Global Information Assurance Certification Paper

What's so hard about implementing Complex Passwords?

Name:Ellsworth Fujii
Userid: efujii001
GIAC Security Essentials Practical Assignment version 1.4.b
Option 1

Abstract: This practical is a case study (Option 1) describing the steps a 1,300-user company took to implement "complex" passwords.

Introduction

Our electric utility company had an existing security policy requiring strong passwords, but no practical means of enforcement. In trying to create an enforcement technique, we decided not to use Microsoft Active Directory's complex password policy. Instead, we investigated and implemented third-party software that checked for both dictionary and company-related words.

Electric utility companies fall under Homeland Security's Presidential Decision Directive 63 (PDD 63), Critical Infrastructure Protection. As such, we must implement strong security safeguards to protect our resources which included having a password policy as an essential part of information security.

Presidential Decision Directive 63 CIP states that:

> Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks.[1]

We needed to ensure that only authorized employees had access to information needed to do their job. Proper authentication, one of the key concepts of information security, helps ensure that this is done.

As stated in the *MCSE Windows 2000 Network Security Design* guide:

> Probably the first tenet of security that everyone learns is, "make sure that the people who need to get into the network can have access and the people who should not have access to the network are blocked (or at least hindered) from entering." ...This means that you must set up your security features to authenticate all user access to

[1] Federation of American Scientists – Intelligence Resource Program
Presidential Decision Directives (PDD 63)
URL: http://www.fas.org/irp/offdocs/pdd-63.htm

system resources. Authentication strategies set the level of protection against intruders trying to steal identities or impersonate users. [2]

Password Policy

Our auditors recommended that complex passwords be part of the password policy. A Microsoft Security assessment done late last year also recommended implementation of complex passwords.

We established these Active Directory password security policies[3]:

- Minimum Password Length
- Maximum Password Age
- Minimum Password Age
- Enforce Password History
- Account Lockout Duration
- Account Lockout Threshold

Microsoft security guidelines recommend that:

> Adopting strong password policies is one of the most effective ways to ensure system security. This is only an example policy. It may not be strong enough for your needs; it is up to each customer to determine how strong is strong enough.
>
> - At a minimum your password must be at least six characters long. For stronger security, choose longer passwords with characters from all four classes.
> - Your password may not contain your e-mail name or any part of your full name.
> - Your password should be changed every 45 days.
> - Your new passwords should never be the same as any of your last eight passwords.
> - Your password should not be a "common" word (for example, it should not be a word in the dictionary or slang in common use). Your password should not contain words from any language, because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds. [4]

A team comprised of individuals from Legal, Internal Audit, Human Resources, Information Technology & Services, and Information Security Manager created our *Information Resource Policies*. The *Information Resource Policies* included Acceptable Use, Identification and Workstation Protection, Information Ownership and Classification, and Remote Access policies. The Information

---

[2] Gouvanus, Gary/King. Robert. "MCSE Windows 2000 Network Security Design". Alameda: SYBEX Inc. 2000: 308

[3] Note that since this paper is discussing a public utility company, we have elected to leave out the specifics of our password policy for security reasons. While not the direct object of this paper, we do list the areas of heightened password security that went in conjunction with our complex password policy.

[4] Microsoft - Implementing Guidelines for Strong Passwords
URL: http://www.microsoft.com/ntserver/techresources/security/password.asp

Technology Governance Group[5] reviewed the final draft before the Financial Vice President approved the Policies. The Password policy contained a complex password statement but did not have a method of enforcing the policy. The complex password policy stated that passwords:

- Must contain at least three of the following groups:
  - Upper case letters
  - Lower case letters
  - Numbers
  - Special symbols
- Must not contain common dictionary words, person's username, person's name or company-related words

In an article by Edward Hurley, on the SecuritySearch website, Rob Cheyne of @stake, had these comments about strong passwords:

> But adding symbols expands the total number of combinations enough to make a password fairly strong. Creating a password with a random mixture of symbols, letters and numbers is the best course, Cheyne said. …Longer passwords will make such an attack harder and could discourage attempts…..Passwords with seven or more characters are more secure, Cheyne said….Changing passwords is another way to combat brute force attacks. Changing passwords every 60 or 90 days could foil such attempts.[6]

Product research/selection

The Microsoft Active Directory password policy did not adequately satisfy our complex password rule requirement. The Active Directory Password Policy did not provide enough flexibility for designing password rules. We needed a password filtering software that would restrict use of words that may be commonly used throughout the company, use of dictionary words, and names or usernames.

Factors that influenced selection of the password filter software:

- Cost
- Implementation process
- Ease of use
- Compatibility with Active Directory
- Flexibility to select password filtering options
- Vendor stability

The research for a commercial password filter solution included magazines, vendor web sites, calls to security counterparts, and to information security

[5] This Information Technology Governance Group is a collection of business managers from around the company that help guide the IT department of melding of IT issues with the corporate business needs.

