emiic

The Password Guide

Table of Contents

Produced by the Chief IT&C Consultant, Emiic Security

Helping keep your secrets safe

www.emiic.net

Introduction

The use of passwords is now a part of daily life for anyone using a data communications or storage device. More and more, these passwords are proving a weak point in the security of our systems and networks yet they are an unavoidably necessity.

With 400MHz Quad Pentium II computers able to test encrypted passwords against and 8 Mbyte dictionary of common passwords in seconds[1] a diligent effort is required by the guardians of our data and communications to ensure that users and organisations data and communications are as secure as possible.

The ideal solution to this problems is to avoid passwords, particularly as a single point of failure. Cost effective biometric systems now exist that can greatly compliment existing security systems or even, in limited cases, replace passwords. Systems for generating pseudorandom super-keys and storing them on physical devices like smart-cards and thumb-drives also exist and are a great alternative to the clumsy old password.

These system are however outside the realm of this paper. Here we will look at making the most of password structure you have and, as this is largely dependent on the commitment of you users, how best to assist them in helping you keep your organisations data safe.

So what can you do to improve the security of your password dependant systems?

The information in this document is intended as a guide for system administrators and senior personnel responsible for information security within an organisation. The author takes no responsibility for loss due to the implementation of these suggestions and professional advice should always be obtained if in doubt.

1 B. Schneier, *Secrets and Lies*. Wiley Publishing, 2000.

Entrust the User

You, as an administrator, can only do so much. On every system the user must play a part in security. If you make things difficult for your users, or are seen to be making things difficult for your users, without clear definition, your users will rebel. Users, in their varying degrees of intelligence and technical experience, will always find ways to circumvent “blocks” you create. Cooperation, mutual respect and trust are the best way to get everyone working toward better security practices.

Treat Your Users Like Adults.

System administrators are often overly critical and suspicious of users. This demeaning behaviour often leads to user backlash and resistance to regulations. Users are trusted with safe practices in many other areas of an organisation and data security should be no different. Having some faith in the users of a system and putting some of the responsibility of security back on them will dissipate much of the resistance to data security.

For example, imagine a staff member is given a key and asked to lock up an office when they leave at the end of the working day. They would most likely comply without question. The responsibilty has been placed upon them and reasons for compliance are clear and obvious. Failure to do so would be seen as putting the organisation and other staff at risk and cause considerable damage to the members dependability. If this key is left in plain sight, attached to a key-ring indicating it's origin, consequently stolen and used to gain unlawful entry to a premises it would also be a reflection of the entrusted employee.

Users comply with security requirements when there is a fear or awareness of the effect failure could have, if only on their reputation. Encouraging users to take on some of responsibility for data security themselves will result in a much more enthusiastic response.

Educate Your Users (Like Adults)

Users or staff often underestimate the consequences of poor digital security and consequently resist compliance or engage in sloppy practices. Simply educating members on the consequences or poor practices has a large impact on their compliance. Ideally this could be conducted after a vulnerability exercise has been conducted to show practical example of the consequences of failure.

Users should be encouraged to look upon passwords as digital keys and treated with the same respect, with similar consequences for negligence.

Make an Example of Those who do not Comply and Reward Good Practices

This can be conducted in a number of ways.

Active vulnerability assessments resulting in simulated negative consequences will have the strongest impact on staff. If users feel they were a point of failure within an organisations security resulting in negative consequences they and others will be encourage to take data security seriously.

Failure to comply with security regulations should also bear consequences for all staff. If noncompliance is detected it is likely that the message of data security not being received more than just that member of staff.

Consequences for staff, beyond simply the member responsible, will have a peer encouragement effect. Weaknesses and strengths in security should be publicised throughout an organisation to the team or section level. If a team or section is continually identified as a weak point in data security members will feel encouraged to improve their practices. Many organisations already practice this with regard to physical security with much success.

