
http://www.arcamax.com/zits

# Graphical Passwords

October 5, 2010 - COMP 5407F

Sonia Chiasson – chiasson@scs.carleton.ca
http://hotsoft.carleton.ca/~sonia



## I'm not paul

- Post-doctoral fellow in computer science
- PhD – computer security and human-computer interaction
- Research – usable security, persuasive technology, serious games

- Graphical Passwords: Learning from the First Twelve Years, Biddle, Chiasson, and van Oorschot. (manuscript, Sept.27, 2010; earlier version as Technical Report TR-09-09, Carleton University, School of Computer Science, Oct.2, 2009

# Why is usability so important?

- An unusable security system will be inherently insecure
- Technical soundness does not matter if people cannot use the system properly or bypass it altogether

3

# Are humans the weakest link?

- Most security breaches attributed to “human error”
- Social engineering attacks proliferate
- Frequent security policy compliance failures
- Automated systems are generally more predictable and accurate than humans

4

# Challenges for users

- Everyday users are not security experts, nor should they be
- Security gets in the way of regular tasks
- Security advice is ever-changing
- Security burden on users is too high

5

# Authentication vs. Authorization

- Authentication: securely identifying users
  - Who is this?
  - Are they really who they say they are?
  - “shared secret” between the user and the system
- Authorization: determining the level of access/privileges/permissions provided
  - Are they authorized to access this resource?
  - Are they authorized to perform this action?

6

# Authentication

- Knowledge-based – something you know
  - passwords
- Token-based – something you have
  - Smart cards
- Physical biometrics – something you are
  - Fingerprints, iris scans, facial recognition
- Behavioural biometrics – something you do
  - Signatures, voice recognition, typing patterns

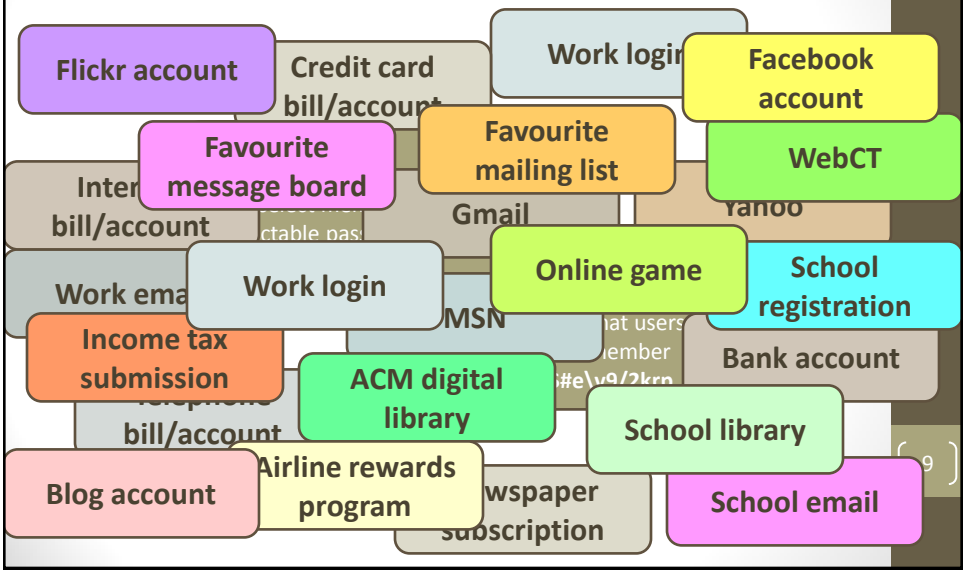
7

# Authentication

- Knowledge-based authentication unlikely to disappear
  - Inexpensive, simple to implement
  - Avoid privacy issues
  - Portability
- Need to balance security and usability
  - Attacks: guessing (general or targeted, dictionary), shoulder-surfing
  - Usability: memorability, interference, ease-of-use

