Myths about Password Settings and Other Nonsense: *How Information Security Tortures Users in the Name of Security*

Eugene Schultz, Ph.D., CISSP, CISM
Chief Technology Officer
Emagined Security

[EugeneSchultz@emagined.com](mailto:EugeneSchultz@emagined.com)

ISSA-Bay Area
San Francisco, California
May 12, 2010
Users—tortured by our password policy (and other) requirements?
Outline

• Introduction
• Debunking myths about password settings
• Other usability problems during user interaction with security systems
• Cost/benefit considerations
• Conclusion
## CIS Windows XP password policy benchmark settings

### 2 Auditing and Account Policies

#### 2.1 Major Auditing and Account Policies Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>8 Characters</th>
<th>12 Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Password Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Password Age</td>
<td></td>
<td>90 Days</td>
</tr>
</tbody>
</table>

#### 2.2 Account Policy

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Password Age</td>
<td>1 day</td>
</tr>
<tr>
<td>Maximum Password Age</td>
<td>90 days</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>8 characters</td>
</tr>
<tr>
<td>Password Complexity</td>
<td>Enabled</td>
</tr>
<tr>
<td>Password History</td>
<td>24 passwords remembered</td>
</tr>
<tr>
<td>Store Passwords using</td>
<td>Disabled</td>
</tr>
<tr>
<td>Reversible Encryption</td>
<td></td>
</tr>
</tbody>
</table>
Other recommended password policy settings

- **Minimum Password Length**. A good value for this field is 8; certain Windows NT-based cracking tools try every combination of every permissible character to crack a password up to 8 characters in length (although it takes a very long time to crack an 8-character password in this manner). Choosing a password of 8 or more characters, therefore, is very advisable.

- **Uniqueness Value**. The uniqueness value represents how many new passwords a user must choose before being able to select one that was previously used. (Remember the formula for the uniqueness value is n+1.) A value of 3 or 4 is generally more than sufficient.

- **Lockout After**. A value of 3 for this field is a typical setting in business-critical processing environments. In other environments, a value of 5 is good. Remember that in Windows NT, the major concern is not the susceptibility to brute-force password-guessing attacks as much as the ability to perform an unauthorized logon because someone has obtained the password file and then cracked passwords.

- **Reset Count After**. A value of 480 minutes (8 hours) for this field is generally sufficient. A lower value could allow a patient attacker to wait for a while and then reinitiate attacks after the reset count has been reset. Note that choosing the Forever alternative here means that there will never be a reset period—the number of bad logons for an account will increment with each bad logon, ultimately until the bad logon limit is reached or until there is a successful logon to the account.

- **Lockout Duration**. A value of 8 hours (a reasonably long period of time) is generally sufficient to discourage hackers from continuing efforts to guess passwords for accounts. Note that the Forever option is also available here—Forever means that if an account is locked, an Administrator must reset the account before it can be used again.

- **Users Must Logon to Change Password**. This setting works exactly as advertised. Choosing it is useful for security in that it helps prevent the possibility that an unauthenticated user can change a password.

Note that when you set or modify Account Policy settings on a domain controller, you cause whatever setting you choose to be propagated to all other domain controllers. These settings then apply to all domain logons, choices of domain passwords, and so forth. If you have Windows NT Workstations that are domain clients, however, you need to set the Account Policy settings individually for each workstation, if you want to control security parameters related to local logons and passwords for each workstation. The domain parameters do not apply to local workstation logons. (Note, however, that in most environments, no accounts should be specified on the workstations beyond the normal Administrator and Guest accounts.)

I recommend the following values for the Account Policy settings:

- **Maximum Password Age**. Values between 30 to 90 days are generally appropriate. The more critical the environment in which Windows NT runs, the more appropriate a lower value is. Remember, however, that if you require users to change passwords too frequently, they will resort to desperate measures that will defeat your good intentions. For example, users who must change passwords every 30 days will choose a password such as “janepassword” during January, “febpassword” during February, “marpassword” during March, and so on.

