PRIVACY, SECURITY AND USABILITY

Security and Usability: User authentication, user warnings

PASSWORDS

Topics for class

- Passwords as a challenge
- How to study passwords
- Mturk password studies
- Studies with real passwords
- Password expiry
- Perceptions and misconceptions about passwords
- Password meters and guidance

Passwords Guessing

- Passwords have been shown to be vulnerable to multiple attacks:
  - Shoulder surfing attacks
  - Online attacks
  - Offline attacks

Password Attacks

- How do attackers steal so passwords?
  - Attackers break in and steal entire password database
  - Database usually scrambled with hash function
  - Attackers make billions of guesses
    - to try to recover as many scrambled passwords as they can

Password Attacks

- Brute-force naive attack:
  - Guess according to order, i.e.:
    - “aaa’,’aab’,’aac’,etc.
- Brute-force educated attack:
  - Use password dictionaries
    - Words which are more likely to be used
    - “password’,’123”,”1234”, etc.

Password Reuse

- Password reuse is very common
  - Attackers explore password reuse

Password Challenge

- Help users pick passwords that are easy to remember
  - But hard for an attacker to guess

Passwords

https://thenextweb.com/insider/2016/03/31/5-technologies-will-flip-world-authentication-head/

Password for Studies

- Passwords created for experiments
  - Lab studies
  - Online studies
- Real passwords
  - Stolen passwords
  - Surveys
  - Legitimate access to actual passwords

Possible Study

- Participants tasks:
  - Create password under a randomly assigned condition
  - Take a survey
  - Recall password
  - Return 2 days later to recall password and take survey
- Study Design tasks:
  - Create an application that requests the password for the user
    - Ask the user to enter the same password twice
      - to avoid typing mistakes
        - Common in online password choices

Possible Study

- Password policy options:
  - Basic
    - E.g., ‘password’
  - Dictionary combined words:
    - E.g., “easyword”
  - Hard passwords:
    - E.g., ‘password9$’
  - Longer multiple word association (minimum length):
    - ‘HamiltonBroadwayshow’

Usability Metric

- Creation attempts and time
- Recall attempts
- Reported sentiment
- Write-down rate
- Study drop-out rate

Password Strength Metric

- Guessability
  - Estimate of how many guesses a sophisticated attacker will need to guess a password
- Usability
  - Have user rate the usability of the method
    - on a Likert scale:
    - ‘annoying’,’difficult’,’fun’,etc.

Password Strength Metric

- Can we find certain rules:
  - Are certain symbols used more?
  - Are certain numbers used more?

Password Meters

- Do people like them?
- Do they help create stronger passwords?
- Do they help create memorable passwords?

Passphrases

- Are passphrases better than passwords?
  - Study “Can Long Passwords Be Secure and Usable?” by Shay et al [2014]
  - Usability comparison
  - System-assigned passphrases vs. passwords
  - System-assigned assures random selection

Methodology

- Mturk Study
- Users are assigned their password or passphrase
- Multiple passphrase, password conditions
- Varied factors:
  - Size of dictionary words are selected from
  - Whether order matters
  - Parts of speech
  - Number of words
  - Instructions

Methodology

- Some possible passwords constructions:
  - 4 common words
    - I love my dog
  - Noun verb adjective noun
    - Baby likes red toy
  - System assigned passwords
    - J:+*8eE~
  - Pronounceable passwords:
    - abanibi

Study findings

- Passphrases are not an ultimate solution
- No clear preference by users
- May not be easier to remember
- Longer, so take longer to type
  - More typing mistakes
  - Pronouncable passwords faster to type
    - than other passwords or passphrases
- Passphrases may provide stronger security
  - Harder to brute-force

