COMP8760 Computer Security

University of Kent

User Authentication

Cracking Textual Passwords and Potential Improvement On Textual Password

Budi Arief

b.arief@kent.ac.uk

Based on slides by Shujun Li

Outline

- Cracking Textual Passwords
  - Attempts Through The Years
  - Attack Techniques and Tools
- Potential Improvement on Textual Password
  - Some Ways to Address the Issues
  - Graphical Passwords
- Summary

Password cracking: **1979**

- Robert Morris and Ken Thomson, "Password security: A case history," *Communications of the ACM*, 22(11):594-597, ACM, 1979
  - In a collection of 3,289 passwords…
    - 15 were a single ASCII character
    - 72 were strings of two ASCII characters
    - 464 were strings of three ASCII characters
    - 477 were strings of four alphamerics
    - 706 were five letters, all upper-case or all lower-case
    - 605 were six letters, all lower-case
    - 492 appeared in dictionaries, name lists, and the like

2,831 passwords

Password cracking: **1990**

- Daniel V. Klein, “Foiling the Cracker: A Survey of, and Improvements to, Password Security,” USENIX Security 1990
  - In a set of 15,000 passwords
    - 25% were cracked within 12 CPU months
    - 21% were cracked in the first week
    - 2.7% were cracked within the first 15 minutes

Password cracking: **2005**

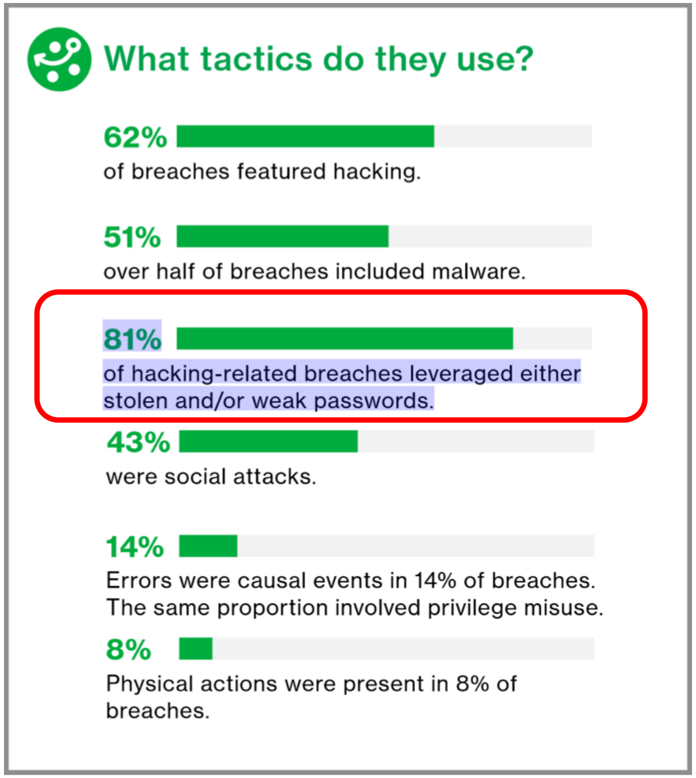
- Arvind Narayanan and Vitaly Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," ACM CCS 2005
  - In a collection of 142 real user passwords
    - 67.6% (96) were cracked with a searching complexity $2.17\times10^{9}\approx2^{31}$

Password cracking: **2013**

- Dan Goodin, “Anatomy of a hack: How crackers ransack passwords like ‘qeadzcwrsfxv1331’,” ars technica, 28 May 2013
  - Three professional crackers were given 16,449 hashed passwords and the best of them was able to crack 90% of the passwords
  - Remark 1: All the passwords are considered harder ones because they are what remained uncracked in a much larger database of leaked passwords
  - Remark 2: Nate Anderson, Ars deputy editor and a self-admitted newbie to password cracking, was able to crack around 50% of the passwords within a few hours

Password cracking: **2017**

- 2017 Verizon Data Breach Investigations Report (DBIR)



What tactics do they use?

62%
of breaches featured hacking.

51%
over half of breaches included malware.

81%
of hacking-related breaches leveraged either stolen and/or weak passwords.

43%
were social attacks.

14%
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%
Physical actions were present in 8% of breaches.

