The Big (Password) Picture

Per Thorsheim

Passwords '12
Authentication methods

- Something you _____
- Something you _____
- Something you _____

- Know / forgot
- Forgot at home
  - Battery’s dead
  - App crashes constantly
  - Too expensive
- Watch
  - Mythbusters
  - Minority Report
- Not supported
Stories you would (not) believe
From the archives
Discovered by @CrackMeIfYouCan (Korelogic)

June 5-6th, 2012

Observations
- Unsalted SHA-1
- No CSO
- No (IRT) response
LinkedIn: Pass Phrases

Over 200 LinkedIn passwords we cracked were over 20 characters long. So how did we crack them? Quotes, Bible verses, band names, song titles and lyrics, etc. all make very bad passwords. If the phrase you have in mind exists anywhere in writing, it’s probably in someone’s wordlist and can be cracked with a rudimentary dictionary attack.

Bad Pass Phrases Found on LinkedIn

- There is no fate but what we make
- You’ll never walk alone
- The light shines in the darkness
- In the beginning was the Word
- Truth sets you free
- Jesus chrysler supercar
- Save the cheerleader, save the world

Other used pass phrases:
- Look at my horse, my horse is amazing from genesis to revelations
- Happy healthy wealthy and wise give me liberty or give me death
- Chi va piano va sano e va lentano
- East of the sun west of the moon
- Every cloud has a silver lining
- Yo no quiero volver me tan loco
- Elvis has left the building
- Big trouble in little china
- What the Puck is happening
- Forever blowing bubbles
- Work smarter, not harder
- You are my sunshine!
- I need a vacation
- You get what you give
- Cisscross appleauce
- Everything is destined

LinkedIn: Pop Colors

The leaked list containing over 5.8 million password hashes from LinkedIn is now over 90% cracked. These are the top colors represented in users’ passwords.

Top Colors Used in LinkedIn Passwords

- Blue: 998
- Green: 665
- Red: 455
- Orange: 417
- Purple: 398
- Pink: 304
- Black: 281
- White: 156
- Gray: 146

* Numbers = unique user passwords

- Can this be connected to LinkedIn?
PINs from the real world

(Somewhere not important)  Stansted airport, London, UK
Heatmapping PINs

RockYou / iPhone data fra http://www.cl.cam.ac.uk/~jcb82/ (Joseph Bonneau ++, University of Cambridge)

Try the @KluZZ version at www.radical.org/pinmap (clientside!)
How did you...?

Social engineering #FTW
(Abusing) Password History
May be bad for you.
Passphrases #2

Multi-word passphrases not all that secure, says Cambridge University

Join thousands of others, and sign up for Naked Security’s newsletter
you@example.com

by Lisa Vaas on March 19, 2012 | 23 comments
FILED UNDER: Featured, Privacy, Vulnerability

Think that a passphrase of multiple, random dictionary words is as unguessable as long strings of gibberish, but easier to remember? Research from the Computer Laboratory at the University of Cambridge suggests that this might not be so.

While passphrases using dictionary words may not be as vulnerable as individual passwords, they may still be cracked by dictionary attacks, the research found.

Security researcher Joseph Bonneau reports, in a recent paper written with Ekaterina Shutova, that his team studied the problem by turning not to the theoretical space of choices but rather the real-life passphrases that people actually string together.

To find such a selection of passphrases, his team used data crawled from the now-defunct Amazon PayPhrase system, introduced last year for US users only.

Linguistic properties of multi-word passphrases

Joseph Bonneau, Ekaterina Shutova

Computer Laboratory
University of Cambridge
{jcb82,es407}@cl.cam.ac.uk

Abstract. We examine patterns of human choice in a passphrase-based authentication system deployed by Amazon, a large online merchant. We tested the availability of a large corpus of over 100,000 possible phrases at Amazon’s registration page, which prohibits using any phrase already registered by another user. A number of large, readily-available lists such as movie and book titles prove effective in guessing attacks, suggesting that passphrases are vulnerable to dictionary attacks like all schemes involving human choice. Extending our analysis with natural language phrases extracted from linguistic corpora, we find that phrase selection is far from random, with users strongly preferring simple noun bigrams which are common in natural language. The distribution of chosen passphrases is less skewed than the distribution of bigrams in English text, indicating that some users have attempted to choose phrases randomly. Still, the distribution of bigrams in natural language is not nearly random enough to resist offline guessing, nor are longer three- or four-word phrases for which we see rapidly diminishing returns.
### Why passwords really suck


First: It's a comic. It's meant to be funny. Why the fuck are we over analyzing this?