For example, IT security and physical security could cooperate in issuing “Breach Notifications” for failures in security. A monthly report of breaches, both physical and data/communications, summarised to section or team level, is made available to all within an organisation. Physical and IT & C security could be further integrated, for example, by doing after hours or spot checks for written passwords in the open.

Awards could be presented or activities organised for sections or teams with a good security record. Disciplinary action should be employed to staff or users continually failing to practice good security techniques.

Emiic is ideally placed to conduct these vulnerability assessments, and produce reports if needed, for both your physical and data security.

In Summary, Employ the Three Step Process

- **Educate users on good security techniques and consequences to them and the organisation of noncompliance.**
- **Entrust the user to some of the security of the organisations data.**
- **Employ strict consequences for individual points of failure due to poor security and publicise weaknesses and strengths.**

Keep the Options Open

In fits of paranoia administrators often unwittingly apply excessive restrictions and limitations on users password choice. While some guidelines should be applied to help prevent against known password attack methods the overall range of password combinations should kept as open as possible. An attacker of a system will look to limit their dictionary attack option as much as possible when beginning an attack.

You must always assume an attacker has access to your password requirements. If an attacker knows, for example, that passwords must be 8 digits they can immediately ignore all seven, nine and ten digit combinations, vastly reducing the number of attack combinations. In an alpha/numeric eight digit password set, legislating that the first digit must be a number reduces the possible combinations by nearly 28% (turning a three day attack into two).

Dictating a set substitution code (ie. E = 3, a = @, l = 1, etc.) also dramatically reduces attack times as an attacker will simply change their dictionary attack set to compensate for the substitution. If these options are left to the discretion of an educated user the attacker must apply all the possible combinations to their dictionary attack set increasing attack times.

Reduce the Intrusion

Really consider the life span you need on your passwords. Short life spans on passwords will only frustrate users and drain them of good password creation potential. Thirty days, for example, is unworkable in most environments and will only lead to insecure practices and poor password creation. It is far better to encourage and enforce strong password and give your users more time between changes. If your users are complaining about the regularity of change requests (it is a good idea to get out of the basement and engage with them occasionally), try explaining the methodology and compromising. For example, you could agree to lift the minimum length to ten digits in exchange for a extra 15-30 days on the cycle.

Keep warnings and annoyances to a minimum. Users do not need more than a couple of days notice to prepare for an expired password. Anymore is simply seen as an unnecessary intrusion and annoyance, particularly on systems with short password cycles (sixty days or less). On systems where use is sporadic then up to four or five days may be necessary to avoid the continual “surprise” factor. Experience shows that the average user will delay changing until expiry, and only then put thought into a new password.

Try to centralise as many systems and databases as possible to a signal authentication system (ie. LDAPS) and make clear which systems share passwords to your users. Continual and disparate notices to change passwords on multiple systems with only aggravate users and lead to resistance.

Maintain Flexibility with Passwords

The number of restrictions applied to users with regard to employing passwords is often overwhelming. Keep password restrictions simple and to a minimum. Publicise these limitation well. It is extremely annoying for users to keep attempting password changes that fail for various reasons.

Sample Password Requirements

Guidelines should emphasise good practices vice bad practices.

• Minimum 8 characters.	Do not set maximums or finite lengths.
• Try using a sentence to generate your password. ○ For example; "***T***he ***d***ay ***I s***tarted ***w***ork ***i***t ***w***as ***9 d***egrees" becomes ***TdIswiw9d***	Encourage the user in good techniques with examples.
• Obfuscate dictionary words inconsistently and use more than one. ○ For example; "***Julie***, my ***F***irst ***K***iss ***Dec92***" becomes ***Ju1i3FKDec92*** ○ For example; "Steal This" becomes ***5tea1Th!s17***	Use positive suggestions as much as possible with examples.
• Avoid key dates (birthdays etc.) and names.	Keep construction restrictions simple. With good education and awareness the user will use common sense.
• Must contain a minimum one number and one letter.	Keep mixing limitations to a minimum. With good education and awareness the user will use common sense.
• Examples of bad passwords; ○ ***P3anut5*** - signal word, basic substitution, too short. ○ ***WifeJenny*** - key name used, dictionary words not obfuscated. ○ ***I@mGr3@t*** - common phrase, consistent substitution.	Demonstrate and explain bad practices for clarity.

