CMSGu2012-08

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Strong Passwords and Passphrases

CERT-MU

National Computer Board
Mauritius

Version 1.0

October 2012

Issue No. 8

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to establish a guideline for password/passphrase construction, protection and maintenance.

1.2 Audience

The target audience for this guideline include everyone who makes use of passwords and passphrases either to surf online or secure their documents, e-mail accounts and computers.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 presents a background on passwords and passphrases.

Section 3 illustrates some password-based attacks.

Section 4 details the dangers posed by passwords and passphrases.

Sec*tion 5* explains how to secure passwords and passphrases.

Section 6 provides a few alternatives to passwords and passphrases.

Section 7 concludes the document.

Section 8 contains a list of references that have been used in this document.

Appendix A defines a set of acronyms used in this document.

2.0 Background

2.1 Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of individual systems, data or an entire organisation.

While the majority of organizations and almost 99% of the home users still rely heavily on passwords as a basic form of authentication to sensitive and personal resources, the insecure maintenance, creation, and network transfer could open the front door of any organization or personal asset to a malicious attacker.

Management staff with outdated mode of thinking still believe that passwords are the most essential, user-friendly way to identify a user on their network or database, while the fact is that users are frustrated with the fact that they need to change their password, that they need to create a “secure” password, or follow instructions on how to keep it as secret as possible. The results are a large number of crackable passwords, the same passwords on multiple systems, and “post it” notes with passwords even including login names.

2.2 Passphrases

Passphrases were thought with the idea to be easier to remember, but virtually impossible to crack. The majority of encryption software require you to use a passphrase for your private key instead of a password. Passphrases are usually something that you always remember either a quote or a favourite sentence and a combination of both numbers and special characters. Although virtually impossible to crack due to their length, both passwords and passphrases can be logged through the use of a keylogger, or sniffed if transmitted over plain text communication channel.

3.0 Password-based Attacks

To understand how to protect yourself from a password attack, you should become familiar with the most commonly used types of attacks. With that information, you can use password cracking tools and techniques to regularly audit your own organization's passwords and determine whether your defences need bolstering. The following sections are a basic coverage of the most widely used types of attacks.

3.1 Password Guessing

The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or automated approach. Password guessing isn't always as difficult as you would expect. Most networks are not configured to require long and complex passwords, and an attacker needs to find only one weak password to gain access to a network. Not all authentication protocols are equally effective against guessing attacks. For example, because LAN Manager authentication is case-insensitive, a password guessing attack against it doesn't need to consider whether letters in the password are uppercase or lowercase.

3.2 Automated Password Guessing

Many tools can automate the process of typing password after password. Some common password guessing tools are Hydra, for guessing all sorts of passwords, including HTTP, Telnet, and Windows logons; TSGrinder, for brute-force attacks against Terminal Services and RDP connections; and SQLRecon, for brute-force attacks against SQL authentication.

Automated password guessing programs and crackers use several different approaches. The most time consuming and most successful attack method is the **brute-force attack**, in which the attacker tries every possible combination of characters for a password, given a character set (e.g., abcd…ABCD…1234…!@#$) and a maximum password length.

3.3 Dictionary Attacks

Dictionary attacks work on the assumption that most passwords consist of whole words, dates, or numbers taken from a dictionary. Dictionary attack tools require a dictionary input list. You can download varying databases with specific vocabularies (e.g., English dictionary, sports, even Star Wars trivia) free or commercially off the Internet.

3.4 Hybrid Password Guessing Attack

Hybrid password guessing attacks assume that network administrators push users to make their passwords at least slightly different from a word that appears in a dictionary. Hybrid guessing rules vary from tool to tool, but most mix uppercase and lowercase characters, add numbers at the end of the password, spell the password backward or slightly misspell it, and include characters such as @!# in the mix. Both John the Ripper and Cain & Abel can do hybrid guessing.

3.5 Password Resetting

Attackers often find it much easier to reset passwords than to guess them. Many password cracking programs are actually password reset tools. In most cases, the attacker boots from a floppy disk or CD-ROM to get around the typical Windows protections. Most password reset tools contain a bootable version of Linux that can mount NTFS volumes and can help you locate and reset the Administrator's password.

A widely used password reset tool is the free Petter Nordahl-Hagen program. Winternals ERD Commander 2005, one of the tools in Winternals Administrator's Pak is a popular commercial choice. Be aware that most password reset tools can reset local Administrator passwords residing only on local SAM databases and can't reset passwords in Active Directory (AD).

