What means weak password?

passwords for: accounts, online services, credit/banking cards, ............

Test it:

- how many passwords do you keep? 2-3...oh wait: 5-6...hm...15-20?
- how random and how long are they? Not random, short
- are some of them equal or similar? Sure, of course
- where do you keep or store them? On a piece of paper, Post-it notes Files (not encrypted) ...

Diagnose: you have a problem with weak passwords
The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs

S. Flach, MPIPKS Dresden

work done jointly with T. Laptyeva and K. Kladko: arXiv:1103.6219

• goal and basic idea
• what is the problem?
• a bit on encrypting and hacking
• and what are CAPTCHAs?
• implementation of basic idea
• instead of conclusions: reactions from a virtual world
goal:

develop a scheme which allows you to
• memorize a short weak password
• have protection of a long strong password

basic idea:
• split a long strong password into two parts: short password SP + strong key SK
• memorize SP only
• encrypt SK with SP using CAPTCHA and phase transition
What is the problem with weak passwords?

- your data are hacked, stolen, destroyed
- companies make losses on identity fraud (total annual cost 2006 in US about $55 billion)

Consequence: You are forced to memorize passwords which are:

- unguessable
- all different
- never written down

These requests become unreasonable and unmanageable
A bit on data encrypting and hacking

Symmetric data encryption:

One password
Plaintext is correlated
Cipher Text is random-like

Hacking:
- the hacker has all information except the password
- brute force method tries all passwords
- looks for correlations in decrypted candidate files
And what are CAPTCHAs?
And what are CAPTCHAs?

**CAPTCHA:**

_Completely Automated Public Turing test to tell Computers and Humans Apart_
It takes about 1-10 seconds to perform a computer based CAPTCHA recognition.
Implementation of basic idea

\[ \mathcal{H} = \sum_{i,j=1}^{N} \left( \frac{1}{2} p_{ij}^2 - \frac{1}{2} u_{ij}^2 + \frac{1}{4} u_{ij}^4 + \mathcal{F}_{ij} \right) \]

\[ \mathcal{F}_{ij} = \sum_{k=\pm 1} \frac{1}{2} \left[ (u_{i+k,j} - u_{ij})^2 + (u_{i,j+k} - u_{ij})^2 \right] \]
Phase transition

Order parameter

\[ M = \frac{1}{N^2} \left| \sum_{i,j} \text{sign}(u_{i,j}) \right| \]

temperature: here simply energy density

operational point: close to transition
Phase transition

order parameter

\[ M = \frac{1}{N^2} \left| \sum_{i,j} \text{sign}(u_{i,j}) \right| \]

temperature: here simply energy density

operational point: close to transition
Maximum return time and chaos

- consider an initial state image at time $t=200$
- define a suitable error function for blurring images
- use symplectic time reversible integrator (Verlet or leap-frog)
- stop at time $t=T$ and return to $t=200$
- due to roundoff errors and chaos we do not return exactly
- measure blurring
- measure maximum $T_m$ up to which recovering is possible
- measure largest Lyapunov coefficient: proportional to $T_m$
Imprint the strong key SK
Evolve forward in time up to the edge of chaos

Store the final state (coordinates, momenta) in two files:
F1 contains signs and all significant digits
F2 contains the rest
Encrypt F2 using short password!
Can we return back?

Decrypt F2 using short password
Glue F1 and F2 together to obtain the correct final dynamical state
Integrate backwards in time
Read the strong key SK!
Detune one oscillator coordinate by 0.000001
Store the final state (coordinates, momenta) in two files:
F1 contains signs and all significant digits
F2 contains the rest
Encrypt F2 using short password!
Fast hacking of strong key impossible:

• via correlations – they are always large

• CAPTCHA recognition – too long even with SP
Reactions of a virtual world

Scientists Develop New Method to Improve Passwords

3 submitted 1 day ago by cryptokey
10 comments share

all 10 comments

sorted by: best

[-] sapiophile 0 points 1 day ago
Brilliant method, and very practical.
Original arxiv paper here. (why link to the slashdot page?)
permalink

[-] skolor 1 point 21 hours ago
I'd say this adds little practical security over simply using a unique salt for each user. We live in a day and age where you can get CAPTCHAs cracked by a human in a developing country for under a penny. Some quick googling turned up a result offering 50,000 CAPTCHAs cracked for $300.
While it is a cost, it isn't necessarily insurmountable, it simply adds a fairly trivial additional cost onto the cracking process.
permalink

[-] phyzone 2 points 1 day ago
So, as I understand this... the user memorizes half of the password, and when they go to decrypt, a CAPTCHA is produced showing the rest of the password. Automated attacks can't verify that a guessed first-half password is correct without powerful OCR.
(What did 'scientists' have to do with this, though? I see no scientific method or exploration of the laws of nature.)
permalink

[-] electronics-engineer 2 points 1 day ago
Happens all the time. Engineers design things, Scientists get the credit. Occasionally, just for variety, the media gives credit to technicians for work done by engineers.
permalink parent
Reactions of a virtual world

The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs (arxiv.org)

73 submitted 1 day ago by addah
85 comments share

A friend of mine has a neat solution (for the user, not website owner) called RndPhrase (Firefox and Chrome extension). Instead of sending the actual password that you typed into form field to the website, it sends a password generated uniquely for that domain. Which can be arbitrarily large, making it very hard to guess.

If a database of passwords is leaked, you only have to change your password at that site, even though you locally use the same password for many websites. And you can use a weak password locally, it will be transformed into a hard to guess password for you.

Look at his own description here: https://github.com/birch/rndphrase/wiki/

Seems neat, but there are many similar utilities. See http://supergenpass.com/ which has been around at least a decade.

Personally, I prefer an encrypted password database like KeePass. Combine it with Dropbox and you have a free, secure password system that is also accessible from multiple computers.

73 points (69% like it)
123 up votes 56 down votes
shortlink: reddit.it/ghne5

programming
4 frontpage 338,410 readers

A reddit for discussion and news about computer programming

- Some seem to think this reddit is for "links that programmers might find interesting or funny". No. It's for programming links. Programming. Programming.
- Just because it has a computer in it doesn't make it programming
- /r/programming is not a place to ask for help, run polls, rant, demo your app (unless your demo includes code or architecture discussion), or otherwise use as a captive audience. For that try /r/learnprogramming or StackOverflow.

And if you're an all-star hacker (or even just beginning) why not join the discussion at
Reactions of a virtual world
Reactions of a virtual world
Reactions of a virtual world
Reactions of a virtual world

Featured on more than 180 web sites including rambler.ru, mail.ru, yandex.ru etc
Pikachu

Not to be confused with Pikachu or Pika.

Pikachu (ピカチュウ, Pikachu) is one of the species of Pokémon creatures from the Pokémon media franchise—a collection of video games, anime, manga, books, trading cards, and other media created by Satoshi Tajiri. As do all Pokémon, Pikachu fight other Pokémon in battles central to the anime, manga, and games of the series. Pikachu is among the most recognizable Pokémon, largely because a Pikachu is a central character in the Pokémon anime series. Pikachu is widely considered the most popular Pokémon, & is regarded as the official mascot of the Pokémon franchise, and has become an icon of Japanese culture in recent years.

Within the world of the Pokémon franchise, Pikachu are often found in houses, forests, plains, and occasionally near mountains, islands, and electrical sources (such as power plants), on most continents throughout the fictional world. As an Electric-type Pokémon, Pikachu can store electricity in its cheeks and release it in lightning-based attacks.