Towards Improving the Usability of System-Assigned PINs: Can Implicit Learning Techniques Help?

by

Israt Jahan Jui

A thesis submitted to the
School of Graduate and Postdoctoral Studies in partial
fulfillment of the requirements for the degree of

Master of Science

in

Computer Science

Ontario Tech University
Oshawa, Ontario, Canada
August 2023

THESIS EXAMINATION INFORMATION

Submitted by: Israt Jahan Jui

Master's in Computer Science

Thesis title: Towards Improving the Usability of System-Assigned PINs: Can Implicit Learning Techniques Help?

An oral defense of this thesis took place on 4th August 2023 in front of the following examining committee:

Examining Committee:

- Chair of Examining Committee: Dr. Ying Zhu
- Research Supervisor: Dr. Julie Thorpe
- Examining Committee Member: Dr. Peter Lewis
- Thesis Examiner: Dr. Loutfouz Zaman

The above committee determined that the thesis is acceptable in form and content and that a satisfactory knowledge of the field covered by the thesis was demonstrated by the candidate during an oral examination. A signed copy of the Certificate of Approval is available from the School of Graduate and Postdoctoral Studies.

Abstract

Personal Identification Numbers (PINs) are widely used for automated teller machines (ATMs), computers, mobile devices, debit cards, and credit cards. People tend to choose easy-to-recall PINs that are related to important dates (e.g., birthdays or anniversaries), or keypad patterns. Unfortunately, such easy-to-recall PINs can be vulnerable to guessing attacks. System-assigned PINs can improve PIN security; however, they are difficult to remember. This thesis designs and evaluates a set of training techniques to improve the usability of system-assigned PINs. We evaluate our designs through two studies (N=126 and N=184), showing that some designs improve usability in terms of login time and user perception. Our results suggest that some designs may also have the potential to improve PIN memorability. Our results should be of interest to practitioners and researchers working on authentication systems and usability.

Keywords: Authentication, Personal Identification Numbers (PINs), Implicit Learning, Contextual Cueing (CC), Usability

Author's Declaration

I hereby declare that this thesis consists of original work of which I have authored. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize the University of Ontario Institute of Technology to lend this thesis to other institutions or individuals for the purpose of scholarly research. I further authorize University of Ontario Institute of Technology to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research. I understand that my thesis will be made electronically available to the public.

Israt Jahan Jui

Statement of Contributions

I hereby certify that I have been the primary contributor of this thesis by designing and implementing the experiments. I have also written most content of this thesis. However, some texts of this thesis are borrowed from the conference paper jointly coauthored with my thesis supervisor Dr. Julie Thorpe.

Acknowledgements

Firstly, I want to give a big thank you to my supervisor, Dr. Julie Thorpe. Her knowledge, guidance, and support have been really important for me in finishing this thesis. She always encouraged me and gave me helpful feedback. This helped me grow in my studies and successfully finish my work.

I am very thankful to my parents. They always believed in me and helped me, even when times were hard. Their love kept me strong. Because of their support and encouragement, I was able to pursue my dreams in North America. Their hard work and strength have always inspired me to do better in everything I do, including my studies. Truly, they have made a tremendous difference in my life.

My brother has been a great source of inspiration and encouragement for me. I appreciate him for always being there.

Furthermore, my heartfelt thanks go out to my friends, specially Tanzina and Alireza from my lab. They have been steadfast companions on this journey, always there to lend a hand when needed. They have made significant contributions to my study, through their constant support and encouragement which made the journey seem easier. Their assistance in countless ways and their unwavering faith in me have left a profound impact that extends beyond the confines of this study. Also, thanks

to Rumpa for always supporting me.

Finally, my little nephew, who I love so much. He brings joy and love into my life, and that has motivated me to do my best.

In short, I am very grateful to all of you. I couldn't have finished this thesis without your love and support. Thank you.

Contents

List of Tables

List of Figures

List of Abbreviations

PIN	Personal Identification Number
CC	Contextual Cueing
SP	Semantic Priming
RP	Repetition
CC-RP	Contextual Cueing and Repetition
CC-v1	Contextual Cueing Version 1
CC-v2	Contextual Cueing Version 2
IL	Implicit Learning

Chapter 1

Introduction

In this chapter, we first explain the system-assigned PINs, their importance, and the problem with system-assigned PINs. Then we briefly describe the thesis contributions to improve the usability of system-assigned PINs usability and user perception. Finally, we present the content organization of this thesis.

1.1 Motivation

As mobile devices, tablets, and personal computers become an increasingly important part of our everyday lives, protecting the security of these smart gadgets becomes essential. Our society becomes more interconnected and reliant on technology, the devices we use daily aren't just tools; they're gateways to our personal, financial, and professional worlds [1]. Mobile devices, tablets, and personal computers are now commonly used by everyone and hold a lot of personal and private information [2].

These devices not only hold personal pictures but also play a crucial role in security checks like multi-factor authentication. This makes it extremely important to have strong security measures in place to protect them and the information they contain.

Personal Identification Numbers (PINs), in this context, have become a foundational aspect of device security. Whether it's to access a banking app, unlock a device, or verify a transaction, PINs are a crucial line of defense. However, the human element, with its tendency to prioritize convenience over security, often results in weak PINs, rendering this line of defense susceptible to breaches. By restricting attempts to enter incorrect PINs, many operating systems protect against unauthorized access. This security mechanism, however, frequently falls short since hackers may still be able to unlock a device through speculation, especially if the PIN was chosen by the user.

Banking and Financial Institutions The finance sector, with its countless mobile banking apps and digital payment systems, relies heavily on PINs as the primary security protocol. Every time a user logs into their bank app or makes a digital transaction, a PIN serves as the primary identity verification step. However, the propensity of users to opt for easily recallable PINs exposes a security vulnerability. A woman in Canada was devastated when her wallet got stolen, and more than $20,000 in fraudulent purchases were made on her credit cards [3]. When she asked the bank to refund her $9,242, they refused to give her back all but $470, citing that the PIN she used was associated with her birthday and, therefore, not secure enough. This is a common problem many people face, as it turns out that using dates as PINs is widespread but insecure [4].

It is found that usually, users choose PINs that are easy to remember but common numeric sequences (1234), repeat the same key (9999), or choose a path of adjacent keys (2580) [5]. The user has this tendency to choose PIN which is related to their birthday and important dates [4]. On the other hand, attackers would only have a 0.03 percent chance of guessing the four-digit PIN in three tries if the PIN is system assigned instead of user-chosen [5]. A system-assigned PIN is randomly generated by the system and assigned to its users. It makes guessing attacks infeasible and provides better security. In the past, banks used to assign PINs to customers for added security. However, in the 1980s, as a marketing tactic, banks started offering the option for customers to choose their own PINs [5]. This has now become the standard practice. However, it has been recommended that banks abandon customer-selected banking PINs, in the long run [4]. In recent years, banks have started to shift back towards using system-assigned PINs for added security [6]. Herein, our training system can be useful. By training users to remember and use system-assigned PINs, financial institutions can drastically reduce the risk of unauthorized breaches, ensuring that users' funds and data remain secure.

Health Care Sector Medical records are among the most sensitive types of personal data. With the advent of telemedicine and digital health records, there's an increasing reliance on PINs to secure this data. Our training system can ensure that medical staff and patients alike utilize robust PINs, minimizing the chances of unauthorized access and potential misuse of medical data [7].

Home and Office Security Systems Digital security systems, whether for homes or offices, often employ PINs as a means of access. Given the real-world implications – where a breach could lead to theft or harm – there's a pressing need for robust PIN security. Moreover, users have this likelihood of reusing their PINs. So, the system-assigned PIN provides more security to users than their chosen one. The system-assigned PIN is also important for home security systems. Nisbet et al studied 3.4 million PIN codes and found that around 11% of users use 1234 as their PIN code in their alarm systems [8] [9]. So, 374,000 out of the 3.4 million house owners and business owners use this PIN for their alarm systems which is very vulnerable to guessing attacks [9]. Easily guessable home security system PINs can cause huge danger and various losses. System-assigned PIN can also ensure more security in home security systems. Our training system can ensure that homeowners and office managers adopt strong, system-assigned PINs, bolstering physical security.

Mobile Industry Implications The advent of FIDO (Fast IDentity Online) standards has revolutionized mobile security. Unlike traditional methods which often depend on passwords, FIDO utilizes local authentication such as biometrics or PINs [10]. Within this system, a device's PIN isn't just a barrier to the device itself but potentially a gatekeeper to various services where FIDO authentication is enabled.

In the realm of mobile and application security, PINs function as the primary access mechanism. A compromised PIN doesn't just jeopardize the device, but potentially every service authenticated via that device. Hence, the robustness of these PINs becomes paramount. Our initiative aims to ensure users are equipped with strong, system-assigned PINs, enhancing their overall security posture. By facilitating easier adoption and recall of these PINs, we aim to bolster the security of devices and services, especially those aligned with the FIDO framework.

Understanding the criticality of PINs in these varied scenarios, it's evident that the often-followed practice of using predictable PINs poses significant risks. The story of the Canadian woman is a stark reminder of the repercussions of such vulnerabilities.

While system-assigned PINs offer an impressive solution in terms of security, their innate unfamiliarity often poses significant usability challenges. Our initiative seeks to bridge this gap. Drawing upon the principles of implicit learning and repetition, we've crafted training systems that blend the high security of system-assigned PINs with the comfort and memorability of user-selected ones. Through a series of user studies, We aim to understand how well our methods work, setting the stage for a balance between strong security and a design that is friendly and easy for users in our online world. Specifically, we conducted two user studies revolving around these research questions:

1. Do our training methods make logging in with a PIN faster?
2. Do our methods enhance the memorability of PINs?
3. How do users perceive the usability of our training techniques?

1.2 Contributions

This thesis presents a comprehensive exploration of novel training techniques aimed at enhancing the user experience and efficiency in the context of system-assigned PINs. Our innovative contributions to this field can be delineated as follows:

1. **Innovative Training Techniques:** We have pioneered a variety of training methods, including Contextual Cueing (versions CC-v1 and CC-v2), Semantic Priming (SP), Repetition (RP), and a novel approach that combines Contextual Cueing and Repetition (CC-RP). These methods, designed to be brief and efficient, typically span a single session lasting 16 to 34 seconds.
2. **Empirical Analysis:** To evaluate the effectiveness and usability of our designs, we conducted two separate studies, involving *N=126* and *N=184* participants,

respectively.

3. Our in-depth examination of the proposed designs reveals considerable improvements over previous approaches to train people to remember their given PINs. Contrary to the spaced repetition approach adopted by Schechter et al., which necessitates training up to four days with 25 times of login with the interaction of median of around 120.8 seconds with the system (the median time is calculated from the Figure 8 given in their study [5] (Figure 3.3)), our training methods drastically reduce this timeframe to a mere 16-34 seconds. As a direct consequence, our techniques also manage to reduce login times. This contrasts significantly with the chunking policy of Huh et al., which results in a median login time of 40 seconds[6]. In contrast, our CC-v2, CC-RP, and RP training techniques yield notably lower login times of 8.19, 7.52, and 6.77 seconds, respectively. The majority of the training groups usually scored higher on the System Usability Scale (SUS) than the control group in terms of how well these training approaches were perceived by users.

These contributions not only advance the state of the art but also pave the way for future investigations. Our findings stimulate discussions and we suggest avenues for future research in this domain.

1.3 Thesis Organization

This thesis is organized as follow:

Chapter 2 explains the authentication, its history, how it is used in different devices. In **Chapter 3**, we review the related work.

In **Chapter 4**, we present our system design.

In **Chapter 5**, we describe our methodology for the research study.

In **Chapter 6**, we analyze the result of our study.

In **Chapter 8**, we provide conclusion and potential directions for future researchers.

1.4 Thesis Summary

Personal Identification Numbers (PINs) are a widely used method for securing access to several services and systems. They are very simple and easy to use, yet they frequently have serious security flaws. When users are given the option to choose their own PINs, the numbers they choose frequently follow recognizable patterns, leaving them open to attacks[4]. This issue is addressed by system-assigned PINs, which increase security by adding randomization to PIN assignments[4]. However, people frequently reject them because they find them hard to remember, which lowers their usability and acceptability.

In response to this difficulty, we created and thoroughly examined five cutting-edge training methods intended to improve the memorability of system-assigned PINs. Our goal was to improve user experience overall without sacrificing the security advantages that system-assigned PINs already provide. Our methods were classified as CC-v1, CC-v2, CC-RP, SP, and RP respectively.

We conducted two extensive experiments with various populations, with N=126 participants in the first research and N=184 participants in the second, to evaluate the effectiveness of these strategies. PINs were issued to the participants at random, and then there was a brief training session. This training session lasted approximately 16 to 34 seconds, designed to be time-efficient and practical for real-world application.

