The Memory Palace: Exploring Visual-Spatial Paths for Strong, Memorable, Infrequent Authentication

Sauvik Das
Georgia Tech
Atlanta, GA, USA
sauvik@gatech.edu

David Lu, Taehoon Lee[1], Joanne Lo
Carnegie Mellon University
Pittsburgh, PA, USA
{davidl1,n/a[1],jylo}@alumni.cmu.edu

Jason I. Hong
Carnegie Mellon University
Pittsburgh, PA, USA
jasonh@cs.cmu.edu

ABSTRACT

Many accounts and devices require only infrequent authentication by an individual, and thus authentication secrets should be both secure and memorable without much reinforcement. Inspired by people's strong visual-spatial memory, we introduce a novel system to help address this problem: the Memory Palace. The Memory Palace encodes authentication secrets as paths through a 3D virtual labyrinth navigated in the first-person perspective. We ran two experiments to iteratively design and evaluate the Memory Palace. In the first, we found that visual-spatial secrets are most memorable if navigated in a 3D first-person perspective. In the second, we comparatively evaluated the Memory Palace against Android's 9-dot pattern lock along three dimensions: memorability after one week, resilience to shoulder surfing, and speed. We found that relative to 9-dot, complexity-controlled secrets in the Memory Palace were significantly more memorable after one week, were much harder to break through shoulder surfing, and were not significantly slower to enter.

Author Keywords

authentication; usable security; spatial memory; visual-spatial memory; method of loci; memory palace; cybersecurity

CCS Concepts

•Security and privacy → Graphical / visual passwords; Usability in security and privacy; •Human-centered computing → Mobile computing;

INTRODUCTION

We introduce the Memory Palace, a novel authentication system that encodes strong, memorable and shoulder-surfing resilient secrets as visual-spatial paths in a procedurally-generated 3D virtual labyrinth. Users navigate the labyrinth in first-person perspective using swipe gestures (see Figure 1) and are authenticated if they can recreate their pre-registered secret path exactly.

A longstanding problem in authentication is remembering secrets after extended periods of disuse. Solving this problem is useful for a growing number of use-cases that require *infrequent authentication*, where end-users need only authenticate into a device or account on occasion. This situation could arise if authentication sessions persist for long time-periods (e.g., social media accounts), if accounts are dominantly accessed on a device with an infinitely persisting session but occasionally accessed on a different device (e.g., Netflix accounts on smart TVs vs. on web browsers), if protected resources are otherwise accessed only occasionally (e.g., conference rooms secured with smart locks), or for fallback authentication where a secondary secret is necessary to recover access to an account if the primary secret is compromised.

For these infrequent authentication use-cases, in addition to security against common attacks (e.g., random guessing, shoulder surfing), two other design dimensions are important. First is *quick encoding* — that is, the authentication secret should be memorable without much practice or reinforcement. Users are unlikely to accept a solution that requires significant upfront training or effort [1]. Second is *deployability*: the solution should be cost-effective and not require specialized hardware. As Bonneau et al. illustrate [7], myriad authentication solutions have been proposed but most are difficult to deploy and thus fail to be widely adopted.

Existing solutions fall short in one or more of these dimensions. Biometric readers require specialized hardware and can be expensive. PINs and graphical passwords [26, 20] are non-invasive and require no specialized hardware, but have problems in either long-term memorability without frequent reinforcement and/or resilience against shoulder surfing. Indeed, strong PINs and passwords are not memorable if not regularly reinforced [8] and many graphical passwords can be easily broken by nearby shoulder-surfers [39, 6]. We need a *something-you-know* authentication solution that requires no specialized hardware, is memorable through periods of extended disuse, and is resilient to shoulder-surfing.

Inspired by findings in cognitive psychology that people have exceptionally strong visual-spatial memories (e.g., memory of commuting paths, wayfinding through familiar buildings) [9, 49, 36], our work asks a simple question: *Using visual-spatial encodings, can we make memorable authentication secrets*

UIST '19, October 20-23, 2019, New Orleans, LA, USA.
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-6816-2/19/10 ...$15.00.
http://dx.doi.org/10.1145/3332165.3347917

[1] Taehoon Lee passed away before the publication of this paper.

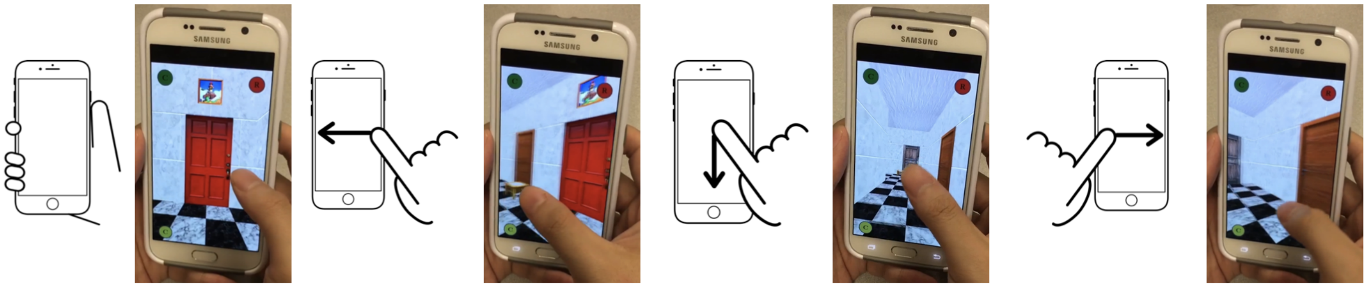

Figure 1: In the Memory Palace, authentication secrets are encoded as paths through a three-dimensional virtual labyrinth. Users navigate the labyrinth using quick swipe gestures in which they can turn, move forwards and go through doors. Landmarks, such as paintings and furniture, as well as colors and textures of walls are randomly interspersed throughout the labyrinth.

that require little reinforcement and are secure against nearby shoulder surfing attacks?

To answer this question, we designed, implemented and evaluated the Memory Palace. We first ran a within-subjects experiment to understand which visual-spatial encoding worked best for memorability: a 2D birds-eye view, 3D third-person view and a 3D first-person view. We found that secrets encoded as paths navigated in a 3D first-person view were by far the most memorable for our participants and implemented our proof-of-concept Android application accordingly.

We then ran a second within-subjects experiment to compare our Memory Palace application against the closest comparable baseline: Android's 9-dot pattern unlock, one of the most popular on-device graphical authentication systems. We compared the two systems across three measures: memorability of secrets after one week, resilience to shoulder-surfing, and entry speed. Our results suggest that, controlling for complexity, secrets in the Memory Palace were significantly more memorable after a week of disuse and were significantly harder to break through shoulder-surfing attacks. We did not find a significant difference in entry speed, but it is likely that 9-dot is a few seconds faster. However, this small additional overhead should be tenable for infrequent authentication contexts given the memorability and security improvements.

Broadly, we present an initial exploration of how to leverage visual-spatial memory for infrequent authentication, show its strong potential, and advocate for further research in this space. More concretely, we offer the following contributions:

- We explore and evaluate three representations for encoding visual-spatial secrets, finding that a 3D first-person view works best for memorability.
- We design, implement and evaluate the Memory Palace, a proof-of-concept visual-spatial authenticator. We find that secrets in the Memory Palace are significantly more memorable and resilient to shoulder-surfing than Android's 9-dot pattern lock.

