Graphical Passwords

Aaron Cutright and Ryan Oshinsky

Definition and Purpose

- An Authentication scheme that works by having the user interact with an image or set of images in a specific pattern to confirm their identity
- The purpose is to increase memorability over a traditional alphanumeric password without sacrificing security
- This could increase entropy in the areas that traditional passwords fail, mainly due to people choosing easy-to-remember strings that are just as easy to crack

Common Graphical Password Schemes

- Select Images from a group [4, 5]
- Gesture Authentication
  - Free-form [1]
  - Grid based [8]
- Passpoints [2]
- Cued click points [6]

Selecting Images from a Group

User selects a number of images from a group

Interference of similar images can cause issues with visual memory

Entropy depends on the number of images in the database and number of images selected

De Angeli et al., 2005

Grid Based Gesture

User creates a pattern on a grid of fixed points

Easy to recreate pattern for log in recognition,password is dependent on fixed points

Entropy cannot easily be increased with the size of the grid

- Users tend to choose non-complex password (like text-based)
- Guessability decreases with size of grid
- Beyond 4x4 grid does not create much change, but ease of entering password decreases since contact points become more dense

Free-Form Gesture

Password is generated from a user drawn gesture

“Free-form gesture passwords are faster to perform, faster to create, faster to log in, and have strong log-in success rates” compared to text passwords

Entropy is related to number of cells on screen and number of points in gesture

Mainly usable only on mobile devices or touch screens, difficult with mouse

Common shapes or patterns can be easy to predict

PassPoints

Password defined by a sequence of points selected by a user over an image

Can be easy to remember and reproduce

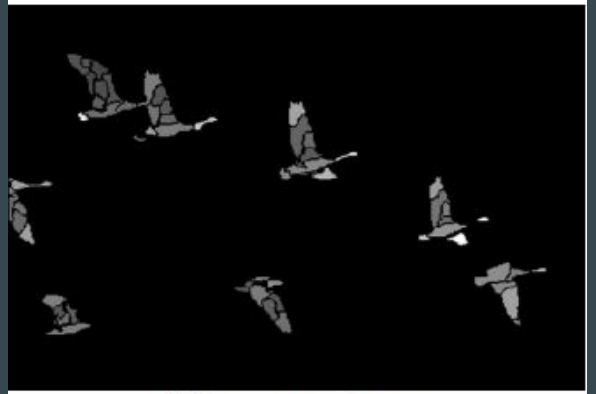
Easy to model user choice and the entropy of click points

Vulnerable to dictionary attacks based on Focus of Attention (FOA) maps

Can use model of user choice entropy to select suitable underlying images

(Dirik et al.,2007) “Modeling user choice in the PassPoints graphical password scheme”

(a) Original image



(b) Focus of attention map

Cued Click Points

Password is determined from users clicking on a point per image for a series of images

The next image is determined by the click location on the last image

Greater memorability over passpoints because only one point needed to be remembered per image

Requires more work for attackers, need to acquire image sets for each user and do hotspot analysis on entire image set

Technique	Process	Memorability	Password Space	Attack methods
Text based	Type in password	Longer random passwords can be difficult	94^K	Dictionary attack, brute force search, guess, spyware, etc.
Select images from a group	Select multiple images from a group	More memorable than text	N choose K N = group, K = images	Brute force search, guess
Grid Based Gesture	Draw something on a 2D grid	Depends on what users draw. User studies showed the drawing sequence is hard to remember	Larger than text based, but decreases significantly with fewer strokes for a fixed password length	Dictionary attack
Free-form gesture	Draw something on top of an image or canvas	Depends on what users draw	N! N = precision required	Guess, dictionary attack
PassPoints	Click on several locations of a picture in the right sequence	Depends on what users draw	N^K N =pixels , K =clicks	Guess, brute force search, FOA maps
Cued Click Points	Click on a single point in a series of images	Easier to remember than passpoints	N^K N=grid-px, K=clicks	Guess, brute force search, FOA maps

Our Implementation

Sources

[1] Yang Y, Clark G. D., Lindqvist J., Oulasvirta A. 2016. *Free-Form Gesture Authentication in the Wild.* CHI'16, May 07 - 12, 2016, San Jose, CA, USA. http://winlab.rutgers.edu/~janne/CHI16-ESMgestures.pdf

[2] Dirik A. E., Memon N., Birget J. 2007. *Modeling user choice in the PassPoints graphical password scheme.* https://cups.cs.cmu.edu/soups/2007/proceedings/p20_dirik.pdf

[3] Gyorffy J. C.,Tappenden A. F., Miller J. 2011.*Token-based graphical password authentication.* International Journal of Information Security. http://link.springer.com/article/10.1007/s10207-011-0147-0

[4] Davis D., Monrose F., Reiter M. K. 2004. *On User Choice in Graphical Password Schemes* https://users.ece.cmu.edu/~reiter/papers/2004/usenix2.pdf

[5] De Angeli A., Coventry L., Johnson G., Coutts M. 2003. *USABILITY AND USER AUTHENTICATION: PICTORIAL PASSWORDS VS. PIN.* Contemporary Ergonomics, Taylor & Francis pp. 253-258 http://www.antonella_de_angeli.talktalk.net/files/Pdf/USABILITY%20AND%20USER%20AUTHENTICATION%20PICTORIAL%20PASSWORDS%20VS%20PIN.pdf

[6] Chiasson S., Van Oorschot P. C., Biddle R. 2007. *Graphical password authentication using cued click points. ESORICS'07 Proceedings of the 12th European conference on Research in Computer Security. 359 -374.* http://dl.acm.org/citation.cfm?id=2393880&preflayout=flat https://www.ccsl.carleton.ca/paper-archive/chiasson-esorics07.pdf

[7] Suo X., Zhu Y., Owen G. S. 2005. *Graphical Passwords: A Survey. Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005) .* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1565273

[8] Aviv A. J., Budzitowski D., Kuber R. 2015. *Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. ACSAC 2015 Proceedings of the 31st Annual Computer Security Applications Conference. DOI = http://dl.acm.org/citation.cfm?doid=2818000.2818014* http://www.usna.edu/Users/cs/aviv/papers/aviv-acascl5.pdf