Why?
Passwords Can Be Better

How?
1. Identify Patterns
2. Measure Pattern Use
3. Find Structural Solutions
4. Estimate Time to Execute
5. The Policy to Strengthen

Results
- Accurate
- Informative
- Simple
- Powerful

Next
OWASP Passfault

Why?
Passwords Can Be Better

How?
1. Identify Patterns
2. Measure Pattern Occurrence
3. Find Weakest Component
4. Estimate Time to Crack
5. Tie Policy to Strength

Results
- Accurate
- Informative
- Simple
- Powerful

Next
Why?

Passwords Can Be Better

Policies don't measure password strength

They just force compliance with bad advice.

You can follow the advice and still make weak passwords.

Password Policies Stink!

Of People and Passwords:
- "Successfully creating a password is significantly more difficult under stricter password policies."
- Password length was the only significant predictor of password strength.

- Kamvar et al., Carnegie Mellon & NIST
passwords are the weakest link

About 71,100 results (0.03 seconds)

Past year

Password Security Remains the Weakest Link Even After Big Data ...
Jun 19, 2011 - Organizations should be implementing several measures to prevent cyber-attackers from stealing sensitive, confidential data.

ZoneAlarm Survey Reveals That Passwords are the Weakest Link in ...
blog.zonealarm.com/.../zonealarm-survey-reveals-that-passwords-are...
Dec 20, 2010 - ZoneAlarm Survey Reveals That Passwords are the Weakest Link in Online Security. By the ZoneAlarm Team. We've got new and interesting survey results ...

Passwords are the weakest link in online security
www.net-security.org/secworld.php?id=10353
Dec 22, 2010 - Passwords are the weakest link in online security. Posted on 22 December 2010. Bookmark and Share. A ZoneAlarm survey showed that 79% of consumers use ...

Passwords Are The Weakest Link In Online Security - Slashdot
tech.slashdot.org/.../passwords-are-the-weakest-link-in-online-securit...
Dec 22, 2010 - Orome1 writes "It's not surprising to find that 79% of consumers use risky password construction practices, such as including personal information and words.

Sony's Weakest Link Hijack | OpenID
openid.net/2011/10/13/sony's-weakest-link-hijack/
6 days ago - These attacks are referred to as "weakest link hijackings" because the hackers attack websites with the weakest security, and then collect user passwords. ...

Cyber Experts Point to Computer Passwords as Weakest Link in ...
www.defenceiq.com › Defence Technology › Articles
Policies don't measure password strength

They test for compliance with good advice

You can follow the advice, and still make weak passwords
Password Policies Stink!

Of People and Passwords:

- "successfully creating a password is significantly more difficult under stricter password policies"
- Password length was the only significant predictor of password strength

- Komanduri et. al., Carnegie Mellon & NIST
Examples

#1 Eagles
- Special Chars
- Number
- Upper and Lower
- Eight Characters
- But still weak

qwerQWER1234!@#$
- Long! Looks strong
- Passes any policy
- But very guessable

xkcd
#1 Eagles

- Special Chars
- Number
- Upper and Lower
- Eight Characters
- But still weak
qwerQWER1234!@#$

- Long! Looks strong
- Passes any policy
- But very guessable
xkcd

困难的密码：

1. 28位熵
2. 按钮的难度：简单
3. 难以记住：难以记住

正确马电池大头针

- 44位熵
- 难度猜测：困难
- 难以记忆：你已经记得它了

20年不懈的努力，我们成功地训练了每个人使用对人类来说难记但对计算机来说易猜的密码。
Are passwords policies in your organization effective?

"No"

*Why do companies create yearly training for passwords if their password policies are working?
Why Not Use Password Strength?

How do you measure password strength?
How?

1. Identify Patterns
   - In the password
     - English Word
     - Leet Speak
     - Dates
     - Hybrid:
     - Backwards Word
     - Random Mix of Characters

2. Measure Pattern Size
   - How many passwords fit in the pattern
     - More Diverse
     - More Meaningful
     - Like a needle in a haystack
     - How big is the haystack?