BACKGROUND & RELATED WORK

Visual-spatial memory

Memory is multi-faceted [43], interwoven with perception and thinking. A full survey is out of scope for this paper, but there are several comprehensive reviews (e.g., [46, 43, 49]). Our exploration of the prior literature on memory led to one memory system, in particular, that is quick-to-imprint, strong for long-term recall, but not yet widely explored for use in authentication: visual-spatial memory.

Prior work studying the brains of superior mnemonists who compete at the highest level of memory competition suggest a large majority use spatial learning strategies [36, 23]. Chief among these strategies is the "method of loci", where items to be remembered are cognitively imprinted at different points in a familiar space [12, 9, 33, 41]: i.e., a memory palace. The method of loci traces it origins to ancient Greek and Roman orators, who used the technique to memorize speeches [9]. An example memory palace might be one's childhood home. Using the method of loci, remembering a list of items such as "ant", "beetle" and "cow" might involve imagining an ant at one's front door, a beetle in the living room and a cow in the kitchen. Whenever one needs to recall these items, they should "mentally walk-through" their childhood home and see the cognitive imprints [9].

The method of loci does not require that the memory palace be associated with a real-world space — imagined or artificially generated palaces work just as well [9, 23]. Recent work has explored the construction of computer-generated virtual memory palaces to assist with remembering arbitrary lists of information (e.g., [34, 33]) — the upshot of this work is that computer-generated memory palaces can be just as effective as spaces based on the physical world, but the more immersive the experience, the better the recall [33].

Inspired by these findings, we hypothesized that it should be possible to generate virtual memory palaces in which we can encode memorable authentication secrets that are simple and quick to learn.

Usable authentication

There are three broad categories of authentication [39, 10]: what you are (i.e., biometrics), what you have (e.g., keycards) and what you know (e.g., passwords). Various "fourth" categories have been proposed but can be considered special cases of the other three, including what you do (e.g., keystroke dynamics [37]) and who you know (e.g., social vouching [10]).

Each of these categories have pros and cons for different contexts [7, 38]. Biometrics are fast, low-effort, and largely secure against all but the most motivated adversaries but are invasive, often require specialized hardware and cannot be reset if compromised. Keycards and other token-based authenticators are also low-effort but also require specialized hardware and require users to physically carry around a token that can be expensive to replace if lost or damaged. Secret-based authenticators issue challenges to users based on their knowledge of a secret: e.g., passwords. They require the least implementation overhead, but can be cognitively demanding — users are already overburdened with the number of passwords and PINs they need to generate, memorize and/or manage [31, 2]. Graphical passwords can reduce cognitive load by leveraging our strong visual memory system, but are often easy to compromise through shoulder surfing or smudge attacks [44, 6, 5]. The Memory Palace is designed to be resilient to these common attacks against graphical passwords while retaining their memorability advantages.

For the infrequent authentication use-case, expensive solutions that require specialized hardware are inappropriate. Secret-based authentication seems to be the most graceful solution, but only if the secrets can remain secure against capture attacks (e.g., shoulder surfing) and if users can remember their secrets through long periods of disuse. Prior work has explored using autobiographical authentication, in which users are asked questions about their day-to-day activities as captured by their smart phones [15, 26, 27]. While effective, these methods are slow and only appropriate for personal devices and accounts that can collect substantive private data about the user.

Visual-spatial authentication

Despite the success of spatial learning strategies for memorization, the study of spatial secrets for authentication remains relatively under-explored. Alsulaiman and El Saddik first proposed “3D passwords” as a form of multi-factor authentication [3, 4]. The core idea was that users would interface with a variety of virtual objects in a 3D virtual world, with each object being mapped to an alternative single-factor form of authentication (e.g., a virtual computer would require the user enter an alphanumeric password or to present a keycard). The end-user’s full secret, then, would be interacting with the right virtual objects in the right order. More recently, George et al. explored 3D passwords for immersive virtual reality systems [25]. While these 3D password systems are similar at a surface-level, our approach is different in a number of ways. First, rather than interact with virtual objects, we have users navigate paths in 3D environments. Second, we implement and evaluate our system on commodity touchscreen devices where no specialized hardware is required. Third, our approach is designed for memorability with little reinforcement.

Another closely related paper we found is that of Renaud and De Angeli [40], in which the authors defined “visuo-spatial” secrets as selecting fixed points in a 2D image. Renaud and De Angeli did not find positive results: participants were not able to remember their secrets as well as expected and the security of the scheme was also weak. We suspected that this negative result was largely due to how Renaud and De Angeli encoded “visuo-spatial’ secrets as points to click on a still image. However, spatial mnemonic techniques, like those employed by memory champions, typically require traversing vivid spatial paths in one’s mind. Renaud and De Angeli’s system, thus, more closely resembles cued-recall graphical passwords like PassPoints [48] and Cued Click Points [11] than a true visual-spatial authentication system. Also related to our approach is GeoPass [45], where secrets are encoded as real-world locations on a map. The Memory Palace differs in two key ways: (i) the secret is the path itself versus only the destination; and, (ii) the secret is in a dynamically generated virtual world rather than a real-world location, which may be more guessable for attackers with prior knowledge of victims.

STUDY 1: HOW MEMORABLE ARE VISUAL-SPATIAL SECRETS IN DIFFERENT PERSPECTIVES?

Following an iterative design process, we first wanted to explore how best to encode visual-spatial secrets to maximize long-term memorability prior to implementing a full prototype. Visual-spatial memory can be triggered in many ways, and we were particularly interested in testing three: a 2D birds-eye view, a 3D third-person view, and a 3D first-person view of a character traversing a path. We selected these three perspectives because they are familiar — the Memory Palace would have to be implemented as a virtual world similar to computer game worlds, and these three perspectives are often used in a gaming context. We conducted a within-subjects experiment to determine which of these representations would maximize memorability after a significant period of disuse — for example, one full week as has been tested in prior work for infrequent authentication [45]. We hypothesized that a 3D first-person perspective would be most memorable as it most resembles people’s real-world use of visual-spatial memory.

H1: Visual-spatial secrets should be significantly more memorable in a 3D first-person perspective than in a 2D birds-eye view perspective or a 3D third-person perspective.

Method

To test this hypothesis, we ran a within-subjects experiment over two sessions separated one week apart with 14 participants. We started by generating complexity-controlled visual-spatial secrets for all three perspectives. Participants were taught three visual-spatial secrets, one in each of the three perspectives we were testing. To mitigate learning effects, participants were taught these secrets in random order.

In the first session, we taught participants each of the three secrets twice and had them demonstrate that they remembered the secret. If they didn’t, we corrected mistakes. The second session occurred one week later. In the second session, participants simply had to demonstrate if they remembered each of the secrets in the same order that they initially learned those secrets. They were given three tries to do so for each secret. The only feedback they were given was if they were correct when they believed they had finished entering the secret.