Following the training, participants were given a distractor task in the form of a questionnaire designed to shift their attention away from the PIN they were assigned. We added this in an effort to more closely mimic real-life situations in which users are not always paying attention to their PINs. Following that, participants were instructed to log in using their given PINs. After that users had to answer a short questionnaire. Participants were prompted to log in once again using their allocated PINs after a break of 24 hours, which was meant to the time frame designed to simulate everyday usage patterns. Whether or whether not they were successful, they had to fill out a post-study questionnaire.

The first study involved four groups, namely CC-v1, Control, RP, and SP, and was conducted on a crowd source platform Amazon Mechanical Turk (MTurk). Based on the findings and insights we gathered from the MTurk study, we introduced modifications to the training techniques and added two new groups for the second study. This subsequent study, conducted with university student participants, also included four groups: CC-v2, Control, CC-RP, and RP.

Our study of the data showed that, compared to the control group, the training sessions significantly reduced login times, confirming the effectiveness of our training methods. After a 24-hour period, all groups' average login times ranged from 6 to 8 seconds, compared to an average of 26 seconds for the control group. The fact that trained participants log in much quicker highlights the potential of our training methods to increase usability.

The shortness of our training sessions is noteworthy. The median training time is between 16 to 34 seconds, they represent a time-efficient solution when compared to existing training interventions that can span several days[5]. In addition, the majority of the training groups usually scored higher on the System Usability Scale (SUS) than the control group in terms of how well these training approaches were perceived by users.

While all training techniques demonstrated a high recall rate for short-term memorability, long-term memorability (after 24 hours) was found to be dependent on the specific training technique. In both the MTurk and student study, CC-v1 and CC-v2 training techniques had better memorability compared to other groups in terms of long-term recall rate. These findings suggest that our training techniques may contribute to the retention of these PINs over a longer period.

Our work is not just moving the current knowledge forward, but also providing a stepping stone for future explorations for system-assigned PINs. Our discoveries spark interesting discussions and give guidance for future studies.

Chapter 2

Background

In this chapter, we provide an understanding of authentication, its origin, and its current applications in various devices. We also discuss and compare proposed authentication schemes.

2.1 History of Authentication

Long before the invention of computers, the idea of authentication, or the act of confirming the identification of a person or item, has been around in various forms. In order to verify a user's identity through authentication, specific unique bits of data are used, called "authentication factors"[11]. In today's digitized world, the demand for authentication is omnipresent. The need for a safe way to authenticate has become very important. Ancient civilizations utilized distinctive seals or signatures to confirm the authenticity of documents, which is considered to be the first form of verification. Wax seals with a distinctive pattern or symbol were once used to certify papers.

In the digital era, the advent of computing systems in the mid-20th century brought about the need for user authentication. Fernando Corbató, a scientist at the Massachusetts Institute of Technology (MIT), created a system in the 1960s that allowed multiple people to use a computer simultaneously[12]. To ensure privacy for each user, Corbató invented the use of passwords. His "Compatible Time-Sharing System" (CTSS) featured a LOGIN command that prompted users to enter a password. Corbató's password system remains dominant because of its simplicity and ease of use. While token-based authentication uses devices to generate codes, they can be lost. Biometrics, like fingerprint and facial recognition, present unique identification methods but come with privacy concerns and can be inconsistent. Graphical passwords use images or patterns but can be easily compromised if observed. Smart cards enhance security by pairing with passwords, but this adds to inconvenience. Behavioral biometrics evaluates patterns in user behavior, yet it demands a lot of data and isn't always consistent. Despite these alternatives, the traditional password has endured due to a balance of security and convenience.

2.2 Authentication in Different Devices

Unique identifiers of Authentication fall into three categories: knowledge factors (what the user knows, such as textual or graphical passwords [13] [14] [15] [16], possession factors (what the user has, often a physical object like a smart card [17], and inherence factors (who the user is, represented through biometrics such as face recognition, fingerprints, or keystroke dynamics) [18] [19] [20]. Authentication methods vary from device to device:

Computers: For computers, the combination of a username and password has been the longstanding method of authentication. It offers a balance of simplicity and security that is universally recognized and understood. With technological advancements, biometric identification, such as fingerprint and facial recognition, has been introduced, especially in modern computers and laptops. While biometrics provides a unique and often more secure method of identification since they are based on individual physiological traits, they are not without limitations. Biometrics can sometimes fail to recognize the user due to environmental factors, wear and tear (like a scar on a fingerprint), or system errors. Furthermore, there are concerns over privacy, data theft, and the inability to change one's biometrics in the event of a security breach, unlike changing a password. In comparison to passwords, while biometrics offer enhanced security, they do not entirely replace the need for passwords in many scenarios due to these challenges. As such, the traditional password system, despite its vulnerabilities, often works in tandem with newer authentication methods to ensure a more comprehensive security approach.

Mobiles: In order to provide secure access, mobile devices often use several techniques. Personal Identification Numbers (PINs), pattern locks, and biometrics like fingerprint and face recognition are some of these. Among all of them, PIN is the most popular and simple authentication system. Most Android and iOS devices use PIN as the backup authentication even though biometrics are used.

Networks and Online Platforms: The standard protocol for user authentication on networks and online platforms include a combination of usernames and passwords. Many of these platforms have augmented their security by offering options for two-factor authentication (2FA) or multi-factor authentication (MFA). 2FA is an authentication mechanism that requires users to verify their identities through two different types of validation. One factor authentication is typically something knowledge-based authentication - password or PINs. The second factor is usually something the user possesses or an inherent, these could include one-time passwords (OTPs), biometric data, or physical hardware tokens, providing an additional level of protection against unauthorized access.

An OTP is a password that is typically emailed to a user's registered cellphone number or email address and is good for just one login session or transaction. OTPs are a more secure form of authentication since they are immune to replay attacks. If an attacker is able to intercept the OTP during a login, they can't reuse it because it's only valid for a single use. If they try to reuse it, the system will reject it as it's expecting a new, different OTP. This is why OTPs offer better security against such replay attacks

FIDO2 (Fast IDentity Online) is another emerging standard for password-less authentication. Unlike traditional methods, FIDO2 uses cryptographic login credentials that are unique to each website. When a user first registers with an online service, their device generates a new pair of keys: a private one, securely kept on the device, and a public one sent and stored by the online service. For subsequent logins, the online service sends a cryptographic challenge to the user's device. The device then responds by signing this challenge with its private key. The service confirms the user's identity by verifying this against the stored public key. This method ensures added security as the private key on the user's device is often safeguarded by a combination of elements like a physical security key, a PIN, or biometrics such as fingerprint or facial recognition. This approach makes FIDO2 resilient against common cyberattacks like phishing. Its wide acceptance across major browsers and platforms, including Android and Windows, underscores its potential to redefine our online authentication systems, moving beyond traditional password vulnerabilities. It can be a potential replacement for text-based passwords[10]. It is a single-factor passwordless authentication and also supports 2-factor authentication. It provides keys that are secure against server breaches, phishing, and replay assaults[10]. It is supported by almost all browsers, and native versions for Android and Windows are available, with more on the way.

Internet of Things (IoT) Devices: IoT devices, including smart fridges, light bulbs, door locks, or garage locks, use digital certificates to securely communicate with each other. User-to-device authentication might also include password and PIN usage, ensuring secure and efficient operation.

2.3 Comparison of Authentication Schemes

A wide range of different authentication systems have been put out during the past 20 years. One-time passwords, hardware tokens, phone-assisted schemes, federated login protocols, graphical password schemes, cognitive authentication methods, biometrics, and password management software are some of these. Bonneau et al.[21] assessed these suggested solutions based on a number of factors, such as usability, deployability, and security advantages. They found that most of the alternative authentication techniques outperform passwords in terms of security, which they anticipated considering that these schemes were developed by the security community. However, the usability performance of various systems varies, showing a need for making them easier to use. Significantly, when it comes to deployability, they found that all schemes underperformed compared to passwords. This makes sense because passwords are old and we are used to them, they are easy to implement. From their study, they could not find any schemes that offer all of these advantages, and none maintains the complete range of advantages offered by historical passwords.

It is obvious that security, usability, and deployability must be balanced as we continue to search for new authentication techniques in a world that is becoming more digital. It is clear that despite their flaws, passwords and PINs remain popular because of their intrinsic benefits and the inherent challenges in replacing an established system.

2.4 History of PINs

Personal Identification Numbers (PINs) are widely popular now. They are usually a string of four to six numbers that serve as a straightforward method to verify a user's identity. Because of their simplicity and usability, they are being used in various fields such as banking, telecommunications, and computer systems.

James Goodfellow, a Scottish engineer, came up with the idea for a PIN in the 1960s. Banks were looking for an automated way to let customers access their money after hours [22]. He took on this issue and created a system that allowed users to withdraw money from automated teller machines (ATMs) using a coded card and a personal number (Figure 2.1). The PIN was proposed as a numerical password that verified a user's identification and generally included four to six digits. The concept was very simple but incredibly powerful, especially with given technical limitations.

However, the first widely publicized cash machine, developed by John Shepherd-Barron and launched by Barclays Bank, came to light in 1967[23]. While Shepherd-Barron was the man behind this first ATM, the system used was not quite as we know it today. The Barclays' machine relied on cheques infused with a mildly radioactive

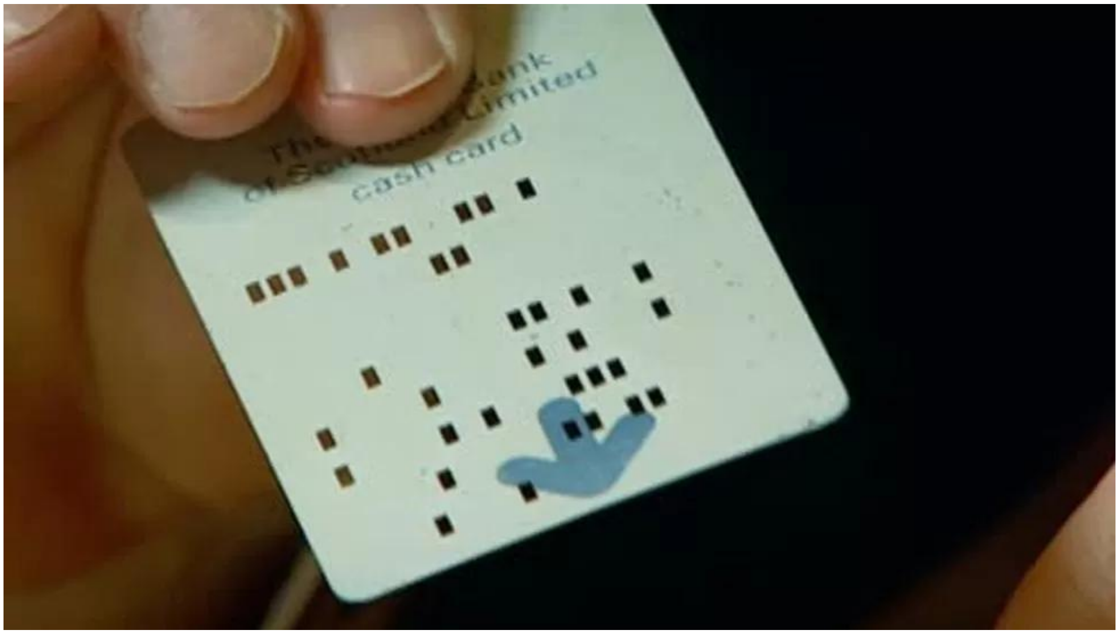


Figure 2.1: First ATM card developed by Mr Goodfellow[23]

substance, which the machine detected before matching the cheque against a PIN (Figure 2.2).

The early ATMs used a two-factor authentication mechanism that required a user to insert a plastic card that had been punched and input the right PIN in order to withdraw money. The ATM verified that the PIN entered matched the card's encrypted PIN. When the user's card and PIN were matched, a successful transaction resulted.

PINs were more widely used as technology advanced outside of ATMs. Now it is widely used in mobile devices, tablets, IoT devices, and even in PCs. Though biometric security methods like fingerprint scanners and facial recognition technologies

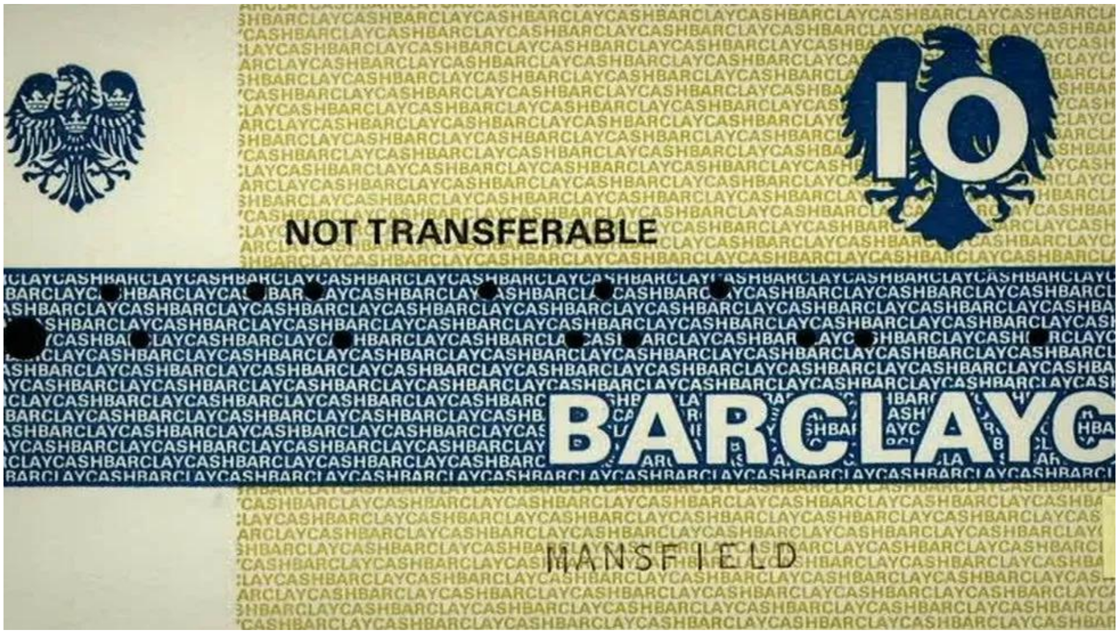


Figure 2.2: The Barclay's cash machine used cheque

were launched, PINs are still being used. These devices allow authentication by basic device-unlock secrets, such as numeric PINs or graphical passwords, whether they run Windows, Android, or iOS[5].

