



What means weak password?



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

Test it:Typical answer:• 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



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 unmanagable

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?



Alan

And what are CAPTCHAs?





CAPTCHA:

Submit

Completely Automated Public Turing test to tell Computers and Humans Apart

Security Check

Enter both words below, separated by a space. Can't read the words below? Try different words or an audio captcha.









It takes about 1-10 seconds to perform a computer based CAPTCHA recognition

| 2) Cheapest CAPTCHA bypass service — Death by Captcha - Mozilla Firefox | | |
|--|---|--------|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp | | |
| C X 🟠 http://www.deathbycaptcha.com/user/login | 😭 👻 Google | م |
| 🧟 Most Visited 🏶 Getting Started 🔜 Latest Headlines | | |
| Cheapest CAPTCHA bypass service — ÷ | | |
| DEATHEY CAPTCHA MyAdTo the smart wa | ols ay to promote | |
| FASTEST DISCOUNT CAPTCHA SOLVERS | of the Month 🔺 | F |
| Home F.A.Q. APIS Order CAPTCHAS Featured Software Contact Us | | |
| CAPTCHA Bypass done right | Last few minutes' average solving time: 15 sec 5 minutes ago: 15 sec 15 minutes ago: 14 sec | _ |
| Don't let CAPTCHAs get in the way of your marketing goals! With Death by Captcha, you can bypass any CAPTCHA from any website. All you need to do is implement our API, pass us your CAPTCHAs and we'll return the text. It's that easy! | (updated every minute) | |
| If you still don't have any marketing tools, check our Featured Software page to find the best marketing software of the web. | Create a FREE account | |
| Death by Captcha Offers: | Log In | |
| An incredible low price of \$1.39 for 1000 decoded CAPTCHAs. A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA decoders. An average response time of 17 seconds, with an average accuracy rate of 85%. And you always only pay for correctly solved CAPTCHA. | n Password: Forgot your password? | |
| | Submit | |
| Supported API clients | Undatos | |
| C PHP Python NET C# & VB Java Perl Autolt3 iMacros | Mar 16: API Client version 4 released for NET C | |
| Done | | zotero |
| | | 19:21 |

07.04.2011

(500

Implementation of basic idea

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



Phase transition

order parameter
$$M = rac{1}{N^2} \left| \sum_{ij} \operatorname{sign}(u_{ij}) \right|$$

temperature: here simply energy density

opertional point: close to transition





Phase transition

order parameter
$$M = rac{1}{N^2} \left| \sum_{ij} \operatorname{sign}(u_{ij}) \right|$$

temperature: here simply energy density

opertional 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 Tm up to which recovering is possible
- measure largest Lyapunov coefficient: proportional to Tm

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



The scheme in a nutshell



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

| Scientists Develop New Method to Improve Passwords : crypto - Mozilla Firefox | | o x |
|---|--|--------------------|
| ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp | | |
| C X 🏠 🎯 http://www.reddit.com/r/crypto/comments/ghlu3/scientists_develop_new_method_to_improve_passwords/ | 🗟 🔂 🔻 🚼 🕶 Google | م |
| Most Visited 🏶 Getting Started 🔊 Latest Headlines | | |
| 🗋 Sergej's World: web page of Sergej 🛪 🧒 Scientists Develop New Method t 🗙 🔸 | | [|
| LL - RANDOM PICS - REDDIT.COM - FUNNY - POLITICS - GAMING - ASKREDDIT - WORLDNEWS - VIDEOS - IAMA - TODAVILEARNED - FFFFFFFUUUUUUUUUUUUU - TREES | - ATHEISM - WTF - STARCRAFT - ADVICEANIN | MORE » |
| CRYPTO comments related | want to join? register in seconds | : English |
| Scientists Develop New Method to Improve Passwords (clashdaters) | 1 1 19 | |
| 3 submitted 1 day ago by cryptokey | search reddit | : |
| 10 comments share | this post was submitted on 03 Apr 2011 | |
| all 10 comments | 3 nainta (C20(Elec it) | |
| sorted by: best | J points (63% like it) | |
| 🔶 [-] sapiophile 8 points 1 day ago | shortlink: redd.it/ghlu3 | |
| Frilliant method, and very practical. | | |
| Original arxiv paper here. (why link to the slashdot page?) | | |
| permalink | | |
| F [-] skolor 1 point 21 hours ago | remember me recover password | login |
| 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. | crypto | |
| While it is a cost, it isn't nearly insurmountable, it simply adds a fairly trivial additional cost onto the cracking | + frontpage 1,840 readers | |
| process. | This subreddit is intended for links and | |
| permalink | practice of <i>strong</i> cryptography, which live | ves at |
| [-] phyzome 2 points 1 day ago* 2- or London the descent of the uncertainty helf of the necessary of and when they are to descent of CADTOLIA is | an intersection of math, programming, a | and |
| So, as I understand this the user memorizes half of the password, and when they go to decrypt, a CAPICHA is produced showing the rest of the password. Automated attacks can't verify that a guessed first-half password is | computer science. | |
| 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.) | Codes and ciphers - for code cracking challenges | g |
| permalink | Network security - the most common | n |
| [-] electronics-engineer 3 points 1 day ago | Web security - less crypto, but still | |
| 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. | securityComputer security - local security | |
| permalink parent | Feel free to message the moderators wi | ith |
| ione | | zoter |
| | DE 🚎 🔺 📭 😫 🛱 🗴 👧 | 18:28 8.04.2011 |