For the 3D first-person view, we had participants walk a predetermined path along an indoor hallway with open doors and corridors. For the 3D third-person view, we purchased a large dollhouse and had participants move a small doll along

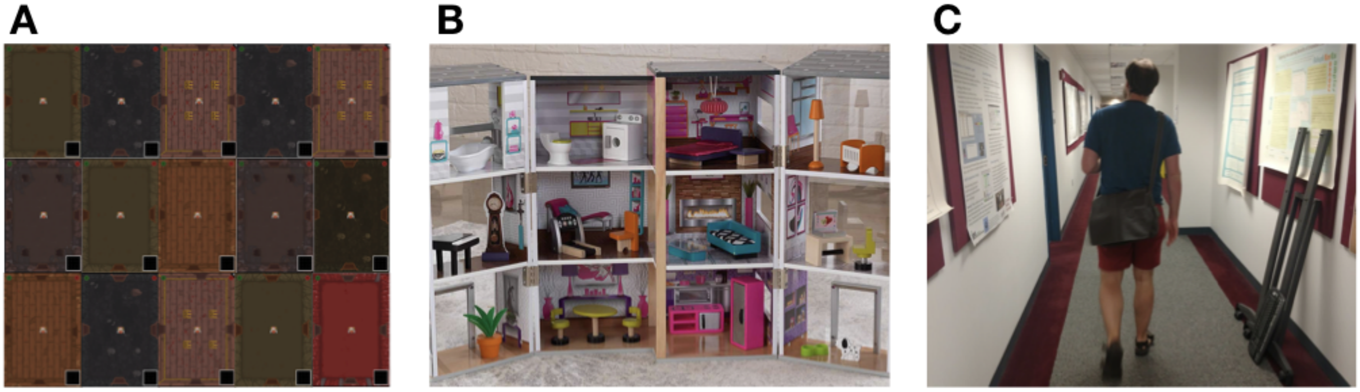

Figure 2: Representations we tested in the first study: (A) 2D birds-eye view (print out of 2D virtual world grid); (B) 3D third-person (dollhouse); and, (C) 3D first-person (walking through a hallway).

a preset path through the various rooms of the dollhouse. Finally, for the 2D birds-eye view representation, we created and printed out a 2D map grid and had participants move a small doll through a contiguous path on the grid. Figure 2 shows an illustrative example of each condition. We note that it is possible that the specific mediums through which we represented these secrets could have influenced the memorability of the secrets in each of these perspectives.

We defined complexity as the Shannon entropy of the theoretical search space for each of the visual-spatial secrets. Specifically, secret complexity was calculated as follows: for each segment in the secret, we enumerated all possible moves a user could make, set each of those moves to be equally probable, calculated the Shannon entropy for that segment, and then summed the entropy for each segment to arrive at the final value. We fixed the entropy of secret to about 14 bits, which is stronger than typical graphical passwords which tend to be quite weak [47, 19]. As an illustrative example, in the 2D perspective, a user has four choices in each non-corner node. Accordingly, a 14-bit secret would be equivalent to a path of length of 7 ($log_2(4^7) = 14$). The same calculation was used to create a path for the other perspectives. For the 3D third-person perspective with the doll house, we also selected a path of length 7 as the avatar could be moved up, down, left and right at any given room. For the 3D first-person perspective where participants were walking through an indoor hallway, we set the secret to a length of 7 contiguous segments where a contiguous segment was defined as a path along which participants were required to walk straight. When participants encountered an intersection or an open door where they could move in any of four directions (left, right, straight or go back), the contiguous segment would end and a new one would begin.

Note that these complexity measures are simply estimates that we used to ensure that secrets across the three conditions were of comparable difficulty. In other words, despite the many weaknesses of using entropy as a measure of secret strength, doing so was suitable for our purposes because our goal was to have comparable conditions, not perfect complexity estimates.

	First	**Second**	**Third**	**Fail**
2D birds-eye	5	4	1	4
3D third-person	5	0	4	5
3D first-person	13	1	0	0

Table 1: Number of required attempts to recall their visual-spatial secrets after one week of disuse. The 3D first person perspective was the most memorable.

	Coefficent	**p-value**	
3D First vs. 2D	-0.88	0.01	**
3D First vs. 3D Third	-0.89	0.01	**
3D Third vs. 2D	0.02	0.99	
Trouble Learning?	0.55	0.02	**
Intercept	0.85	<0.001	***

Table 2: Regression coefficients correlating number of required attempts to correctly recall the given visual-spatial secret after one-week of disuse with representation. Bonferonni correction was applied. The 3D first person perspective was the most memorable.

Ethics and Compensation

Once we acquired IRB approval, we recruited participants through a study participation pool at our institution. Participants were compensated $10 for participating in both of the separate 30-minute sessions.

Results

We recruited 14 participants. Eight of our participants were female and six were male. Five of our participants were between 18-24 years old, another five between 25-34, two were between 35-44 and one was over 60.

Table 1 shows the number of attempts participants required to accurately remember their three secrets in the second session of the study. Fewer attempts equates to greater memorability. Concretely, all fourteen participants remembered the 3D first-person secret, thirteen of whom remembered it on the first try. In comparison, just 9 and 10 participants, remembered their secrets for 2D birds-eye view and 3D third-person perspectives, respectively, and only five participants remembered their secrets on the first attempt for each of those two perspectives.

To evaluate if these differences were statistically significant, we ran a random-intercepts Poisson regression. The dependent variable was the number of attempts a participant required to remember their secret, the independent variable was the perspective in which the secret was encoded (3D first-person, 3D third-person, 2D birds-eye), and we included a binary measure of whether or not a participant had trouble learning the secret in the first session as a covariate. For secrets participants could *not* recall in the second session within the allotted 3 tries, we substituted a value of 5 for the dependent variable (in practice, these participants may have never remembered their secrets).

We included a random-intercept term for each participant to account for repeated-measures (as we observed three data points per participant in our within-subjects design, one per condition). We chose a Poisson distribution for our model as our dependent variable was essentially a count variable, i.e., the number of attempts a participant needed to remember the secret. The Poisson distribution has been shown to best model count variables [24].

Table 2 shows the results of the regression. The important rows of the table are the top 3, which compares the 2D birds-eye (2D), 3D first-person (3DF), and 3D third-person (3DT) perspectives against each other. Negative coefficients suggest that the model estimates that the first condition in the comparison (before the versus) required fewer attempts to remember the secret than the second condition in the comparison (after the first), and therefore was more memorable. A positive coefficient suggests the opposite. We can see that, as we hypothesized in H1, the secrets were significantly more memorable for participants in the 3D first-person perspective ($b_{3DFv2D} = -0.88, p = 0.01$; $b_{3DFv3DT} = -0.89, p = 0.01$).

Based on these results, we implemented our proof-of-concept visual-spatial authentication application, The Memory Palace, as a 3D first-person perspective virtual world.

SYSTEM DESIGN: THE MEMORY PALACE

We implemented a proof-of-concept Memory Palace application on Android using OpenGL. We selected Android and OpenGL in part because of our original motivation to create a system that could be easily deployed on commodity devices. In our implementation, authentication secrets are encoded in the form of a visual-spatial path in their own procedurally generated virtual world, or "memory palace." Authentication, then, is a matter of retracing one's secret path through the familiar virtual world (See Figures 1 and 4).

Procedurally generating the Memory Palace

The Memory Palace application generates virtual palaces algorithmically. In designing our procedural generation algorithm, we had three high-level goals. First, we wanted *connected rooms to be distinctive* to allow users to clearly recognize different segments of their secret paths. Second, we wanted *individual doors within rooms to be unique* to facilitate memory of where to go next. Finally, we wanted the palace to be *theoretically infinite* such that an attacker would be given no feedback if a wrong turn was made — they would simply have to guess when to stop and restart. To meet these design goals, we used two layers of procedural generation: the first to create the palace layout and the second to customize rooms.

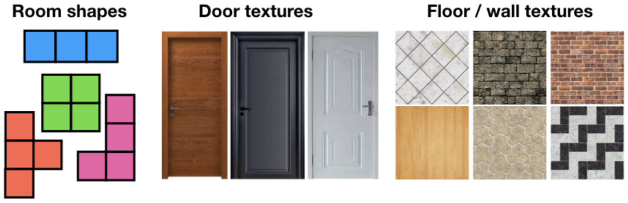

Figure 3: Individual rooms were customized and varied by shape, door texture, floor and wall textures, and decorative artwork. We show a subset of these customizations here.