Even if PINs have played a crucial role in the development of digital security, it is important to note that they are not resistant to breaches. Methods such as 'shoulder surfing' (observing someone enter their PIN) and brute force attacks (trying all possible combinations) pose significant risks. Nevertheless, their simplicity, ease of use, and compatibility with two-factor authentication have ensured that PINs remain a vital part of our digital security landscape.

Chapter 3

Related Work

We focus our review on PINs: both user-chosen and system-assigned. Since some of our training methods involve the use of implicit learning techniques, we also discuss authentication methods that employ implicit learning.

3.1 User-Chosen PINs

A study by Bonneau et al.[4] found that many people choose PINs based on birthdays or other memorable dates. Based on a survey of over 1100 banking clients, they evaluated the spread of banking PINs and the regularity of access control behaviors such as exchanging PINs with partners and repeating the same PINs. They found a pattern of choosing birth dates or other memorable dates, as in user-chosen PINs. Another study, researchers analyzed 3.4 million four-digit PINs sourced from leaked passwords[24][25]. He found that 1234 was used by 10.7% of all PINs, followed by 1111 and 0000. Moreover, keyboard patterns like 2580, which is a “straight-shot” down the center of a keypad, and ”across the corners” combinations are notable. Veras et al. [26] discovered that over 15% of passwords have sequences of 5-8 consecutive digits, 38% of which could be categorized as a date. They developed a dictionary of about 15,000 well-known dates that could guess 1% of the passwords from the RockYou dataset. Furthermore, they discovered that around 4% of the passwords used by RockYou were only made up of numbers, which are easily cracked by using a dictionary with about 200,000 entries. They discovered that over 4.5% of RockYou passwords might be classified as dates, either as wholly numeric dates or as dates that spell out the month's name. Khan et al.[27] found that users prioritize memorability over security when choosing PINs and sometimes repeat the same PIN for multiple assets. In their study, the participants were less concerned about their PINs entered via physical methods than those entered on digital platforms. Even though both types of PINs are essentially digital, it's the mode of entry that differentiates them. This is because a possible attacker can break the physical (e.g., digital keypad-based entry systems for garages or homes) PIN, which could result in criminal penalties such as breaking and entering. Users not only choose easy-to-remember PINs but also passwords. While security issues are present in user-chosen PINs across groups, there can be differences based on the user's backgrounds (e.g., language or country of origin) [28].

Ur et al. explored whether users' beliefs of password security reflect reality[29]. They also interviewed users about the security and memorability of various password and password-generating policies. They discovered that participants perceived a password to be considerably less remembered if it was lengthier or included numbers. Other user password studies have indicated that users choose simpler credentials that include names, short words, dates, and patterns, resulting in weaker and easier-to-guess passwords[30][31][32][33][34][35].

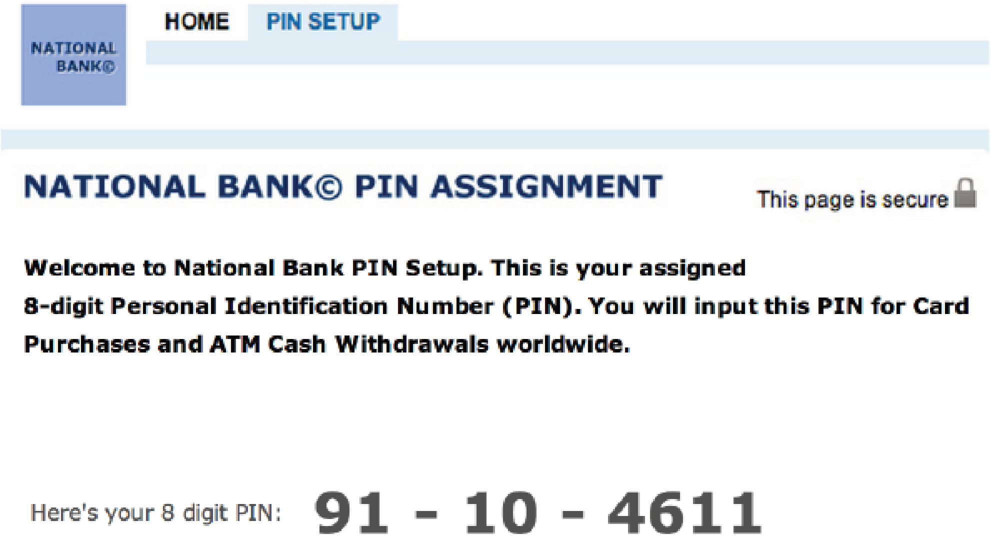
Since user-chosen PINs are easy to remember, some people may think that upgrading four-digit PINs to six-digit PINs can solve the security issue. However, Munyendo et al.[36] found that the 6-digit PIN provides minimal security advantages which are not worth the usability losses such as being faster or simpler to input and easier to remember. Their study asked participants to update 4-digit PINs to 6-digit PINs for their smartphones. They found that an attacker who knows the previous 4-digit PIN can predict over 25% of the 6-digit PINs within ten tries and more than 30% in 30 tries. They conducted an online survey with 1010 participants to replicate significant, real-life scenarios in which customers update their 4-digit PIN to a 6-digit PIN. All the participants were asked to create a PIN code to protect their smartphones. Later they were asked to update their 4-digit PIN to a 6-digit PIN. The authors found that implementing measures like device upgrades and ensuring that a 6-digit PIN doesn't include the user's 4-digit PIN as a sub-sequence significantly improved security, making them harder to guess. According to their findings, updates give little or no protection against targeted or untargeted internet attacks. They found that 6-digit PINs have a negative impact on ease of use and memorability, but users perceived them to be safer. They asked the participants questions to understand users' perceptions of security, memorability, and usability. According to their findings, users believe their 4-digit PINs are easier to remember and simpler to use than 6-digit PINs. However, the participants believed that 6-digit PINs were safer. User-chosen 6-digit PINs are not any more secure than 4-digit. In fact, However, 6-digit PINs are typically more unsafe than 4-digit PINs when a targeted attacker who has knowledge of their previous 4-digit PINs makes up to 10 attempts. However, their result shows that 6-digit PINs offer only a marginal improvement in security compared to 4-digit PINs. Moreover, 6 digit PINs are sometimes even more easily guessed compared to 4-digit PINs. This means that even with longer PINs, the security offered by the PIN-based system is still limited and vulnerable to attacks.

In another study, Wang et al[28] found that demographics create differences in choosing PINs. They conducted a study to compare the characteristics, distribution, and security of Personal Identification Numbers (PINs) chosen by English and Chinese users. They used visualization techniques, semantic models, and Natural Language Processing (NLP) techniques to analyze the PINs. The results showed that there were structural and semantic differences between the PINs of the two user groups. This suggests that different user demographics or backgrounds might adopt varied PIN creation strategies. Understanding these subtle can be instrumental in enhancing authentication mechanisms, tailoring security recommendations, and predicting potential vulnerabilities specific to certain user groups in the context of our work.

3.2 System-Assigned PINs

A system-assigned PIN is randomly generated by the system and assigned to its users. It makes offline guessing attacks infeasible and ensures better security than user-chosen PINs. In the past, banks used to assign PIN codes to customers for added security. However, in the 1980s, as a marketing tactic, banks started offering the option for customers to choose their own PIN codes[5]. This has now become the standard practice. However, Bonneau et al.[4] recommended that banks abandon customer-selected banking PINs in the long run. In recent years, banks have started to shift back towards using system-assigned PIN codes for added security[6]. Though system-assigned PINs are secure, they have very low memorability [37]. James et al.[38] found that older adult users had difficulty remembering their PINs and struggled with face-based authentication systems. They asked participants to memorize 4-digit multiple PINs and tested this weekly over a period of three weeks. They practiced learning the PIN code by typing in the code for a specific account five times. Later in the authentication step, participants were asked to input their PIN five times for each account. They found that older people performed low compared to young adults and their total accuracy was below average. Young participants' successful attempts (out of five total attempts) in Week three were around 3.9 whereas elder users' were about 1.5. Their result suggested that the younger generation can spend up to 50 percent less time to pass the authentication procedure in both PINs and graphic access mechanisms.

Huh et al. [6] used number-chunking techniques (breaking a single number into multiple smaller numbers) to investigate the memorability of system-assigned PINs, focusing on the implications of increasing PIN length, from 4-digit PINs to 8 digits. For example, if the PIN is 480271, then according to their chunking method, it will be shown as 48-0271. In their number chunking policies, they included at least one chunk with 4 digits, with the smallest chunk having no fewer than 2 digits. During the study, each participant was given a system-generated PIN code with a random chunking policy. They were asked to re-enter their assigned PIN three times. Later the participants were asked a series of questions about cognition and memory strength. After that, they were asked to re-enter their assigned PIN code again. Users who successfully input the PIN correctly after 2 days later were asked to enter the PIN code again. They found without chunking policy, 4 and 6-digit system-assigned PINs had a 74% and 55% success rate two days after it was assigned with mean login time of 22.6 and 35.5 seconds respectively. Using Chunking policy, 6 digits PINs have a 57% success rate after two days of assignment and the mean login time was 41.7 (6:2-4) and 40.7 (6:4-2) seconds.



NATIONAL BANK© PIN ASSIGNMENT

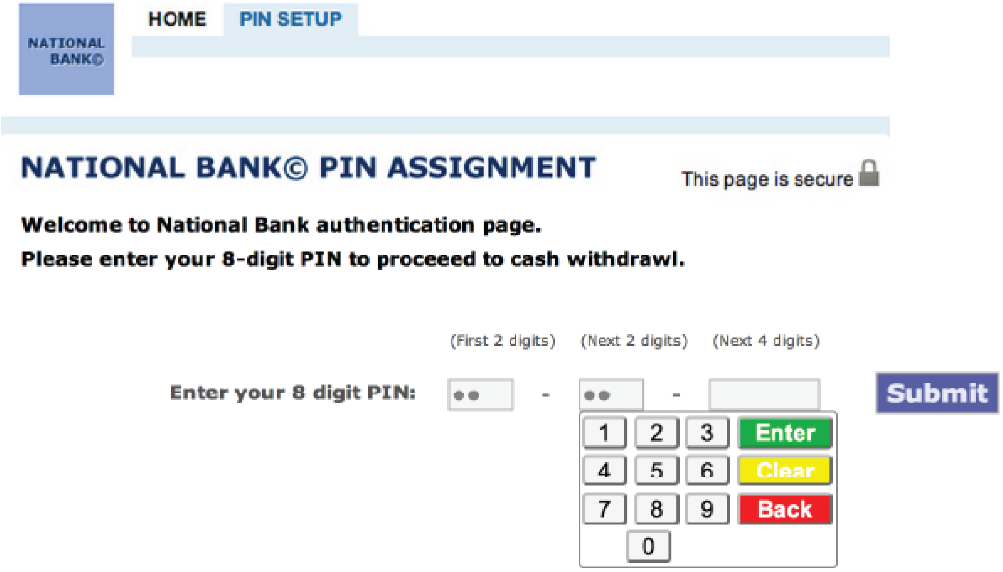
This page is secure

Welcome to National Bank PIN Setup. This is your assigned 8-digit Personal Identification Number (PIN). You will input this PIN for Card Purchases and ATM Cash Withdrawals worldwide.

Here's your 8 digit PIN: 91 - 10 - 4611

Figure 3.1: User study screenshot: Assigned PIN - from Huh et al. study on chunking policy [6]

To improve the memorability of system-assigned secrets Al Ameen et.al [39] proposed a method called CuedR. This method provides users with multiple cues, such as visual, verbal, and spatial, to help them memorize and recall random passwords assigned by the system. Their results showed 100% recall of passwords within three attempts. Still, this approach may not be used in PINs. Another study has been done to address the trade-off between password security and memorability. Huh et al.[40] proposed a new password scheme called "Surpass". They assessed the security and recall of the 8 characters of Surpass's password by adjusting the number of



NATIONAL BANK© PIN ASSIGNMENT

This page is secure

Welcome to National Bank authentication page.
Please enter your 8-digit PIN to proceeed to cash withdrawl.