3.6 Password Cracking

Although password resetting is a good approach when all you need is access to a locked computer, resetting passwords attracts unwelcome attention. Attackers usually prefer to learn passwords without resetting them. Password cracking is the process of taking a captured password hash (or some other obscured form of the plaintext password or challenge-response packets) and converting it to its plaintext original. To crack a password, an attacker needs tools such as extractors for hash guessing, rainbow tables for looking up plaintext passwords, and password sniffers to extract authentication information.

3.6.1 Hash Guessing

Some password cracking tools can both extract and crack password hashes, but most password crackers need to have the LM password hash before they can begin the cracking process. (A few tools can work on NT hashes.) The most popular Windows password hash

extractor is the Pwdump family of programs. Pwdump has gone through many versions since its release years ago, but Pwdump4 is the current version.

To extract password hashes using Pwdump, you must have administrative access to the local or remote machine you're attacking, and you must be able to use NetBIOS to connect to the admin$ share. There are ways around the latter requirement, but the tool alone requires it. When you run Pwdump4 successfully, it extracts LM and NT password hashes and, if Windows' password history tracking is active, all hashes for older passwords. By default, Pwdump saves password hashes to the screen, but you can also output them to a file, and then feed them to a password cracker.

Many password cracking tools accept Pwdump-formatted hashes for cracking. Such tools usually begin the cracking process by generating some guesses for the password, then hashing the guesses and comparing those hashes with the extracted hash.

Common password crackers are John the Ripper and Cain & Abel. John the Ripper, which comes in both Unix and Windows flavors, is a very fast command-line tool and comes with a distributed-computing add-on. Cain & Abel can break more than 20 kinds of password hashes, such as LM, NT, Cisco, and RDP.

3.6.2 Rainbow Tables

These days, password crackers are computing all possible passwords and their hashes in a given system and putting the results into a lookup table called a rainbow table. When an attacker extracts a hash from a target system, he or she can simply go to the rainbow table and look up the plaintext password. Some crackers (and Web sites) can use rainbow tables to crack any LM hashes in a couple of seconds. You can purchase very large rainbow tables, which vary in size from hundreds of megabytes to hundreds of gigabytes, or generate your own using Rainbow Crack. Rainbow tables can be defeated by disabling LM hashes and using long, complex passwords.

3.6.3 Password Sniffing

Some password crackers can sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process. Cain & Abel both sniffs authentication traffic and cracks the hashes it retrieves. Other

sniffing password crackers are ScoopLM and KerbCrack, a sniffer and cracker for cracking Kerberos authentication traffic. None of these can crack NTLMv2 authentication traffic.

3.7 Password Capturing

Many attackers capture passwords simply by installing a keyboard-sniffing Trojan horse or one of the many physical keyboard-logging hardware devices for sale on the Internet. For $99, anyone can buy a keyboard keystroke logger that can log more than 2 million keystrokes. Physical keyboard logging devices less than an inch long can easily be slipped between the keyboard cord and the computer's keyboard port. It is also very easy to sniff passwords from wireless keyboards even from a city block away.

4.0 Dangers posed by Passwords/Passphrases

On any given system, certain users have privileges that the others don't and shouldn't even have. By identifying yourself on your computer or any given web site, you are granted with access to your work environment and personal data, data which you define as sensitive and data you wouldn't want to make public, the way a company doesn't want to give a competitor an access to its intranet, for instance. Abusive scenarios posed by exposing accounting data are:

4.1 Identity theft

Identity theft might occur once your accounting data is somehow known to another person using it to impersonate you in order to get hold of you digital identity. This might result in both financial damages, as well as personal ones.

4.2 Sensitive data exposure

The content of your e-mail correspondence, personal projects, documents and photos, could be exposed to a malicious hacker or someone targeting especially you as an individual.

4.3 Company data exposure

Unethical intelligence by getting sensitive confidential internal information through a badly maintained and kept accounting data would have an enormous impact on the company you're working for. I doubt you would like to be the one who exposed the next 6 months" marketing and advertising plans to a competitor.

4.4 Involvement in criminal activities

The use of your account could be used in various criminal activities if not well maintained and kept secret. Remember the trace leads back to your account.

5.0 Securing Passwords/Passphrases

5.1 Construction

Users should construct a password/passphrase that meets the minimum following criteria:

- Password/passphrases should ALWAYS contain:
  - At least eight characters (but more is highly recommended)
  - Both upper and lower case letters
  - At least one number
  - At least one special character (e.g., !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Password/passphrases should NOT:
  - Be based on personal information, such as names of family, dates, addresses, phone numbers, etc.
  - Be based on work information, such as room numbers, building name, co-worker's name, phone number, etc.
  - Use word or number patterns like, aaabbb, qwerty, zyxwvuts, 123321, abcABC123, etc.
  - Be a word found in any dictionary in any language, slang, dialect, jargon, etc.
  - Be based on your username, your real name, handle, nickname, screen name, etc.