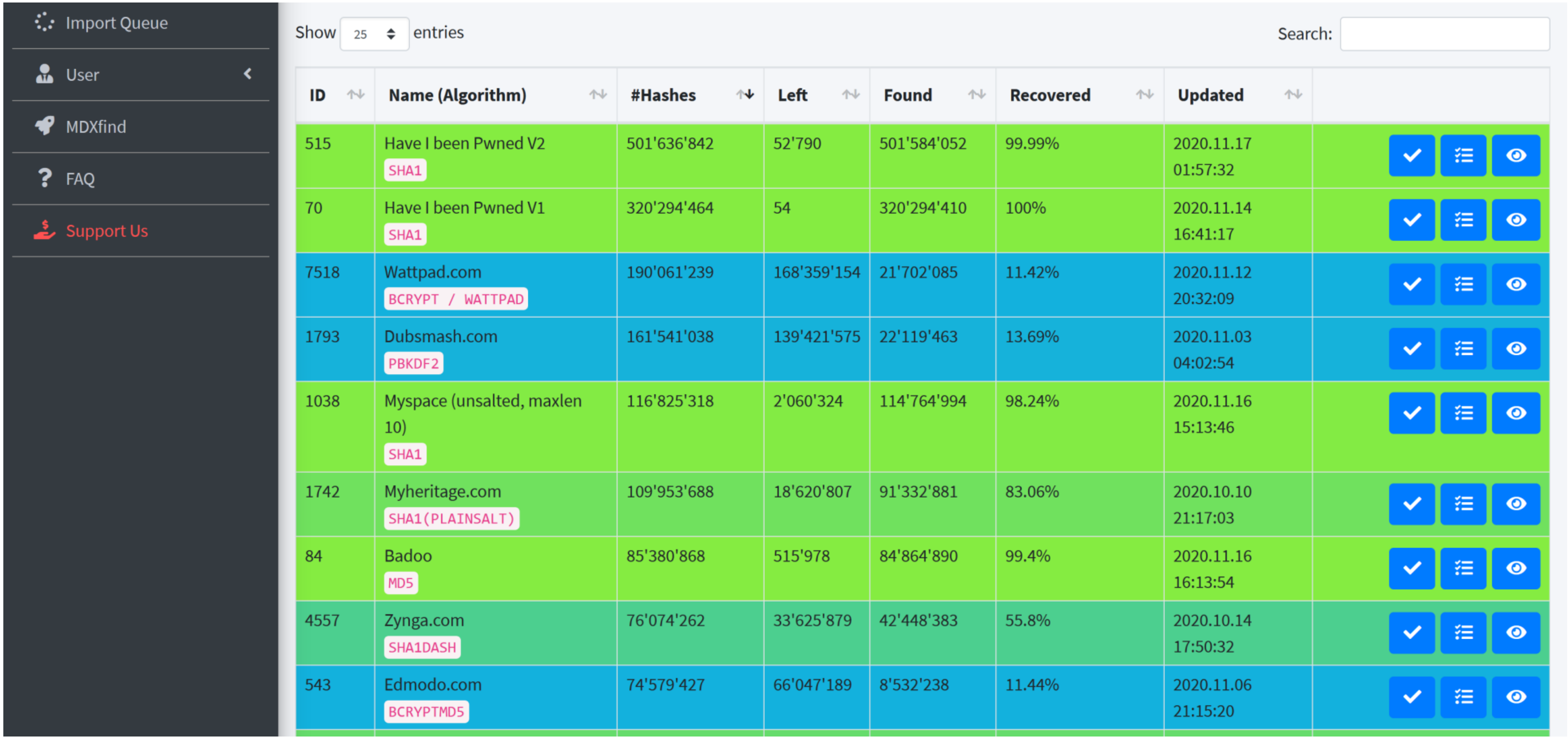
2017 Data Breach Investigations Report

Executive Summary

verizon

Password cracking: **2020**

- Cracked passwords on hashes.org as of 2020



ID	Name (Algorithm)	#Hashes	Left	Found	Recovered	Updated	
515	Have I been Pwned V2 SHA1	501'636'842	52'790	501'584'052	99.99%	2020.11.17 01:57:32	✓ ☰ 👁
70	Have I been Pwned V1 SHA1	320'294'464	54	320'294'410	100%	2020.11.14 16:41:17	✓ ☰ 👁
7518	Wattpad.com BCRYPT / WATTPAD	190'061'239	168'359'154	21'702'085	11.42%	2020.11.12 20:32:09	✓ ☰ 👁
1793	Dubsmash.com PBKDF2	161'541'038	139'421'575	22'119'463	13.69%	2020.11.03 04:02:54	✓ ☰ 👁
1038	Myspace (unsalted, maxlen 10) SHA1	116'825'318	2'060'324	114'764'994	98.24%	2020.11.16 15:13:46	✓ ☰ 👁
1742	Myheritage.com SHA1(PLAINSALT)	109'953'688	18'620'807	91'332'881	83.06%	2020.10.10 21:17:03	✓ ☰ 👁
84	Badoo MD5	85'380'868	515'978	84'864'890	99.4%	2020.11.16 16:13:54	✓ ☰ 👁
4557	Zynga.com SHA1DASH	76'074'262	33'625'879	42'448'383	55.8%	2020.10.14 17:50:32	✓ ☰ 👁
543	Edmodo.com BCRYPTMD5	74'579'427	66'047'189	8'532'238	11.44%	2020.11.06 21:15:20	✓ ☰ 👁

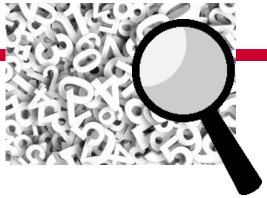
Outline

- Cracking Textual Passwords
  - Attempts Through The Years
  - Attack Techniques and Tools

- Potential Improvement on Textual Password
  - Some Ways to Address the Issues
  - Graphical Passwords

- Summary

So passwords can be cracked (easily)!



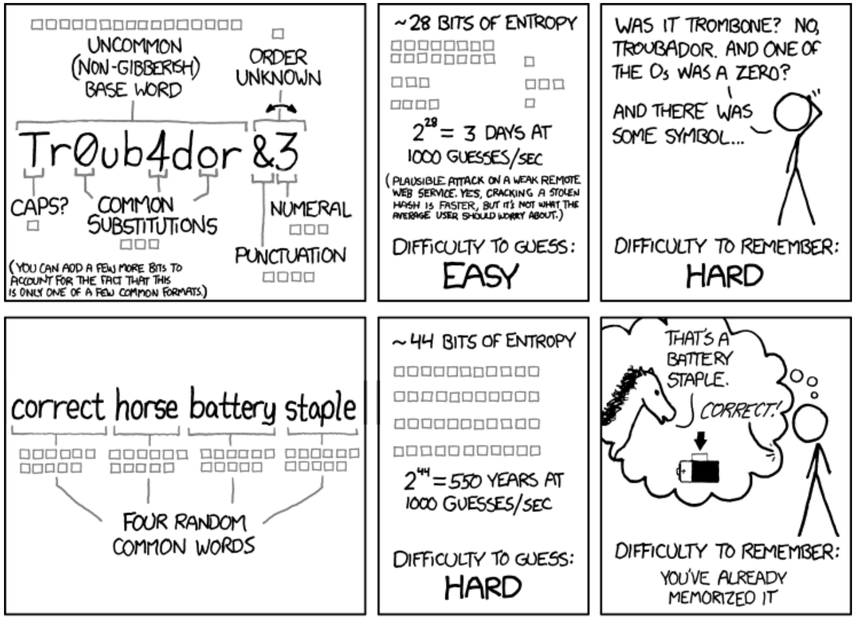
- Simple **brute force**
  - Possible if the (actually used) password space is not large enough
  - Offline attacks
    - Get a hashed password (and the salt) and try all possible passwords
  - Online attacks
    - Try up to *n* (a small number) allowed passwords for each of *N* (a large number) accounts
    - Can use a botnet to launch a large-scale attack
    - CAPTCHA can make it harder, but most CAPTCHAs are insecure

So passwords can be cracked (easily)!

- **Dictionary attack** (smart brute force)
  - Steps
    1. **Build a dictionary** of passwords that are more likely used by the target user(s)
    2. **Rank the passwords** by their usage frequency (if data available)
    3. **Try all passwords** in the dictionary, starting from the most frequently used one
  - Can use more than one dictionary
  - Can use personal info to build a personal dictionary
  - Can be combined with other attacks, e.g., dictionary attack + simple brute force of a prefix and an affix (if both are short enough)

So passwords can be cracked (easily)!

- **Rule-based attacks** (smart brute force)
  - Using a number of rules to create more guessed passwords
    - Case toggle (e.g., l ⇔ L)
    - Character replacement (e.g., l ⇒ 1, s ⇒ $, a ⇒ @, 0 ⇒ o or O)
    - Character insertion (e.g., add a white space)
    - Character deletion (e.g. delete all occurrences of a specific letter)
    - …


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(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.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

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.

So passwords can be cracked (easily)!

- More **advanced (smarter) attacks**
  - **Divide and conquer**: different models for different types of passwords
  - **Linguistic models**: considering linguistic features of passwords (e.g., what make a password more pronounceable and memorisable)
  - **Training-based approaches**: using a leaked password database to learn how to build a password cracker to attack a target database (potentially using an AI model)
  - **Probabilistic models**: considering conditional probabilities (normally learned from a leaked password database)
  - …

So passwords can be cracked (easily)!

- An advanced password cracking method: PCFG (Probabilistic Context-Free Grammars)
  - Basic grammar models based on three types of sub-strings: L (letters), D (digits) and S (special characters)
    - Example: \$password123 $\Rightarrow$ $S_1L_8D_3$
  - Learning a PCFG from a training database
    - Example: $\text{Prob}(S_1 \to L_8D_3)=0.6$, $\text{Prob}(S_1 \to D_3L_8)=0.4$; $\text{Prob}(S_1 \to ?)=0.2$, $\text{Prob}(S_1 \to \#)=0.3$, $\text{Prob}(S_1 \to \$)=0.4$, $\text{Prob}(S_1 \to .)=0.1$; …
  - Using the learned PCFG to generated a ranked list of password guesses according to their probabilities

- Matt Weir et al., “Password Cracking Using Probabilistic Context-Free Grammars,” IEEE S&P 2009 (GitHub source code)

Password cracking tools: hashcat

- One of the two most popular offline password crackers
- “World’s first and only in-kernel rule engine”
- Free and open-source (MIT License)
- Multi-OS and multi-platform (CPU, GPU, DSP, FPGA, etc., that comes with an OpenCL runtime)
- Multi-hash (multiple hashes at the same time)
- Multi-devices and multi-device-types (multiple devices and device types in the same system)
- Supports distributed cracking networks
- Supports automatic keyspace ordering Markov-chains
- 200+ hash-types implemented with performance in mind
- Built-in benchmarking system
- Integrated thermal watchdog
- …

Please use this tool legally, ethically and responsibly!

Password cracking tools

- John the Ripper (JtR / JTR)
    - One of the other most popular offline password cracker

- THC Hydra (or simply Hydra)
    - Online password cracking tool

- Aircrack-ng
    - Password hacking tool for WiFi

- …

Please use these tools legally, ethically and responsibly!