To create the palace layout, we start with an empty grid and stochastically generate rooms in the shape of Tetris pieces. These Tetris-piece shaped rooms are stacked together into contiguous blocks. This process allows for variation in room shape and size while still allowing rooms to neatly fit. Each room is connected to least 2 other rooms, with the doors connecting rooms randomly placed along shared walls. Initially, we generate a layout that fills out a 21x21 grid (each room takes up 3-4 grid blocks depending on its shape). The entry point into the palace is the center grid block (the grid block at the 11th row down, and 11th column over). If a viewer navigates close to the periphery of the pre-generated palace, additional rooms are procedurally generated near the corresponding border(s). The generated palace is stored in local memory so that the layout persists.

Once the room layout has been determined, we decorate and texture each room to be visually distinctive from its adjacent rooms. We start by selecting locally unique wall and floor textures, such that no adjoining room has the same texture combination. We then pseudo-randomly place decorative artwork (e.g., credanzas, vases, paintings) along the walls of the room. Finally, for each door in a room, we: (i) pick a texture for the door (e.g., wood, metallic, white), and (ii) place a unique wall painting decoration on top of the door. The combination of door texture and decoration should be unique for each door in a room. We take these steps to make doors visually distinctive and to facilitate later recall. Room decorations are also stored in local memory so that they persist across sessions. Figure 3 shows a subset of these decorations.

Authenticating with the Memory Palace

Much like when creating a new password or graphical password, authentication with the Memory Palace first requires registering a new secret. To create a new secret, users are placed at the entry point (the center grid block) and asked to trace a path through the virtual world — taking any turns they'd like and moving anywhere they wish. They are then

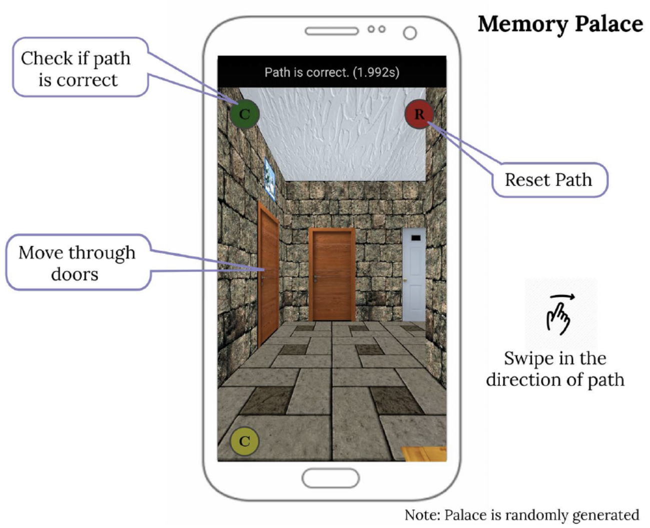
Memory Palace
Check if path is correct
Path is correct. (1.992s)
C
R
Reset Path
Move through doors
Swipe in the direction of path
C
Note: Palace is randomly generated

Figure 4: The final user interface for the Memory Palace. Users are embedded within a procedurally generated game world and can navigate through hallways in the first-person perspective using swipe gestures. When authenticating, users are initially placed in the center of the virtual world.

asked to confirm their path a second time. After registering their secret, users can later authenticate by re-tracing their secret path exactly.

Users can create paths as long or short as they prefer. As we procedurally generate the palace, there is no “edge” and the search space is infinite — attackers cannot automatically assume how far a user might have gone in one direction.

User interface

Figure 4 shows the final user interface. While authenticating, users can see, through a first-person vantage point, their current room in the memory palace and a ‘C’ and ‘R’ button on the two top corners of the screen. Users could click the ‘C’ button to *check* their current path against their secret — the equivalent of hitting the *return* key when entering a password, and the the ‘R’ button to restart if they made a mistake.

Users can navigate the palace using swipe gestures. Two modes are available: swiping in the direction of travel or swiping in the opposite direction of travel.

We also implemented a “fast” mode in which users can incrementally draw their path (fully or partially) to quickly traverse the palace. The phone vibrates for each registered segment to provide users with haptic feedback. However, we suspected that fast mode would be a luxury utilized by relatively few advanced users and focused our evaluations on the standard method of path entry (swipe gestures).

STUDY 2: EVALUATING THE MEMORY PALACE

Recall that our initial motivation for designing the Memory Palace was to create a memorable, secure on-device authentication scheme for infrequent use-cases. To evaluate our design against this initial motivation, we experimentally evaluated the Memory Palace against a comparable baseline, Android’s 9-dot pattern lock, along three key measures: memorability after a period of extended disuse, resilience to shoulder-surfing attacks, and entry speed. Memorability after extended disuse was our key measure of interest — we designed the Memory Palace for infrequent authentication use-cases where secrets should be memorized long-term without much reinforcement [6]. We also tested for resilience against shoulder surfing because a common criticism of graphical authentication techniques is their weakness to capture attacks [6, 44]. Finally, we selected authentication speed because of its importance in usability and deployability — authentication mechanisms that are slow are frustrating and less likely to be adopted [28, 7].

Selecting an appropriate baseline comparison group was difficult given our use-case. Alphanumeric passwords and PINs are known to be less memorable than their graphical alternatives [44] and generally require significant reinforcement before they are memorized [8]. Common forms of fallback authentication that are designed to be memorable with little reinforcement, like challenge questions, cannot be complexity-controlled and do not require explicit memorization of a secret. Moreover, challenge questions are inappropriate for non-personal devices and accounts. Accordingly, these baselines make it impossible to design an internally valid experiment. Given these considerations, graphical passwords seemed the most appropriate comparison group as they are: (i) designed for memorability; (ii) can be complexity controlled; and, (iii) are familiar to most end-users. Accordingly, we picked Android’s 9-dot pattern lock as a baseline because it is a graphical authentication system that is widely utilized and well studied.

We had three hypotheses of how the Memory Palace would perform relative to Android 9-dot pattern lock corresponding to each of the aforementioned evaluation metrics:

H2: Controlling for complexity, secrets in the Memory Palace should be significantly more memorable than secrets in Android’s 9-dot pattern lock after a week of disuse.

H3: Controlling for complexity, secrets in the Memory Palace should be significantly more resilient to shoulder-surfing attacks than secrets in Android’s 9-dot pattern lock.

H4: Controlling for complexity, entry of authentication secrets in Android’s 9-dot pattern lock should be faster than in the Memory Palace.

Method

To test our hypotheses, we ran a second within-subjects experiment with 20 participants. Participants took part in two time-separated sessions. In the first session, participants were made to learn a preset authentication secret on both the Memory Palace and Android’s 9-dot pattern lock on a Samsung Galaxy Android phone that we provided. To ensure that the secrets were comparable, the order in which participants learned the two secrets was randomized, and the complexity of the secrets were selected to be very similar — the Memory Palace secret had approximately 20-bits of entropy, and the 9-dot pattern lock had approximately 18-bits of entropy. Both of these are stronger than average graphical passwords [47] and, in turn, could serve as better memory tests.

