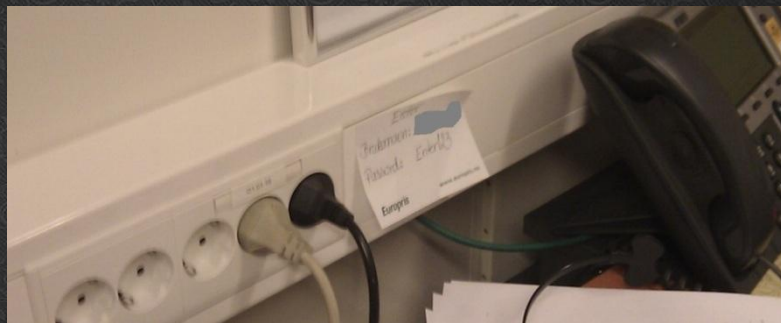
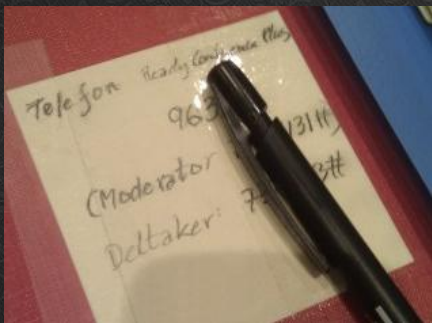


# The Big (Password) Picture

Per Thorsheim  
Passwords<sup>12</sup>

# 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

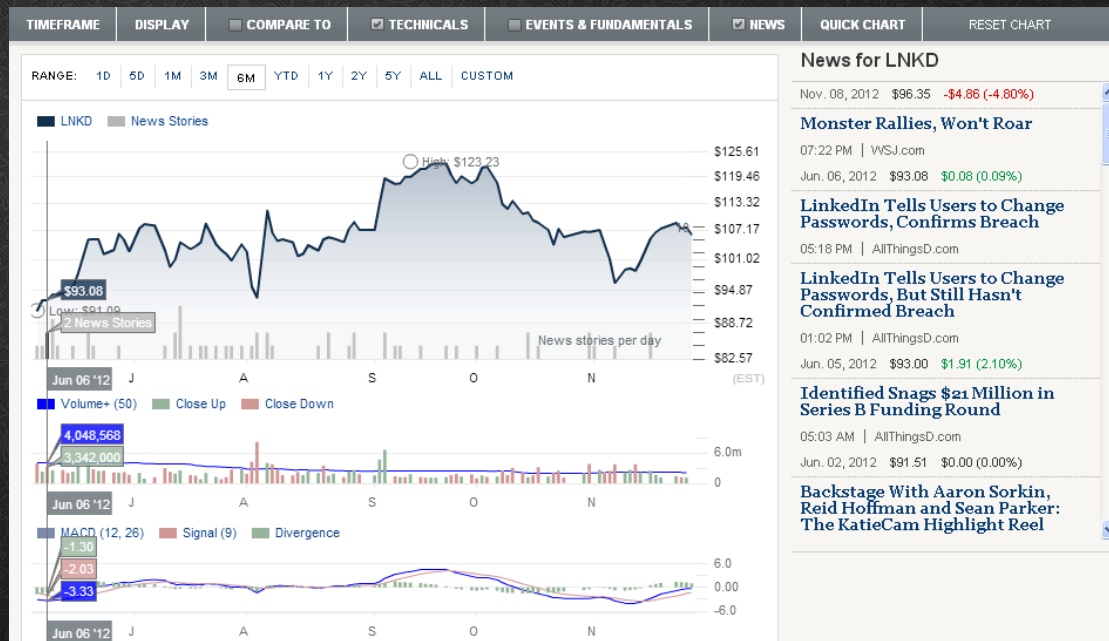


Stories you would (not) believe

From the archives



- Discovered by @CrackMelfYouCan (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



#### 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 lontano  
east of the sun west of the moon  
every cloud has a silver line  
yo no quiero volver me tan loco  
elvis has left the building

big trouble in little china  
what the f\*ck is happening  
forever blowing bubbles  
work smarter not harder  
you are my sunshine <3  
I need a vacation  
you get what you give  
crisscross applesauce  
everything is destined

Information & statistics by:  
Per Thornheim &  
Jeremi Goosney (@jggoosney)

Infographic & ideas by:  
Tom Kristian Tønnesen  
**EVRY**

## 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



\* Numbers = unique user passwords



= Can this be connected to linkedin?