Outline

- Cracking Textual Passwords
  - Attempts Through The Years
  - Attack Techniques and Tools

- Potential Improvement on Textual Password
  - Some Ways to Address the Issues
  - Graphical Passwords

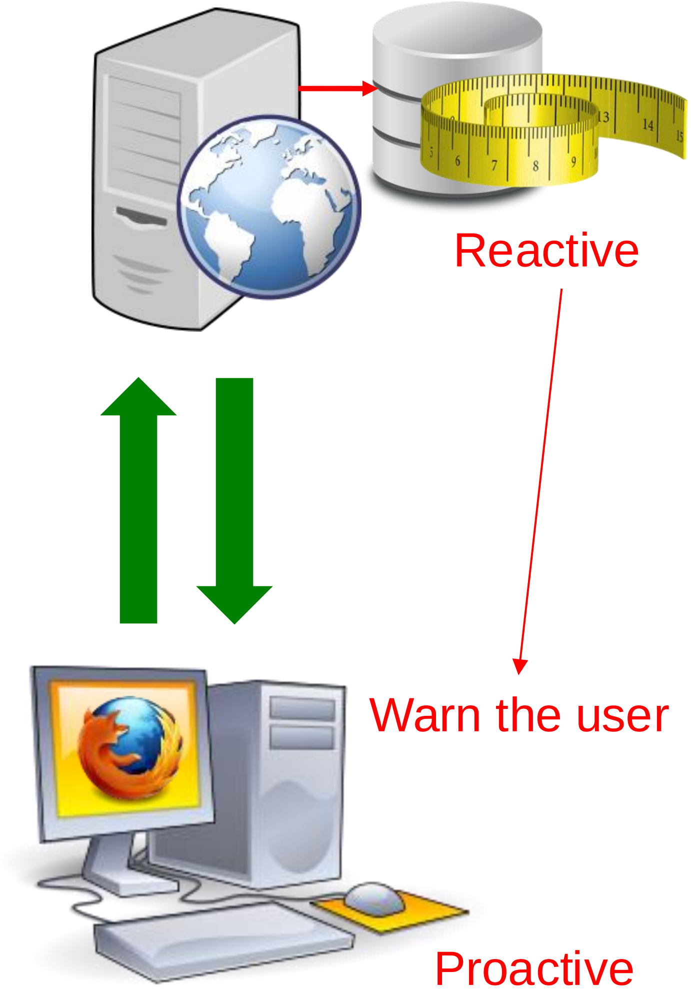
- Summary

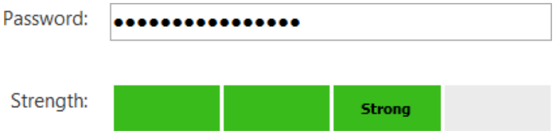
What can we learn from reality?

- The security-usability dilemma
  - Stronger passwords are more secure but harder to remember by humans
  - Weaker passwords are easier to remember by humans but also easier to be cracked
  - Strong passwords for humans ≠ Strong passwords for automated password crackers
- End users have a tendency of choosing usability over security: using easy-to-remember passwords
- End users have **not** changed their ways of using (weak) passwords very much since 1970s!

Password checkers

- A password checker checks the strength of a given password and warns the user about its weakness
  - **<u>Proactive</u> password checkers** work at the **client** side when the user is entering his/her password
  - **<u>Reactive</u> password checkers** work at the server side after users set their passwords (by scanning all passwords of all users)
  - Both proactive and reactive password checkers are based on one or more **<u>password meters</u>** that estimate the security strength of a given password

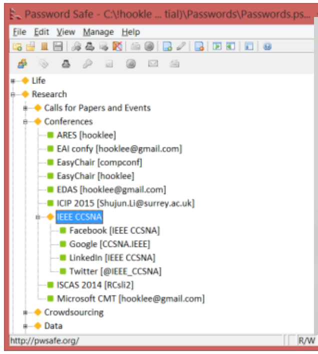



Password: ••••••••••••••••

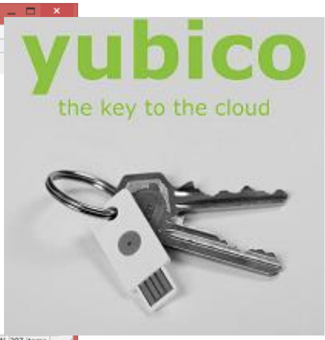
Strength: Strong

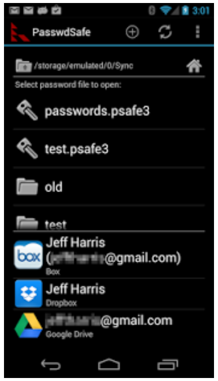
Password managers

- A password manager is a software/hardware tool managing credentials of multiple accounts of the user
  - A **master password** is normally required to manage all passwords
  - **Local password managers** run from a local computer (could be a smart phone) and store the data locally
  - **Web-based password managers** run from the Web or the cloud and store the data remotely in a remote web site
  - **Cloud-based password managers** run from local computer or the Web and store the data remotely in a cloud
  - Data across devices could be **synchronized**



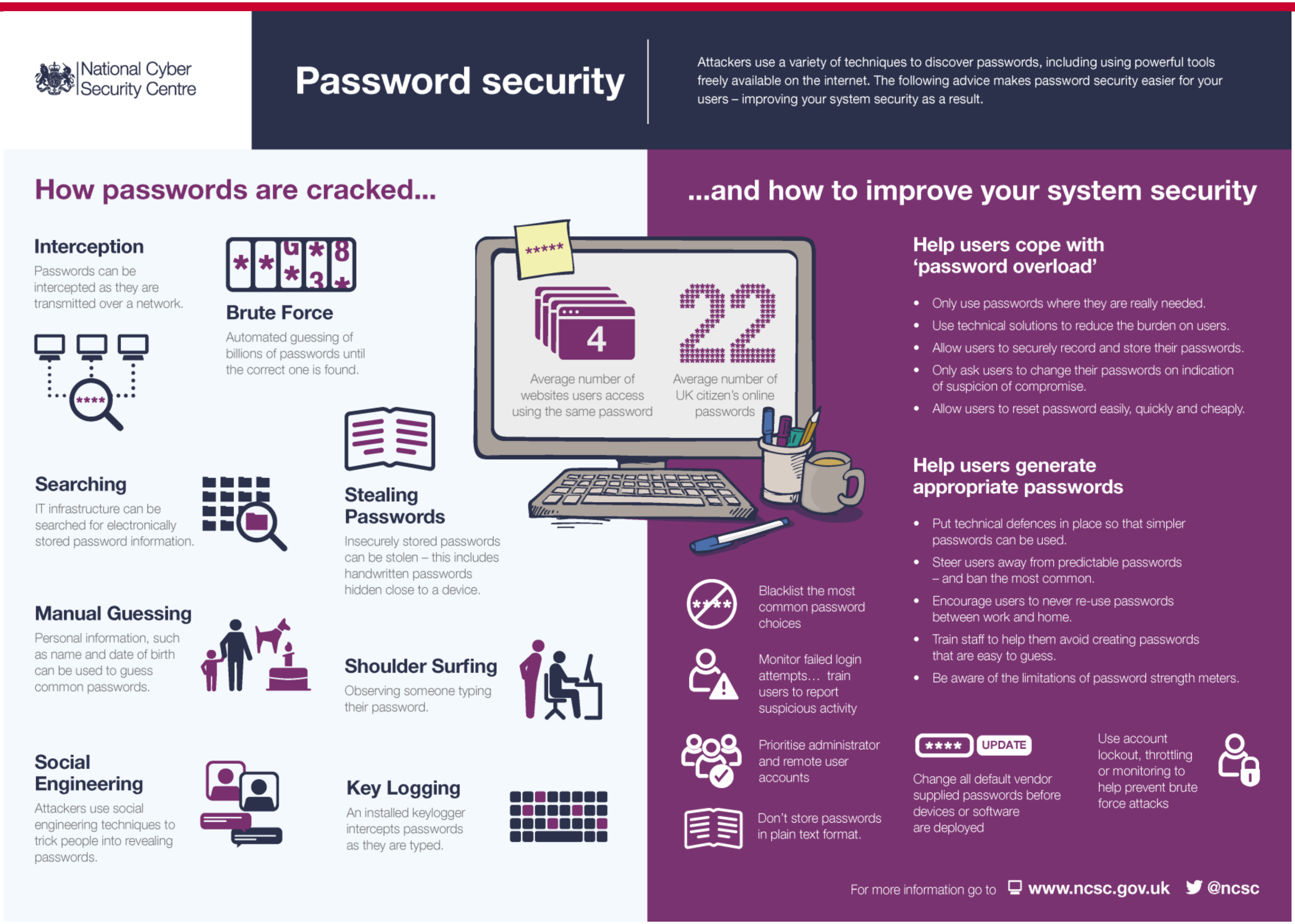
```
Password Safe - C:\!hookle ... tial)\Passwords\Passwords.ps...
File  Edit  View  Manage  Help
Life
Research
    Calls for Papers and Events
    Conferences
        ARES [hooklee]
        EAI confy [hooklee@gmail.com]
        EasyChair [compconf]
        EasyChair [hooklee]
        EDAS [hooklee@gmail.com]
        ICIP 2015 [Shujun.Li@surrey.ac.uk]
        IEEE CCSNA
            Facebook [IEEE CCSNA]
            Google [CCSNA.IEEE]
            LinkedIn [IEEE CCSNA]
            Twitter [@IEEE_CCSNA]
        ISCAS 2014 [RCsli2]
        Microsoft CMT [hooklee@gmail.com]
    Crowdsourcing
    Data
http://pwsafe.org/    R/W  207 items
```





```
3:01
PasswdSafe
/storage/emulated/0/Sync
Select password file to open:
passwords.psafe3
test.psafe3
old
test
Jeff Harris
([redacted]@gmail.com)
Box
Jeff Harris
Dropbox
[redacted]@gmail.com
Google Drive
```

