# Examining Visual-Spatial Paths for Mobile Authentication

David Lu
davidl1@andrew.cmu.edu

Taehoon Lee
taehoonl@andrew.cmu.edu

Sauvik Das
sauvik@cmu.edu

Jason Hong
jasonh@cs.cmu.edu

Carnegie Mellon University
5000 Forbes Avenue, Pittsburgh, PA, USA, 15213

## ABSTRACT

Inspired by people's strong memory for visual-spatial paths (e.g., commuting paths), we present in this paper an introductory exploration of the use of these paths for memorable, strong mobile authentication. In a preliminary study, we evaluated several low-fidelity representations for encoding relatively strong (~20 bit) secrets as visual-spatial paths: a 2D birds-eye view, a 3D third-person view, and 3D immersed view. We found that the 3D immersed view worked best for memorability, and used this initial study to inspire the design for a novel mobile authentication application: the Memory Palace. We ran a within-subjects experiment to evaluate our Memory Palace authentication concept against Android's 9-dot Patternlock along two dimensions: memorability and resilience to shoulder surfing. Results from our experiment suggest people have significantly higher memorability for visual-spatial secrets encoded in the Memory Palace which were also significantly more resilient against shoulder surfing. We conclude with directions for further work: specifically, creating sharable paths for more socially compatible authentication and segmenting secret paths for simple, non-binary access control.

## 1. INTRODUCTION

Currently, over two billion people worldwide are using smartphones [1], and it is projected that over six billion people, or 70% of the world's population will have a smartphone by 2020 [2]. Simultaneously, smartphones are capturing more personal data—e.g., location information, internet search histories, and financial transactions. In other words, smartphones are increasingly becoming a key hub into people's increasingly digitized lives.

Still, a large percentage of smartphone users use weak or no authentication, despite myriad existing solutions [3]. Existing solutions may be subpar for numerous reasons: they require memorizing complicated secrets that may be easily stolen through shoulder surfing, they complicate the sharing access to the device, and they only support binary all-or-nothing access to the device. Accordingly, it seems that the design space for useful smartphone authentication remains to be fully explored.

To address the aforementioned, we present a preliminary exploration and evaluation of The Memory Palace, a concept mobile authenticator that encodes strong secrets into visual-spatial paths that are traversed in procedurally-generated virtual worlds. We take this approach because there is significant evidence that suggests people are better at remembering visual spatial information (e.g. a path between points) than semantic information (e.g. random string of numbers) [4]. Thus, we believe it is possible to build a better authenticator based on visual spatial secrets rather than semantic secrets. This observation is the key insight behind graphical passwords, for example, but existing graphical passwords solutions often have many of the downsides previously mentioned (e.g., are easily shoulder surfed or otherwise provide relatively low security).

In contrast, our approach of using visual-spatial could potentially mitigate those downsides. For example, strong secret paths should still be highly memorable, but the complexity of the virtual world should make it difficult to shoulder surf. In addition, the use of familiar spatial metaphors such as guest rooms and path segments should facilitate device sharing and tiered access control. Accordingly, our key contribution in this paper is the introduction, design and preliminary evaluation of the Memory Palace.

## 2. THE MEMORY PALACE

Memory Palace is loosely based on the mnemonic device of the same name, also known as the method of loci. The method of loci is a memory technique where a person visualizes a spatial path to recall information. With our implementation, users encode their authentication secrets in the form of a path in their own procedurally generated "memory palace." (See Figure 1)

To figure out the best representation of the Memory Palace, we conducted an initial user study to determine the representation in which participants can best remember a secret path. We asked 14 participants to memorize paths in different forms, and asked them to recreate the paths in the next session. From our initial study, we found that a first person, 3D perspective was more memorable than a 2D, bird's eye view perspective. Accordingly, we created a Memory Palace application in which users traversed through their procedurally generated palace in a first-person perspective.

**Figure 1: Screenshots of the Memory Palace App. Create a path in the app, and save it as the secret for your smartphone.**



*Symposium on Usable Privacy and Security (SOUPS) 2016*, June 22-24, 2016, Denver, Colorado.

The Memory Palace app's layout is a procedurally generated set of 3D rooms, where rooms are linked through doors. To make each room memorable and different, each room was designed to be uniquely distinguishable. To navigate, the user can swipe in their desired direction to move around the world. When a user wants to create a path as the password, he/she will trace a path throughout the rooms until a specific destination. Once the user repeats the path for confirmation, it will be stored as an authentication secret.