Information & statistics by:  
Per Thornheim &  
Jeremi Goosney (@jggoosney)

Infographic & ideas by:  
Tom Kristian Tønnesen  
**EVRY**

# Security Usability

iPad

19:51

71 %

CPH Advantage

Avbryt

**CPH Wireless Internet**

Københavns Lufthavn **CPH**

[Home](#) [About CPH Advantage](#) [Help & Support](#) [Departures](#)

**GET ONLINE** ↓  
SELECT YOUR METHOD BELOW

**LOG ON TO FREE WIFI WITH CPH ADVANTAGE**

E-MAIL ADDRESS:

PASSWORD:

LOG IN

Lost your password?

**SIGN UP FOR A MEMBERSHIP  
AND GET FREE WI-FI**

We may not provide you with a mobile office - but it's close. We're here to spoil you like never before.

[Sign up now](#)

**LOG ON THROUGH LOCAL PARTNER**

PARTNER:

USER NAME:

PASSWORD:

Local

☐ I agree with the terms

LOG IN

boingo  
TRUSTEE  
Wilsons  
Lone  
Tideline  
TV-BÅNENE  
vodafone  
2  
3

**PAID ACCESS**

Pay online and surf instantly



GO TO PAYMENT

# PINs from the real world

(Somewhere not important)

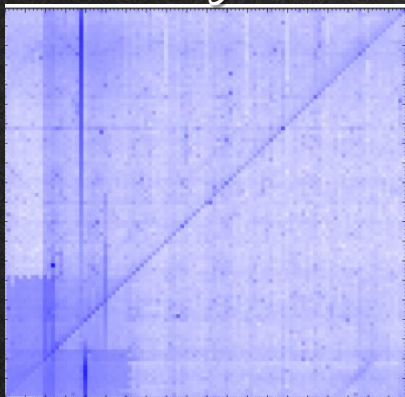


Stansted airport, London, UK

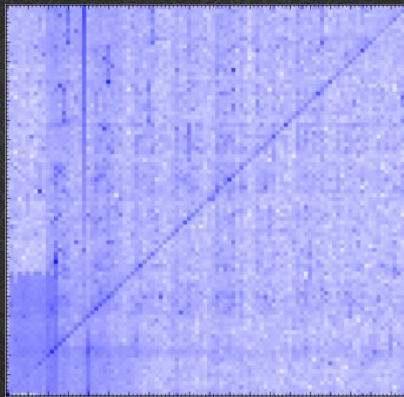


# Heatmapping PINs

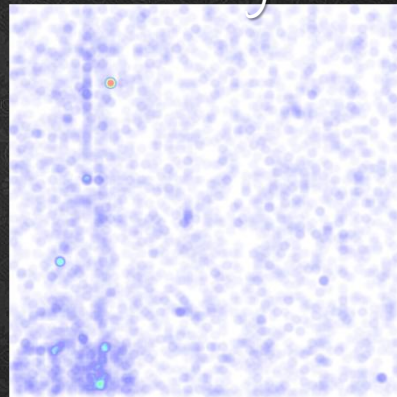
Rockyou



iPhone



Physical Access  
Control System



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](http://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

[Don't show me this again](#)

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?



Computer Laboratory

[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.

# Passphrases #2

<p>□□□□□□□□□□□□□□</p> <p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor&amp;3</p> <p>CAPS? □ COMMON SUBSTITUTIONS □□ NUMERAL □□ PUNCTUATION □□□</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONE OF A FEW COMMON FORMATS.)</p>	<p>~ 28 BITS OF ENTROPY</p> <p>□□□□□□□□ □ □□□□□□□□ □ □□□ □□□ □□□□ □</p> <p><math>2^{28} = 3 \text{ DAYS AT}</math> 1000 GUESSES/SEC</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: <b>EASY</b></p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p>  <p>DIFFICULTY TO REMEMBER: <b>HARD</b></p>
<p>correct horse battery staple</p> <p>□□□□□ □□□□□ □□□□□ □□□□□ □□□□□ □□□□□ □□□□□ □□□□□</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~ 44 BITS OF ENTROPY</p> <p>□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□</p> <p><math>2^{44} = 550 \text{ YEARS AT}</math> 1000 GUESSES/SEC</p> <p>DIFFICULTY TO GUESS: <b>HARD</b></p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p>  <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED  
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS  
TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Tuesday, August 16, 2011

## Why passwords really suck

RE: <http://securitynirvana.blogspot.com/2011/08/xkcd-936-discussion-continues.html?m=1>