Password guidance



National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.

4

Average number of websites users access using the same password

22

Average number of UK citizen's online passwords

...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

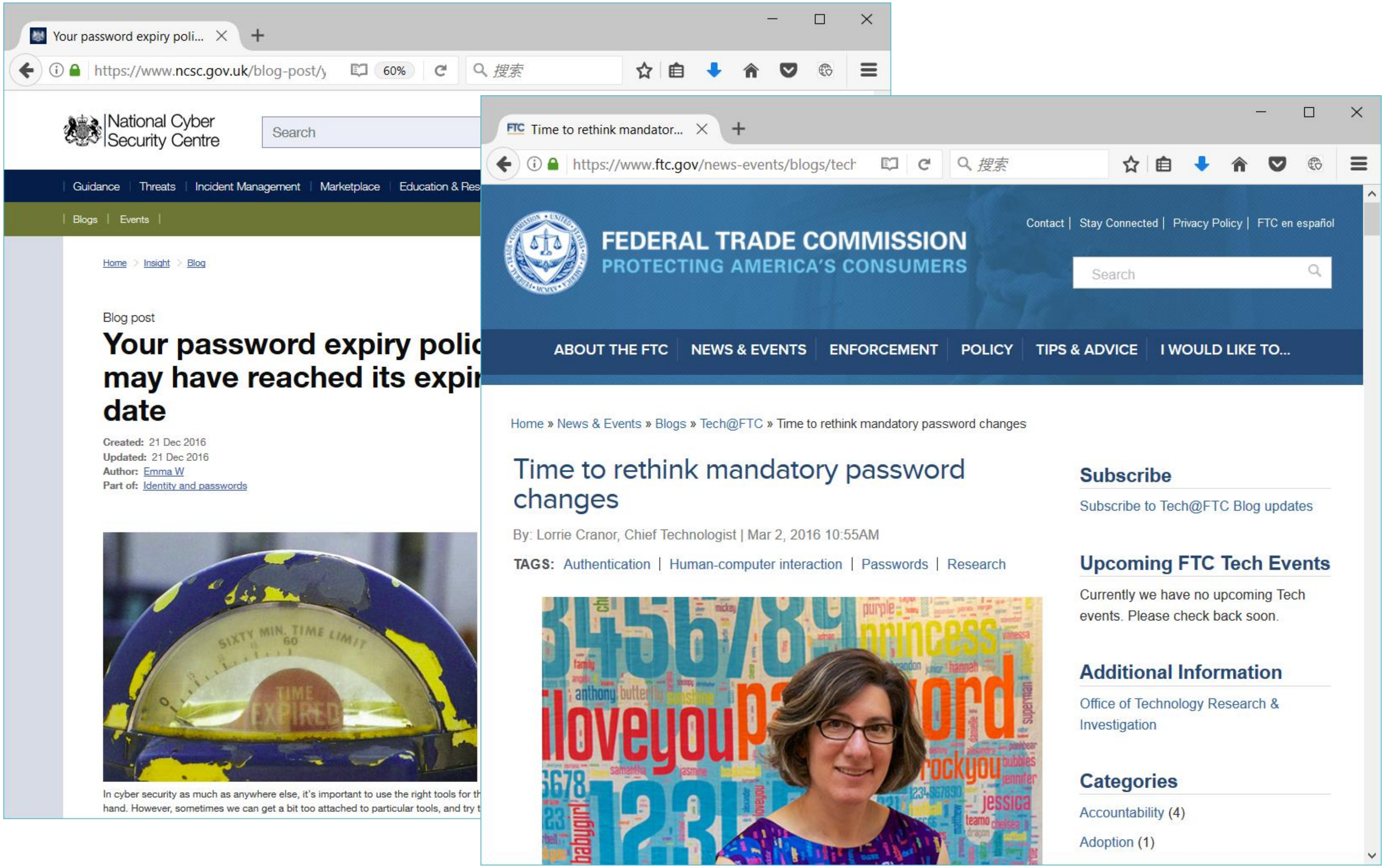
Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to www.ncsc.gov.uk @ncsc

Password policies



Your password expiry poli...

https://www.ncsc.gov.uk/blog-post/y

National Cyber Security Centre

Guidance | Threats | Incident Management | Marketplace | Education & Res

Blogs | Events

Home > Insight > Blog

Blog post

Your password expiry polic may have reached its expir date

Created: 21 Dec 2016
Updated: 21 Dec 2016
Author: Emma W
Part of: Identity and passwords

In cyber security as much as anywhere else, it's important to use the right tools for th hand. However, sometimes we can get a bit too attached to particular tools, and try t

Time to rethink mandator...

https://www.ftc.gov/news-events/blogs/tech

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected | Privacy Policy | FTC en español

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

Home » News & Events » Blogs » Tech@FTC » Time to rethink mandatory password changes

Time to rethink mandatory password changes

By: Lorrie Cranor, Chief Technologist | Mar 2, 2016 10:55AM

TAGS: Authentication | Human-computer interaction | Passwords | Research

Subscribe

Subscribe to Tech@FTC Blog updates

Upcoming FTC Tech Events

Currently we have no upcoming Tech events. Please check back soon.