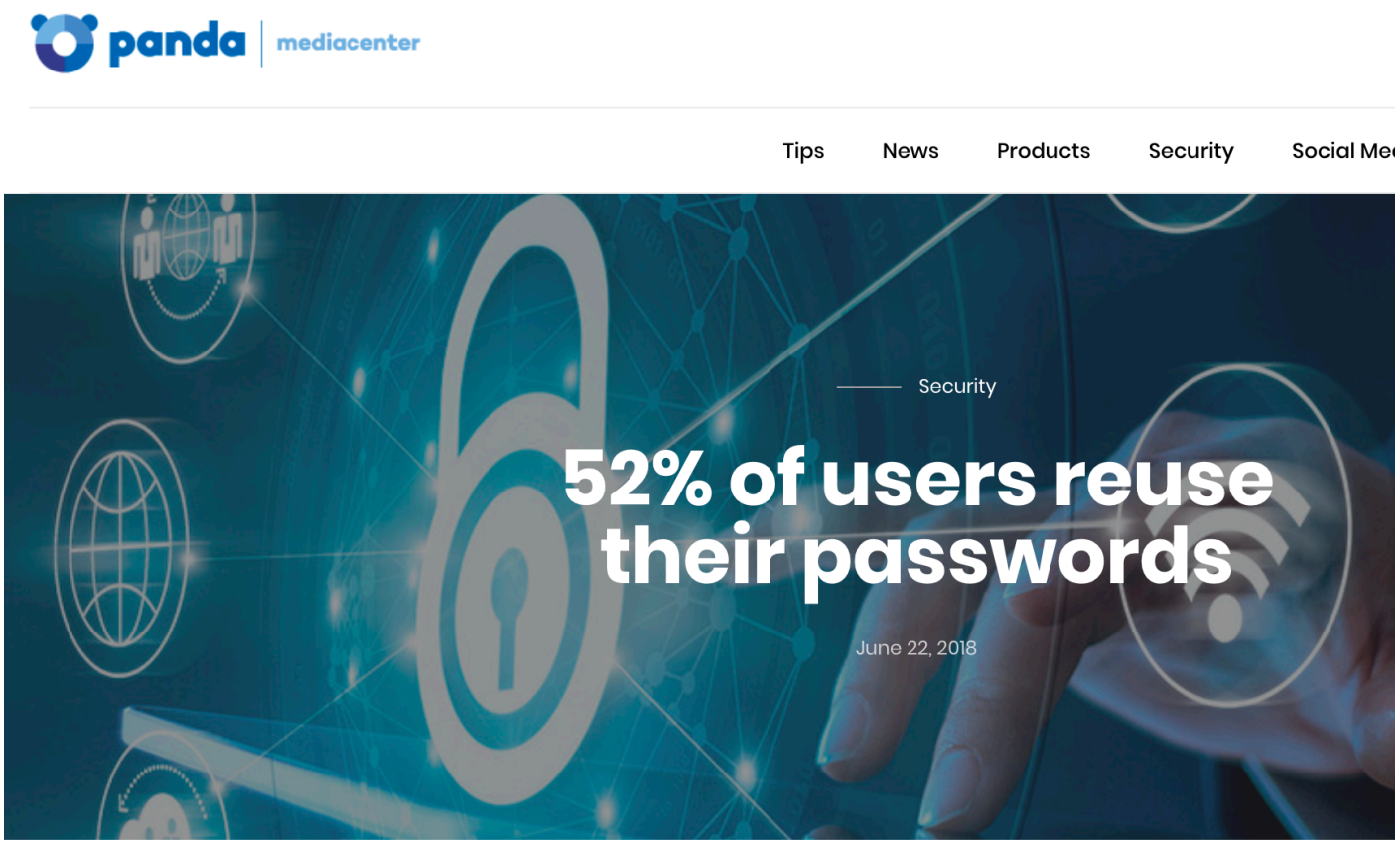
Studying real passwords

- Public password datasets exist
  - For example a 2-million dataset from dazzlepond.com
    - http://datashaping.com/passwords.txt
- Create a usability study
  - Run on Mturk, other crowdsourcing platforms
- Password management by users
  - Observe/interview users
    - How do users choose/save all of their passdwords?

Password Aspects

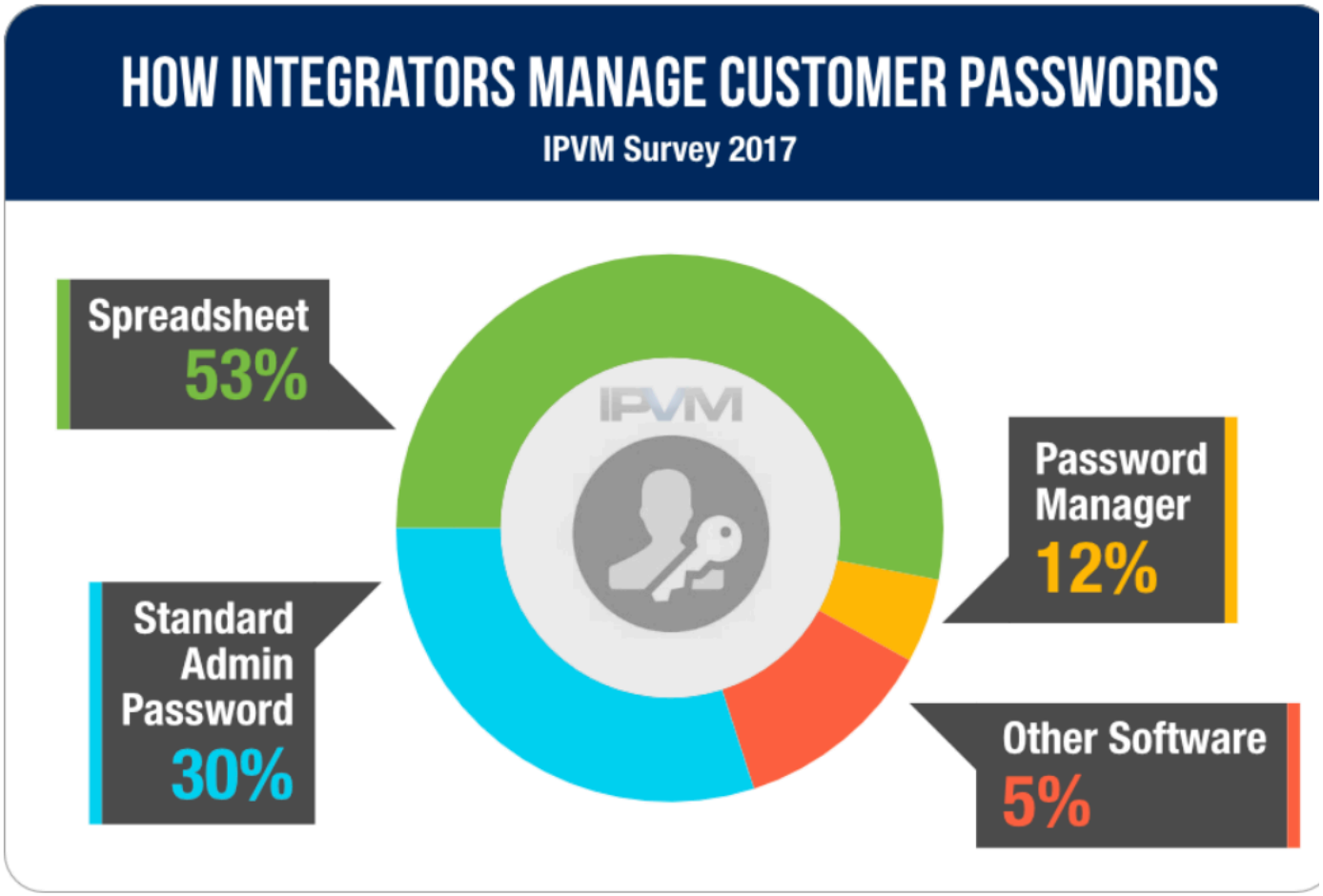
- People to tend to reuse passwords for many applications
  - To help remember passwords
- Practice less secure than writing down passwords
  - Or using a password manager
- Password manager can choose passwords for users
  - How to make them more usable
  - Why