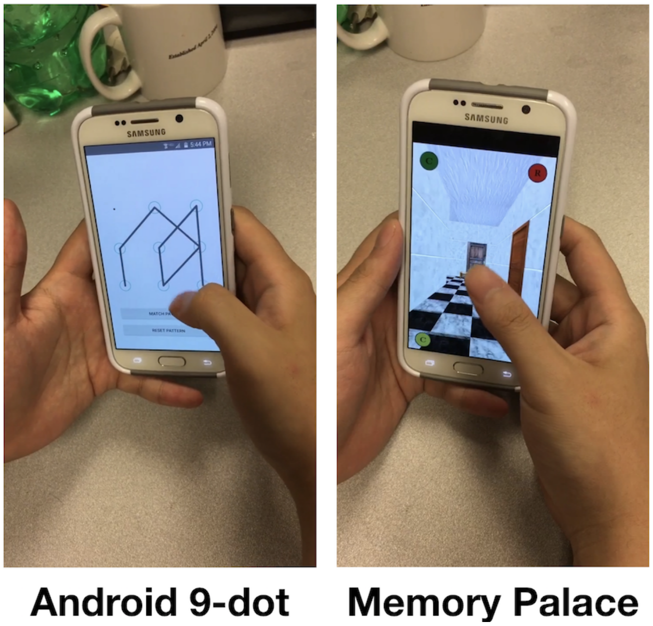

Figure 5: Screenshots of the over-the-shoulder perspective videos participants were shown and instructed to replicate after one viewing. The full videos are provided in the supplementary materials.

In the first session, for each of the two conditions, participants were initially shown the secret they needed to remember by a member of the research team and were then asked to replicate the secret correctly twice. In the second session, which occurred seven days after the first, participants were asked to replicate both the 9-dot and Memory Palace secrets they had previously learned in the same order they had initially learned the secrets. They had up to three attempts to replicate each secret. We recorded the number of attempts participants required to correctly remember their secrets, as well as the entry speed for the first successful attempt.

Later in the second session, we had participants play the role of a shoulder-surfing adversary. We showed participants two over-the-shoulder perspective videos of someone entering an authentication secret — one for the Memory Palace, and one for Android's 9-dot pattern lock. These secrets were new and approximately the same complexity as the secrets participants were previously asked to memorize. Figure 5 shows screenshots of these videos. Participants were shown each video once (simulating a shoulder-surfer) and were asked to replicate the secrets immediately afterwards. The order in which they were shown the videos and asked to replicate the secrets was randomized.

Finally, we finished the study with a brief semi-structured exit interview in which we asked participants questions about their overall impression of the Memory Palace as well as strategies they employed for memorizing their secrets. While not directly connected to any of our hypotheses, we include some of these qualitative responses to provide additional insights into the experience of using the Memory Palace.

1-week recall	**Att. 1**	**Att. 2**	**Att. 3**
Memory Palace	9	4	1
9-dot	6	0	0

Table 3: Number of attempts participants required to recall their secrets after one week. The Memory Palace secret was significantly more memorable than the 9-dot baseline.

Ethics and compensation

After we acquired IRB approval, we recruited participants through a study participation pool at our institution. Participants were compensated $10 for participating in both of the separate 30-minute sessions.

Results

Out of our twenty participants, ten were male and ten were female. Six of our participants were between 18-24 years old, nine were between 25-34 years old, and five were between 35-44 years old.

Memorability

We first tested H2 — that secrets in the Memory Palace would be significantly more memorable than Android 9-dot secrets. We found strong evidence in support of this hypothesis.

Table 3 shows how many attempts participants required to remember their Memory Palace and Android 9-dot secrets. Overall, 70% of our participants (14/20) could recall the Memory Palace secret within three attempts, compared to just 30% of participants (6/20) who could recall the 9-dot secret within three attempts.

To test the significance of this result, we followed the same analysis methodology we employed in study 1 — we ran a random-intercepts Poisson regression. The dependent variable was the number of required attempts to correctly remember the given secret in the second session. Participants who were not able to remember their secrets in the second session were assigned a value of “5” (though, in practice, these participants may have never remembered their secret). The independent variable was the condition: Memory Palace or 9-dot. None of our participants had trouble remembering their secrets initially, so there was no need to control for difficulty learning the secret in the first session as we had done in study 1. Finally, we gave each participant their own random intercept term to account for multiple observations per participant (i.e., one for the Memory Palace condition, one for the 9-dot condition). The results of the regression are shown in the first column of Table 4.

The important information is in the top row — the coefficient represents the model's estimate for how many more (positive) or fewer (negative) attempts are necessary to recall the correct secret in the Memory Palace than 9-dot. The results show that participants required significantly fewer attempts to remember their Memory Palace secret than their Android 9-dot secret after 1-week ($b = -0.42, p < 0.02$).

In a post-hoc analysis, we split participants into one of four groups: those who remembered *both* the Memory Palace and

	No. of Attempts		Adv. Success		Entry Speed	
MP vs. 9-dot	-0.42	*	-3.63	**	-0.43	
Intercept	1.31	**	0.64		15.54	**

* p < 0.05, ** p < 0.001

Table 4: Coefficients for all three regression models comparing the Memory Palace and Android 9-dot pattern lock. Memory Palace secrets were significantly more memorable and harder to break through shoulder-surfing.

9-dot secrets ($n = 5$), those who remembered *only the Memory Palace* secret ($n = 9$), those who remembered *only the 9-dot* secret ($n = 1$), and those who remembered *neither* secret ($n = 5$). All but one of the six participants who could recall their 9-dot secret was also able to remember their Memory Palace secrets, but only five of the 14 who remembered the Memory Palace secrets were able to remember the 9-dot secret. This finding suggests that the Memory Palace helps people who *cannot* remember 9-dot secrets long-term and does not hurt people who *can* remember 9-dot secrets long term — it is strictly more memorable, and not just for certain people.

In our exit interview, we asked participants to discuss their strategies for memorizing secrets in the Memory Palace. Most participants ($n = 14$) mentioned memorizing step-by-step directions in the same way they would attempt to memorize walking somewhere in the physical world: e.g., "two rights, a left, and then straight". A few participants ($n = 3$) mentioned memorizing door colors and keeping an eye out for landmarks (e.g., decorations and paintings, $n = 4$).

We also asked participants who were not able to successfully replicate their Memory Palace secrets about the difficulties they encountered. One participant, P15, who could not remember either secret said that while the Memory Palace secret was easier to remember than 9-dot, she had difficulty with error recovery — once she made a mistake, it was impossible to recover. This participant mentioned that a multi-sensory experience might have helped: for example, if there was ambient music or sound that she could use as a cue to recall whether or not she was on the right track. There is some prior work to support P15's suggestion — multi-sensory experiences in virtual worlds are indeed more memorable [22]. P14 also expressed concerns about error recovery, saying that if he gets lost, the maze like properties of the Memory Palace would make it very difficult to recover. Both P17 and P18, who also couldn't remember either secret, mentioned that they would have preferred more distinctive landmarks and visual cues to facilitate their memory of the secret.

Ultimately, cues that facilitate the memorability of Memory Palace secrets may also affect their resilience to shoulder-surfing attacks. However, it may be possible to make secrets in the Memory Palace even more memorable by making more visually distinctive landmarks and by integrating sound.

Resilience to shoulder-surfing

We next tested H3 — that the Memory Palace should be significantly more resilient to shoulder surfing than Android 9-dot authentication. We also found strong evidence in support of this hypothesis.

Only 5% (1/20) of participants were able to successfully replicate a Memory Palace secret given an over-the-shoulder perspective video of the secret being entered on a phone, compared to 65% (13/20) who were able to accurately replicate a 9-dot secret from the video.