[6] Hurley, Edward, "Proper Password Policy is Imperative". 08 Jul 2002. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci837272,00.html

companies (Microsoft, Gartner Research). Prices varied since there were password filter-only software as well as security-integrated software that included password as well as other security features. We had a short deadline to implement complex password enforcement so our primary factors influencing our software selection were ease of installation and minimum administration.

We found a favorable review *PassFilt Pro* in the Windows & .NET Magazine. The article mentioned that: "*PassFilt Pro* can also check for consecutive identical characters, such as the username within the password."[7]

PassFilt Pro from Altus Network Solutions was selected as our complex password software. The price of $295 per domain controller[8] was reasonable. There was no annual maintenance fee but a $50 per domain controller upgrade fee. *PassFilt* Pro 2.0.3 was compatible with Active Directory 2003. *PassFilt Pro* came with a 27,000-word English dictionary file that could be modified so we could include our list of company-related words.

PassFilt Pro version 2.0.3 provided these password options*:

- Ensure passwords contain characters from a minimum number of the following four categories: (1) numeric characters (2) upper case characters (3) lower case characters (4) non-alphanumeric characters.
- Minimum and maximum number of numeric characters (0-9) and upper and lower case characters (A-Z, a-z)
- Minimum and maximum number of non-alphanumeric characters (like @,#,$, etc.)
- Reject passwords with consecutive identical characters (e.g. aa, bb, etc.)
- Reject passwords that begin or end with a number.
- Force passwords to contain a number or non-alphanumeric character in a specific position.
- Reject passwords that contain any portion of the user's full name or the username within any portion of the password.
- Check the user's proposed new password against a customizable dictionary looking for a case-insensitive exact match or a case-insensitive substring match (i.e. dictionary word is found anywhere within the password).

* Options listed in *PassFilt Pro* documentation from CD

Altus Network Solutions' website contained good information as well as an FAQ and software features section. The site also contained straightforward customer support information.

[7] "Enforce Strong Network Password Creation". Windows & .NET Magazine. April 2003: page 20.
[8] Price listed as of Summer 2003.

Testing

A bad experience several years ago of a password policy change made to the production environment taught us that even if the implementation of complex password software seemed straightforward, we needed to thoroughly test.

The test lab was built on Active Directory with an Exchange 2000 server and a workstation. This environment was adequate to create new accounts and test various password expiration and change scenarios.

We called *PassFilt Pro* Support to discuss the implementation process, basically reviewing the documentation that was provided. The process was straightforward but we didn't want to encounter any surprises.

The installation of *PassFIit Pro* simply involved running the install.exe that copied several files to the System32 folder on the Domain Controller. Important note: *PassFilt Pro* had to be installed on each Domain Controller.

The "Passwords must meet complex requirements" policy under the Default Domain Policy had to be disabled per instructions. The Domain Controller needed to be rebooted to load the PassFilt.dll file and complete the installation process.

The *passfiltpro*.*adm* template needed to be added to the current policy templates. This paper will not detail the step-by-step process to add the *PassFilt Pro* template since their documentation clearly explains this process. The *PassFilt Pro* template contains the Registration and Password Filter Configuration settings.

The Password Filter Configuration for *PassFilt Pro* version 2.0.3 provided 15 security options. We had to be careful that the password options we selected did not make it too difficult for users to create a new password. Although we didn't plan to use all the security options, we tested each option to ensure that the product performed as advertised.

We sent questions via e-mail and received next day responses from their after hour e-mail support. This was very important to us due the multiple hour time difference between their office and ours.

We had issues with the dictionary file that came on the CD since it contained words that were less than four characters. Although we could see a legitimate reason for these short words, we felt that in our environment it wasn't necessary to make it so restrictive. Example of a problem words are "as" or "cat" which make up parts of other larger words. Altus Network Solutions must have had similar requests since they provided a new dictionary file that only contained words which were four characters and greater.

We also added some company-related and cultural-related words to the dictionary list. We added words such as *aloha*, *Maui*, *Oahu*, *Kauai*, *rainbow*, *p@$$word*, and *h@wa11*. It simply involved editing the text file and adding these words to the end of the list. This file must be copied to each domain controller whenever the list is updated.

We liked the feature that performed a case-insensitive comparison of words. This will help prevent use of personal names that was a concern.

The tests satisfied our complex password requirements. We adjusted the Maximum Password Age fields to force frequent password changes. The *PassFilt Pro* software also ensures that new passwords (for new accounts and password resets) conformed to the policy settings.

One of the problems we discovered was that the error message for passwords that did not meet the complex password rules could not be changed. This will be discussed further in the Issues section.