8

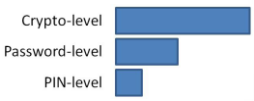
# The Password Problem




9

# Password spaces

- Theoretical password space
  - The total number of all possible passwords
  - Text passwords:
    - 95 typeable characters on English keyboard
    - 8 character passwords
    - → $95^8 = 2^{53}$
- Effective password space
  - The subset of passwords that are chosen by users
  - Shaped by user choice, not mathematical formulas, difficult to estimate
  - Text passwords:
    - Dictionary words, proper names, words + number, keyboard patterns
- Typically reported in bits → $2^{53}$ = 53 bits




10

# Password hashing

- Passwords should not be stored in clear text
- A cryptographic one-way hash is used
  - System does not "remember" the actual password
  - Crypto hash: easy to compute, infeasible to reverse, infeasible to find different messages with same hash, infeasible to modify message without affecting its hash
- During login
  - User input is hashed
  - Hashed value is compared to stored hash
  - If match, login accepted

11

# Guessing attacks

- Exhaustive/brute force attack
  - Systematically trying all elements in a search space
  - May optimize by guessing shorter passwords, or higher probability passwords first
  - With enough time and processing power, all passwords will be guessed
  - Defenses:
    - Online attack: can limit number of guesses per account
    - Offline attack: iterative hashing and salting can slow guessing

12

# Guessing attacks

- Dictionary attacks
  - Guessing passwords using a relatively short pre-compiled list/dictionary of high-probability passwords
  - Based on empirical evidence (passwords from sample population) or assumptions about user behaviour
  - Ordered from highest probability passwords first
  - Exploits patterns in user choice
  - Automated tools like John the Ripper and RainbowCrack

13

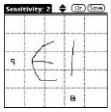
# Capture attacks

- Shoulder-surfing :
  - using direct observation or external recording devices to gain knowledge of password
- Malware
  - Unauthorized software which can capture user input
  - Mouse-loggers, screen scrapers, key-loggers
- Phishing
  - Tricking users into entering their credentials at fraudulent sites
- Social engineering
  - Tricking users into revealing their credentials by any means

14

# Why Graphical Passwords?

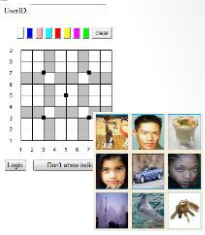
- Psych studies demonstrate superior memory for visual information (pictorial superiority effect) (Kirkpatrick,1894; Shepard,1967; Madigan, 1983)
- Paivio's dual-coding theory (Paivio, 2006)
  - Images mentally represented perceptually and symbolically
- Graphical passwords take advantage of this characteristic

15

# Graphical password categories

- Recall (drawmetric)
  - Users must recall and reproduce a secret drawing
  - No cue or memory prompt
- Recognition (cognometric)
  - Users memorize a portfolio of images and must recognize their images from among decoys
  - Humans have exceptional ability to recognize previously viewed images, even when seen only briefly
- Cued-recall (locimetric)
  - Users remember and target specific locations within images
  - Cue triggers memory of the password




16

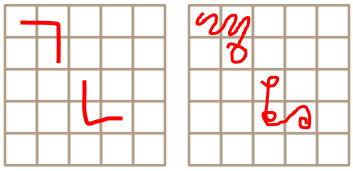
# Applicability

- Most schemes still in the research arena
  - Lack security or usability evaluation, or have major flaws that must be addressed
- Commercial products:
  - Passfaces
  - Smart phone screen unlock
  - grIDsure


17

# Recall: Draw-A-Secret

- Drawing: one or more pen strokes separated by pen-up events
- Encoding: sequence of grid cell coordinates and pen-ups
  - 1,1,1,2,2,2,9,9,3,3,4,3,4,4,9,9
  - Password length = 6
  - Many-to-one mapping

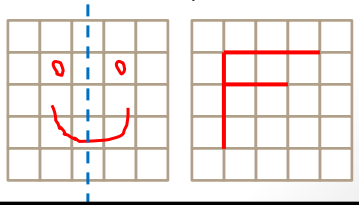


- Theoretical password space
  - Based on coarseness of the grid, password length
  - 5x5 grid, max password length of 12
  - → 58 bits