Pass Reuse



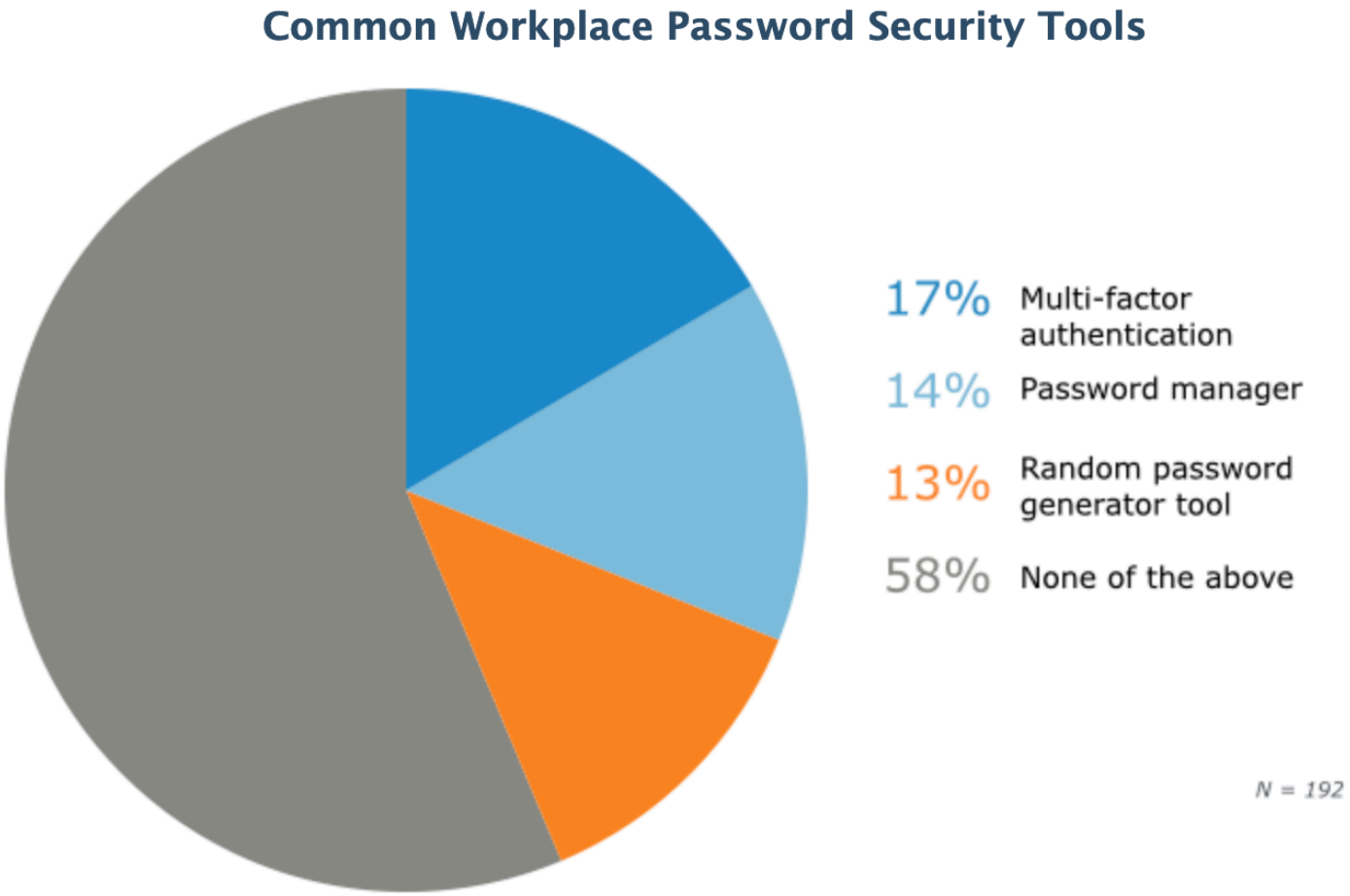
https://www.pandasecurity.com/mediacenter/security/password-reuse/