We documented the installation process and security options that were tested. And, used this when we implemented in the production environment.

Education

We felt that education would be the hardest task of implementing the complex password software. Some of our users have a difficult time just changing their passwords and now we were asking them to come up with more difficult passwords.

Most security features will create additional burden, and there needs to be a compromise between security and inconvenience. As a security professional, sometimes it is hard to find and implement this balance.

A section from Maximum Windows 2000 Security states that:

> Password security is an ongoing battle between system administrators and users. But with a smart password policy, administrators can accomplish good password security and users can still remember their passwords.
>
> Part of the problem is that so many system administrators believe the myth that a password like krP4@sWq is a strong password…..The problem is that totally random passwords are simply difficult to remember. And a password that is difficult to remember is not a good password at all.[9]

We scheduled password information sessions at various locations throughout the company. Training material provided step-by-step instructions for changing their

[9] Anonymous. Maximum Windows 2000 Security. Sams Publishing. December 2001 URL: http://safari.oreilly.com (Safari Bookshelf)

passwords. It also provided them hints for selecting their new complex passwords. The attendance to these information sessions was voluntary and not attended by a lot of people. Some people took the training material back to their fellow employees.

We also created a short video clip of the information provided at the information sessions. We felt that this would reach individuals who didn't have time to make it to the formal information sessions. The objective of the video clip was to provide enough information but not make it too long. The link to the video clip was placed on the Security intranet website. To assist with the number of calls expected to the Helpdesk, we also planned to have individuals who had questions regarding complex passwords directed to the video clip.

We also sent users e-mails informing them of the deployment date, link to the video clip, and new complex password rules. This method reached more individuals, which was a good thing, but it also initiated more calls and questions to Helpdesk. Some individuals who had problems changing passwords panicked, because they felt uncomfortable about the new rules.

Installation and Deployment

As mentioned earlier, we had a short implementation timeframe. The complex password policy was adopted last year and we didn't have a method of ensuring that the policy would be followed. The IT Security Officer and Executive Management were also asking for a timely deployment.

We used the documentation from our testing to deploy *PassFilt Pro* on to the production Domain Controllers. We decided to use 5 of the 15 options to comply with the IT security policy. We didn't want it to make it too difficult for users to come up with a password but ensure that the passwords met the complex password rules. We had a debate whether to include the option that rejects passwords which end with a number but felt that we could always change this rule setting as well as other setting later as our users became better at choosing sophisticated passwords.

A SCMagazine cover story stated that users are the weakest link and had this quote about handling passwords:

> "It may be tempting to create passwords so they are easier to remember, but you are playing firth into the hacker's hands. The challenge in creating a hacker-proof password is to make the password difficult to guess without making it impossible to remember," says Vincent Weafer, senior director of Symantec Security Response.[10]

We decided to deploy *PassFilt Pro* on a Tuesday. Our Helpdesk is usually busy with calls on Mondays and we didn't want to interfere with other departments who were also busy on Mondays.

[10] Armstrong, Illena. "Passwords Exposed." SC Magazine. June 2003 (2003): 28

Users were already required to change their passwords every 90 days and were being prompted 15 days before they were required change their passwords. We consciously left this in place so that not all users would be forced to enter complex passwords on the same day and flood the help desk with calls. Our recommendation to users was not to wait until they were forced to change their passwords but to change them soon after the 15-day warning began appearing. But, as expected, there were people who waited until the very last day. Now, being forced to come up with a complex password or not able to log in, they had a harder time making up a password that met the complex rules.

Since we had only a fair turnout to our training sessions, one of our most effective communication pieces was a mail-merge email reminder. We extracted the username and date password changed from Active Directory and calculated the number of days before their password would expire. Every week, we sent users who would be receiving the 15-day password change warning an e-mail reminding them of the complex password rules and directed them to the Security intranet website for additional information. These reminders were well received and users appreciated and felt that it was good customer service.

In another article by Edward Hurley, he states that a security officer tests the strength of his employee's passwords every month. Mr. Hurley, states that:

> Trying to crack employee passwords is just one step in crafting a password policy with some bite. User education is another important piece of the puzzle. They need to know that their password choices affect the security of the company.[11]

We are planning to run a password cracker to test the passwords sometime in the future. We will obtain management approval before conducting these tests based on articles describing cases where individuals without proper authorization have been dismissed. One of the reasons for performing this test will be to determine whether to implement the option to reject passwords that end with a number.

Issues

How to get the word out? This was the main issue confronting the deployment of complex passwords. A team made up of staff from the Helpdesk and IT security discussed the methods which could be used to educate the users. As with any other IT security initiative, users are too busy to take the time to learn about security.