Additional Information

Office of Technology Research & Investigation

Categories

Accountability (4)
Adoption (1)

Outline

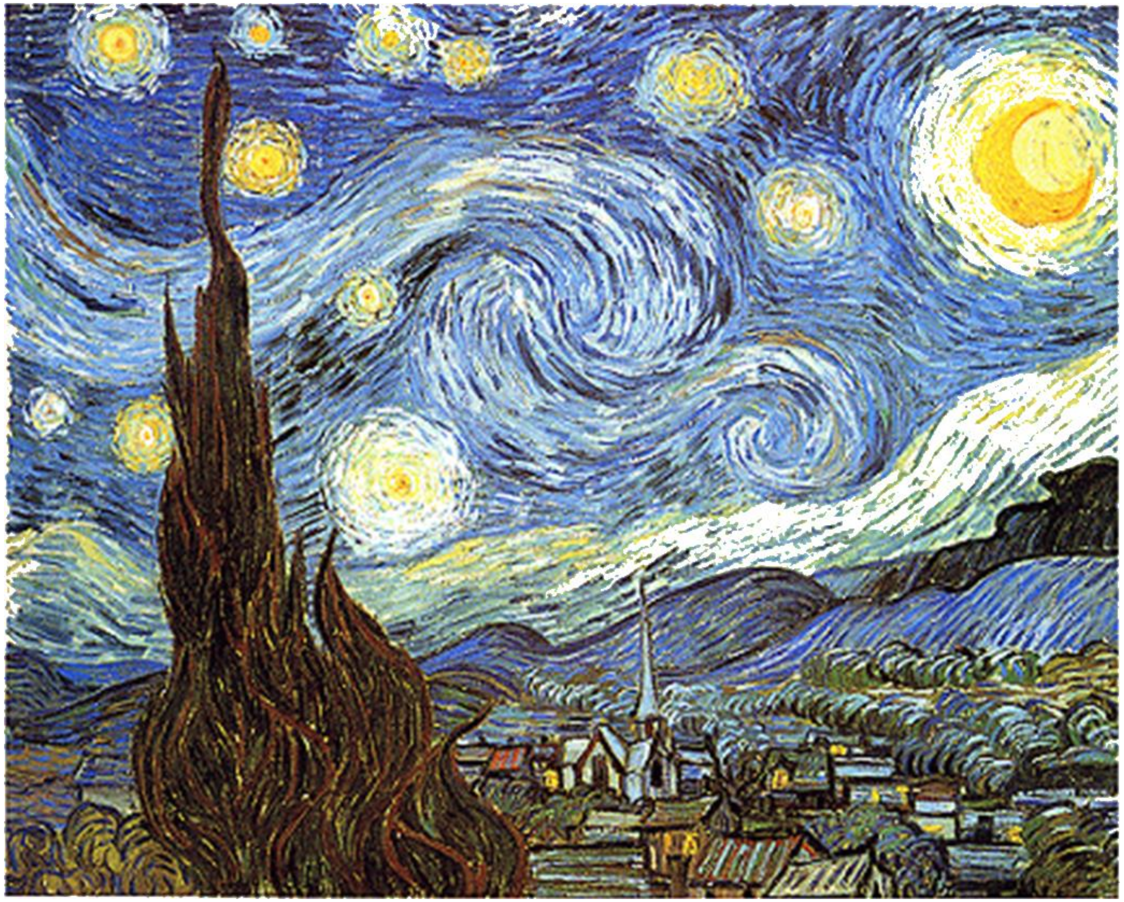
- Cracking Textual Passwords
  - Attempts Through The Years
  - Attack Techniques and Tools

- Potential Improvement on Textual Password
  - Some Ways to Address the Issues
  - Graphical Passwords

- Summary

Why may graphical passwords help?

- An old saying: “A picture is worth a thousand words.”



Why may graphical passwords help?

- Graphics and images contain richer information than texts, and harder to be exactly described by both humans and computers
  - ⇒ Larger password space?
  - ⇒ Less weak passwords?
  - ⇒ More difficult to construct dictionary?
  - ⇒ Easier to remember and harder to forget?
  - ⇒ Harder to tell them to others? (At least via phone ☺)
  - **⇒ A better balance between usability and security?**

Yet another advantage

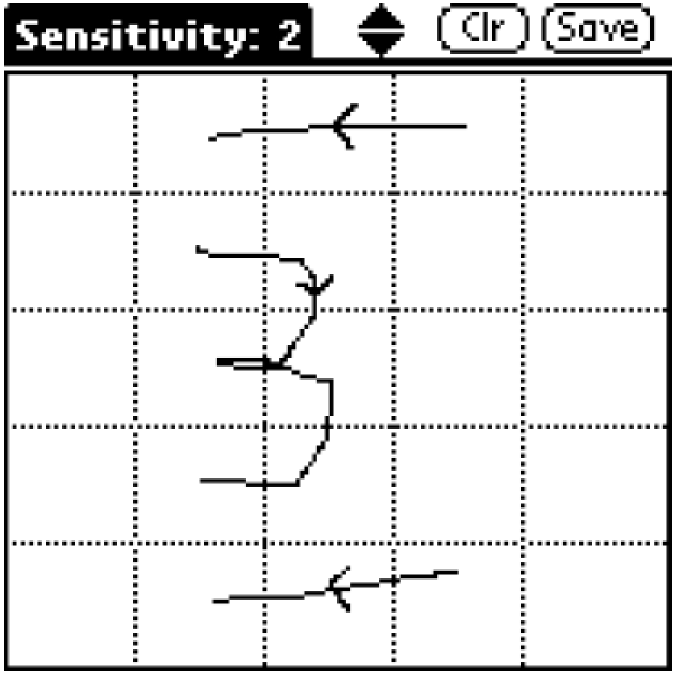
- Graphical passwords are more secure against side channel attacks:
  - Martin Vuagnoux and Sylvain Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," USENIX Security Symposium 2009
  - Kehuan Zhang and XiaoFeng Wang, "Peeping Tom in the Neighborhood: Keystroke Eavesdropping on Multi-User Systems," USENIX Security Symposium 2009

A classification of graphical passwords

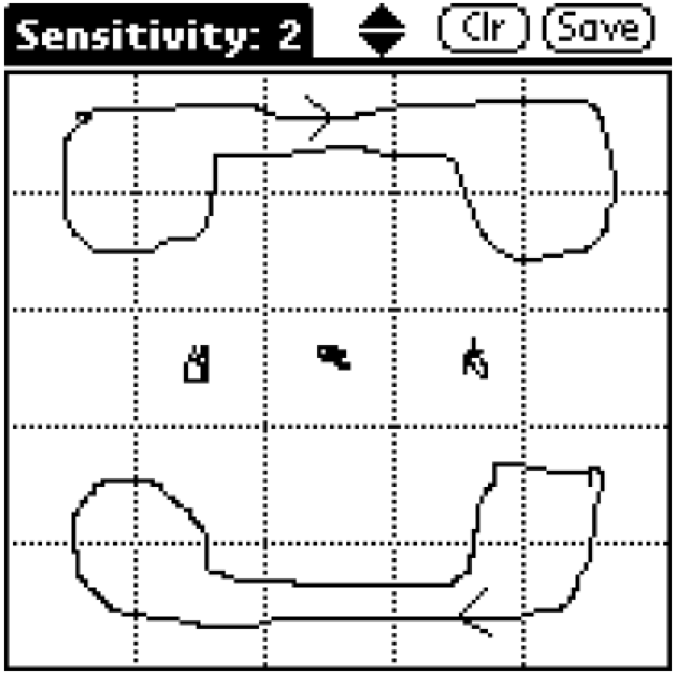
- Class 1: Drawing-based passwords
- Class 2: Location-based graphical passwords
- Class 3: Recognition-based graphical passwords
- Hybrid graphical passwords: more than one class

Class 1: DAS (Draw-A-Secret)

- Ian Jermyn et al., “The Design and Analysis of Graphical Passwords,” USENIX Security Symposium 1999 (Best paper and best student paper awards!)