The following section describes how to create a password/passphrase which includes all aspects of the criteria above making it hard to guess yet easy to remember. Be aware that some systems do not allow password/passphrases to meet all of the above criteria – for password/passphrase construction on such systems, follow all possible recommendations and contact your system administrator for suggestions on compensating for these limitations.

One way to meet the suggested criteria is to mix special characters, upper and lowercase letters, and numbers, and associate them with a phrase or song titles.

5.2 Protection

Password/passphrases are an important tool available to users to protect resources. Unfortunately, people are not accustomed to memorizing difficult password/passphrases that include numbers and special characters. This is made more difficult due to the ever-increasing number of password/passphrases required in today's world. Many people have chosen to write down their password/passphrases and keep them in an unsecured area, such as under their keyboard, filed in a rolodex, or posted on their computer screen. All users

should use the following security measures to protect their password/passphrases and associated accounts:

- Password/passphrases should be memorized and not written down or stored on-line. If you must write down a password/passphrase it must be stored in a secure location allowing only authorized access, such as a locked filing cabinet or safe.
- Password/passphrases assigned to individuals should not be shared with anyone, even your supervisor. All password/passphrases must be treated as sensitive/confidential information.
- Anyone requesting an individual's password/passphrase should be referred to the Information Security Office and this guideline.
- Password/passphrases should not be included in e-mail messages or other forms of electronic communication such as instant messengers, chat rooms, and wireless text messaging, etc.
- User accounts that have system-level privileges granted through group memberships or programs (such as the "Administrators" group in Windows or "sudo" in Unix) should have a different password/passphrase than all other accounts held by that user.
- Never use a university password/passphrase when joining internet sites, such as eBay, Yahoo, Hotmail, Amazon, etc.
- All accounts used for business or financial transactions should use a unique password/passphrase.
- Don't talk about a password/passphrase in front of others or reveal a password/passphrase over the phone.
- All default password/passphrases must be changed as soon as possible.

5.3 Maintenance

It is important to remember that given enough time, any password/passphrase can be guessed using currently available software; therefore, it is critical that password/passphrases be changed regularly based on complexity rules. Users should not reuse any recent password/passphrases when creating a new password/passphrase. The recommended password/passphrase change interval is every 180 days when constructing a password/passphrase following the minimum recommendations in this guideline.

5.4 Safety Tips

- If you suspect that an account or password/passphrase has been compromised, change the password/passphrase or disable the account immediately, then contact your system administrator.
- Do not use the same password/passphrase for all internet accounts (e.g., Yahoo Hotmail, Skype, Facebook etc.).
- Where possible, don't use the same password/passphrase for various access needs. For example, select one password/passphrase for your windows account and a separate password/passphrase for your admin account. Ideally, you should have different password/passphrases for different systems.
- Do not use the "Remember Password/passphrase" feature in applications such as Outlook, and MSN Messenger.
- Never provide any current password/passphrase or variation of it to an internet site that requests your e-mail address and then requests a password/passphrase.
- If exceptional circumstances require you to disclose a password/passphrase, the password/passphrase should be changed as soon as possible.

6.0 Alternatives to Passwords/Passphrases

6.1 Biometrics

Biometrics is the next generation of authentication methods. Although it is still in its early implementation period due to the associated costs, and sometimes the number of false results, biometrics will change the way we authenticate ourselves, hopefully with 99% accuracy. Simply, biometrics cannot be stolen, cannot be forgotten, neither can they be given to another person. Biometrics systems may include fingerprint systems, voice recognition systems, Eye/Retina scanner systems, hand geometry systems and handwriting systems.

6.2 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) functions give entities, namely employees or servers the ability to communicate, authenticate, sign and verify identities by creating digital certificates, each of which containing private and public keys. The public key is available to anyone wanting to exchange data with the entity and the private key is the only way for the entity to decrypt, or identify itself properly. PKI is very useful when communicating over insecure networks like the Internet and both on the internal servers.

Although passwords will continue to represent the most common authentication method for a long time to go, companies and users that have already realized their weaknesses are slowly switching to other possible alternatives. Encryption will be the next big thing for the majority of small and middle size companies as well as the adoption of various biometrics methods.

7.0 Conclusion

Although passwords and passphrases protect a user's authenticity, they are not completely fool-proof. That is why users should be cautious when choosing and maintaining them and in some cases they should also use an alternative solution for enhanced security.

8.0 References

- Password Construction and Maintenance, The University of Arizona
- Windows IT Pro, **http://www.windowsitpro.com**
- 365 Computer Security Training, **http://www.computer-network-security-training.com**
- WindowsSecurity.com, **http://www.windowsecurity.com**