(First 2 digits) (Next 2 digits) (Next 4 digits)

Enter your 8 digit PIN: ●● - ●● -

Figure 3.2: PIN entry chunking UI by Huh et al.[6]

permitted character changes from 1 to 4. According to the findings, password memorability rose as the amount of replacement characters grew, going from 65% for the first randomly generated passwords to 76% when three character modifications were accepted. However, this scheme is only for 8 characters, so it may not generalize for longer or shorter passwords.

A system-assigned PIN can be vulnerable to shoulder-surfing attacks like a user-chosen PIN. Cardaioli et al.[41] studied ATM PINs. In their study, the participants were typically instructed to cover the typing hand with the other hand in order to safeguard their PINs from malicious bystanders. Nevertheless, this approach is vulnerable to shoulder-surfing attacks performed via hidden cameras installed near the ATM to catch the PIN pad. The researchers kept in mind the situation where an ATM PIN pad of the same brand or model as the target can be accessed by the attacker.

The attacker then makes use of that model to guess the numbers the victim pushed when entering the PIN. Their attack's success is due to deep learning architecture that can predict the PIN from the position and motions of the typing hand. They conducted a thorough experimental investigation with 58 users. They can correctly predict 30% of 5-digit PINs using their method in just three tries. In another study, Schneegas et al.[42] investigated the frequency and severity of shoulder surfing attacks on smartphones during authentication events. They found that the opportunity for shoulder surfing-based observation attacks existed in about 10% of all authentication events, with familiar places being particularly vulnerable. In particular, when the attacker was near to the target device, shoulder-surfing assaults on touch-based unlock events were found to be very effective. So, even if a user uses a system-assigned PIN it will not give the user safety from shoulder surfing attacks. However, De Luca et al.[43] presented 'EyePassShapes', an eye-tracking authentication to fight against shoulder surfing attacks. Still this authentication system depends on eye movement, which can be different for each individual and it is not as simple as PINs. Saad et al.[44] developed a mobile application called DSSytem to notify users about potential shoulder surfers. So, it is helpful for system-assigned PINs.

3.3 Authentication Training Techniques

Many studies have examined the use of training techniques to improve the usability of system-assigned authentication secrets. Not all techniques are equally successful; some research found that about half of people prefer to stick to their own memorization strategy [45]. We have categorized existing training techniques as (a) repetition-based or (b) implicit learning-based.

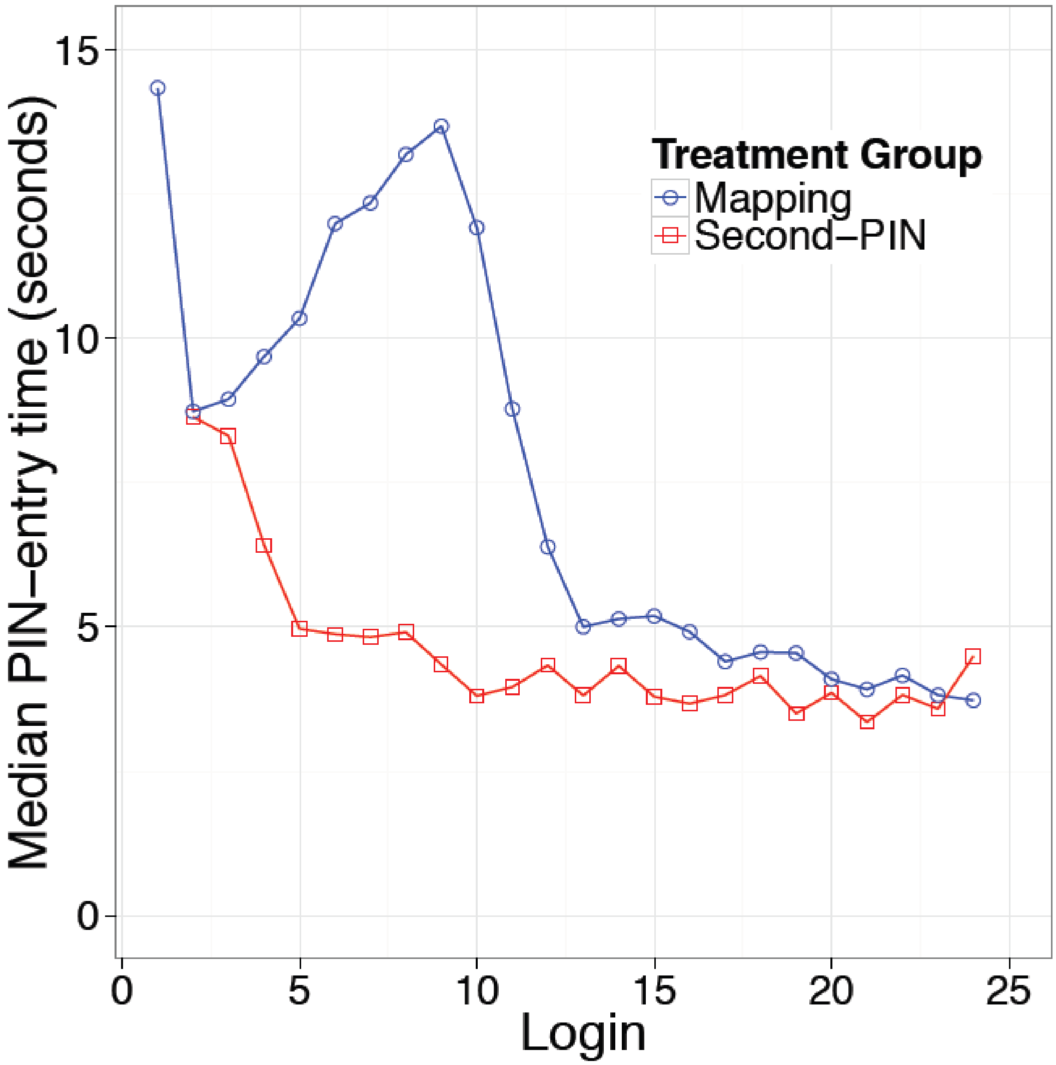


Figure 3.3: Median PIN-entry time for first 24 logins studied by Schechter et al. [5]. The first login time for the Second-PIN treatment (20.85 seconds) is outside the range of the graph.

Repetition-based Schechter et al. [5] studied spaced repetition training techniques to improve the memorability of system-assigned PINs. Their study consisted of two independent experiments: one was based on their previous method [46], assigning users a secondary numeric PIN that they had to enter after their selected PIN each time they logged in (Second PIN). The other technique used a novel strategy that involved changing the layout of the numeric keypad for each login(Mapping). They switched up the standard sequence of the digits on the keypad (as on a phone or calculator). They designed it such that the user's selected PIN would display on the screen in an unpredictable pattern. In the study, participants were required to log in to perform a distractor task, which was a shortened version of an attention game used in a previous study. This task involved five attention trials (lasting 30 seconds each), during which a word ('left' or 'right') was displayed randomly on one side of the screen. Participants were instructed to type a letter from the respective side of the keyboard, ignoring the side of the screen where the word was displayed. Participants were required to wait 30 minutes between each game, and they were given a total of 8 days to complete all 50 games. Each time they played, they had to log in, play the attention-test game for 30 seconds, and then a timer would count down the 30 minutes until they could play again, requiring another login. After their first experiment, they shortened the study to 25 logins within four days. For the Second-PIN approach, the user needs to enter the given PIN first and can bypass the need to enter the user-chosen PIN. The majority of participants were able to enter their assigned PIN without assistance, demonstrating that repetition training was successful over several logins. It took median 3 times of login for users to learn the PINs. Their median learning time for mapping was 117 seconds and for Second PIN was 40 seconds. However, their training time was up to 4 days of 25 times logins. Figure 3.3 shows the median time taken for each login by users. By calculating the time from the figure, we found that their average training time for all 25 times login was around 120.8 seconds. Besides, 10% of the population never acquired their secret in mapping treatment, suggesting that repeated training may not be helpful for all users. Furthermore, it takes four days of training and interaction of around 120.8 seconds, which is too long for users.

Blocki et al. [47] studied spaced repetition by using four Person-Action-Object (PAO) stories to improve the memorability of passwords. Each story had an individual famous person chosen by the users, a machine-generated random action-object pair, and a specific scene in which the participants imagined the narrative taking place. After developing their PAO tales, participants were asked to recall the action-object pairings when they viewed the accompanying scene-person pair. Over the course of more than 127 days, a spaced repetition schedule was used to assess this memory. In 10 tests spread out over around 158 days, the findings revealed that 77% of participants correctly remembered all four stories. The study's effectiveness was dependent on a strict practice routine. In real life, users might find it hard to stick to these memory practice schedules. This could make it harder for them to remember the PAO stories and their passwords.

Implicit learning-based techniques can take many forms. Implicit learning is a natural, unconscious process wherein people create associations without being aware of it or intending to[48]. This sort of learning can occur in the absence of executive attention and is unrelated to individual variations in working memory. Implicit learning is the non-episodic learning of complicated knowledge unconsciously, with no awareness of what has been acquired[49]. Some graphical authentication techniques have been designed that involve testing the accuracy of responses to challenge images, [50], [51] given a registration-time training that employs priming. MooneyAuth [51] employed priming with Mooney pictures[52] to help with the long-term memory of a set of system-assigned images and associated labels. A Mooney image is a two-tone version of a picture with little information that is difficult to classify unless the viewer has already seen the original image. A user is shown Mooney pictures, their related original photos, and labels throughout the training step. As a result, an implicit connection is made between the Mooney picture and the authentication password in the user's memory. A user must label a collection of Mooney photos at the authentication step, and if the user has already seen the images during the enrollment phase, they do it much more accurately. Their novel dynamic scoring technique outperforms the static scoring technique proposed by Denning et al. [50]. They examine the impact of Mooney pictures' long-term priming for a period of up to 8.5 months. Another technique [53] aims to employ implicit learning techniques in order to resist coercion attacks. The proposed system involves a game in a 30 to 45-minute training session, through which the user learns a secret. Login consists of playing the game to demonstrate faster speeds upon the learned sequences. The idea is interesting as users cannot be compelled to disclose the secret since they do not know it consciously, however, it has long (30-45 minute) training times and only 71%, 47%, and 62% of participants could successfully authenticate immediately one week, and two weeks later respectively.

Contextual Cueing describes how constant and recurring contextual information in the visual environment might help an observer's visual processing and attention[54].

In other words, observers can identify or recognize items more quickly and effectively when the environment is predictable based on past interactions with it. It shows how our brains use the order and stability of our visual surroundings to communicate with the outside world more efficiently.

For example, if a person is driving to his/her home country, he/she does not need to rely on each of the street signs or check every turn while he/she is navigating. His/her actions of turning and slowing down are instinctively influenced by context cues like a known building or a tree that he/she has seen countless times before. In another example, your office desk is filled with so many items. If you need to locate a certain book from your desk, you might notice that the book is usually situated next to your coffee mug and notepad. Over time, this contextual cue of the coffee mug and notepad assists you in finding the book faster. All these are manifestations of Contextual Cueing. Semantic priming is like a mental trick where seeing or hearing something can change how you respond to something else later, even if you did not really notice that first thing[55]. When a number is glimpsed momentarily, it might not be consciously acknowledged. Yet, this brief exposure can subtly alter the individual's response to a subsequent number they encounter.

Consider John, a 28-year-old software engineer with a penchant for word games. While engrossed in a cognitive experiment, the term "doctor" is flashed on the screen so fleetingly that John doesn't consciously register it. Moments later, he's presented with a word puzzle: "U R S E." Unbeknownst to him, his mind has already been influenced by the previous word [26]. As a result, he quickly recognizes and completes the word "NURSE." This phenomenon, where a prior stimulus, in this case, "doctor," influences John's response to the subsequent word puzzle, exemplifies semantic priming.

The use of Contextual Cueing (CC)[56] and Semantic Priming (SP)[57] techniques were proposed by Joudaki et al. [58] for training users to recall a system-assigned passphrase. In their research, they designed and tested the system that implemented this perspective using two implicit learning methods: Contextual Cueing and Semantic Priming, with the aim of improving memorability. They had six condition groups, which are 1) CC-SP 2) Control 3) CC 4) SP 5) Repetition 6) Recognition. All these group users were given system-assigned passphrases. Except for the Control group, the users went through training. Later they were asked to log in with their assigned passphrases. The second session was held after two days. The users were asked to input their assigned passphrases. Later after 1 week of the first session, those users were asked again. Their research found that their process significantly upgraded the usability of system-assigned passphrases in terms of recall rate. Joudaki et al. [58] found that Contextual Cueing combined with Semantic Priming (CC-SP) condition works best for short-term and long-term memorability. The recall rate for the first session for this (CC-SP) condition, is 97.69%. On the other hand, the recall rate for the control group is 84.73%. For long-term memory, their experiments showed that the combination of these two techniques (CC-SP) worked best, with 91% recalling their passphrase after two days (vs. 74% in the control group) and one week later (88% vs. 57%). Joudaki et al. [58] additionally showed that this technique was more successful than repetition alone (82% recalled after 2 days and 65% after one week). Additionally, the CC-SP training technique significantly reduced login times. However, the approach had limited security that is comparable to that offered by a system-assigned PIN, but it is not as useful in as many settings as a PIN would be.