3. Find Weakest Combination
   - Combined size of the patterns is the measurement of strength.
   - Worst Case Scenario:
     - Hacker knows what patterns you used.

4. Estimate Time to Crack
   - Represents current hardware
   - Communicates the risk
   - Enables self-training

5. Tie Policy to Strength
   - Set the policy to an acceptable level of risk
     - Simpler configuration
     - Better manage risk
Identify Patterns

In the password

- Random Cyrillic Characters
- English Word
- Word with Special Character Substitution
- Spanish Word
- Backwards Word
- Leet Speak
- Slang Words
- City Names
- Dates
- Misspelled Word
- Word with Special Character Inserted
- Diagonal Keyboard Sequence
- Random Latin Characters
Measure Pattern Size

2

How many passwords fit in the Pattern
- More Accurate
- More Meaningful

Like a needle in a hay stack.
How big is the hay stack*

*Gibson Research Center, "Password Haystacks"
Obscurity Vs. Security

Password Pattern Size
• favors secure patterns
• Not obscure patterns.

Backwards Word = Word
Find Weakest Combination

Combined size of the patterns is the measurement of strength.

Worst Case Scenario:
- Hacker knows what patterns you used.
Estimate Time to Crack

4

- Represents current hardware
- Communicates the risk
- Enables self-training
Tie Policy to Strength

5

Set the policy to an acceptable level of risk

- Simpler configuration
- Better manage risk
Results

**Accurate**
Identifies more weak passwords, yet allows strong passwords that don’t pass traditional policies

**Informative**
Provides detailed analysis of the password so users quickly learn how to create strong passwords without training

**Simple**
Communicates the risk of poor passwords with the “time to crack”

**Powerful**
Empowers administrators to know and control the strength of passwords for the organization

---

Current Password Advice
- It’s not wrong...
- It’s not exactly right

Length is King
- 12 random characters
- 2 random words
- 2 misspelled words
Accurate
Identifies more weak passwords, yet allows strong passwords that don't pass traditional policies

Informative
Provides detailed analysis of the password, learn how to create strong passwords
Accurate
Identifies more weak passwords, yet allows strong passwords that don't pass traditional policies.

Informative
Provides detailed analysis of the password so users quickly learn how to create strong passwords without training.

Simple
Communicates the risk of poor passwords with "time to crack".

Powerful
Pass traditional policies

Formative

Uses detailed analysis of the password so users quickly know to create strong passwords without training

Simple

Communicates the risk of poor passwords with the "time to crack"

Powerful

Empowers administrators to know and the strength of passwords for the organization
People

Communicates the risk of poor passwords with the
no crack"

Powerful

Empowers administrators to know and control the
strength of passwords for the organization
Current Password Advice

- is not wrong...
- but it's not exactly right
- it encourages one type of pattern

Length is King

- 12 random characters
- 4 random words
- 2 misspelled words
Next
Java Library

- Beta
- Stable
  - 3500 lines of Code
  - 3000 lines of Unit Tests
Improvements

More Patterns

Real-time analysis

More Meaningful Dictionaries
Web Projects

Applet
- Alpha
- Returns JSON
- Password never leaves the Browser

JSON Service
- Alpha
- Easy Platform Independence
- Servlet
- Google AppEngine

jQuery Plugin
- Beta
- Load from the menu path
- Use Equal or jQuery.js
JSON Service

- Alpha
- Easy Platform Independence
- Servlet
- Google App Engine

https://passfault.appspot.com
Applet

- Alpha
- Returns JSON
- Password never leaves the Browser
JQuery Plugin

- Future
- Derived from the Demo Page
- Use Applet or JSON service
Possible Projects

C
C++
JavaScript
JavaScript with GWT
.NET

Linux
Windows
Next
OWASP Passfault

Why?
Passwords Can Be Better

How?
1. Identify Patterns
2. Measure Pattern Use
3. Find Weaknesses
4. Reduce Time to Crack
5. Tie Policy to Strength

Results
Accurate
Informative
Simple
Powerful

Next