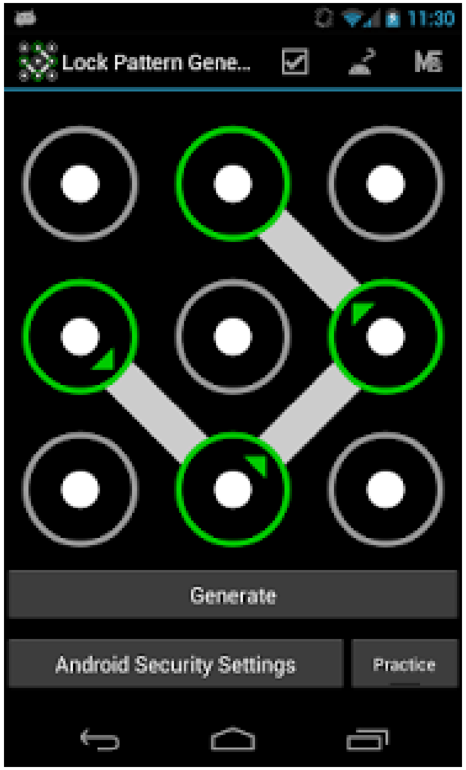
Sensitivity: 2



Sensitivity: 2

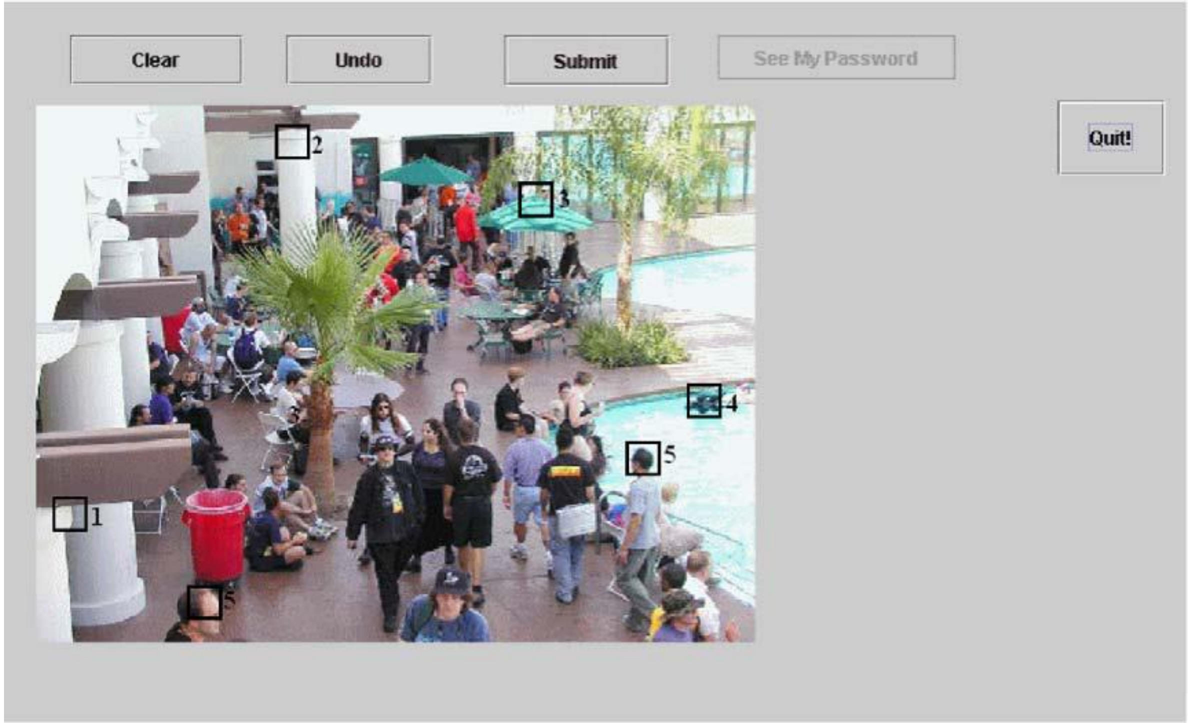
Class 1: Android unlocking patterns

- A variant of DAS has been adopted by Google for its Android OS as an unlocking scheme and widely used by Android users



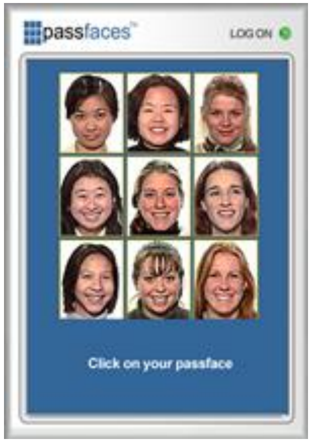
Class 2: PassPoints

- Susan Wiedenbeck et al., “PassPoints: Design and longitudinal evaluation of a graphical password system,” *International Journal of Human-Computer Studies*, 63:102-127, Elsevier, 2005

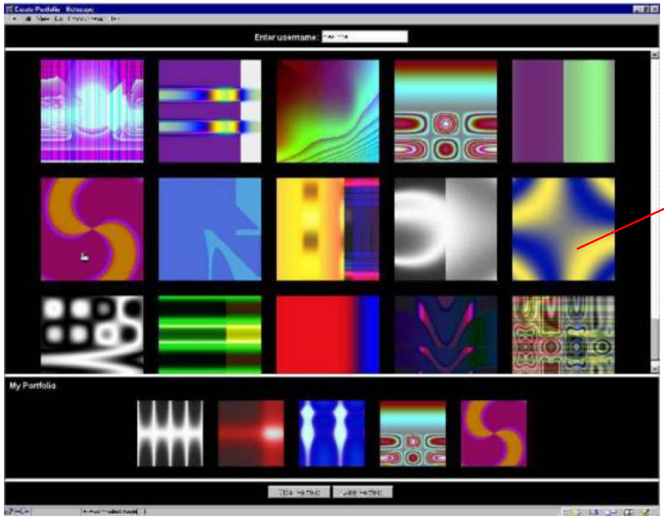


Class 3: Passfaces and Déjà Vu

- Passfaces$^{\text{TM}}$



- Déjà Vu (Dhamija & Perrig, USENIX Security 2000)



Random art
http://www.random-art.org

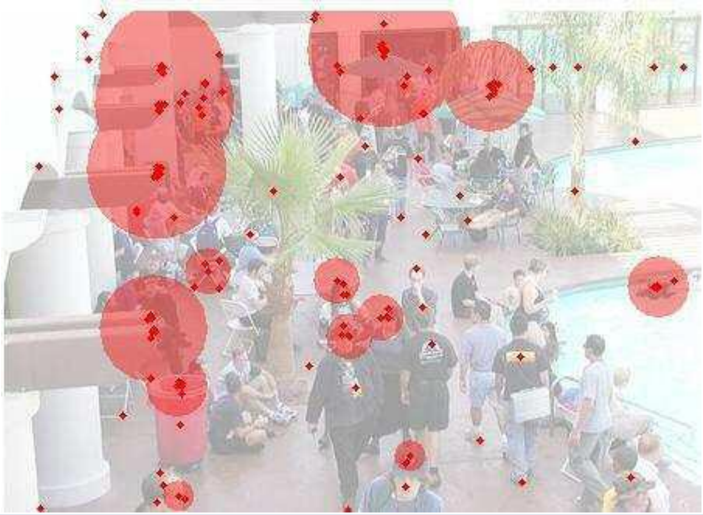
Users’ choices are not random!

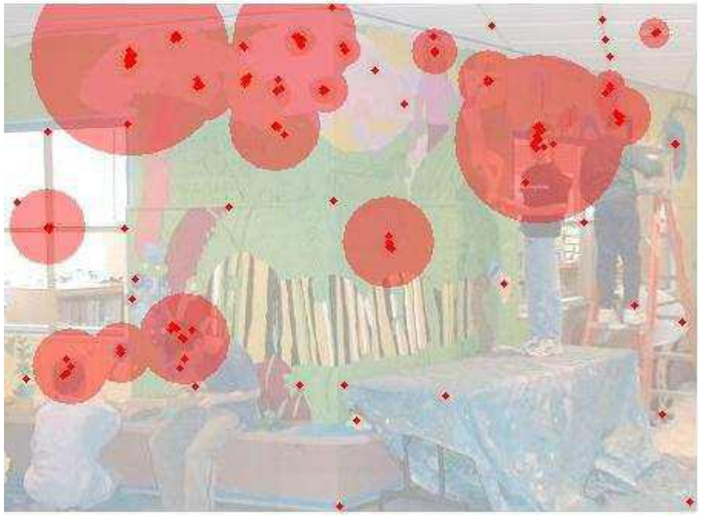
- Darren Davis et al., “On User Choice in Graphical Password Schemes,” USENIX Security Symposium 2004

Users tend to choose faces of beautiful women and/or of people in their own race

Dictionary attacks come back!

