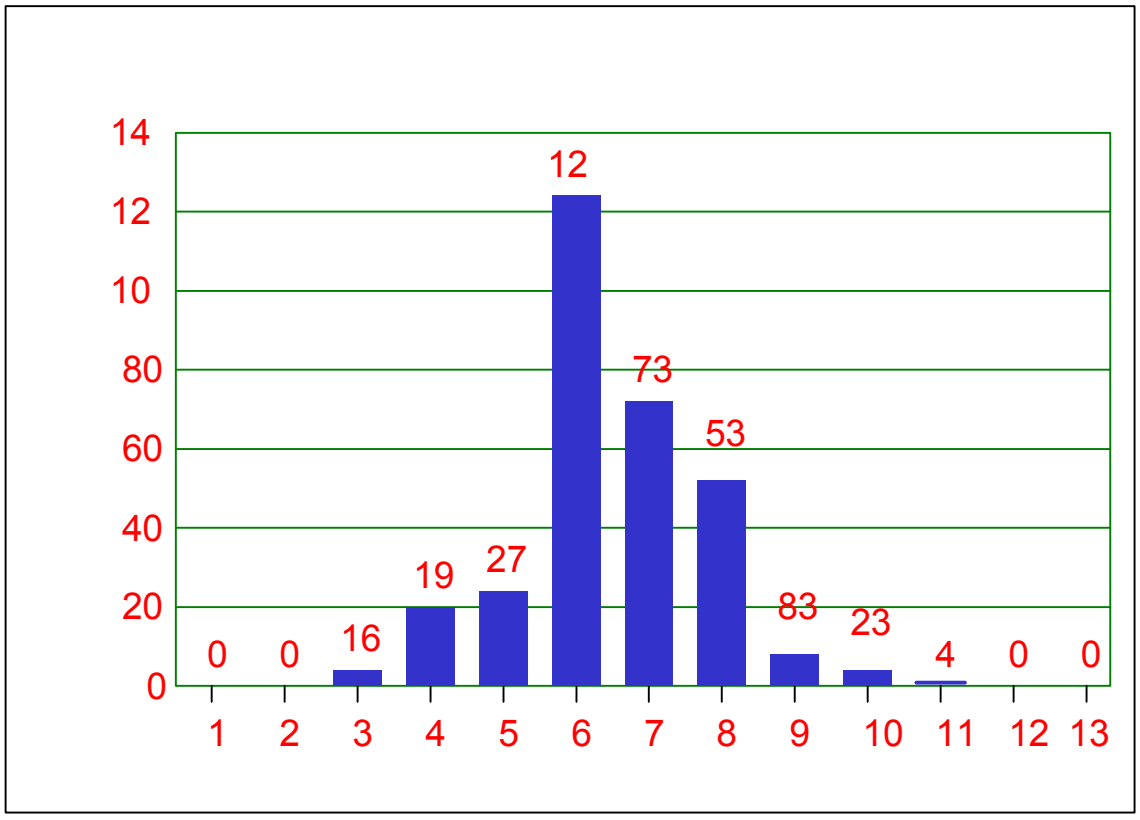
In 1980s, a study conducted by Robert Morris, Sr. and Ken Thompson and reported in their paper "Password Security: A Case History" provided some interesting details on the difference in security with specific password lengths and character sets. The report provided the details of their analysis of 3,289 cleartext passwords. The following text shows some of their results.

Character Sets

Number and percentage of passwords with:

Lowercase	2,745	86.8%
Uppercase	1,737	54.9%
Numbers	1,240	39.2%
Extended	49	1.6%

Lengths



According to Morris, Sr, and Thompson, "On a PDP-11/70, the time required to search through all character strings of length 8 from a 36-character alphabet is 112 years." Some very interesting facts on passwords as shown in the study include:

- 54% of the passwords fell between 3 and 6 characters in length.
- Most passwords in this study contained large amounts of lowercase letters
- Almost 50% of the passwords consisted of only lowercase, uppercase or lower+uppercase characters
- In approximately 20 years, the average length of a password has only increased by 2 characters while computing power has skyrocketed.
- For every 20 passwords you find, there is a good chance that one of the passwords will also be chosen by another user.
- These duplicated passwords also tend to fall into already easily guessable categories like dictionary words or names.

- The study showed that usernames make up the worst possible choice of passwords — these passwords are easily guessed.
- As the second worst category to choose from, the use of dictionary words were definitely too widespread.
- Using words lists, the researchers were able to effectively find 999 passwords of 31.6% of the total.
- Password length won't increase substantially without operating system requirements guidance or enforcement.
- Passwords will become easier to guess.
- People will be using the same password on various independent systems.
- Poor passwords will continue to be the leading breach of security systems

Some things that can be done to improve the security of password systems

- Improve length requirements
- Check against username and other likely choices
- Enforce regular, but not overly frequent, changes
- Run your own attacks against the system to ensure it can withstand them
- Educate users as to their role in system security
- Audit password changes and invalid logins
- Establish a timely review of your audit logs
- Lock out accounts after X invalid attempts
- Don't allow easy access to your password file
- Limit the methods of usurping authentication by privileged users

It is important to note that even if you perform all the previously listed actions to improve your password security, all you have really done is lengthen the time you can use passwords securely. Every corporation's, as well as individual's, goal should be to find another type of authentication mechanism, such as the use of digital certificates and public keys.