18

# Recall: Draw-A-Secret

- User choice issues (Pass-Go)
  - Preference for symmetric passwords with few strokes
  - 40% passwords symmetric about the vertical or horizontal axis
    - 72% passwords had 4 or fewer strokes
    - 19% passwords were alphabetic characters or symbols
  - Passwords not equi-probable
  - Dictionaries including these 3 subsets range from 31-41 bits
- Observation risk
  - Observing one login instance reveals the entire password
- Phishing
  - No server probes needed



19

# Recognition: PassFaces

- Users select portfolio face from panel of decoy faces, repeats for several panels.
- Images in a panel remains constant between logins but image positions are shuffled
- System must retain knowledge of images
- Typical configuration
  - 4 panels, 9 faces per panel
  - User portfolio contains exactly 4 images
  - Theoretical password space:
    - Based on number of panels and number of faces per panel
    - → $9^4 = 6561 = 2^{13}$
    - Comparable to PINs
    - To make comparable to 6-character lowercase passwords
    - → 6 panels of 26 faces = $2^{28}$

20

# Recognition: Passfaces

- User choice issues
  - Attractive female faces of their own race
  - Knowing one face, could predict next face likely selected
  - 25% of passwords guessed in 13 attempts
  - Weakest 10% of passwords guessed in 2 attempts (male participants)
  - Solution: system-assigned passwords
- Observation risk
  - One login enough to reveal entire password
- Phishing requires either
  - earlier server probe to get user's images
  - Man-in-the-middle attack relaying info between phishing site and legitimate site

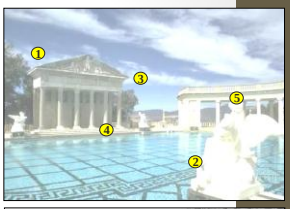
21

# Recognition: Convex Hull Click

- At each round, users must recognize their icons, form an imaginary triangle between them, click within the triangle.
- Portfolio images are assigned
- System retains knowledge of icons
- Theoretical password space = 32 bits
- Observation
  - Would require many logins to learn entire user portfolio
- Phishing
  - Many server probes to get all of the icons in the user portfolio
  - Man-in-the-middle needed

22

# Cued Recall: PassPoints




- Password is a set of ordered clicks on one image
- Login clicks must be in order and within system-defined tolerance area
- Discretization needed for password hashing while allowing approximately correct entries
- Theoretical password space
  - 451x331 pixel image, 5 clicks, 19x19 tolerance
  - $((w * h) / t^2)^c = ((451x331) / 19^2)^5 = 2^{43}$

| Image size | Tolerance size | Number of click-points | Password space |
|---|---|---|---|
| 451 x 331 | 19 x 19 | 5 | 43 |
| 1024 x 768 | 19 x 19 | 5 | 56 |
| 451 x 331 | 13 x 13 | 6 | 59 |
| 1024 x 768 | 13 x 13 | 6 | 73 |

# Cued Recall: PassPoints

- User choice issues
  - Hotspots: areas with higher probability of being chosen
  - Geometric patterns: lines or patterns formed by the user's click-points with higher probability of being chosen
  - "Human-seeded" dictionary attacks guessed 4-10% passwords within 100 guesses
  - 48-54% passwords guessed with 35-bit dictionary of patterns
- Observation
  - One observation is enough to collect password
- Phishing
  - One earlier server probe to retrieve user's image


24

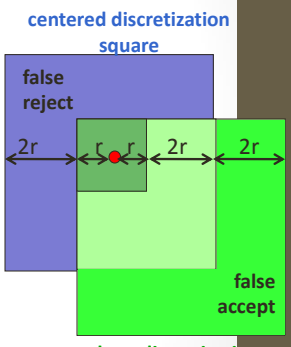
# Robust vs Centered Discretization

**Robust**

- Proposed by Birget et al. for use with PassPoints
- Features:
  - r = minimum acceptable tolerance (in pixels)
  - Uses 3 grids, squares are 6r x 6r
- Post-hoc analysis
  - 13x13 tolerance, 21% false reject rate
  - Dictionary attack at r=6 pixels guessed 45% of click-points