The creation of secrets in the Memory Palace is scalable, allowing users to create paths as long or short as they prefer. Furthermore, in fast mode, a user can navigate a path in one, incrementally drawn motion, which should allow for quick entry of paths that are progressively encoded into muscle memory.

# 3. TESTING THE CONCEPT

To evaluate our Memory Palace authentication concept, we conducted a second, within-subjects experiment with 20 participants. To better understand the benefits and limitations of our authentication, participants were tasked with learning an authentication secret on both the Memory Palace and Android 9-dot pattern lock. Our focus was to test our authentication concept along three key usability and security metrics: memorability, entropy, and resilience against shoulder surfing. We measured memorability by asking each participant to memorize a random password in random order and to try and unlock the smartphone using each method a week later. We held the entropy of the secret close to constant in our study—the Memory Palace secrets had 20 bits of entropy (a path of length 10) whereas the 9-dot pattern lock secrets had 18 bits of entropy. Additionally, we tested resilience against shoulder surfing by showing participants videos of a person entering a password using 9-dot pattern lock and the Memory Palace, and asking each user to unlock the phone.

**Figure 2: The results of the user study comparing the Memory Palace and Android 9-dot Patternlock (N=20).**

| Method | 1-week Recall Rate | Entropy | Resilience |
|---|---|---|---|
| Memory Palace | 70% | 20 bits | 95% |
| Android 9-dot | 30% | 18 bits | 35% |

From Figure 2, 70% of the participants remembered the Memory Palace password, whereas only 30% remembered 9-dot Patternlock. The Memory Palace was also resilient to 95% of participants attempted to shoulder surf the password, whereas Patternlock was only resilient to 35% of participants.

# 4. DIRECTIONS FOR FUTURE WORK

Along with the memorability and security benefits, the Memory Palace offers other possible benefits we have not yet tested. When smartphone users share their phones, most of the time, the borrower only needs a single feature such as making phone calls. A common concern is data privacy, since the owner is giving away full access to the phone. [5]. With the Memory Palace, we are able to introduce a concept called guest passwords, where users can set an alternative path on their smartphones. This new path, or "guest room", only allows access to certain parts of the user's smartphone, such as just the phone feature, or the texting feature. This allows users feel more secure when allowing other people to borrow their phone.

In addition, the Memory Palace potentially facilitates non-binary, multi-tiered authentication. Currently, having different passwords for more sensitive parts of a phone is complicated. With the Memory Palace, we can create path extensions of the base password to unlock more secure features of one's phone, such as a banking app. This allows users to set more secure passwords while using the same system. Additionally, since the password is an extension of the base password path, we hypothesize users will be able to memorize the more secure password more easily than remembering a new, more secure password.

# 5. CONCLUSION

The Memory Palace is a new authentication concept that encodes memorable, strong secrets as visual-spatial paths through a virtual world. Our initial studies show that the Memory Palace has potential: participants were able to remember more secure authentication secrets more reliably. However, there are other potentially fruitful, but untested benefits to the Memory Palace that we intend to explore in future work: e.g., decreasing the required entry time, introducing incremental, tiered authentication and introducing guest rooms for shared access. In summary, we believe that this paper has explored a promising, novel approach to smartphone authentication that opens up a new design space.

# 6. ACKNOWLEDGMENTS

This work was made stronger by feedback from other members of CMU's CHIMPS Lab research group. Special thanks to Joanne Lo for her helpful assistance in the execution of the studies.

# 7. REFERENCES

1. Kissonergis, Phillip. (Oct 2015) "Smartphone Ownership, Usage and Penetration by Country," *http://www.smsglobal.com/thehub/smartphone-ownership-usage-and-penetration/*.
2. Lunden, Ingrid. (Jun 2015) " 6.1B Smartphone Users Globally By 2020, Overtaking Basic Fixed Phone Subscriptions," *http://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/*.
3. Van der Meulen, Rob., Rivera, Janessa. (Feb 2014) " Gartner Says 30 Percent of Organizations Will Use Biometric Authentication for Mobile Devices by 2016," *http://www.gartner.com/newsroom/id/2661115*.
4. Legge, E., Madan, C., Ng, E., and Caplan, J. (2012). "Building a memory palace in minutes: Equivalent memory performance using virtual versus conventional environments with the Method of Loci," *ActaPsychologica, 141 (3), 380-390.*.
5. Karlson, Amy K., Brush, A.J. Bernheim, Schechter, Stuart., (2009) "Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones," *Microsoft Research*.