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

Anbefaling	NorSIS	Nettvett
Bruk kombinasjon av tall og bokstaver		Y
Passordet må være lett å huske		Y
Passordet må være lett å huske, men vanskelig for andre å gjette		Y
Passordet bør bestå av en kombinasjon av små og store bokstaver, tall og spesialtegn		Y
Vær forsiktig med å bruke det samme passordet på flere tjenester		Y
Unngå bruk av ord som finnes i ordlister eller knyttet til personlig informasjon		Y
Passordet bør ikke inneholde bokstavene Æ, Ø eller Å		Y
Tips: Bruk L33T språk (bokstav <-> tall erstatninger)		Y
Minstelengde	8	8
Bruk store og små bokstaver	Y	Y
Tips: forkortede setninger (5rEfd7M)	Y	Y
Baser ikke passord eller PIN-koder på personlig informasjon	Y	
Unngå ord som finnes i ordbøker (gjelder alle språk)	Y	
Unngå bokstavkombinasjoner som ligner på ord	Y	
Passord bør være så langt som mulig, og minst 8 tegn	Y	
Benytt ulike passord for ulike tilganger	Y	
Bytt passord med jevne mellomrom	Y	
Bruk passfraser (setninger)	Y	
Oppgi aldri passord eller koder til noen – selv ikke banken	Y	
Passord skal være på minimum åtte tegn, og skal inneholde både bokstaver, tall og eventuelt spesialtegn	Y	
Alle standard brukeridenter og passord fra leverandører skal endres før produktet settes i produksjon	Y	

# Headshot password profiling

Winner: female redheads



Losers: male «Unix Guru»



# Evolution of Practices



# 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 @KluZZ
    - <http://securitynirvana.blogspot.no/2010/02/password-meta-policy.html>

# Guarding your usernames

What we need:

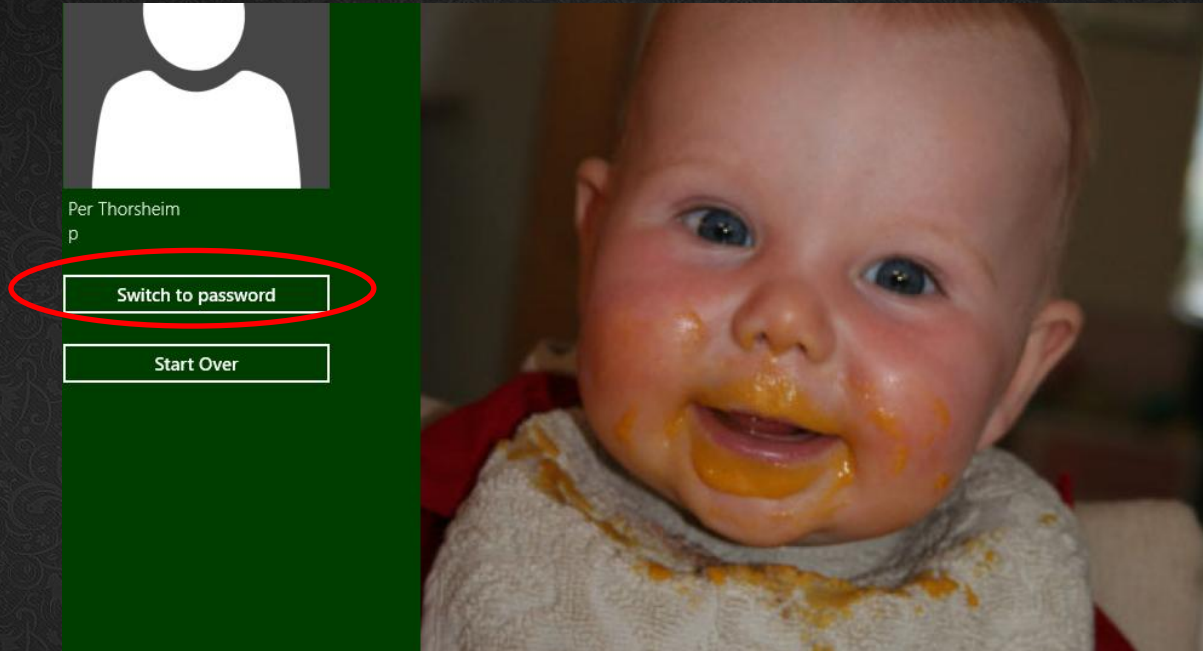
- URL
- Username
- Password

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](http://securitynirvana.blogspot.com)



@thorsheim