Password Managers



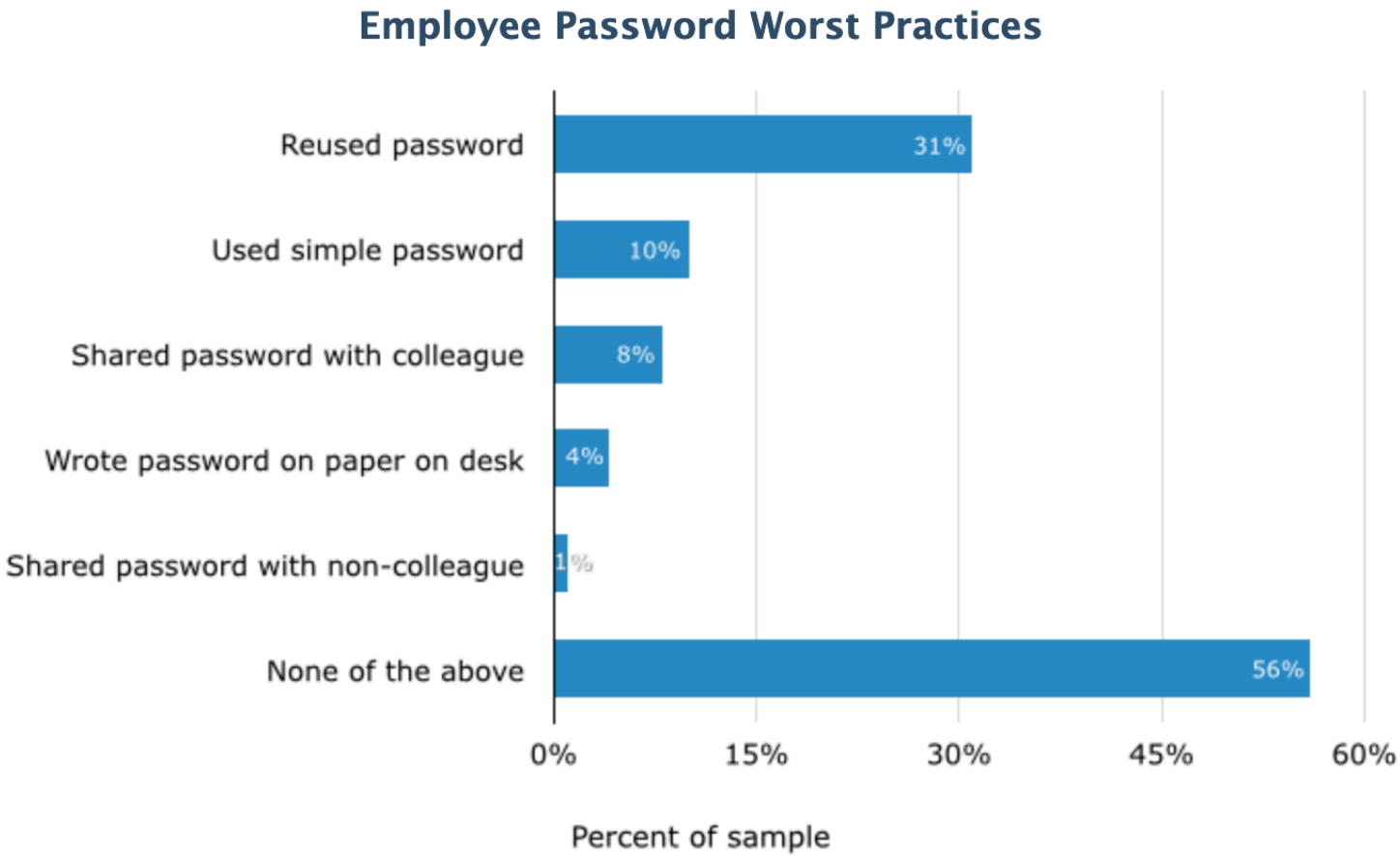
https://ipvm.com/reports/manage-pass

Password Managers



https://www.softwareadvice.com/security/industryview/password-workplace-report-2015/

Password Managers



https://www.softwareadvice.com/security/industryview/password-workplace-report-2015/

Changing Password Regularly

- Many organizations require users to change their password after a certain period
  - Usually a few months
  - To lock out attackers who learned users' passwords
  - Do users choose a secure passwords when choosing a new password?

Changing Password Regularly

- Research found that users tend to make small changes to their existing passwords [Zhang et al CCS 2010]
  - Passwords can be cracked based on knowledge of previous passwords
  - Changes included:
    - Capitalizations of certain characters, duplication, substitution of numbers, etc.

Changing Passwords Regularly

- Research found that users tend to make small changes to their existing passwords [Zhang et al CCS 2010]
  - 17% of passwords cracked in less than 5 guesses
    - Online attack
  - 41% of passwords cracked within 3 seconds
    - Offline attack

Changing Passwords Regularly

- Research found that users who are annoyed at frequent requests will generate weaker passwords
  - Mazurek et al., 2013

Changing Passwords Regularly

https://community.spiceworks.com/topic/1628354-get-your-passwords-are-like-underwear-bumper-sticker

Treat Your Passwords Delicately

- Kaspersky-Passwords

Digital Identity Guidelines

- NIST has recently finalized new guidelines
  Revising password security recommendations
- NIST aims to enhance economic security
  - And improve usability at the same time
    - “improve our quality of life”
- NIST Digital Identity Guidelines

Digital Identity Guidelines

- **Remove periodic password change requirements**
  - Multiple studies have shown requiring frequent password changes to be counterproductive to good password security

Digital Identity Guidelines (cont.)

- **Drop the algorithmic complexity song and dance**
  - No more arbitrary password complexity requirements
    - needing mixtures of upper case letters, symbols and numbers
  - It's been shown repeatedly that these types of restrictions often result in worse passwords

Digital Identity Guidelines (cont.)

- **Require screening of new passwords against lists of commonly used or compromised passwords**
  - One of the best ways to ratchet up the strength of your users' passwords

Choosing Stronger Passwords

- How can we help users choose more secure passwords?
  - Provide guidelines for choosing stronger passwords
  - Find a usable method that we can recommend to users
  - Understand users reasons for choosing certain passwords
    - Do users know how to choose strong passwords?
      - If not, create an application to guide them

Choosing Stronger Passwords

- How can we help users choose more secure passwords? (cont.)
  - Create good feedback methods when asking users to choose passwords
    - Use a password meter, convey to users what is weak in the passwords they chose

Choosing Stronger Passwords

- Some methods users may use to create (unsecure) passwords
  - Keyboard patterns
    - Qwerty
  - Adding ‘!’ At the end of the character
  - Changing a certain character
    - Passw0rd instead of Password
- These methods do not create strong passwords

Choosing Stronger Passwords

- Guidelines for choosing stronger passwords:
  - Don’t reuse passwords
  - Use 2-factor authentication
    - Harder to attack
    - Typically attacker needs access to your device
  - Choose long and unpredictable passwords
    - Don’t use your pet names, family member names, etc.
    - Don’t use birthdates, songs, cars, sports, etc.
  - Make up a sentence
    - Entropy of password is higher

BEYOND TEXT PASSWORD AUTHENTICATION

Beyond text passwords - topics

- What other kinds of authentication are there?
  - Graphical Passwords
  - Multi-Factor authentication
  - Backup authentication – secret questions

Authentication beyond text passwords

- What other kinds of authentication are there?
  - Graphical Passwords
  - Biometrics
  - Hardware Tokens
  - Phone-based authentication
  - Federated ID's
  - Password managers
  - Multi-factor authentication

Authentication beyond text passwords

- What other kinds of authentication are there?
  - Password Recovery
    - Via secret question
    - Via email link
    - Via social authentication
  - Continuous authentication - behavioral authentication
    - Pressure on keys, timing between keys
    - Browsing models, etc.

