Dylan Kapnias (u18108467) – COS 330 Practical 2

Graphical Password Authentication

Graphical password authentication is a type of password authentication that uses an ID (such as username or unique number identifier) for identification, and the relying party uses a combination of ID and an authenticated password for authorization.

This works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). This can generally be broken down into 3 different methods:-

- Drawmetric - Where the user creates and/or recreates a secret drawing. Android's *Patternlock* and Microsoft Window's *Picture Password* are examples.
- Searchmetric - Where the user must select an already known image from a selection of other images (distractors).
- Locimetric - Where a user must recall a sequences of pixel positions within an image.

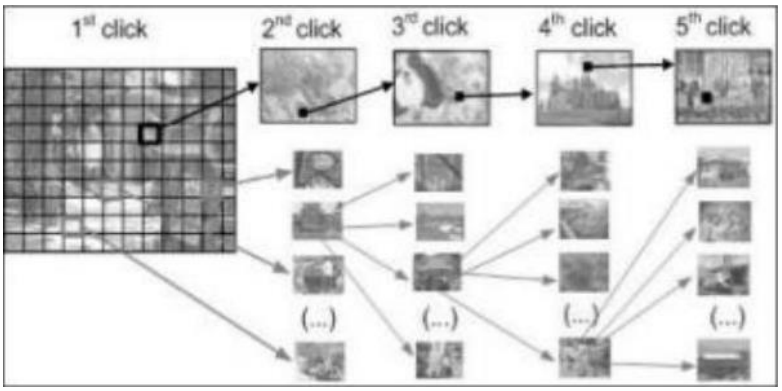

Fig 1: Example of a Locimetric authentication [1]

Possible attack vectors on graphical user authentication (GUA) are/and can attempt to be mitigated by:

- Brute Force attacks - Whereby the attack attempts to guess the password either by using a pre-defined dictionary of passwords or by simply making educated guesses. Prevention tactics could possibly be to have a large enough password space to make brute force impractical [2].
- Shoulder surfing - Whereby the attacker simply watches over your "shoulder" when you input the password, and later replicates it. Due to this mainly being a social issue, the only prevention tactics would be to educate the user into being more cautious when using the password.

References

[1] Towseef Akram et al, International Journal of Computer Science and Mobile Computing, 6(6), June-2017, pg. 394-400, https://www.ijcsmc.com/docs/papers/June2017/V6I6201784.pdf

[2] Robert George Rittenhouse et al, International Journal of Security and its Applications, 7(3), January-2013, pg. 347-356, https://www.researchgate.net/publication/237048875_Security_in_Graphical_Authentication