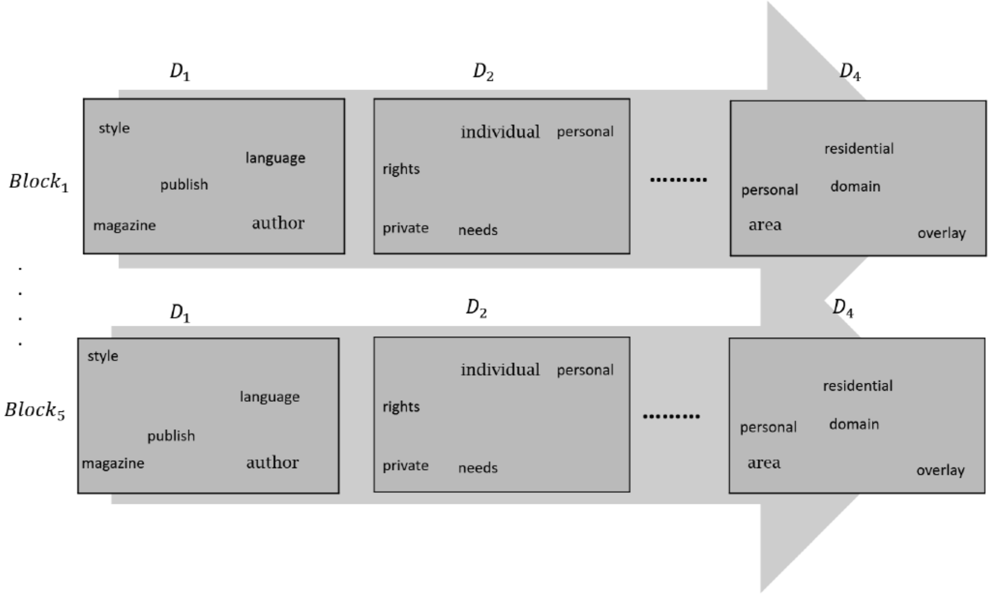


Figure 3.4: An example of displays arrangement during the training sessions from the system-assigned passphrase study by Joudaki et al.[58]

Others Most people memorize their secrets in their own way. Renaud et al. [45] found that people have their own way to memorize their PINs. Renaud et al. [45] offered users a memorization technique but half of the participants did not use their method and preferred to stick to their own strategy. Besides, some people like to memorize the string of letters corresponding to their PIN to remember their assigned PINs[5].

Our work is inspired by the CC-SP system [58]; however, since we focus on PINs instead of passphrases, our UIs are different. We implement entirely different UIs that aim to evoke CC and SP (as described in Section 4). Besides, it is clear that the spaced repetition approach of 25 repetitions works well for memorability [5] but is an extraordinarily long training time. Our techniques aim to keep training times minimal and in a single session.

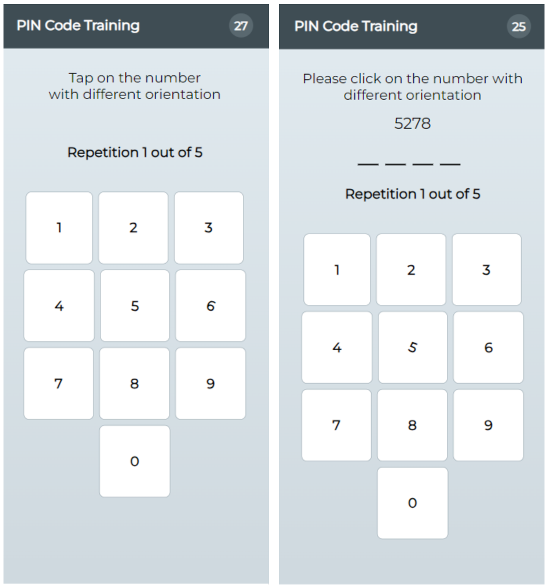
Chapter 4

PIN Training System Designs

Our training system designs were inspired by work on reinforcing system-assigned passphrases [58], which found that a short training session that employs implicit learning techniques improves usability. We describe our design of different systems to evoke two implicit learning techniques: Contextual Cueing (see Section 4.1), and Semantic Priming (see Section 4.2). We implemented another system that only uses simple repetition (see Section 4.3). Each of these designs asks the user to input their system-assigned PIN 5 times. The decision to require 5 repetitions is based on Joudaki et al.'s findings [58] and our early verification in pilot testing that the input time continued to reduce until about 4 repetitions. Users have 30 seconds to input each digit, or the training will time out and require restarting. When users incorrectly input a digit, the system will tell them it is incorrect.

For all of the following designs, with the exception of CC-v2, the login UI is the same as one would typically see on a PIN login screen (see Figure 5.1(b)).

4.1 Contextual Cueing (CC) Designs



Tap on the number with different orientation

Repetition 1 out of 5

Please click on the number with different orientation

5278

Repetition 1 out of 5

(a) CC-v1 (b) CC-RP

Figure 4.1: Training UIs for (a) CC-v1 and (b) CC-RP. The user must input their correct PIN 5 times to complete training. The Login UI for both of these designs is the same as a typical PIN login screen (see Figure 5.1).

Contextual Cueing (CC) is a psychological process in which learned contextual signals are used to help with visual search[56]. The term *context* refers to the physical arrangement of items in visual displays[56]. CC has been found to enhance usability in the context of system-assigned passphrases [58], whereby the user is shown a unique 2D arrangement of words; the 2D location of the target word among the arrangement of the others is learnt through a short training session involving 5 repetitions of each 2D arrangement. In the past, a number of methods including chunking [6] have been used with different levels of success to make PINs easier to remember. However, CC has never been employed in PIN systems. CC integration with PINs faced a unique challenge in that the arrangement of the PIN pad is constrained. Changing the order or 2D arrangement of digits on the PIN pad might cause users to become confused because they are used to the conventional layout of these numbers. The approach we designed to make use of the existing 2D arrangement of digits for CC-v1. We modified this approach slightly in CC-v2 through the use of an overlay of colour for selected digits (see Section 4.1. In the CC training phase, a user must search to locate the target (in our case the system-assigned digit) among a set of distractors (in our case the other digits); thus the target should be not easy to find, but possible for a user who is paying attention. Our design tilts the target digit and asks users to select the tilted digit. Each of the 4 system-assigned digits are presented in this way, in sequence, five times; at the end of training, the user is expected to have learnt the position of each of their 4 digits.

- **CC-v1** presents a sequence of 4 screens, where for each they are asked to tap on the number with different orientations. Each screen shows one digit of the system-assigned PIN on a regular PIN pad (see Figure 4.1(a)). The sequence of 4 screens is shown 5 times.

- **CC-RP** is the same as CC-v1, but the user's system-assigned PIN is also shown at the top of the screen (unlike CC-v1; see Figure 4.1(b)). This addition to the CC-v1 model was motivated by our findings from Study 1 (MTurk), which found CC-v1 had many login attempts, but higher memorability than those other groups. We wanted to integrate a reinforcement mechanism through repetition by displaying the user's system-assigned PIN at the top of the screen. The objective of this hybrid strategy was to increase the memorability of the PINs by utilizing both the implicitly learnt CC cues and the repetitive exposure to the entire PIN. Our goal was to strengthen the CC-v1 and RP methods by merging their designs.

- **CC-v2** aims to differentiate between the 2D contexts (screens) for each of the 4 system-assigned digits. We maintain our goal of keeping the arrangement of digits using the traditional PIN pad layout; however, a set of digits on each screen are overlaid with lightly shaded orange and have stronger borders. The screen for each digit retains its layout for both training sessions(see Figure 4.2 and login (see Figure 4.1). In all other aspects, CCv2 is the same as CCv1.

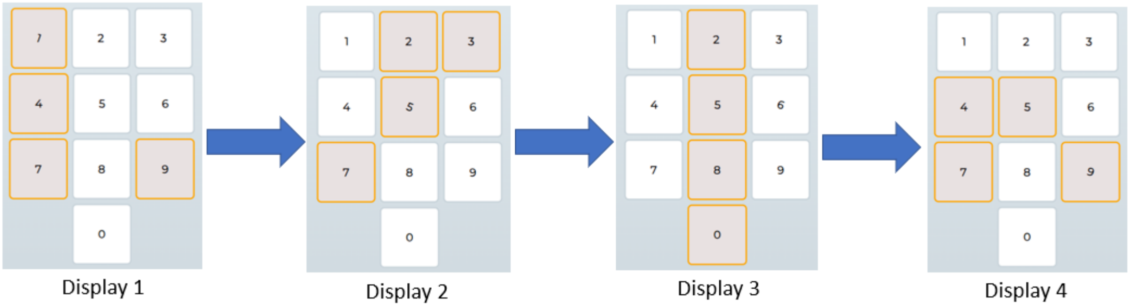
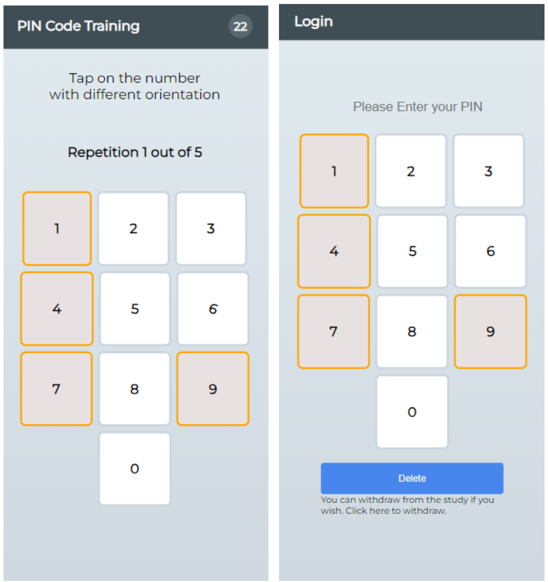


Figure 4.2: An example of displays arrangement during the training session- from CC-v2



PIN Code Training

Tap on the number
with different orientation

Repetition 1 out of 5

Login

Please Enter your PIN

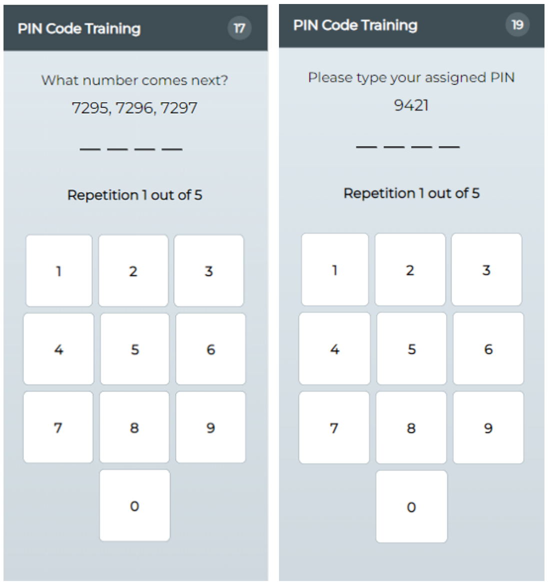
You can withdraw from the study if you wish. Click here to withdraw.

(a) CCv2 Training (b) CCv2 Login

Figure 4.3: CC-v2's (a) training and (b) login screens for the same digit. Note that each of the 4 digits in the system-assigned PIN has a different pattern of orange digits. Note that the background patterns remain for login, but the tilting of digits used for training is not present during login.

4.2 Semantic Priming (SP)

A common definition of semantic memory is the collection and organized storage of human knowledge. It includes a wide range of knowledge that we have gathered over time, such as concepts, words, decision-making techniques, and general comprehension of the outside world[57]. Our ability to recognize the term "Banana" as a particular fruit or the Eiffel Tower as a famous structure in France are both functions of this area of our memory. On the other hand, Priming describes a performance improvement in cognition or perception that is prompted by a situation or prior knowledge[59]. We may recognize or learn something more quickly since we've already seen similar situations in the past. We looked at the use of semantic priming for system-assigned passphrases after being inspired by Joudaki et al.'s research [58]. Our goal was to design an approach that could work with the conventional PIN interface. Our design aimed to get users thinking about the PIN as a whole (rather than 4 distinct digits), in a way that would work for any digit sequence (regardless of whether it had an underlying pattern such as a date). We choose to ask the user to complete a simple counting series of numbers; the final number which the user is asked to input is their system-assigned PIN (see Figure 4.4a). In the training session, users needed to input their PIN 5 times.



PIN Code Training 17

What number comes next?