- **Minimum Password Age**. The purpose of setting a minimum password age is to prevent users who have just changed their passwords from changing them right back again. This value should be low—perhaps 1 day—not so much for reasons related to security, but because requiring that users wait very long to change their passwords prevents users who learn that their password is weak from changing their passwords themselves. The only way they can change passwords quickly is to call a system administrator or help desk, thus potentially resulting in a backlog of help requests.
Passwords as authentication credentials

- The most common authentication-related user task is entering a password
- Provided that the interaction sequence for password entry is reasonably simple and intuitive, users can accomplish this task rapidly and easily
- The most frequent types of user errors include:
  - Data entry errors ("typo’s")
  - Entry of the password in the wrong field or area
  - Failure to remember one’s password
Today’s password cracking tools are incredibly efficient

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Passwords per Second</th>
<th>Time until Cracked</th>
</tr>
</thead>
<tbody>
<tr>
<td>LanMan</td>
<td>4,500,000</td>
<td>&lt; ½ minute</td>
</tr>
<tr>
<td>NTLM</td>
<td>4,250,000</td>
<td>&gt; 3 minutes</td>
</tr>
<tr>
<td>MD5</td>
<td>3,100,000</td>
<td>&gt; 4 minutes</td>
</tr>
<tr>
<td>SHA1</td>
<td>1,600,000</td>
<td>&gt; 9 minutes</td>
</tr>
<tr>
<td>SHA256</td>
<td>370,000</td>
<td>&gt; 41 minutes</td>
</tr>
</tbody>
</table>
Improving password security

• To remedy the problem of users choosing “way too easy-to-crack passwords,” an information security function can require measures such as
  - Restrictions on self-generated passwords
  - Passphrases
  - Computer-generated passwords
  - Password cracking
• BUT—is a so-called “stronger password” really stronger?
• AND—if stronger passwords are really stronger, are they worth the toll on the user community that they typically inflict?
Does password length really make a difference?

- Herley found that any length of Windows passwords greater than 8 characters resulted in only a very marginal increase in resistance to cracking

BUT

- The longer the password, the more difficult it was to remember
- Exception—today’s password cracking tools, as good as they are, do not even attempt to crack Windows passwords that are at least 15 characters long
• Vu, Proctor, Bhargav-Spantzel, Tai, Cook, and Schultz showed that creating passphrases yielded more crack-resistant passwords only when users were also told to embed a digit and special character into the passphrase
  - Embedding a digit and special character also resulted in less ability to remember passwords during both short-term and long-term recall
  - Embedding digits and special characters resulted in significantly more time needed to generate and recall passwords, and almost twice as many errors before they could recall the password
  - Results cast doubt on recommendations to use passphrases to improve password memorability and resistance to cracking
Does passphrase length really help? (1)

• In a study by Proctor, Vu and Schultz, all users generated and recalled passwords for three different accounts.
• To generate a password, half of randomly assigned users were instructed to create a sentence and then to combine the first letter of each word in the sentence to form a password using three rules for each sentence:
  - Must have at least six characters
  - Must make sense
  - The sentence (and password) for each account must be unique
• Remaining users were given two additional instructions:
  - The sentence (and password) must contain a special character (e.g., !, @, or #)
  - The sentence (and password) must contain a digit
Does passphrase length really help? (2)

- The 3-restrictions group took less time to generate a password, although there was no significant difference between the groups in the number of attempts needed to generate an acceptable password.
- It took twice as long for participants with 5 restrictions to login with a password than those with 3 restrictions.
- Forgetting was significantly higher for the 5 restriction group at both short- and long retention intervals.
- There was no significant difference between groups in terms of percentage of passwords cracked!
Do password filters really help? (1)

- In another experiment by Proctor, Vu and Schultz, seven password restrictions were imposed, namely that the password must:
  1. Be at least 6 characters long
  2. Contain at least one uppercase letter
  3. Contain at least one lowercase letter
  4. Contain at least one digit
  5. Contain a special character (e.g., ! or #)
  6. Be unique from the passwords generated for the other accounts
  7. Not contain the person’s username or any variant of it

- Users had to choose and remember passwords for 1, 3 or 5 accounts

- lc5 was used to crack passwords for four hours
• The lc5 program cracked 40% of the passwords from the 5-accounts group, 60% from the 3-accounts group, and 62% from the 1-account group
• There was no significant difference between groups in
  - Time to generate each password
  - Login time
• Forgetting was highest for the 5-accounts group
  - E.g., 69% of the 5-accounts group was unable to recall the password for at least one account, compared to 19% for the 3-accounts group, compared to 15% for the 1-account group
• Among other things, results show that imposing proactive password restrictions does not necessarily produce more crack-resistant passwords
  - Generated passwords had to satisfy seven password criteria, yet approximately half of passwords were cracked within four hours
Changing passwords frequently: Good or bad?