- Julie Thorpe and P.C. van Oorschot, "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords," USENIX Security Symposium 2007

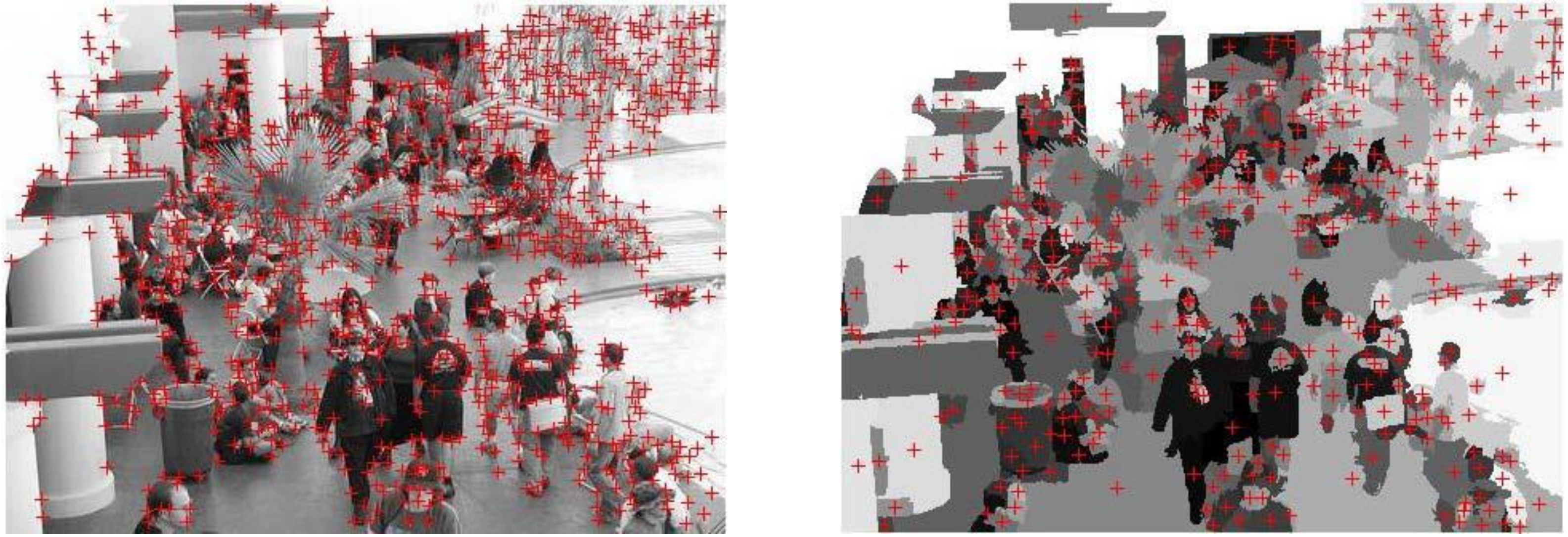




A dictionary of click points (hotspots) can be harvested from a set of human users (at the attacker's disposal), or automatically determined by some image processing algorithms ⇒ For automated attack, 8% passwords were cracked within 2^{32} guesses

Dictionary attacks come back!

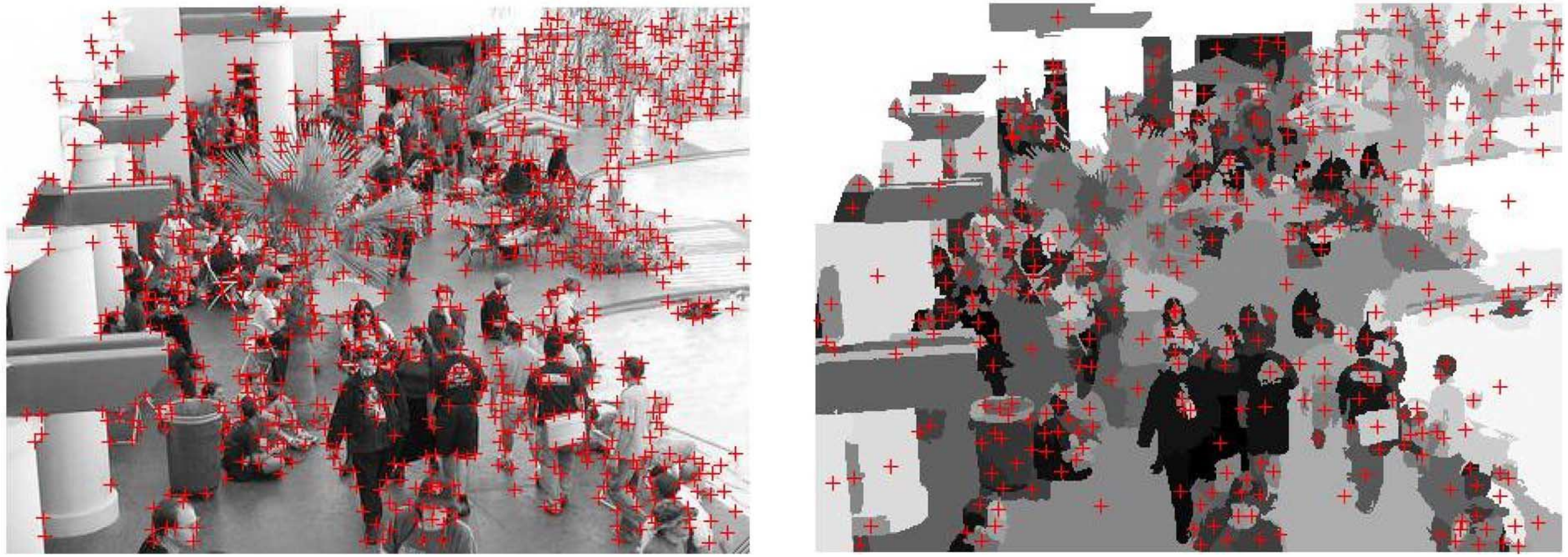
- Amirali Salehi-Abari et al., “On Purely Automated Attacks and Click-Based Graphical Passwords,” ACSAC 2008, IEEE Computer Society



An improved dictionary attack: 16% passwords cracked using a dictionary of less than $2^{31.4}$ entries

Dictionary attacks come back!

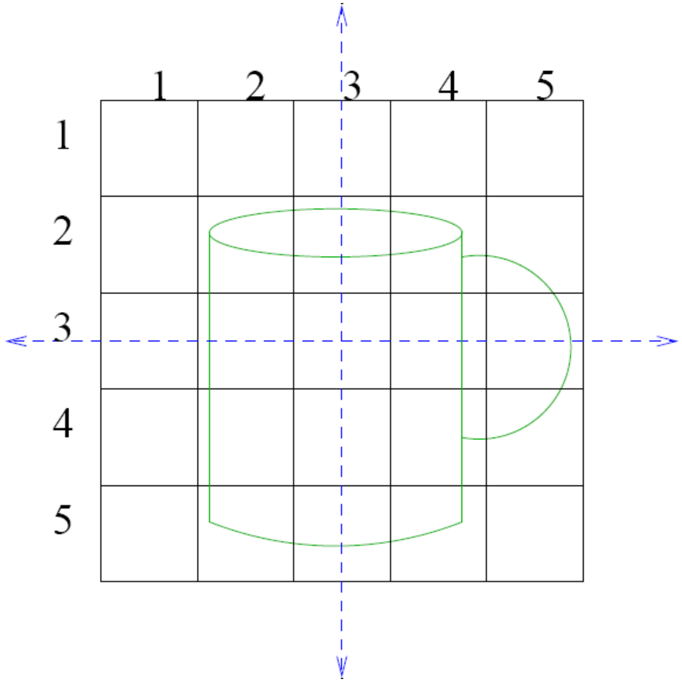
- P.C. van Oorschot et al., "Purely Automated Attacks on PassPoints-Style Graphical Passwords," *IEEE Transactions on Information Forensics and Security*, 5(3):393-405, 2010



Improved dictionary attacks: 7-16% passwords cracked using a dictionary of 2^{26} entries, 48-54% passwords using a dictionary of 2^{35} entries

Dictionary attacks come back!