7295, 7296, 7297

Repetition 1 out of 5

PIN Code Training 19

Please type your assigned PIN

9421

Repetition 1 out of 5

(a) SP (b) RP

Figure 4.4: Training UIs for (a) SP and (b) RP. The user must input their correct PIN 5 times to complete training. The Login UI for both of these designs is the same as a typical PIN login screen (see Figure 5.1).

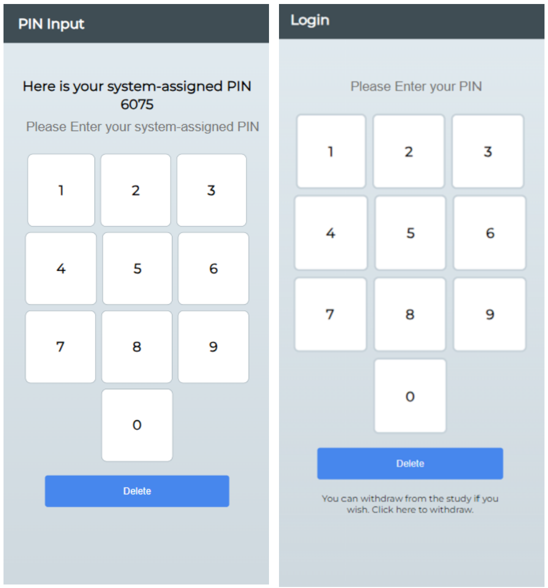
4.3 Repetition (RP)

In this design, users were simply asked to enter the system-assigned PIN five times (see Figure 4.4(b)). In this condition, there was no implicit learning technique involved. The purpose of this is to determine whether simple repetition, without any change to the UI, could offer an improvement.

Chapter 5

Methodology

We aim to evaluate whether our training designs improve usability through two studies. Study 1 was run on Amazon Mechanical Turk (MTurk), and Study 2 with students in our university. Study 1 aimed to evaluate our initial designs (CC-v1, SP, and RP as described in Section 4). Study 2 updated the designs based on findings in Study 1, and thus focused on CC-v2, CC-RP, and RP (as described in Section 4). Each study also had a control group that did not involve any training; they were asked to type the given PIN number once (see the Control group UI in Figure 5.1).



Here is your system-assigned PIN
6075

Please Enter your system-assigned PIN

Please Enter your PIN

You can withdraw from the study if you wish. Click here to withdraw.

(a) Registration (b) Login

Figure 5.1: Control group UIs for (a) Registration and (b) Login.

5.1 Study Tasks and Structure

Each study consisted of a registration session (where training is provided, where applicable), and a login session 24-48 hours later. Both studies were approved by our university's research ethics board. Minor differences between Study 1 and Study 2 are discussed in their respective sections below. Both studies had the same general 2-session and task structure:

Session 1 (registration):

1. Consent form. Participants were asked to read and sign a consent form; after they agree, they are randomly assigned to one of 4 groups.

2. PIN assignment. Users are assigned a randomly generated PIN. Users not in the control group receive a brief (approx. 30-seconds) training as described in

Section 4. Figure 4.2 shows arrangements of the display during the training.

3. Questionnaire. We ask 5 demographic questions (age, gender, education, primary area of study or work, and first language).

4. Login. Users were asked to log in with the assigned PIN. If users were unable to remember the assigned PIN, they were given the option to redo the training (applicable for CC-v1, SP and RP) or see the PIN again (Control group only).

5. Feedback. We ask for feedback on the training.

Session 2 (login):

1. Login. Users had 5 attempts to input the correct PIN number. If a user is unable to input the correct PIN within 5 attempts, they are considered to have forgotten the PIN. Joudaki et al. also implemented 5 attempts to input the correct PIN number [58].

2. Final questionnaire. This includes questions related to the training, assigned PIN, and the system usability.

MTurk Study Participants over age 18 from the USA were recruited from Amazon Mechanical Turk (MTurk). They were randomly assigned to one of 4 groups: CC-v1, SP, RP, or Control. They were compensated based on the minimum wage in the United States($7.25/hour), and since each was expected to take less than 5 minutes, they received $0.60 USD for completing each session. Partial compensation was available upon withdrawal. Here is the breakdown of partial compensation upon withdrawal:

For session 1:

Task 1: Users would be given a system-assigned PIN and may receive a brief training, which would take approximately 30 seconds.

Task 2: Users needed to complete the personality questionnaire, which took approximately 1-2 minutes (compensation \$0.20 USD).

Task 3: Users had to login with the system-assigned PIN, which they spent less than 1 minute (compensation 0.20 USD).

Task 4: Users completed a usability questionnaire, which took approximately 30 seconds (compensation \$0.20 USD).

For session 2:

Task 1: Users had to log in with the same PIN which they logged in within the 1st session. It took them less than a minute (compensation \$0.10 USD).

Task 2: They were asked some important usability questions which will take 1 minute to complete (compensation \$0.50 USD).

For Session 1 Task 2, we also asked 20 questions to measure the big five factors of personality[60]. We had hoped to collect enough information to do an analysis of how usability relates to personality, but unfortunately, the return rate for Session 2 was low. We removed this for Study 2 as we did not anticipate collecting sufficient data for such an analysis.

Student Study Students from our university were recruited via broadcast email. They were randomly assigned to one of 4 groups: CC-v2, CC-RP, RP, or Control. We changed our compensation model to encourage a higher return rate. Participants who completed Session 1 were entered into a draw to win 1 of 2 \$100 CAD bank deposits, Tim Hortons, or Amazon Gift cards of their choice. Upon completion of Session 2, they were provided a \$5 CAD bank deposit, Tim Hortons or Amazon Gift

Card as per their choice.

5.2 Implementation Details

To conduct our research, we developed a website that hosted our user interfaces, which were exclusively accessible via mobile devices. This design decision ensured the data collected was directly associated with mobile usage. For the privacy and security of our participants, we adopted careful data collection methods.

In the MTurk study, we refrained from collecting any personally identifiable information from the participants. This approach ensured complete anonymity and protected the participants' identities.

For the Student study, however, we needed to collect the participants' email addresses to distribute rewards. We employed a strict data handling protocol to maintain privacy: once the rewards were distributed, we promptly removed the email addresses from our database. This was to ensure the data was anonymized, eliminating potential privacy concerns.

To secure this data handling process further, our system employed a cryptographic function, SHA256, in combination with a 30-character secret key to generate a one-way hash function. This function converted participant IDs and email addresses into anonymous IDs. The resulting anonymous ID could not be reversed-engineered to reveal the original ID or email address, thus ensuring data privacy. For returning participants in session 2, the same cryptographic operation was performed on the entered ID or email address, allowing us to link their sessions without compromising their identity.

Importantly, we implemented a mechanism to lock the system for each user for

24 hours after their first session. This meant that even if a user managed to discover the link to the second session before we officially provided it, they could not bypass the waiting period and prematurely access the system.

Chapter 6

Results

Here we describe our participant demographics and dropouts, discuss the efficacy of our training designs, and analyze factors that may help inform future training designs.

6.1 Participant Demographics

Within each study, we observed fairly consistent demographics between the groups. The Student study (vs. MTurk) had a less educated, younger group with more identifying as female and fewer identifying English as their first language.

MTurk Study. We recruited *N=689* individuals from MTurk. Across all groups, more participants identified as male (55-59%) than female (41-44%). Most participants were between the ages of 18 and 35. Across groups, most participants had a bachelor's degree, and many had a master's degree. Computing & IT emerged as the most common field of work or study (40.2-54.5%). Over 90% of the participants in all groups identified English as their first language. Table 6.1 presents the demographic details of our participants.

		Control	CC-v1	SP	RP			Control	CC-v1	SP	RP
Gender	Female	44.1%	42.8%	40.7%	41.6%	**Study/Work**	Social Sci. & Humanities	1%	1%	4.2%	1.1%
	Male	54.8%	57.2%	59.3%	58.4%		Science	1.1%	1%	2.1%	1.6%
	Non-Binary	0%	0.0%	0.0%	0.0%		Health Science	12.8%	9.1%	9.5%	11.4%
	N/A	.11%	0%	0.0%	0.0%		Engineering & Applied Sci.	2.4%	4.3%	8.5%	11.4%
Age	18-25	35.6%	35.4%	20%	38.4%		Energy & Nuclear Sci.	2.7%	3.4%	3.2%	2.7%
	26-35	39.4%	35.6%	42.9%	42.7%		Education	10.6%	12.0%	5.8%	9.2%
	36-50	14.4%	15.9%	20%	13.0%		Business	13.8%	13.9%	12.2%	13.0%
	51-65	7.4%	3.7%	4.3%	4.3%		Computing & IT	54.5%	48.6%	46%	40.2%
	65+	0.5%	1.6%	1.6%	0.0%		Other	0.0%	6.3%	8.5%	3.8%
	N/A	2.7%	7.8%	11.2%	1.6%		N/A	1.1%	0.4%	0.0%	5.6%
Education	High school	3.2%	4.3%	7.9%	6.0%	**Language**	English	92.6%	90.4%	97.9%	98.9%
	Bachelor's	66.5%	68.3%	68.3%	74.5%		French	3.2%	4.3%	1.1%	0.5%
	Master's	23.4%	20.2%	20.6%	19.0%		Other	1.6%	4.3%	0.5%	0.0%
	PhD/higher	3.2%	5.3%	2.1%	0.0%		N/A	2.6%	0.0%	0.5%	1.5%
	N/A	3.7%	1.9%	1.1%	0.5%						

Table 6.1: MTurk study: demographics across the four conditions.

		CC-v2	Control	CC-RP	RP			CC-v2l	Control	CC-RP	RP
Gender	Female	61.2%	54.0%	61.5%	63.5%	**Study/Work**	Social Sci. & Humanities	12.2%	8.0%	5.8%	11.5%
	Male	30%	46%	36.5%	34.6%		Science	18.4%	1%	11.5%	19.2%
	Non-Binary	4.0%	0.0%	0.0%	1.9%		Health Science	14.3%	26%	25%	23.1%
	N/A	4.8%	0.0%	2.0%	0.0%		Engineering & Applied Sci.	22.4%	24%	26.9%	21.2%
Age	18-25	77.6%	90%	78.8%	75%		Energy & Nuclear Sci.	2.7%	3.4%	4.5%	3.8%
	26-35	16.3%	6%	11.5%	17.3%		Education	10.2%	6%	13.5%	7.7%
	36-50	6.1%	4%	5.8%	5.8%		Business	8.2%	8%	9.6%	1.3%
	51-65	0%	0%	0%	0.0%		Computing & IT	10.5%	2%	5.8%	7.7%
	65+	0%	0.0%	0.0%	0.0%		Other	0.0%	10.8%	0%	0%
	N/A	0%	0.0%	3.9%	1.9%		N/A	1.1%	10.8%	1.9%	0.0%
Education	High school	61.2%	68%	59.6%	63.5%	**Language**	English	65.3%	72%	65.4%	69.2%
	Bachelor's	24.5%	22%	25%	28.8%		French	2%	4%	1.9%	1.9%
	Master's	8.2%	4%	7.7%	3.8%		Other	32.7%	24%	28.8%	28.9%
	PhD/higher	0%	0%	1.9%	1.9%		N/A	0%	0.0%	3.9%	0.0%
	N/A	6.1%	6.0%	5.8%	2.0%						

Table 6.2: Student study: demographics across the four conditions

Student Study. We recruited *N=201* students from our university. Across all groups, more participants identified as female (61-66%) than male (30-36.5%). The majority of participants were between the ages of 18 and 25. Most participants had a high school diploma (60-68%), followed by a bachelor's degree (22-29%) as their highest education to date. Field of study was divided among many disciplines. English was the first language for most (65.3%–72%). Table 6.2 presents the demographic analysis of the participants.

MTurk Study. We were surprised to find that many users in MTurk have multiple accounts. Our website placed the assigned PIN in local storage; when multiple ac-

Groups	**First Session**	**Valid Users**	**Second Session**
Control	167	79	32
CC-v1	181	84	34
SP	178	87	32
RP	172	64	28
Total	698	314	126

Table 6.3: MTurk study: number of participants per session, per group. Valid users are those who passed our Session 1 check for using a single MTurk account.

counts have the same PIN it means (with high likelihood) that they are coming from the same web browser/user. We found that 54.3% of participants were from users holding multiple accounts. We discarded data from these participants and did not invite them to Session 2. The dropout rate for Session 2 was 60.5%. **Table** 6.3 shows participant details per group. Given that a significant number of the users stored their assigned PIN (see Section 6.2), we were left with a small sample size per group (approx. 12-15 per group) that did not offer sufficient statistical power. Joudaki et al. [58] used a large sample size which is similar to our studies. Thus we do not run statistical tests on MTurk study data, but report its results as pilot study data, as it was useful to inform our Student study.

Student Study. The multiple-account problem we observed in MTurk was not present in this study, as we collected valid students' university email addresses (for compensation). After 24 hours of the completion of Session 1, we sent an email to invite participants for Session 2. Of the 201 participants recruited, 184 returned for Session 2 (8.46% dropout rate).