**Centered**

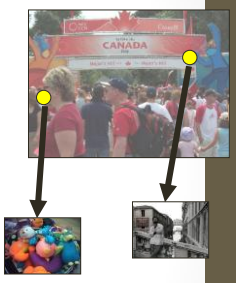
- Proposed by Chiasson et al.
- Features:
  - Uniform tolerance around click-points
  - Behaviour is more predictable by users
  - Eliminates "false accepts" and "false rejects"
- Post-Hoc Analysis
  - Dictionary attack at r=6 guessed 14% of click-points




25

# Cued Recall: Cued Click-Points (CCP)

- Passwords consist of
  - 1 click-point per image
  - Next image determined by current click-point
  - No order to remember
- One-to-one cued-recall
- Implicit feedback
  - Useful only to legitimate users, not attackers




26

# Cued Recall: CCP

- User choice issues
  - Hotspots remain an issue, but require significantly more work for attackers
  - Patterns eliminated
- Observation
  - One observation is enough to get password
- Phishing
  - Requires multiple server probes to get all of the images or man-in-the-middle

27

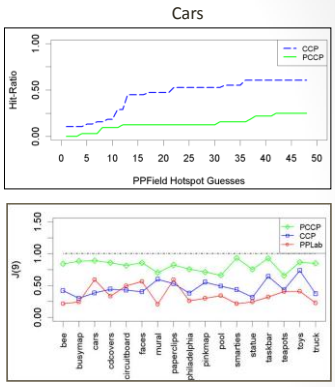
# Cued Recall: Persuasive Cued Click-Points (PCCP)

- Similar to CCP
- Safe-path-of-least-resistance
  - Addition of viewport to influence user choice
  - Shuffling allowed
  - Persuasive technology


28

# Cued Recall: PCCP

- User choice:
  - Dictionary attack
    - PCCP click-points do not fall into known hotspots
  - Spatial statistics
    - J-statistic: measures the spatial distribution of a dataset (Baddeley & Turner, 2005 )
    - PCCP click-points not forming new hotspots
  - No hotspots, no patterns




29

# Usability

- Multiple password interference
  - Memory of one password interferes with memory of other password
  - What about interference from decoys? What about password changes?
- Ease of use
  - Login times, login success rates, memorability
  - Number and types of errors
    - Dangerous errors can affect security
  - Feedback to legitimate users without leaking info to attackers
- User studies are necessary
  - Evaluate usability, practical security

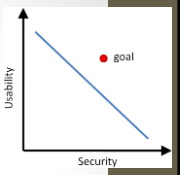
30

# Evaluation checklist

1. Are target users, domains, and applications clearly identified?
2. Are evaluation parameters, and the theoretical password space, clearly stated?
3. Does the analysis explain the effect of user choice on password distributions, with discussion of the effective password space?
4. Does the analysis consider the full range of attacks plausible in the targeted domain and application?
5. Has at least a lab user study been done (or other types of higher ecological validity), with results compared to appropriate alternatives?
6. Is password interference discussed (e.g., as informed by a user study)?
7. Do the user study and security analysis use the same parameters?

31

# Desirable characteristics for knowledge-based passwords




1. Theoretical password space sufficiently large for its intended domain.
2. Avoidance of exploitable reductions in security due to user choice of passwords, e.g., through persuading password choice towards flatter distributions.
3. At least mild resistance to different types of capture attacks including shoulder surfing and key logging, through variable response (challenge-response) design.
4. Cues aiding memorability, design features minimizing password interference.
5. Usability as close as possible to text passwords (e.g., login success rates, login times, password creation times).
6. Implicit feedback to legitimate users, when passwords are multi-part.
7. Leveraging of pre-existing user knowledge where possible, rather than having users memorize entirely new and/or random information.

32