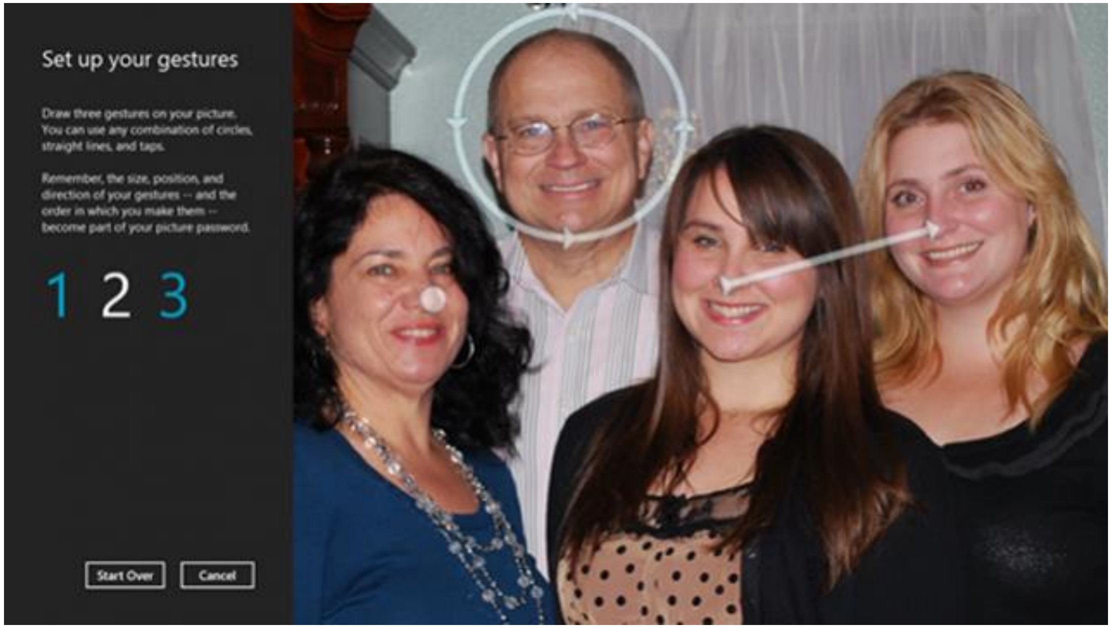
- Julie Thorpe and P.C. van Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," USENIX Security Symposium 2004
  - Mirror symmetric DAS passwords are used to construct a dictionary



The sub-password-space is exponentially smaller than the full space

Dictionary attacks come back!

- Ziming Zhao et al., “On the Security of Picture Gesture Authentication,” USENIX Security Symposium 2013
  - 10k Windows 8 picture passwords were collected from 800 users
  - A training-based approach: 24% of passwords cracked in one database with a dictionary of size is 2^{19} (total password space 2^{31})



Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

Remember, the size, position, and direction of your gestures -- and the order in which you make them -- become part of your picture password.

Dictionary attacks come back!

- Sebastian Uellenbeck et al., “Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns,” ACM CCS 2013
  - High bias in the pattern selection process
  - Security equivalent to three-digit PINs for guessing 20% of all pass-patterns

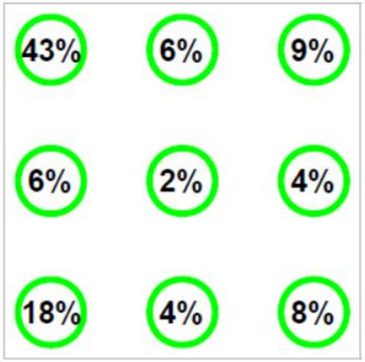


Figure 7: Bias of the initial point.

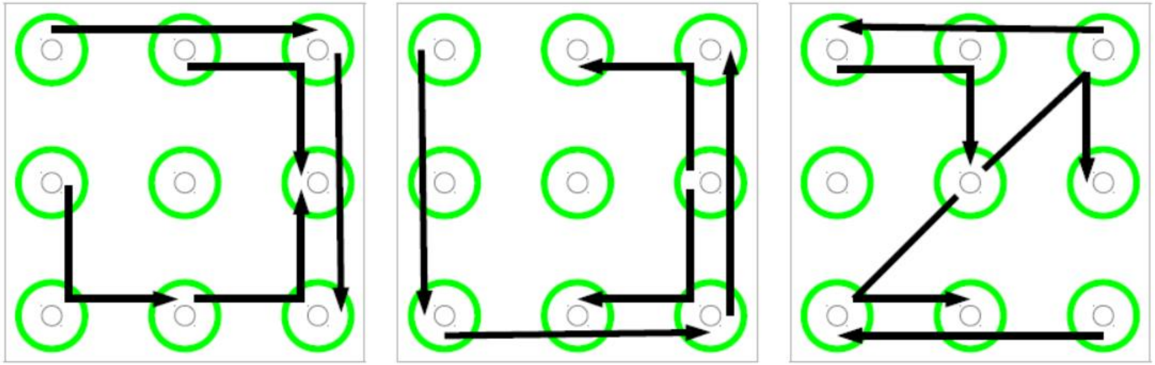


Figure 8: The most frequent 3-grams, from most frequent (left) to less frequent (right).

Usability problems!

- Karen Renaud and Antonella De Angeli, "My password is here! An investigation into visuo-spatial authentication mechanisms," *Interacting with Computers*, 16:1017-1041, Elsevier, 2004
- Problem 1: the incredible difficulty related to choosing the background image
- Problem 2: the user's difficulty in pin-pointing a good pass-point
- ⇒ "The cognitive aspects of visual information processing would appear to make the use of spatial position untenable for authentication systems"

Outline

- Cracking Textual Passwords
  - Attempts Through The Years
  - Attack Techniques and Tools
- Potential Improvement on Textual Password
  - Some Ways to Address the Issues
  - Graphical Passwords
- Summary

Summary

- Textual password is still the most popular method of authentication
  - However, there are some issues, especially with weak (textual) passwords
  - Some tools (such as password manager) can help
- Graphical passwords are not significantly more secure than textual passwords!
  - Some are weaker than strong textual passwords
  - Graphical passwords have their own unique usability problems!
  - ⇒ Graphical passwords do not seem to be a valid replacement of textual passwords

We will continue in the class and in Week 17 (next week)

- Week 16 class: later today (Thu 21 Nov 2024)
  - Putting into practice what we have learned in Week 16, including:
    - Password hashing and salting, dictionary attacks, breaking graphical password
- Week 17: Other ways of authenticating users
  - Beyond passwords
    - Other Knowledge-based (something you know but you don’t normally call it a password)
    - Possession-based (what you have)
    - Inherence-based (who you are = biometrics)

Important: Week 17 New Timetable

- Week 17: Reschedule of the Monday lecture
  - Due to conflict of commitments, the lecture on Monday 25 Nov 2024 needs to be rescheduled
  - New lecture slot: Thursday 28 Nov 2024
    - Time: 14:00-15:00
    - Venue: Kennedy Seminar Room 10
  - As a summary, ***all** of Week 17's events for COMP8760* will be on **Thursday 28 Nov 2024**
    - Lecture 1: 10:00-11:00 (SLT2)
    - Lecture 2: 14:00-15:00 (KenSR10)
    - Class: 15:00-17:00 (Jennison Computer Suite 2 Red)