Second: People don't use shitty passwords because they can't remember good passwords. People use shitty passwords because they don't care. They think no one will ever crack THEIR passwords, or because they're crap typists.

Therefore, any content below can only be pedantic.
## Password Policy Insanity

<table>
<thead>
<tr>
<th>Anbefaling</th>
<th>NorSIS</th>
<th>Nettvett</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bruk kombinasjon av tall og bokstaver</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Passordet må være lett å huske</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Passordet må være lett å huske, men vanskelig for andre å gjette</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Passordet bør bestå av en kombinasjon av små og store bokstaver, tall og spesialtegn</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Vær forsiktig med å bruke det samme passordet på flere tjenester</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Unngå bruk av ord som finnes i ordlister eller knyttet til personlig informasjon</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Passordet bør ikke inneholde bokstavene Æ, Ø eller Å</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Tips: Bruk L33T språk (bokstav &lt;-&gt; tall erstatninger)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Minstelengde</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Bruk store og små bokstaver</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Tips: forkortede setninger (5rEf7M)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Baser ikke passord eller PIN-koder på personlig informasjon</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Unngå ord som finnes i ordbøker ( gjelder alle språk)</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Unngå bokstavkombinasjoner som ligner på ord</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Passord bør være så langt som mulig, og minst 8 tegn</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Benytt ulike passord for ulike tilganger</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Bytt passord med jevne mellomrom</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Bruk passfraser (setninger)</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Oppgi aldri passord eller koder til noen – selv ikke banken</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Passord skal være på minimum åtte tegn, og skal inneholde både bokstaver, tall og eventuelt spesialtegn</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Alle standard brukeridenter og passord fra leverandører skal endres før produktet settes i produksjon</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>
Headshot password profiling

Winner: female redheads

Losers: male «Unix Guru»
Evolution of Practices

Old Practice

Bad Practice

Current Practice

Good Practice

Best Practice

Next Practice?
Best practice = «Be Compliant»

- **PCI-DSS password requirements:**
  - Minlen 7
  - Alphanumeric
  - Change every 90 days
  - Auditors not willing to discuss tradeoffs

- «We’re compliant» equals CRAP?
Applied Risk Analysis

(You *really* should crack your passwords!)
Profiling People/Passwords

- Specialforces.com
  - Guns & ammo, male audience, «male» passwords

- Hemmelig.com (no sex/escort forum)
  - Male/female usernames & passwords
  - Heavy use of sexual words, foul language

- Can we improve this sort of «profiling»?
System Generated Passwords

- Helpdesk = biggest threat to password security
  - Involves humans
- The Password Meta Policy (demo)
  - Blogpost + code from @KluZ2
    - http://securitynirvana.blogspot.no/2010/02/password-meta-policy.html
Guarding your usernames

What we need:
- URL
- Username
- Password

Easy to get:
- «Hi, I forgot...»
- «Hi, I forgot...»
- Uhm....
What exactly is a «passphrase»?

- No unified definition (?)
  - Do we need one?
    - It helps us understand what we are searching for...
  - Can it be done?
    - Simplified chinese anyone?
Windows Picture Password
Nice idea, high usability, but?
UPEK / Windows 8

- Elcomsoft discovers Upek stores encrypted passwords
- Adam Caudill / Brandon Wilson does RE & PoC
- Passcape comment to my blog:

Anonymous October 2, 2012 3:35 PM

Windows 8 picture password (as well as pin) is just a toy with lack of security. Here's explained why: http://www.passcape.com/index.php?section=blog&cmd=details&id=27
About @mat

(Basically it scared me shitless)
Some ideas:

- Password generators vs Checkers
- Alexa top 100: maxlen & Unicode 6 support?
- People/site/service password profiling
- Rate-limiting algorithms – also physical
- Cross-site «magic question» analysis
- RL Win8 picture password patterns
My big (picture) password

A few personal words at the end.
Want more work?

Per Thorsheim
securitynirvana.blogspot.com
@thorsheim