Best Practices for Password Management of Encrypted USB Flash Drives

This document focuses on the need for proper password management when using secure USB flash drives.

Intended Audience

If you have a need for mandatory password protected portable data storage you must consider best practices for password management of these devices. Security industry organizations such as the SANS Institute and (ISC)^2 put a strong emphasis on the handling of passwords in access controls. This best practice offers technical decision guidance and highlight important focus areas when electing a solution. The password management highly affects the overall costs of the solutions to it is important to recognize this from a business decision perspective.

Introduction

When selecting a secure USB drives solution the need for a solid password management is a must have. As the secure USB drive is mandatory password protection the way you handle and maintain the password and its change and reset processes are pivotal to the security of the solution. It is critical that the password management follows security industry best practices to motivate the investment into hardware encryption as a chain is only as strong as its weakest link. Weak password management will lead to weak security no matter the level of encryption. As stated in information system security best practice from (ISC)^2 for CISSP® CBK® [1]it is clear that a device that relies on a password for its access control its security is completely reliant on the management of that password to uphold the security of the protected stored data.

Password management is often one feature of many in a broader device management solution but it is the most critical feature given the nature of the design of these solutions.

These best practices focuses on achieving a full password management solution, this can only be achieved when the secure USB flash drives are centrally managed.

Best Practice Advise

It is advised to adhere to the following best practices in the management of passwords of portable devices.

- Ensure the solution does not allow the user to enter the password in any free text field on the devices such as in a hint or other field as this will lead to unwanted user behavior.
- Offer the option of a password hint but ensure that it cannot contain the password. If your policy decision is to disallow hints confirm that it can be deactivated.
- The user's data must be intact after the password reset has been completed.
- The solution must prompt a password change directly on each password reset process. This avoids the risk of someone breaching the password reset process and then making use of the old and new password without the end-user being aware of them being exposed.
- The password reset must never expose the old forgotten password to administrators as this is not a need to know information and could cause a breach situation. Users are known to

[1] Official (ISC)2 Guide to the CISSP CBK, Second Edition, 2009

share passwords between services and a flawed password handling process can expose a password that is used in system that has a higher classification than the drive itself. The SANS Institute Password Policy template which states refers to this as: *one user [must be able to] take over the functions of another without having to know the other's password.*

- The password reset process should be activated by the administrator not the end user. If it is left to the end user to activate or enroll in a password reset scheme it has been found that they most often don't take the needed steps, that is until they forget their password and it is too late to activate the password reset process. User adoption in enrollment processes is simply a highly recognized software system problem; any measures that can be put in place to avoid end-user frustration should be available as the cost of non-adoption in this case is unacceptable.
- Offer a secure self-service password reset option which works locally on the users trusted user account. This avoids unnecessary helpdesk calls.
- Offer an out-of-band method for resetting password using voice or text messages utilizing a challenge response scheme. This allows for trusted password resets where there is no Internet available. This ensures the availability of information at all times for authenticated users even when they have forgotten their device passwords.
- Avoid schemes that offer password backups. Storing an unencrypted, or even an obfuscated, list of password at a central location is a flawed security practice according to the SANS Institute: *do not store passwords in clear text or in any easily reversible form*[2] . It is creating an unnecessary aggregated information asset that will require additional steps to be protected.
- Never accept the usage of master passwords as a substitute for a real password management scheme. The reasons for avoiding one password for all devices are numerous. One is the risk for a 'keys to the kingdom' attack. If the master password is known by a group people in plain text of it risks exposing all drives if one individual becomes an insider threat. It also exposes the organization to the risk that administrators are unaudited checks on user's devices. Further is divides responsibility of the drives since now numerous individuals could have had access to the device. The biggest pitfall of master password is in their maintenance as that one password to rule them all must be kept and when it is exposed it needs to be changed immediately on all devices, a completely unmanageable approach.
- To increase user adoption of the secure USB drives it may be advisable to allow a secure automatic unlock (Single Sign On, SSO) if the users have already authenticated themselves. This approach saves time and maintains the security since the drives will ask for the password when used on any other system but the registered users own trusted system.

Conclusion

A robust password management can help maintain the security of the hardware encrypted secure USB flash drives. A flawed approach to password management can degrade the most highly certified and validated solution. By making it easy and secure for the users to perform password resets unwanted user behavior is avoided. A functioning password management system will also make sure that the costs for maintaining the solution is kept low.

[2] http://www.sans.org/security-resources/policies/Password_Policy.pdf