GRAPHICAL PASSWORDS

Types of graphical passwords

- Recognition
  - Recognizing objects within images
- Pure Recall (memory)
  - Drawing a picture, tracing a pattern, tapping specific points
- Cued-Recall
  - Drawing or taping on top of an image cue

Graphical Passwords Advantages

- Picture superiority effect:
  - pictures and images are more likely to be remembered than words
  - demonstrated in numerous experiments using different methods
  - "human memory is extremely sensitive to the symbolic modality of presentation of event information" [Yullie 2014]
  - Explanations for the picture superiority effect are not concrete and are still being debated

Graphical Passwords Advantages

- Pointing/clicking/tapping/drawing may be easier/faster than typing
- Seems more appealing/fun than text passwords
- May be harder to store or share password
- Less susceptible to phishing attacks

Graphical Passwords Disadvantages

- Doesn't work for vision impaired
- Requires a screen
  - May require a minimum screen resolution
    - May not be appropriate for IoT devices
- Some types may be particularly vulnerable to shoulder surfing
- Design should have a large enough password space
  - Otherwise, passwords may be guessed easily

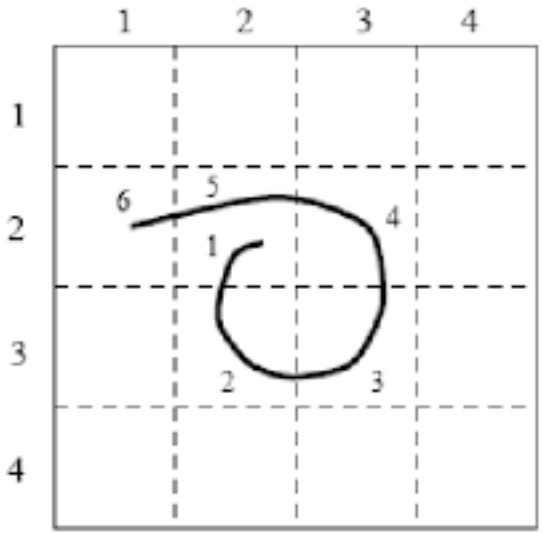
Graphical Passwords Disadvantages

- User chosen systems may be vulnerable to predictable user behavior
- May be harder to store
  - for people who want help remembering

Draw-a-Secret (DAS)

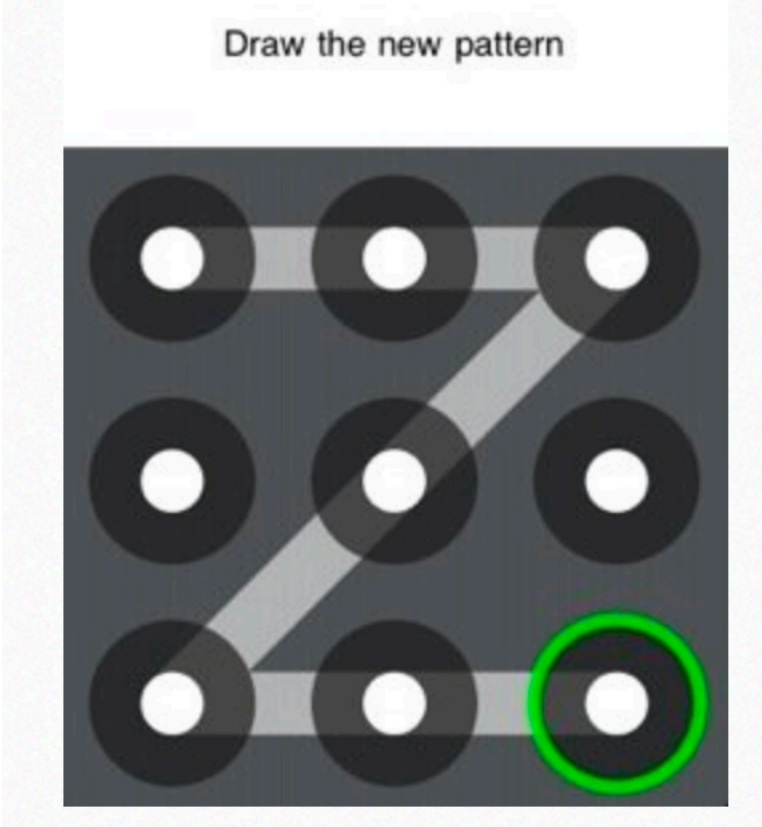
- A graphical password input scheme
  - Developed by Jermyn et al 1999
- Replaces alphanumeric password strings, with a picture drawn on a grid
- Instead of entering an alphanumeric password, this authentication method allows users to use a set of gestures drawn on a grid to authenticate

Draw-a-Secret (DAS)



https://www.researchgate.net/publication/224096712_Pure_and_cued_recall-based_graphical_user_authentication/figures?lo=1

IoS lock pattern



https://geekeasier.com/how-to-add-pattern-lock-to-iphone-ipad-or-ipod/1046/

Passfaces

- Graphical passwords that use faces as a unique verification technology for secure logon.
- Offering two factor authentication

Passfaces

- An individual is assigned a set of five faces
- Given an orientation session to imprint those faces into his brain
  - usually lasting two to four minutes
- Studies show that a person can recognize a distinct face years after first exposure to that face

Passfaces

- Authentication phase:
  - Single round:
    - The user is presented with a grid of nine faces
    - Only one face on the grid is from the user's unique set of faces
      - the rest are decoys.
    - User must select his specific face on the grid to get passed the digital gate

Passfaces

- Authentication phase:
  - This process continues for the other four faces of his set.
  - If user fails to recognize or select all of his faces, he is taken back a step to try again
  - If too many failures occur, he is locked out of the application.