6.2 Storage

In our Session 2 questionnaire (at the end of the study), we emphasized that it was OK for participants to choose to record their allocated PIN and urged them to let us know if they did so. We also detected if a participant copied their system-assigned PIN. For the remainder of our analysis, we did not include data from those participants who told us they wrote down their PIN or were detected as having copied it. To determine whether a training technique can influence storage rates in the Student study, we test the following hypotheses:

H_0: *There is no significant association between groups and their storage behavior.*

H_A: *There is a significant association between groups and their storage behavior.*

MTurk Study The **Table** 6.4 represents the number of Amazon MTurk participants per group who recorded their system-assigned PIN. According to the data gathered from our Amazon MTurk participants, there is no obvious distinction between the groups in terms of storing their PINs. This decision is taken from the fact that each group recorded roughly the same number of system-assigned PINs. This finding supports our null hypothesis, which holds that there is no significant connection between the group categorizations and the corresponding storage behaviors. Given this consistency, we determined that running a statistical analysis on this particular data was unnecessary.

Student Study: Our data collected from university students shows that a few users chose to record their system-assigned PINs. Table 6.5 explains this behavior and lists the number of users and their corresponding groups. This table shows how the

Groups	**Stored PIN**	**Percentage**
Control group	18	56.25%
CC-v1 group	19	58.82%
SP group	20	62.5%
RP group	14	50%
Total	71	

Table 6.4: MTurk Study: the number of users who stored their system-assigned PIN

Groups	**Recorded**	**Percentage**
Control group	13	30.23%
CC-v2 group	5	11.1%
CC-RP group	8	18.37%
RP group	9	17.02%
Total	35	

Table 6.5: Student Study: the number of users who stored their system-assigned PIN

various groups performed in terms of PIN recording, such as Control, CC-v2, CC-RP, and RP.

In order to discern any statistically significant variations in PIN storage behavior across different groups, we carried out a χ^2 test with (*df=3*, *N=184*) The resulting statistic was $\chi^2 = 5.47$, with an associated $p = 0.14$.

Conventionally, a p-value below the standard threshold of 0.05 indicates a statistically significant result. However, in this case, the p-value exceeded this benchmark, leading us to the conclusion that the differences in PIN storage behavior among the groups studied are not statistically significant.

It is worth noting that our sample size might have limited the statistical power of our analysis, potentially contributing to the lack of detectable storage effects. Therefore, while our current findings suggest no significant differences in PIN storage behavior across groups, further research involving a larger sample size may yield different results.

6.3 Login Time

Login time is an important usability metric that relates to ease of use and user satisfaction. For a positive user experience, quick login times are important. Users could become impatient if it takes too long, which can lead to users choosing their own, less secure PIN. We measure login time as the time from the login page loading until the time the user successfully logs in (which includes the time for login failures, if any). Please note that here we did not analyze time for those users who could not log in after 5 attempts.

MTurk Study Table 6.6 summarizes the MTurk study's login time data. All groups had similar login times in Session 1, which was shortly after PIN assignment. A Kruskal-Wallis test was conducted to determine differences among groups. The results were not statistically significant, $H(3, N = 689) = 1.5709, p = .666$. However, in the Session 2 login recall test, the CC-V1 group exhibited a noticeably higher login time than the other groups. Thus we examined the number of login attempts in Figure 6.4, which indicates that CC-v1 had a larger number of failed login attempts than other groups (among those who eventually remembered). We hypothesized that this might be due to the PIN pad being identical for each digit, such that out-of-order errors could be common. This finding motivated the design of CC-v2, examined in the Student study.

In the first session, the time spent in login was quite similar for all groups. However, if we see the second session, Figure 6.2 shows that CC-v1 has comparatively higher login time than other groups.

	Groups	**Mean (± Std)**
First Session	**Control group**	5.3 ± 5.2
	CC-V1 group	5.31 ± 5.2
	SP group	5.2 ± 7
	RP group	5.72 ± 7
Second Session	**Control group**	17.74 ± 15.15
	CC-v1 group	21 ± 18.514
	SP group	13.7 ± 29.74
	RP group	13.9 ± 18.47

Table 6.6: MTurk Study: login time prior to successful login for both sessions

	Groups	**Mean (± Std)**
First Session	**CC-v2 group**	4.76 ± 2.88
	Control group	3.87 ± 3.32
	CC-RP group	3.45 ± 2.24
	RP group	3.48 ± 1.64
Second Session	**CC-v2 group**	8.19 ± 6.53
	Control group	26.94 ± 57.78
	CC-RP group	7.52 ± 10.72
	RP group	6.77 ± 9.9

Table 6.7: Student Study: login time prior to successful login for both sessions

Student Study We found the login time for all training-based groups (CC-v2, CC-RP, and RP) was lower than Control in Session 2 (see Table 6.7). To determine if our training techniques improve Session 2 login time, we examine the following hypotheses for Session 2:

H_0: *The login time distributions are similar between groups.*

H_A: *The login time distributions differ between groups.*

we performed one-way ANOVA, which found a statistically significant difference in mean login time between at least two groups F (3,118) = 3.397, $p < 0.05$, η^2=0.08. For further analysis, we report a Tukey HSD pairwise comparison in Table 6.8. The

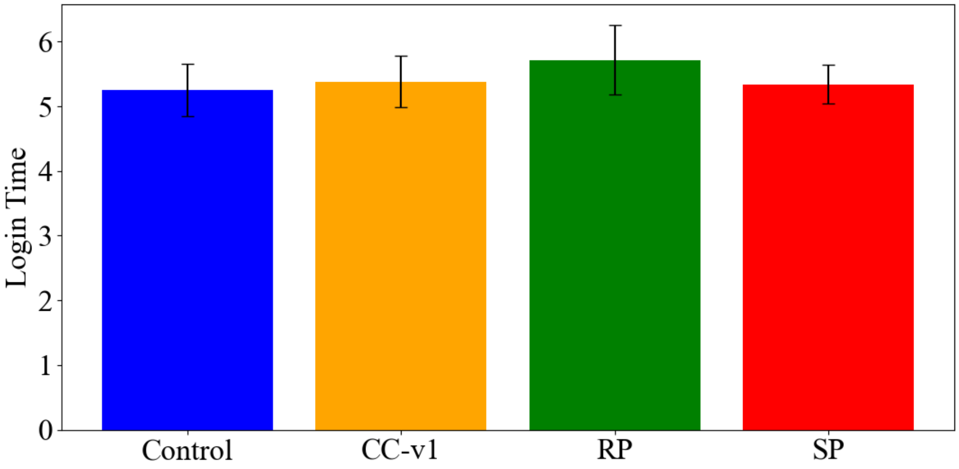


Figure 6.1: MTurk Study: Bar Chart for successful login time of all the groups for the first session

analysis indicates that CC-v2, CC-RP and RP have significantly lower login times compared to Control. This rejects our null hypothesis and accepts our alternative hypothesis which suggests that training has an impact on users' login time.

From Table 6.8 we can see that CC-v2, CC-RP and RP group have significant difference compared to control group. Which rejects our null hypothesis and accepts our alternative hypothesis which emplies that training has impact on users' login time.

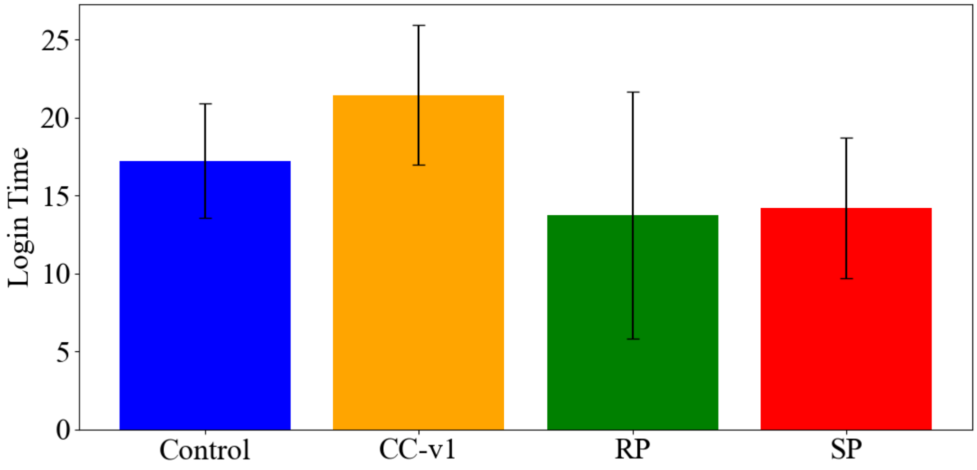


Figure 6.2: MTurk Study: Bar Chart plot for successful login time of all the groups for the second session

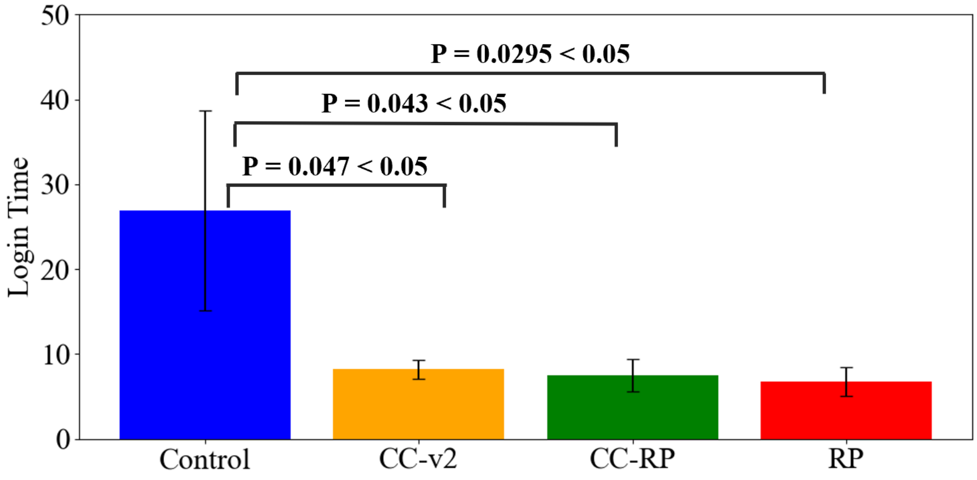


Figure 6.3: Student Study: Bar chart for login times of all the groups for the second session

Conditions	**Adj. P value**
CC-v2* and Control	**0.047 <0.05**
CC-v2 and CC-RP	0.9996
CC-v2 and RP	0.09963
CC-RP* vs Control	**0.043 <0.05**
Control and RP*	**0.0295 <0.05**
CC-RP vs RP	0.9995

Table 6.8: Student Study: the results of One-way Anova with Tukey HSD test for the pairwise comparison for the login time for the experimental conditions. Bold rows are significant differences.The asterisk-marked conditions are the ones that performed better than the paired condition.

6.4 Recall Rate

To answer our main research question - whether implicit learning techniques improve memorability, we have analyzed data from both studies.

Our findings regarding the recall rate for each group per session are illustrated in the figures provided. In order to determine if the training had any effect on the recall rates of the users, we tested the following hypotheses:

H_0: *The training has no impact on the recall rate of the participants*

H_A: *The training will have an impact on the recall rate of the participants*

MTurk Study During the first session of MTurk Study, all participants were able to remember their PIN. The control group, CC-v1 group, SP group, and RP group all demonstrated a 100% recall rate, with no participant forgetting their PIN.

We ignore the participants who recorded their assigned PINs. Table 6.9 presents the recall rates for the second session, excluding the participants who recorded their PINs. The CC-v2 group had the highest recall rate at 73.33%. The control group, SP group, and RP group all had a 50% recall rate. We could not find any significance in this data which accepts our null hypothesis.

Student Study In our second study, we again evaluated the recall rates for each group per session. Same as Mturk Study, we got 100% recall rate in the first session.

In this Table 6.9 the 'Remembered' column from Student study shows the percentage of participants that correctly remembered the PIN During the second session. During the first session, we observed a high recall rate across all groups. The second session, however, shows a decline in these rates, which prompted us to look at

	Groups	Remembered
MTurk Study	**CC-v1 group**	73.33%
	Control group	50%
	SP group	50%
	RP group	50%
Student Study	**CC-v2 group**	85%
	Control group	80%
	CC-RP group	79.49%
	RP group	82.5%

Table 6.9: Recall rate of the second session for each group excluding the user who recorded the PINs

these results in more detail. We are more interested in long-term memory (the second session). We conducted a chi-squared (χ^2) test to evaluate if the relationship between the groups and login success rate were statistically significant. χ^2(3, N = 149) = 0.449, p =.930, indicates that there was no significant relationship between these groups. As a result, the login success rate did not differ substantially across the four groups.

6.5 Incorrect Logins

We continue to focus our analysis on both studies to learn more about the recall rate **MTurk Study** During the first session, we thoroughly examined the successful login attempts. Different user groups required a different number of attempts to complete a successful login. It is interesting to note that all groups had a median number of attempts that was zero, meaning the majority of users were able to log in on their first attempt. This indicates strong performance in short-term memory tasks across all groups.