- Bunting found that “proactive interference” from *older* passwords creates difficulty for users trying to remember their *current* passwords.
- A survey of 3,050 Web users conducted by Rainbow Technologies found that 55% of the respondents admitted to writing down at least one password:
  - Eight percent of users indicated that they wrote down *all* of their passwords.
- SafeNet conducted a follow-up to the Rainbow Technologies survey:
  - Fifty percent of the respondents indicated having written down at least one password.
  - Ten percent said that they *always* wrote down their passwords.
  - About 50% of the respondents admitted that they often needed to have their passwords reset because they forgot them.
Users also have plenty of problems with other security methods!

![Smart Card](image)

**Smart Card International**

12345 54321 12345

L. SMITH 12.82

![BioCert](image)

![RSA SecurID](image)

Copywrite © 2010 Emagined Security - All rights reserved
By now you should be getting the picture!

Security engineers

The user

The CISO
User resistance to security measures

- Systems with poor usability design tend to cause elevated user resistance (e.g., Al-Ghatani & King, 1999)
- This resistance surfaces in various ways
  - Passive resistance
  - Negative verbal behavior
  - Reluctance to engage in tasks
  - Attention lapses
  - Behaviors that damage systems
  - Many others
- Lessening or eliminating user resistance through effective human usability design is an important goal
Signs of user resistance

- Using automated (e.g., “scripted”) login sequences or ssh agent to login to systems
- Using slight variations of a password every time a password must be changed
- Writing down passwords and then posting them in easy-to-find places
- Setting up and using methods of remote access that bypass firewalls
- When organizations implement strong authentication technology, only to scrap it shortly thereafter due to a plethora of complaints

“User resistance to security” is too often really “resistance to user-unfriendly security tasks!”
Pop quiz: Which of the following is most likely to compromise passwords?

A. A password cracking tool
B. Social engineering
C. A keystroke sniffer
D. Passwords written down on “yellow stickies”
And the answer is…

- C (with B often being used in conjunction with C)
- So why do we
  - Not invest more resources in mitigating the risk associated with C (and also B)?
  - Have so many A- and D-related requirements that cause so many problems for users?
Note that answer D was the worst answer—very few security breaches involve passwords that have been written on a slip of paper any more.

Users write down passwords when they cannot have confidence in remembering them.

- Due in large part to difficulty of remembering passwords when password rules are too stringent.

People keep cash in wallets and generally manage to avoid losing their wallets—why not passwords, too?
Do we really weigh costs versus benefits? (1)

• If only 10 percent of Wells Fargo’s approximately 48 million customers requires assistance from the bank’s help desk to reset their passwords, and if each reset were conservatively estimated to cost approximately $20, the total yearly cost would amount to $96 million
Do we really weigh costs versus benefits? (2)

- In a recent paper, Cormac Herley of Microsoft presents an economic analysis to calculate the value of user time
  - Approximately 200 million US adults go online daily
  - If these people were to earn twice the minimum wage, one minute of their time every day would total $16 billion every year
  - The cost-benefit implications for the cost of information security measures (especially password-related measures) are thus very apparent
Conclusion (1)

- In many ways, we torture users
- Many of our beliefs and practices concerning passwords clash with the results of controlled, empirical research
- It is also extremely unlikely that many commonly used password policy settings produce anything near to a favorable cost-to-benefit ratio
- Why not use one-time passwords instead?
- Why not include usability testing as part of the security product evaluation process?
• Remember what Einstein said about insanity!
Questions?

Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
USA
+1 (650) 593-9829
eugeneschultz@emagined.com
Web: www.emagined.com
Blog: blog.emagined.com
Dashboard: dashboard.emagined.com

For a PDF copy of these slides send email to:
seminar@emagined.com