| 🕗 Slashdot Search (20) - Mozilla Firefox | |
|---|---|
| <u>File Edit V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp | |
| C X 🏠 http://it.slashdot.org/index2.pl?fhfilter=max+planck | 🔊 🟠 🔹 Google 🔎 |
| 🔊 Most Visited 🌮 Getting Started <u>Ы</u> Latest Headlines | |
| C Sergej's World: web page of Sergej × 🔀 Slashdot Search (20) × ÷ | |
| Slashdot Q max planck | Submit Story Log In Join |
| stories Slashdot is powered by <u>your submissions</u> , so send in your scoop | Follow us: 🔝 📑 🕒 |
| popular Scientists Develop New Method To Improve Passwords | Ads by Google |
| ask slashdot from the start-thinking-of-random-things dept. book reviews games An anonymous reader writes | UNIFIED COMMUNICATIONS SSL CERTIFICATES |
| idle "Scientists at Max-Planck-Institute for Physics of Complex Systems in Dresden, Germany have developed a novel method to improve password security. A strong long password is split in two parts. The first part is memorized by a human. The second part is stored as a CAPTCHA-like image of a chaotic lattice system." | Multiple domain names Unlimited server license One incredible price |
| cloud Read the 104 comments Captcha security cryptography hardware 2011 2010 linux 2011 2010 | |
| management Facebook Ads Could 'Out' Gay Users (196) | Recent Tags |
| mobile F1 Simulators Revealed 72 | government |
| Tool Use By Humans Pushed Back By 800,000 Years (189) | privacy |
| Storage Comcast Customers Urged To Opt-Out of Settlement (128) | usa yro |
| New Ancient Human Identified (148) | |

18:32

08.04.2011

DE 🚎 🔺 📭 🛃 🛄 🔒 🐚

Done



1 🕹 🖊

















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



















| Pikachu - Wikipedia, the free encyclopedia - Mozilla Firefox | | |
|--|------------------|---------------------|
| <u>File Edit View History Bookmarks Tools H</u> elp | | |
| C X 🟠 W http://en.wikipedia.org/wiki/Pikachu | 🖆 🚮 😭 🝷 🥵 Google | م |
| 🔊 Most Visited 🐢 Getting Started 🔊 Latest Headlines | | |
| W Pikachu - Wikipedia, the free encyclo ÷ | | |
| | 👗 Logi | in / create account |



Article Discussion

WIKIPEDIA The Free Encyclopedia

Main page Contents Featured content Current events Random article Donate to Wikipedia

 Interaction Help About Wikipedia Community portal Recent changes Contact Wikipedia

Pikachu

From Wikipedia, the free encyclopedia

Not to be confused with Picacho or Pika.

Pikachu (ピカチュウ Pikachū[?]) 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.^[1] 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,^[2] 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,^[3] 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.^[4]

Contents [hide]

1 Concept and creation



Search

Read View source View history

Q

Ð