To test if this difference was significant, we ran a random-intercepts logistic regression. The dependent variable was a binary measure of whether (1) or not (0) an adversary could successfully replicate the secret they saw in the video. The independent variable was the condition: Memory Palace or 9-dot. Finally, we gave each participant a random-intercept term to account for repeated observations. The results are shown in Table 4 and suggest that shoulder-surfing adversaries had significantly less success breaking the Memory Palace than 9-dot pattern lock ($b = -3.63, p < 0.001$).

It is important to note that while our results are very promising, this improvement in security is likely a best-case estimate — indeed, the secrets we selected are stronger than average and participants were more familiar with 9-dot than the Memory Palace. If the Memory Palace were deployed in the real world, adversaries would likely develop new strategies for breaking those secrets. Still, our results suggest that the Memory Palace provides better security against observation attacks than 9-dot.

During the exit interview, we probed participants on their overall impression of the Memory Palace. In this process, five explicitly mentioned that they thought of the Memory Palace as being especially secure. Notably, all of our participants played the role of an adversary trying to crack an actual secret, and thus their perception was not solely based on an abstract notion of the steps an attacker might take. While end-user *perceptions* of security are not as important as the aforementioned empirical results, perceptions can still be important — end-users are unlikely to actually use authentication mechanisms they do not believe provide an adequate level of security.

Entry speed

Lastly, we tested H4 — that entry of Android 9-dot secrets should be faster than entry of Memory Palace secrets. However, we did *not* find statistically significant evidence in support of this hypothesis.

Figure 6 shows the distributions of how long it took participants to enter their whole secret in 9-dot and in the Memory Palace. While the averages were approximately the same because of an outlier in the 9-dot condition, the median entry time for 9-dot was about 9.6 seconds as compared to 13.3 seconds for the Memory Palace.

To test if this difference was statistically significant, we ran a random-intercepts linear regression. The dependent variable was entry speed on the first successful attempt to replicate the secret. The independent variable, again, was the condition: Memory Palace or 9-dot. We again provided each participant

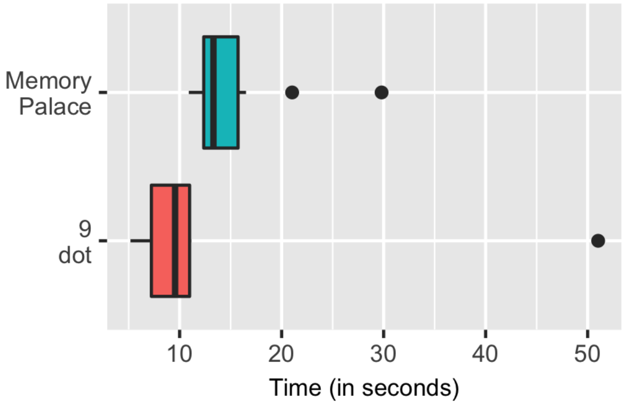

Figure 6: Box plot of the entry time distributions for Memory Palace and 9-dot secrets. 9-dot was faster than the Memory Palace, though the difference was not found to be statistically significant. The median entry time difference was about 3.7 seconds (9.6 seconds for 9-dot, 13.3 for Memory Palace).

with a random-intercept to account for repeated observations in our within-subjects design. The results are shown in the third column of Table 4.

The difference in entry speed of secrets in 9-dot versus the Memory Palace was not found to be statistically significant. We note, however, the absence of a significant effect does not necessarily mean that there is no difference — the difference may well be found to significant with a larger sample size. Indeed, only six (out of 20) participants remembered their 9-dot secrets, so we could only collect 9-dot entry speed data for those participants.

In the exit interview, six participants mentioned that they found entering secrets in the Memory Palace to be somewhat slow. This is to be expected, as participants were likely comparing secret entry in the Memory Palace to 9-dot, which is partially designed for speed. Furthermore, we never explicitly told participants that the Memory Palace was designed for infrequent usage. Accordingly, it is likely that participants considered the use-context for the Memory Palace to be for day-to-day smartphone authentication. P6, who was the most critical in the exit interview, mentioned that because the threat of her phone being stolen was low, she wouldn't want to use the Memory Palace as her primary means of phone authentication due to its speed. She did, however, mention that would use the Memory Palace on devices that she used less frequently.

In sum, while 9-dot seems to be a bit faster than the Memory Palace, the difference was not found to be statistically significant. While this small difference may not be desirable for frequent use cases (e.g., day-to-day smartphone access), it should be tenable for infrequent authentication use cases given the memorability and security improvements of the Memory Palace. It is also worth noting that because participants' were made to memorize a secret that is likely stronger than the secrets that would be used outside of a lab setting, the actual entry speed of average Memory Palace secrets should be faster.

Other impressions

Outside of memorability, perceived security and entry speed, some participants had other impressions of the Memory Palace that we captured in the exit interview. Several participants ($n =$ 5) mentioned that they found the Memory Palace to be "cool", "fun" and like a "video game." One participant even mentioned wanting some sort of gamification element integrated into the system, such that they would receive a prize for successful authentication. While seemingly trivial, end-users typically begrudge good cybersecurity behaviors [16]. As prior work suggests, a system that end-users perceive as enjoyable is more likely to be adopted and spread [21]. Several other participants ($n = 4$) mentioned that they found the Memory Palace to be interesting and easy to use.

DISCUSSION

There are a growing number of use-cases that require infrequent authentication. Examples of such use-cases include shared, protected resources that are only occasionally accessed by any one individual (e.g., smart locks on conference rooms), accounts with long, persisting sessions that sporadically require re-authentication (e.g., Facebook, Netflix), and fallback authentication for when users forget their primary secrets. For these use cases, what-you-know authentication can be appropriate as it is cheap, familiar and easy to deploy. However, the secrets end-users need to remember should be memorable without requiring constant reinforcement, as well as resilient to common attacks such as shoulder surfing. Inspired by people's strong visual-spatial memory, we designed and evaluated the Memory Palace as a possible solution. The Memory Palace is a new visual-spatial authentication system where people authenticate through their knowledge of a secret path in a procedurally-generated virtual world.

We ran two studies to iteratively design, implement and evaluate the Memory Palace. In the first study, we evaluated three different perspectives in which to encode visual-spatial secrets, finding that a 3D first-person perspective is best for memorability when compared to a 2D birds-eye perspective and a 3D third-person perspective. Based on this initial result, we designed and implemented a proof-of-concept Memory Palace Android application in which users navigated a 3D virtual world in the first-person perspective. We then ran a second within-subjects experiment to evaluate its memorability, resilience to shoulder surfing and entry speed as compared to Android's popular 9-dot pattern lock.

We found that, controlling for complexity, secrets in the Memory Palace are significantly more memorable and resilient to shoulder-surfing attacks. While we did not find a statistically significant difference in entry speed between the Memory Palace and 9-dot, we suspect that the Memory Palace may be slower. This time overhead may be acceptable, however, for end-users in contexts that require only infrequent authentication given the strong memorability and security improvements. In addition to these empirical results, the Memory Palace offers an security benefit over alternative graphical authentication schemes: the search space for Memory Palace secrets is theoretically infinite.

Implications, Limitations and Future Work

We have only begun exploring the design space of visual-spatial authentication, in general, and of the Memory Palace specifically. Indeed, the Memory Palace might offer other benefits we hope to test in future work.

Natural metaphors for shared authentication:
There are a growing number of use-cases in which people need to share devices with others or in which groups of people collectively own resources that require digital protection [16, 13, 14, 42]. Existing solutions for sharing access to personal or communal devices are often socially inappropriate or cumbersome [18]. A visual-spatial metaphor can make this sharing more natural — one can envision, for example, teaching friends how to reach a "guest room" in the Memory Palace to get limited access to a personal device, or having a "kids" room and a "parents" room in the same palace for families who share devices and want to enforce parental controls.