Encourage the use of Password Storage

If your users are in an environment where they have access to numerous systems they are quickly going to amass a number of passwords to remember. This is on top of the many passwords they are required to remember in their personal lives, ie. home computer login, on-line banking, web-mail, ISP mail, My-space, Amazon, frequent flyer program, wireless LAN key, the list goes on and on. It is inevitable that good passwords are going to difficult to remember. Your users will resign themselves to coming up with easy to remember (insecure) passwords used multiple times across systems.

It may be ideal, depending on you situation to encourage the use of a password storage system to encourage the use of good passwords. If your users believe you are making an effort to assist them in maintaining good data security practices, this will have a positive effect on their behaviour.

Physical Storage

This will greatly depend on how much trust you have in people that have physical access to your premises and the facilities for physically securing documents. If your users are in a very public area with a large volume of untrusted traffic you are not going to encourage the writing down of passwords.

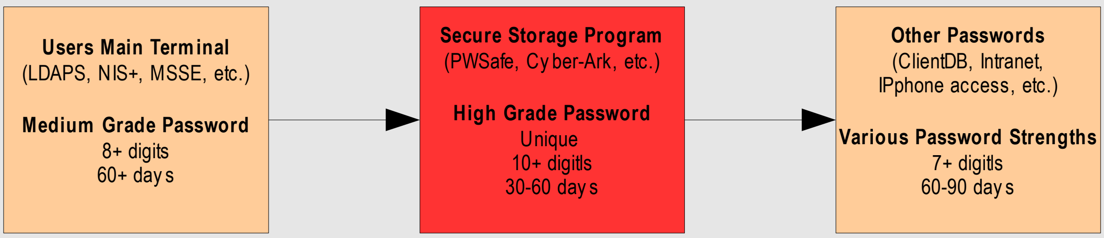
However, if each of your staff has a physically secure place (safe, lock-box, secure locker, etc.) and you trust the users collectively, you may very well encourage them, for less critical systems, to spend some time coming up with a series of good passwords, writing them down and locking them away.

Digital Storage

Preferably though, you would encourage the use of digital storage of passwords.

Your Digital Safe must have a unique password. There is no point your users putting all your valuable data into a digital safe and giving it the same password as their Windows login. Due to the well publicised deficiencies in Windows local passwords this would expose all the users passwords to attack once access is gained to the carrier system. Encourage and enforce a good, strong password for this system, justified by the effort saved not having to remember multiple passwords and other sensitive data.

Ensure your password storage program is from a trusted source. *Password Safe* (http://passwordsafe.sourceforge.net/) is an example of a good digital storage program. It uses high-grade encryption, is light on system resources and is easy to use. Spend some time reading reviews from security professionals about your chosen software before implementation or contact an *Emiic* consultant for further advice.



Example of password plan showing guidelines for managing password on your system and the access chain.

Conclusion

Passwords are an ever increasing weakness in our modern digital storage and communications environments. They are however, in many cases unavoidable. Poor password practices lead to many security breaches. Whilst viruses may allow access to vulnerable systems, strong passwords (and good software selection) will continue to protect your critical data while you return your access controls to a safe level.

Password security is linked to the general security of you organisation. Users should be encouraged to treat data security as any form of organisation and personal security. Once users see a clear benefit to password discipline, good practices and compliance, in general, will follow. There will however, always be minority exceptions in those that do not take data security seriously. You must deal firmly and seriously with these vulnerabilities as should be done with any organisational security breach or fraud.

Encourage and assist your users wherever possible with there own password security. If they feel you are on the same side you will find them much more pro-active towards good practices. Once good password practices become the accepted normality within your organisation the more secure your data will be.

For further information on the best practices and technology for securing your network and systems please e-mail us at *info@emiic.net* or go to our web-site at *www.emiic.net*.