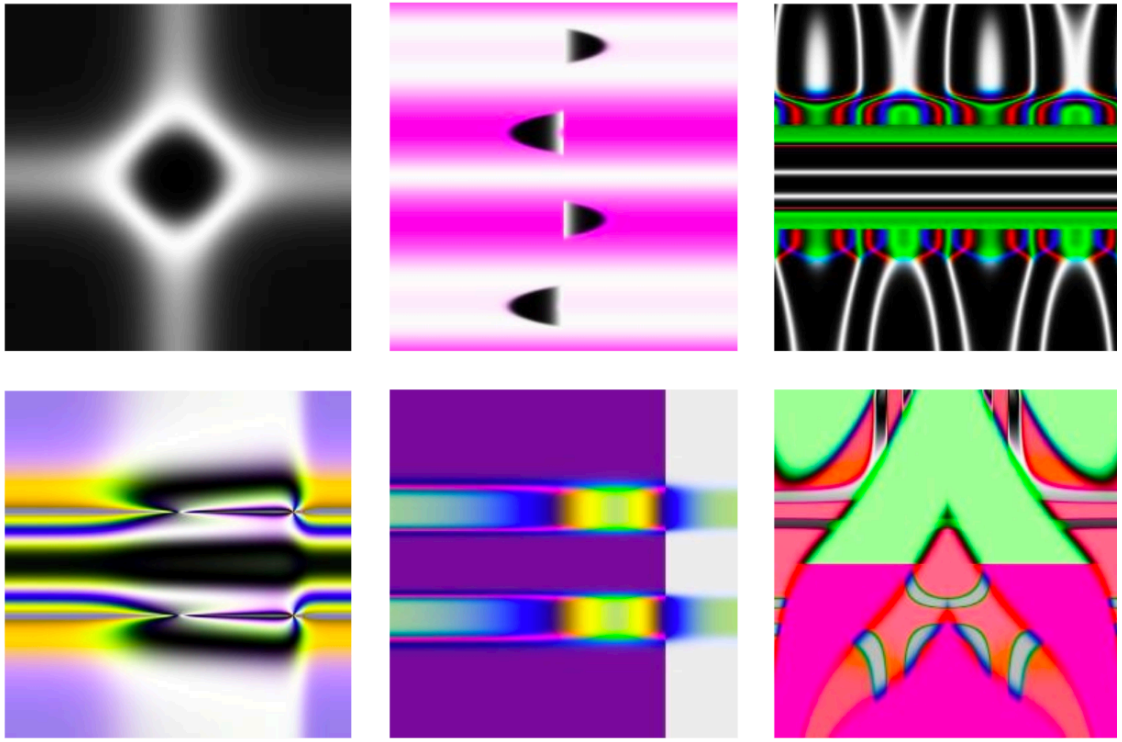
Passfaces

http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf

Deja-Vu [Dhamija and Perrig 2000]

- Approach relies on *Recognition-based*
  - rather than *recall-based* authentication
- Authenticates a user through her ability to recognize previously seen images
- Advantages:
  - prevents users from choosing weak passwords
  - makes it difficult to write down or share passwords with others

Deja-Vu [Dhamija and Perrig 2000]



https://www.usenix.org/legacy/events/sec2000/full_papers/dhamija/dhamija.pdf

Deja-Vu

- Research showed higher usability than traditional passwords and pins
- Create/login time longer than traditional passwords
  - But higher password memorability

Deja-Vu

	PIN	Password	Art	Photo
Create	15	25	45	60
Login	15	18	32	27
Login (after one week)	27	24	36	31

Table 1: Average seconds to create/login

	PIN	Password	Art	Photo
Failed Logins	5% (1)	5% (1)	0	0
Failed Logins (after one week)	35% (7)	30% (6)	10% (2)	5% (1)

Table 2: % Failed logins (# failed logins/20 participants)

Passpoints [Wiedenbeck et al 2005]



Passpoints [Wiedenbeck et al 2005]

- Relies on recognition and cued-recall
- Study compared usability and security in comparison to choosing an 8-character alphanumeric password