The IT Security Policy states that passwords should not be written down. This was an important issue when considering implementation of complex passwords. We reminded people that passwords should not be written down on the policy

[11] Hurley, Edward, "Testing Password Strength Gives Policy Some Bite". 23 Oct. 2002 http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci858747,00.html

and stressed this at the information sessions and in the material but it is very difficult to enforce this policy. We have to rely on the individual and their managers to enforce this policy.

As mentioned in the Testing section, the error message provided by *PassFilt Pro* was not customizable. The error message provided the Active Directory security setting information, minimum length and history parameters, but a user had to guess why their password did not meet the complex password rule. This was frustrating for a lot of users. It took a lot of time to explain what the rules were without asking them for the exact password they were trying to use.

The electric company has a mainframe running ACF2 as the security software. The current version of ACF2 did not allow for complex passwords and this became a minor but important issue when complex password was implemented on Active Directory. Most of the Active Directory password policy parameter is also used by ACF2. There was no single-sign on or password synchronization product so users are required to change their LAN and mainframe passwords. Unless the user changed both passwords on the same day, passwords expire on different days. The result was a bit of confusion when the ACF2 password didn't have to be complex, which sometimes resulted in users having a simple mainframe password and a different complex Active Directory password.

Post-implementation issues

One of the main issues was the volume of Helpdesk calls. And, the majority of the problem was that the password that they selected contained a word that was in the dictionary list. Users had a hard time coming up with non-words. It took time to explain the complex password policy. For example, they tried passwords like 2David, Sassy#, 4name@, and AlohaH9. We had to explain that any dictionary word, even a nickname, if found in the dictionary list (even mixed case) would be rejected as a password. Some users were not aware of the new complex password rules.

The number of calls to the Helpdesk increased 100% when the complex password policy was implemented. We have just completed the first cycle of password changes so we anticipate the number of calls to decrease.

Some people called that they did not know that there were new complex password rules. Some people don't have e-mail so they didn't receive any notices of the new rules.

Lessons Learned

The primary issue concerned education of the complex password rules. Therefore, mandatory information sessions would be advisable. Although, there should be a balance in the number of reminder notices so users don't look at them as SPAM. Providing more information to them when they first have to use complex password is recommended. Our technique of pulling out a list of user

accounts that were about to have their passwords expire and using that list with mail-merge to email reminders was one of our most successful communication devices.

Complex password rules could have been posted on bulletin boards throughout the company. Employees should have been sent informational flyers and told to have them posted on their personal bulletin boards for reference.

A single-sign on solution would probably have reduced the confusion and frustration. This would have eliminated them from having to change their passwords on multiple platforms.

We should have upgraded mainframe security software, ACF2, to the version that allows for complex passwords. Users were a bit confused because the LAN required complex passwords but the mainframe didn't. We plan to upgrade to the new version of ACF2 within the next few months.

We didn't have a good idea of how many people knew of the complex password rules. Although information sessions were held and e-mails were sent, we really didn't know how many people were informed and whether they comprehended the complex password policy. This unknown factor frightened some of us. If the Helpdesk received too many calls, there was a possibility that *PassFilt Pro* would be disabled.

Fortunately, it didn't come to that and the complex policy is in place today. The technical and implementation effort of the implementation went very smoothly. Users experienced the heartaches of learning the new rules during the first cycle of password changes. As we enter the next cycle of changes, there has been increased acceptance and lower calls to the Helpdesk. If we followed the lessons learned, the implementation of complex password would not have been as complex.

Internet Source

Federation of American Scientists – Intelligence Resource Program
Presidential Decision Directives (PDD 63)
URL: http://www.fas.org/irp/offdocs/pdd-63.htm

Microsoft - Implementing Guidelines for Strong Passwords
URL: http://www.microsoft.com/ntserver/techresources/security/password.asp

Hurley, Edward, "Proper Password Policy is Imperative". 08 Jul 2002.
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci837272,00.html

Aultus Network Solutions – *PassFilt Pro* Eliminating Weak Passwords

URL: http://www.altusnet.com/passfilt/)

Hurley, Edward, “Testing Password Strength Gives Policy Some Bite”. 23 Oct. 2002
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci858747,00.html

References

Gouvanus, Gary/King. Robert. “MCSE Windows 2000 Network Security Design”. Alameda: SYBEX Inc. 2000: 308

Anonymous. Maximum Windows 2000 Security. Sams Publishing. December 2001 URL: http://safari.oreilly.com (Safari Bookshelf)

Armstrong, Illena. ”Passwords Exposed.” SC Magazine. June 2003 (2003): 28

“Secure User Id/Password Software”. Information Security magazine (2003 Buyers’ Guide). December 2002: (55 – 56)

“Enforce Strong Network Password Creation”. Windows & .NET Magazine. April 2003: 20