Scalable authentication:
The Memory Palace should facilitate non-binary, scalable authentication by modulating access control to different protected resources through incremental path extensions. Existing approaches for scalable authentication typically require users to have memorized multiple independent secrets (e.g., [29]). The most complex secrets are used and, in turn, reinforced least frequently and are thus more likely to be forgotten. We have already shown that infrequently used secrets are more memorable with the Memory Palace. Moreover, it should be possible to create path extensions on top of a base secret to unlock more sensitive features of an account or device (e.g., permission to add new users or change the security settings of a device). This would allow users to use the context of their base secret as a memory aid to recall their extended secret.

Authentication for Gaming, Virtual and Augmented Reality:
The Memory Palace should also be viable for emerging use-cases for authenticationo in gaming and VR / AR systems: e.g., for seamless in-game purchases, or for entering protected environments in virtual worlds. As AR/VR technologies are more immersive than touchscreens, visual-spatial secrets may be even more memorable in these media [33].

Field evaluations of visual-spatial authentication:
Our work evaluated the Memory Palace in a controlled lab setting with limited ecological validity. In turn, studying the usability and security of the Memory Palace in real-world settings is a fruitful area for further exploration. We hope to run a long-term field evaluation of the Memory Palace with real users who create their own secrets to authenticate in to real resources. Using this real-world data will also afford us an opportunity to evaluate the strength of the visual-spatial secrets that users create themselves.

Negative Implications:
Following recommendations from the community [30], we also want to discuss two potential negative implications of the Memory Palace. The first negative implication is that the Memory Palace may not be accessible. Indeed, the Memory Palace, in its present form, would not be usable for people with visual and/or motor impairments. The Memory Palace might also be more difficult for users who have less familiarity with navigating virtual worlds. A second potential negative implication is that the Memory Palace is likely to make sharing access credentials more difficult — while this could be viewed as a plus for security as noted above, the requirement to keep individual secrets in shared contexts can be socially inappropriate and contribute to an ecosystem of individual over social cybersecurity practices [35, 17, 18].

Limitations:
The key limitations of our work are manifold. To name a few: (i) we did not test recall after one week; (ii) we did not test memory of multiple visual-spatial secrets; and, (iii) we did not study how end-users would generate their own visual-spatial secrets. We also note that ecological validity is a limitation in our study designs: participants were assigned visual-spatial secrets to memorize (as opposed to creating their own) and were not using these secrets to secure a device or account they personally used. These are all significant limitations that will need to be addressed before we can recommend the Memory Palace be widely adopted into real world use-cases. In future work, it would pertinent, for example, to assess how people *generate* their own visual-spatial secrets in the Memory Palace, as has been done in prior work for related graphical authentication techniques [32]. Our goal in this paper was to explore the use of visual-spatial authentication as a memorable, shoulder-surfing resilient alternative to popular graphical authentication schemes like Android's 9-dot for the increasing number of use-cases that require infrequent authentication. Accordingly, while we acknowledge that our work has a number of limitations, we argue that the Memory Palace opens up a promising new design space for visual-spatial authentication.

CONCLUSION

The Memory Palace is a novel system that encodes authentication secrets as visual-spatial paths through a procedurally-generated virtual world. Our evaluations show that the Memory Palace is effective and has strong potential. Compared to Android's 9-dot pattern lock, secrets in the Memory Palace were significantly more memorable after 1-week and significantly harder to break through shoulder surfing. While the Memory Palace might be a bit slower than 9-dot, we argue that, given the memorability and security improvements, this additional overhead may be tenable for the growing number of use-cases that require only infrequent authentication. Moreover, there are other potentially fruitful, but untested benefits to the Memory Palace that we intend to explore more deeply in future work: e.g., decreasing entry time through faster input mechanisms; introducing scalable authentication through path segmentation; exploring guest room metaphors for facilitating shared access; and, evaluating the Memory Palace for authentication in AR / VR environments. In sum, we contribute a promising, novel approach to authentication that opens up a fruitful design space for reinventing authentication.

ACKNOWLEDGMENTS

In memory of our co-author, Taehoon Lee. A longer dedication to Taehoon is included in the supplementary materials. We thank Erik Harpstead for agreeing to be a model for Figure 2C and our anonymous reviewers for their helpful feedback.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Communications of the ACM (CACM)* 42, 12 (dec 1999), 40–46. DOI: http://dx.doi.org/10.1145/322796.322806

[2] A Allan. 2004. Passwords are near the breaking point. *Gartner Research Note* December 2004 (2004). http://www.donotspam.de/dokumente/gartner

[3] Fawaz A Alsulaiman and Abdulmotaleb El Saddik. 2006. A novel 3D graphical password schema. In *2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems*. IEEE, 125–128.

[4] Fawaz A Alsulaiman and Abdulmotaleb El Saddik. 2008. Three-dimensional password for more secure authentication. *IEEE Transactions on Instrumentation and measurement* 57, 9 (2008), 1929–1938.

[5] Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. 2010. Smudge Attacks on Smartphone Touch Screens. *USENIX conference on Offensive technologies* (2010), 1–7.

[6] Robert Biddle, Sonia Chiasson, and P C Van Oorschot. 2009. Graphical Passwords : Learning from the First Twelve Years. *Security* V (2009), 1–43. DOI: http://dx.doi.org/10.1145/2333112.2333114

[7] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *IEEE Symposium on Security and Privacy (S&P'12)*. IEEE, 553–567. DOI: http://dx.doi.org/10.1109/SP.2012.44

[8] Joseph Bonneau and Stuart Schechter. 2014. Towards reliable storage of 56-bit secrets in human memory. In *Proc. USENIX Sec.'14*.

[9] G. H. Bower. 1970. Analysis of a Mnemonic Device. *American Scientist* 58, 5 (1970), 496–510.

[10] John Brainard, Ari Juels, Ronald L Rivest, and Michael Szydlo. 2006. Fourth-Factor Authentication : Somebody You Know Categories and Subject Descriptors. *Proceedings of the 13th ACM conference on Computer and communications security* (2006), 168–178. DOI: http://dx.doi.org/10.1145/1180405.1180427

[11] Sonia Chiasson, Paul C Van Oorschot, and Robert Biddle. 2007. Graphical password authentication using cued click points. In *European Symposium on Research in Computer Security*. Springer, 359–374.

[12] Tim Dalgleish, Lauren Navrady, Elinor Bird, Emma Hill, Barnaby D. Dunn, and Ann Marie Golden. 2013. Method-of-loci as a mnemonic device to facilitate access to self-affirming personal memories for individuals with depression. *Clinical Psychological Science* 1, 2 (2013), 156–162. DOI: http://dx.doi.org/10.1177/2167702612468111

[13] Sauvik Das. 2016. Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity. *it - Information Technology* 58, 5 (jan 2016), 237–245. DOI: http://dx.doi.org/10.1515/itit-2016-0008

[14] Sauvik Das, Laura A Dabbish, and Jason I Hong. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors.

[15] Sauvik Das, Eiji Hayashi, and Jason Hong. 2013. Exploring Capturable Everyday Memory for Autobiographical Authentication. In *Proc. UbiComp'13*.

[16] Sauvik Das, Hyun Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The Effect of Social Influence on Security Sensitivity. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS'14)*.