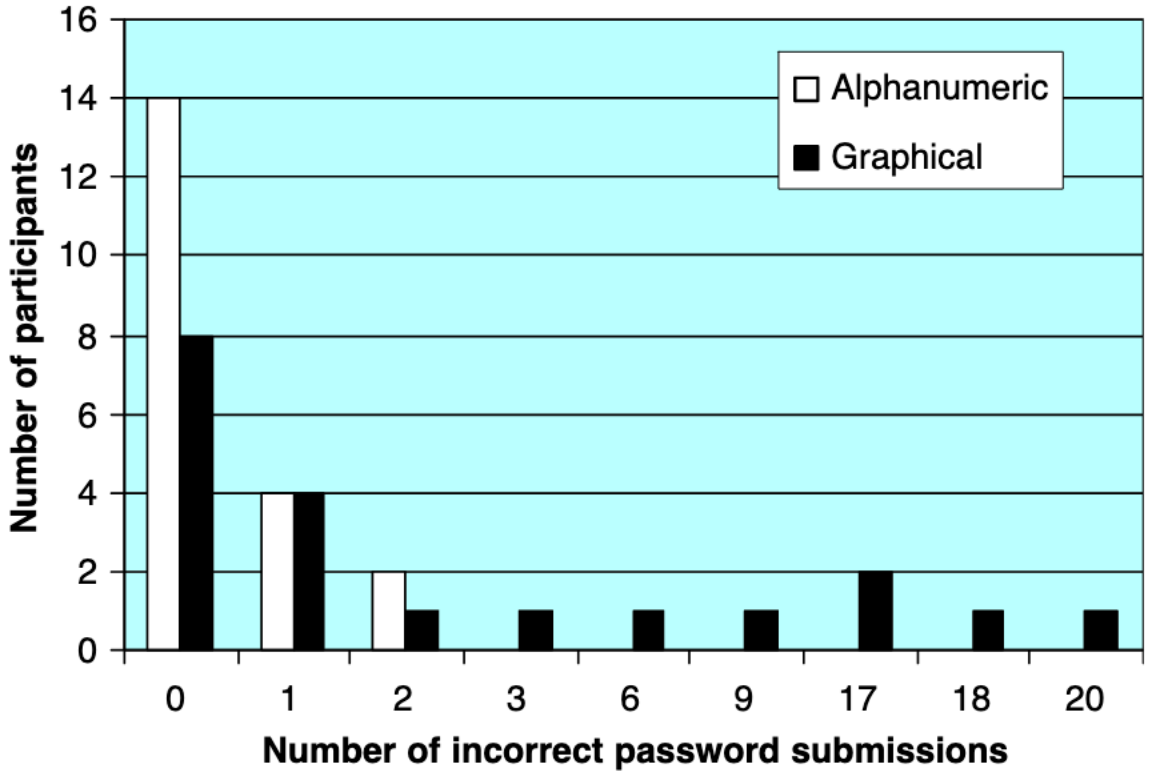
Passpoints [Wiedenbeck et al 2005]

- Password creation:
  - Users select and enter five distinct points on the picture
    - with no point within the tolerance around any other chosen point
    - Provide a password space about as large as or larger than an alphanumeric password of eight characters
  - Participants told that they would have to remember the points and the order in which they were input
  - To reinforce the password the user entered the password repeatedly
    - until he or she achieved ten correct password inputs.

Passpoints [Wiedenbeck et al 2005]

- Password Retention Testing:
  - User had to enter the password correctly one time
  - Repeated once at the end of the first session
  - Then after 2 and 6 weeks

Passpoints [Wiedenbeck et al 2005]

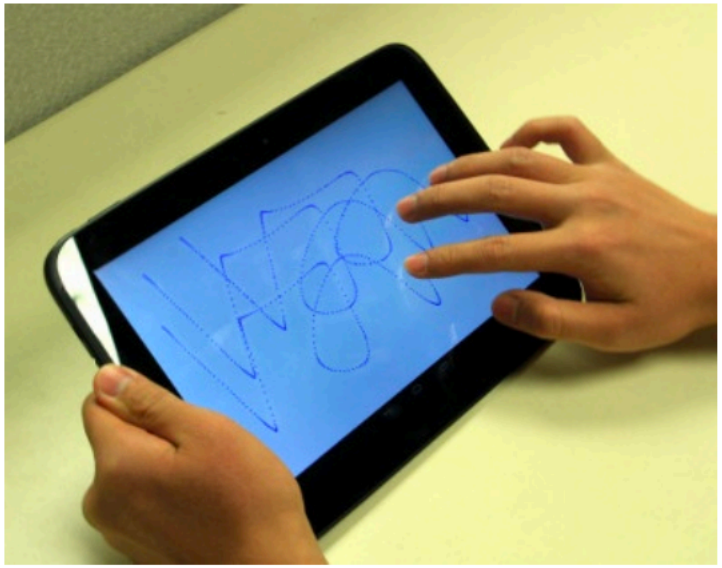


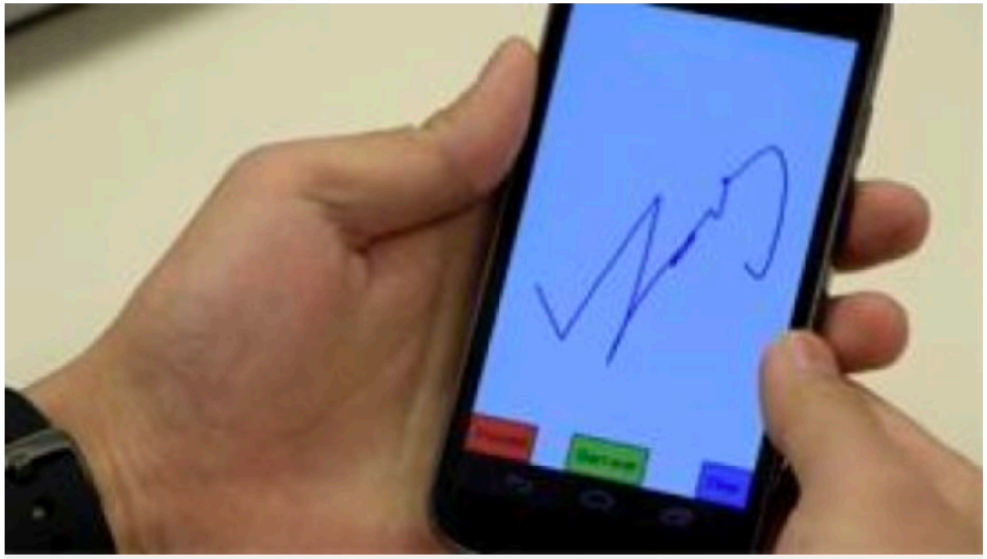
Windows 8 picture password

Squiggly Lines [Lindqvist 2018]

- Squiggli Lines PBS
- Squiggly Lines

Squiggly Lines





https://www.sciencedaily.com/releases/2016/03/160310082606.htm

Yulong Yang, Gradeigh D. Clark, Janne Lindqvist, Antti Oulasvirta. **Free-Form Gesture Authentication in the Wild**. *Association for Computing Machinery's Conference on Human Factors in Computing Systems*, 2016 DOI: 10.1145/2858036.2858270

BIOMETRICS

Types of Biometrics Available

- Fingerprint
- Face
- Hand geometry
- Voice
- Handwriting
- Iris
- Retina
- Heart rhythm
- Keystroke dynamics
- Gait

Advantages

- Your fingerprint is your ID
- Your fingerprint is pretty unique
- Your finger is convenient to carry
  - Is biometrics the ultimate authentication solution?

