- Passwords - Common Attacks and Possible Solutions -
By Dancho Danchev
dancho.danchev[at]hushmail.com

Overview

Making sure authorized users have access to either sensitive company information or their personal e-mail can be a daunting task, given the fact that an average user has to remember at least 4/5 passwords, a couple of which have to be changed on a monthly basis. The majority of users are frustrated when choosing or remembering a password, and are highly unaware of the consequences of their actions while handling accounting data.

This article will provide you with an overview of how important, yet fragile, passwords security really is; you will be acquainted with different techniques for creating and maintaining passwords, and possible alternative methods for authentication, namely Passphrases, Biometrics and Public Key Infrastructure(PKI).

Dangers posed by passwords

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Management staff with outdated mode of thinking still believe that passwords are the most essential, user-friendly way to identify a user on their network or database, while the fact is that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.

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:

- 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.

- 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.

- 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.

- 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.

The Most Common Password Exposure Scenarios

- Physical security breach
A physical breach of your computer will completely bypass even the most sophisticated authentication methods, even the most secure encryption ones. A keylogger, both software and hardware might be installed, your secret PGP key might as well be exposed, thus all your accounting and encrypted data will be compromised. It doesn't matter how long, or secure your password is as physical security breaches are one of the most critical ones.

- Unintentionally shared
A user might share his/her accounting data without even realizing that by exposing it at the risk of a potential break-in increases. A password is usually shared with friends, bosses, and family under different circumstances. A "benefit" considered by some users is the convenience for two persons or more, to know certain accounting data in order to gain access to a certain resource. Passwords might also be shared in an informal talk with coworkers discussing the latest company's password policy, or the way they choose their passwords, how they maintain them and in some cases how the management will never find out about their thought to be secret ways of storing the accounting data. One of the most critical and easy to conduct ways of obtaining sensitive data is simply to ask for it, both in a direct or an indirect way, which is what social engineering is all about.

- cracked
Sometimes in case of a partial break-in, the encrypted password file of a company might be exposed to a malicious attacker. If it happens, the attacker will start password cracking the file, namely trying all the possible combinations with the idea to find the weakest passwords and gain privileges later on. In case the company is aware that its passwords' file has been compromised, it should immediately notify all employees to change their passwords, so even if weak passwords are exposed, they wouldn't be valid ones anymore. However, if the company is not aware of its password file exposure, it should constantly try to crack its password file just like an attacker would do and filter out the weakest passwords.

- sniffed
Are you aware how many employees are accessing sensitive data through their already breached computer or their friend's one? Having strong password doesn't guarantee its integrity when it's not securely transmitted over the Internet. Don't give your employees the ability to choose between plain text or SSL authentication; instead, enforce all network communications in encrypted mode.

Another highly recommended option would be to provide everyone with "last login from…" feature, so that in case they notice an unauthorized login, they would report it right away.

- guessed
A large number of users are tricking the established password policies by somehow creating a believed to be strong, while weak or common sense password. Although nowadays this method is rarely used compared to the ones we've already discussed above, it should be kept in mind that certain users are still choosing passwords based on objects or brands around their desk.

The Most Common Password Maintenance Mistakes

- Auto fill feature
The majority of applications will allow you to remember your passwords and accounting data, but unless you're sure that the computer is reasonably protected from possible physical security breaches, you're strongly advised not to have your passwords remembered in this way. Make sure this option is not used at public access places like netcafes' etc.

- "post it" notes
Passwords are often written down and even worse, posted next to the monitor or around the desk. This could easily be observed by malicious attackers or insiders, so avoid it.

- "the secret place"
A lot of people believe they have found the secret place under the keyboard or anywhere around the desk, which is very unacceptable considered the fact that if observed enough, they would reveal their believed to be secret place, get distracted and have their accounting data leaked out. Even so, a large number of people keep certain accounting data on papers, PDAs etc.,so a possible strategy until they remember their accounting data and get rid of the note they keep with them all the time would be the following; have at lest 6/7 different and fake passwords around the real one, you might even cross a couple of them, even the actual one. This would be very beneficial keeping in mind that hopefully two/three false logins will lock the account, and in case your note gets exposed, it would be still a matter of luck for the attacker to use the right one. Although this method provides no guarantees, and is not recommended at all, it is a very short solution to remember your password and get rid of your note right away!

How to Choose a Secure Password

Choosing secure passwords consists of knowing what their insecurities are, how passwords are cracked and what's behind the "at least 8 characters long, consisting of lower and capital letters, special characters and a number" requirement. Basically, the shorter the password, the more opportunities for observing, guessing and cracking it. A password cracker would try to guess all the possible combinations of letters, numbers and characters until he/she finds the right one. Given the number of letters in the alphabet and the amount of numbers(0/9), the second, namely a numbers' based password, will give the attacker fewer opportunities to crack. Another commonly used technique is the use of a dictionary file against the encrypted passwords database, so that the weakest and most obvious passwords in terms of words listed in a dictionary will get exposed; this is why a longer password consisting of letters, numbers and characters would make it a little bit time consuming for an attacker attempting to crack the stolen passwords file. Whenever you create a password, consider the following:

- make it at least 7 characters long, combination between small and capital letters, at least one number and special character like !@#$%^*()_+
- do not simply use a dictionary word or a logical sequence of characters like aaa555ccc, 1234567890 etc.
- try not to use a password you have already used on another system, ignore have the same password on all assets you have access to at any cost

A combination of the following strong, yet easy to remember passwords techniques you may use are:

- choose a dictionary word like success, then reverse it sseccus
- add numbers in front or at the end of it 146sseccus or sseccus953
- consider adding at least one special character like !@#$%^&*()_+ anywhere
- The use of at least one capital letter would increase the crackable possibilities even more
- replace certain characters with numbers that you associate with them, security would be s3cur1ty where e stands for 3 and i stands for 1
- Separate each letter with a number, security would be s1c3u2r4i6t5y

How to Remember Passwords

Remembering several passwords for different assets is a huge problem for the majority of users. That's why they either ignore remembering, thus writing them down, or create weak, but easy to remember passwords. Whereas, remembering passwords might not be such a difficult task if the majority of users stop thinking of them as a combination of bulk characters, but as a way to identify themselves the way the do when taking money from a cash machine. In this case, it's all their company's and personal data they should try to protect.

- associate them

Association plays an important role in the memorizing process. Given a certain period of time, someone can teach you Japanese if he/she finds out the way you memorize and, most importantly, associate things. Visualization of the password is another important aspect of memorizing it, and within a short period of time you would be entering it even without thinking what you're entering - a temporary habit, given the fact that the majority of organizations require constant password change.

- explain them to yourself
For instance the password Y13#tiruceC basically represents the word security backwards, where the first and the last letters are capital, and the first capital letter is followed by your best friend's birth date, plus a special character. Instead of representing a bulk of characters like it used to be, now your password is your own encrypted language.

Possible Solutions

When enforcing authentication methods on both network and security policy levels, the majority of users proved to be unreliable in storing and creating strong passwords. The service desk is often too busy to handle "forgotten passwords" requests, and unless the company doesn't undertake a passwords awareness initiative, the problem will continue to grow.

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, favorite sentence or 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.

Biometrics

Biometrics is the next generation of authentication methods. Although it's 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.

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.