[17] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. ACM Press, New York, New York, USA, 1416–1426. DOI: http://dx.doi.org/10.1145/2675133.2675225

[18] Sauvik Das, Gierad Laput, Chris Harrison, and Jason I Hong. 2017. Thumprint: Socially-Inclusive Local Group Authentication Through Shared Secret Knocks. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM Press, New York, New York, USA, 3764–3774. DOI: http://dx.doi.org/10.1145/3025453.3025991

[19] Darren Davis, Fabian Monrose, and Michael K Reiter. 2004. On User Choice in Graphical Password Schemes. In *Proceedings of the 13th USENIX Security Symposium (SEC'04)*. https://dl.acm.org/citation.cfm?id=2516700

[20] Rachna Dhamija and Adrian Perrig. 2000. Deja Vu : A User Study Using Images for Authentication. *Proc. of the 9th USENIX Security Symposium (SSYM)* 9, 102590 (2000), 1–4. https://www.usenix.org/events/sec00/full

[21] Astrid Dickinger, Mitra Arami, and David Meyer. 2008. The role of perceived enjoyment and social norm in the adoption of technology with network externalities. *European Journal of Information Systems* 17, 1 (2008), 4–11. DOI: http://dx.doi.org/10.1057/palgrave.ejis.3000726

[22] Huong Q Dinh, Neff Walker, Chang Song, Akira Kobayashi, and Larry F Hodges. 1999. Evaluating the Importance of Multi-sensory Input on Memory and the Sense of Presence in Virtual Environments. In *Proceedings IEEE Virtual Reality (Cat. No. 99CB36316)*. 222–228.

[23] Joshua Foer. 2012. *Moonwalking with Einstein: The art and science of rembering everything*. Penguin.

[24] William Gardner, Edward P. Mulvey, and Esther C. Shaw. 1995. Regression analyses of counts and rates: Poisson, overdispersed Poisson, and negative binomial models. *Psychological Bulletin* 118, 3 (1995), 392–404. DOI:http://dx.doi.org/10.1037/0033-2909.118.3.392

[25] Ceenu George, Daniel Buschek, Mohamed Khamis, and Heinrich Hussmann. 2019. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. (2019).

[26] Alina Hang, Alexander De Luca, and Heinrich Hussmann. 2015a. I Know What You Did Last Week! Do You?. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. 1383–1392. DOI: http://dx.doi.org/10.1145/2702123.2702131

[27] Alina Hang, Alexander De Luca, Matthew Smith, and Michael Richter. 2015b. Where Have You Been ? Using Location-Based Security Questions for Fallback Authentication. *Symposioum on Usable Privacy and Security* (2015), 169–183.

[28] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2016. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *SOUPS '14: Proceedings of the Tenth Symposium On Usable Privacy and Security*. 213–230.

[29] Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, and Ian Oakley. 2013. CASA: A Framework for Context-Aware Scalable Authentication. In *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS'13)*.

[30] Brent Hecht, Lauren Wilcox, Jeffrey P. Bigham, Johannes Schoning, Ehsan Hoque, Jason Ernst, Yonathan Bisk, Luigi De Russis, Lana Yarosh, Bushra Anjum, Danish Contractor, and Cathy Wu. 2018. It's Time to Do Something: Mitigating the Negative Impacts of Computing Through a Change to the Peer Review Process. (2018). https://acm-fca.org/2018/03/29/negativeimpacts/

[31] Cormac Herley and P van Oorschot. 2009. Passwords: If We're So Smart, Why Are We Still Using Them? *Proceedings of the 13th International Conference on Financial Cryptography and Data Security (FC'09)* (2009). DOI: http://dx.doi.org/10.1007/978-3-642-03549-4_14

[32] Christina Katsini, Christos Fidas, George E Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. Influences of human cognition and visual behavior on password strength during picture password composition. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. ACM, 87.

[33] Eric Krokos, Catherine Plaisant, and Amitabh Varshney. 2018. Virtual memory palaces: immersion aids recall. *Virtual Reality* 0123456789 (2018), 1–15. DOI: http://dx.doi.org/10.1007/s10055-018-0346-3

[34] Eric L.G. Legge, Christopher R. Madan, Enoch T. Ng, and Jeremy B. Caplan. 2012. Building a memory palace in minutes: Equivalent memory performance using virtual versus conventional environments with the Method of Loci. *Acta Psychologica* 141, 3 (2012), 380–390. DOI: http://dx.doi.org/10.1016/j.actpsy.2012.09.002

[35] Heather Richter Lipford and Mary Ellen Zurko. 2012. Someone to watch over me. In *Proceedings of the 2012 workshop on New security paradigms - NSPW '12*. 67. DOI: http://dx.doi.org/10.1145/2413296.2413303

[36] Eleanor A. Maguire, Elizabeth R. Valentine, John M. Wilding, and Narinder Kapur. 2003. Routes to remembering: The brains behind superior memory. *Nature Neuroscience* 6, 1 (2003), 90–95. DOI: http://dx.doi.org/10.1038/nn988

[37] Fabian Monrose and Aviel D. Rubin. 2000. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems* 16, 4 (2000), 351–359. DOI: http://dx.doi.org/10.1016/S0167-739X(99)00059-X

[38] Lawrence O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (2003), 2021–2040. DOI: http://dx.doi.org/10.1109/JPROC.2003.819611

[39] Karen Renaud. 2005. Evaluating Authentication Mechanisms. In *Security and Usability*, Lorrie Faith Cranor and S Garfinkel (Eds.). O'Reilly Media, 103–128.

[40] Karen Renaud and Antonella De Angeli. 2004. My password is here! An investigation into visuo-spatial authentication mechanisms. *Interacting with Computers* 16, 6 (2004), 1017–1041. DOI: http://dx.doi.org/10.1016/j.intcom.2004.06.012

[41] Oscar Rosello, Marc Exposito, and Pattie Maes. 2016. NeverMind : Using Augmented Reality for Memorization. *UIST'16 Adjunct* (2016), 215–216. DOI: http://dx.doi.org/10.1145/2984751.2984776

[42] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI '07)*. ACM Press, New York, New York, USA, 895–904. DOI: http://dx.doi.org/10.1145/1240624.1240759

[43] Larry R. Squire. 2004. Memory systems of the brain: A brief history and current perspective. *Neurobiology of Learning and Memory* 82, 3 (2004), 171–177. DOI: http://dx.doi.org/10.1016/j.nlm.2004.06.005

[44] Xiaoyuan Suo, Y. Zhu, and G.S. Owen. 2005. Graphical passwords: A survey. In *Proc. ACSAC'05*. IEEE. DOI: http://dx.doi.org/10.1109/CSAC.2005.27

[45] Julie Thorpe, Brent MacRae, and Amirali Salehi-Abari. 2013. Usability and security evaluation of GeoPass: a geographic location-password scheme. In *Proceedings of the Ninth symposium on usable privacy and security*. ACM, 14.

[46] Endel Tulving. 1985. How many memory systems are there?. 40, 4 (1985), 385–398. http://psycnet.apa.org/journals/amp/40/4/385/

[47] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, Thorsten Holz, Horst Görtz, and Ruhr-university Bochum. 2013. Quantifying the Security of Graphical Passwords : The Case of Android Unlock Patterns Categories and Subject Descriptors. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS'13)*. 161–172. DOI: http://dx.doi.org/10.1145/2508859.2516700

[48] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies* 63, 1-2 (jul 2005), 102–127. DOI:http://dx.doi.org/10.1016/j.ijhcs.2005.04.010

[49] F.A. Yates. 1966. *Art of Memory*. London: Pimlico.