Issues and limitations

- High accuracy may requires expensive and large special equipment
  - But hardware is becoming less expensive and more available
- Some biometrics difficult to capture under some conditions
  - low light, dry skin, injury, etc.
- Some biometrics change over time

Issues and limitations

- May increase value of a person's body parts to an attacker
  - May induce crime
- May be difficult to cancel or reset
  - You only have one set of fingerprints!
- May leak personal information
  - Age, ethnicity, etc.
- Privacy concerns

Biometric Standards

- NIST Biometrics Standards

MULTI-FACTOR AUTHENTICATION

Multi-Factor Authentication

- So far we discussed single-factor authentication
- Has some disadvantages:
  - A token works as long as you don’t give it away
  - Password can be guessed or eavesdropped on
  - We can compensate by combining both

Multi-Factor Authentication

- Driver license combines two authentication methods:
  - What you have
    - the card itself
  - Who you are
    - Your picture, signature

Multi-Factor Authentication

- Authentication may use more than one factor
  - Two, three, etc.
  - We assume that two are better than one
  - However, usability has to be maintained!
    - Not to cause inconvenience to user

Multi-Factor Authentication

- Advantages:
  - Adds extra layer of security on top of passwords
  - Stealing a password is not enough
  - Usually does not rely on human memory

Advantages and Disadvantages

- Disadvantages
  - Slows down login process
    - Some are slower than others
  - Hardware tokens cost money, inconvenient to carry, might be lost
  - Some vulnerable to certain types of attacks
    - Man-in-the-middle, Phone hijacking, Social engineering

Security of TFA

- More secure
- Stops most hacking attacks
- Users perceive it as more secure

Usability of TFA

- Research shows that:
  - TFA is slower
  - Users feel it is less usable
  - Less convenient
  - Harder to use

Conclusion

- TFA is perceived as more secure, less usable

BACKUP AUTHENTICATION

Secret Questions - Motivation

- Inexpensive
  - Helps avoid helpdesk call
- Webmail providers can use email for reset only if user has another email account
  - New users may not have those
- Intuitively seems easy
  - Is it?
- Should be secure
  - Studies suggest it is not [Bonneau 2015]

Secret Questions Study*

- Used real-world Google large dataset [Bonneau 2015]
- Users often don't answer questions truthfully
  - Users share some answers which make them weaker
    - Easier to guess
- Poor memorability
  - 40% were not able to remember passwords

* Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google [Bonneau et. Al 2015]

Secret Questions Study 2

- User study for 4 webmail providers [Schechter et. Al 2009]*
  - AOL, Google, Microsoft, and Yahoo
- 17% of user acquaintances able to guess their answers
  - participants unwilling to share passwords with these acquaintances
- Participants forgot 20% of their answers within six months
- 13% of answers could be guessed within five attempts
  - by guessing the most popular answers of other participants
    - partially attributable to the geographic homogeneity of our participant pool

* It's No Secret. Measuring the Security and Reliability of Authentication via “Secret” Questions [Schechter et. Al 2009

AOL Secret Questions

- What is your pet's name?
- Where were you born?
- What is your favorite restaurant?
- What is the name of your school?
- Who is your favorite singer?
- What is your favorite town?
- What is your favorite song?
- What is your favorite film?
- What is your favorite book?
- Where was your first job?
- Where did you grow up?

Google Secret Questions

- What is your primary frequent flier number?
- What is your library card number?
- What was your first phone number?
- What was your first teacher’s name?

Microsoft Secret Questions

- Mother's birthplace
- Best childhood friend
- Favorite teacher
- Favorite historical person
- Grandfather's occupation

Yahoo Secret Questions

- Where did you meet your spouse?
- What was the name of your first school?
- Who was your childhood hero?
- What is your favorite pastime?
- What is your favorite sports team?
- What is your father's middle name?
- What was your high school mascot?
- What make was your first car or bike?
- What is your pet's name?

Yahoo Hack [2014]

- “a copy of certain user account information was stolen from the company’s network”
- “The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, ***encrypted or unencrypted security questions and answers***.”

Yahoo 2014

Security questions

Time to Kill Security Questions—or Answer Them With Lies

Please Reset Your Mother's Maiden Name

https://www.wired.com/2016/09/time-kill-security-questions-answer-lies/

Recommendations

- Lock out users who make incorrect but popular guesses
- Remove most easily guessed questions
- Disallow popular answers
- Occasionally ask secret questions after user has logged in successfully

Expert Recommendations

- Stop using secret questions

Can we do better?

- Working in groups, come up with 3 secret questions and/ or an alternative approach to backup authentication
- Write them on the board
- We'll discuss them in class

WebAuthn

- A new Official Web Authentication API standard [March 4, 2019]
  - Enables password-free login
- WebAuthn

WebAuthn

- User Registration and Initialization:
  - Users registers to a website
  - User chooses an authenticator
  - Security key, biometrics, etc.
- User Authentication:
  - User will authenticate to the service of choice
  - Choosing multiple authenticators enables password recovery

WebAuthn

- Challenges:
  - Are users likely to accept biometrics?
    - Biometrics is kept securely on user device and not sent to server
  - Adoption by individual service providers may take time
    - Will security industry support the new standard

Questions?

Questions?