We also analyzed login attempts during the second session (Table 6.10). Our find-

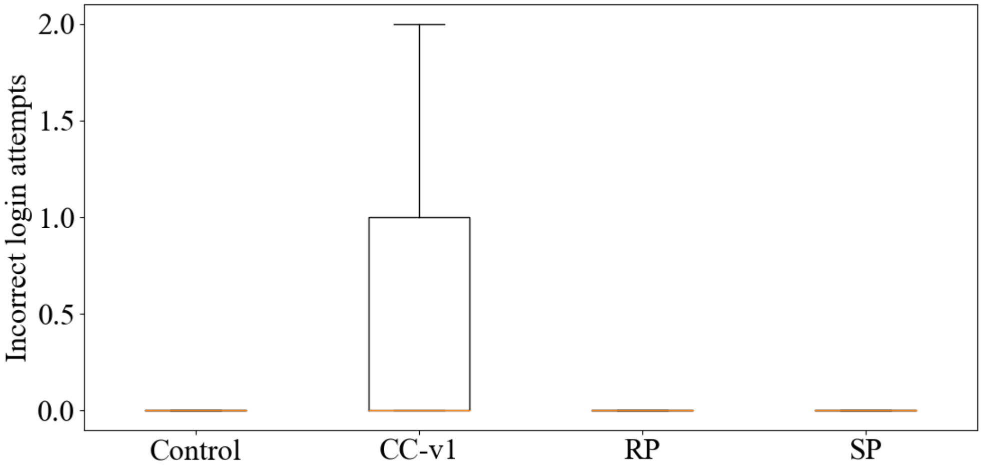


Figure 6.4: MTurk Study: Box and Whisker plot for the incorrect PIN of all the groups for the second session

ings suggest the CC-V1 group required the highest number of attempts for successful login, followed by the SP group. To visualize these differences, we created box and whisker plots for the second session (Figures 6.4), clearly showing the variation in login attempts for incorrect PINs across groups. Figure 6.4 shows an interesting difference. The CC-v1 group required noticeably more tries than other groups during the second session to complete successful logins. Please note that we are only consid-

	Groups	**Mean (± Std)**
First Session	**Control group**	0.25 ± 0.717
	CC-v1 group	0.18 ± 0.73
	SP group	0.23 ± 0.79
	RP group	0.32 ± 1.05
Second Session	**Control group**	0.22 ± 0.5
	CC-v1 group	0.5 ± 1.02
	SP group	0.41 ± 0.87
	RP group	0.07 ± 0.27

Table 6.10: MTurk Study: login attempt prior to Successful login for both sessions

ering those users who successfully login in the both sessions and we are only counting incorrect attempts.

We have created a box and whisker plot for the login attempts of all groups for both sessions. In the first session, we did not find that many differences, however, in the second session We found that CC-v1 had the highest login attempt.

Student Study Here we have also analyzed the login attempt of the users. Table 6.10 shows the mean, and SD of 1st and 2nd sessions respectively. For the first session, the RP group required the fewest mean number of attempts whereas the control group required somewhat more attempts which had the highest mean number of attempts. Interestingly, the CC-v2 group had the highest mean number of tries during the second session, indicating a higher level of unpredictability as seen by the higher standard deviation.

On the other hand, from Figure 6.6, the CC-v2 group recorded the lowest rate of incorrect PIN entries. We analyze the errors participants make when they forget their PIN in Figure 6.5. For the sake of this analysis, we consider the user's attempt that was closest to their assigned PIN. Our analysis shows that the CC-v2 group had the lowest rate of incorrect PIN entries. Moreover, all of the users in this group could still accurately recall at least three digits of their PINs, or they remembered all digits of their PINs but failed to input them in the correct order. However, we have run Kruskal-Wallis test was to assess the differences among groups for second session, the results indicated no statistically significant differences, $H(3, N = 122) = 3.8762, p = .275$. The CC-RP group had the highest incidence of providing all digits but in incorrect orders. It seems that users from this group had less trouble recalling the individual digits of their PINs, but they had trouble remembering their order.

This pattern points to a certain type of cognitive load in which recalling the numbers themselves is easier than recalling their sequence in memory.

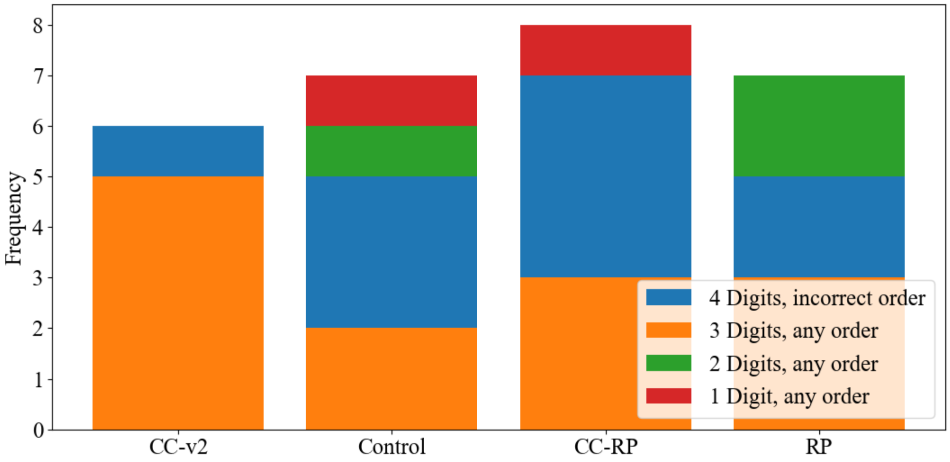


Figure 6.5: Student Study: the distribution of wrong PIN entries

	Groups	Mean (± Std)
First Session	**CC-v2 group**	0.10 ± 0.42
	Control group	0.14 ± 0.65
	CC-RP group	0.075 ± 0.33
	RP group	0.03 ± 0.19
Second Session	**CC-v2 group**	0.12 ± 0.33
	Control group	0.54 ± 0.93
	CC-RP group	0.06 ± 0.36
	RP group	0.21 ± 0.55

Table 6.11: Student Study: login attempt prior to Successful login for both sessions

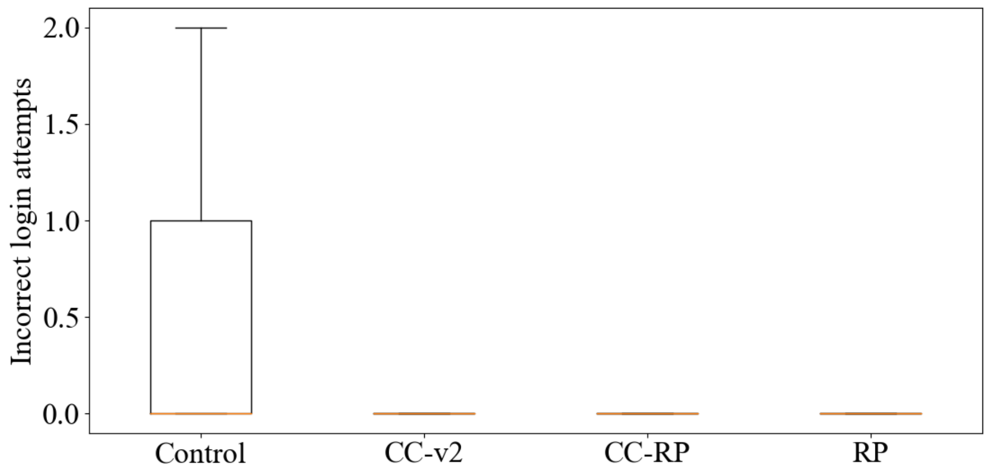


Figure 6.6: Student study: Box and Whisker plot for the incorrect PIN of all the groups given by users for the second session

6.6 Training

During the study, we have analyzed the training time. We tried to find that if the learning happened in that time or not.

MTurk Study In this study we have analyzed the training data for each group 6.12 shows that after the 1st repetition, the training time dropped. For the MTurk study, we found that after the 1st repetition the training time dropped and continues to decrease until it begins to level off between repetitions 3 and 4. This means that the learning happened and that's why the last round of training had the lowest time.

Student Study We have also analyzed the training time for this study participants. The table 6.13 shows that for CC-v2 and CC-RP have the last repetition time was the lowest one. Inters tingly, The table also shows that CC-v2 training comparatively took more time than other groups.

Group	**1st Round Training**	**2nd Round Training**	**3rd round Training**	**4th Round training**	**Last Round Training**
CC-v1 group	6.24 (±5.64)	4.01 (±3.48)	3.76 (±4.09)	3.5 (±3.399)	3.28 (±2.56)
RP group	4.28 (±2.29)	3.61 (±2.47)	2.69 (±1.69)	2.39 (±1.43)	2.48 (±1.46)
SP group	7.412 (±3.77)	3.99 (±2.91)	3.11 (±2.17)	2.94 (±1.95)	2.63 (±1.253)

Table 6.12: MTurk Study: Mean (± Std). Training time taken for CC-v1, SP and RP groups for users

Group	**1st Round Training**	**2nd Round Training**	**3rd round Training**	**4th Round training**	**Last Round Training**
CC-v2 group	12.58 (±8.44)	8.54 (±5.57)	6.17 (±4.23)	4.59 (±3.09)	4.21 (± 3.097)
CC-RP group	7.41 (±3.77)	3.99 (±2.19)	3.11 (±2.17)	2.94 (±1.95)	2.63 (±1.25)
RP group	5.53 (±1.92)	3.47 (±1.37)	2.66 (±1.49)	2.29 (±0.91)	2.53 (±1.72)

Table 6.13: Student Study: Mean (± Std). Training time taken for CC-v2, SP and RP groups for users

We have also analyzed the users who remembered the PINs training time and also the ones who did not remember the PINs separately. Table 6.14 and 6.15 exhibit that users who forgot the PINs, took more time to take the training than the users who forgot the PINs.

Group	**1st Round Training**	**2nd Round Training**	**3rd round Training**	**4th Round training**	**Last Round Training**
CC-v2 group	13.36 (±10.92)	12.2 (±9.3)	9.92 (±6.74)	5.04 (±3.55)	4.84 (± 4.34)
CC-RP group	7.8 (±3.91)	3.98 (±1.96)	3.16 (±1.86)	3.15 (±2.12)	2.84 (±1.29)
RP group	5.38 (±2.02)	3.33 (±1.18)	2.42 (±0.83)	2.13 (±0.67)	2.3 (±1.05)

Table 6.14: Student Study: Mean (± Std). Training time taken for CC-v2, SP, and RP groups for users who did not remember the PIN

Group	**1st Round Training**	**2nd Round Training**	**3rd round Training**	**4th Round training**	**Last Round Training**
CC-v2 group	12.7 (±8.5)	8.57 (±5.12)	5.83 (±3.92)	4.56 (±3.2)	4.18 (± 3.17)
CC-RP group	6.75 (±3.63)	4.05 (±2.1)	2.85 (±2.17)	2.5 (±1.04)	2.44 (±0.95)
RP group	4.96 (±1.33)	4.01 (±1.95)	3.11 (±1.38)	2.93 (±1.35)	3.69 (±3.89)

Table 6.15: Student Study: Mean (± Std). Training time taken for CC-v2, SP, and RP groups for users who remembered the PIN

6.7 Registration Time

We have analyzed the average time it took for people to register during the first session of both the MTurk Study and the Student Study. These studies involved different groups: CC-v1, RP, SP in the MTurk Study, and CC-v2, CC-RP, RP in the Student Study. From Table 6.16 exhibits that in Mturk study, the RP group registered more quickly than the CC-v1 and SP groups. They took an average of 15.46 seconds to finish, while the CC-v1 group took 20.79 seconds and the SP group 18.05 seconds.

	Groups	**Mean(± Std)**	**Median**
MTurk Study	**CC-v1 group**	20.79 (± 15.05)	16.19
	RP group	15.46 (± 6.59)	13.99
	SP group	18.05 (± 8.97)	15.71
Student Study	**CC-v2 group**	36.09 (± 15.78)	34.24
	CC-RP group	20.36 (± 7.38)	19.90
	RP group	16.43 (± 5.14)	16.29

Table 6.16: Average and median registration time for both studies

On the other hand, in Student Study, the RP group also completed more quickly than the other groups. Their average time was 16.43 seconds. This was quicker than the CC-v2 group (36.09 seconds) and the CC-RP group (20.36 seconds).

Our overall training time for all the groups are comparatively less than the existing method(e.g. spaced repetition by Schechter et al. [5] which takes upto 4 days and 25 times of logins with median of 120.8 seconds of interaction. Our median training time is 16-34 seconds which is very less than compared to their proposed training's median time.

Our findings suggest that users from the RP group completed the registration faster than other groups.

Groups	**MTurk Study SUS Average (± Std) Score**	**Student Study SUS Average (± Std) Score**
Control	58.51 (± 12.73)	65.79 (± 19.50)
CC-v1	70.98 (± 11.71)	—
RP	61.25 (± 16.54)	76.86 (± 15.90)
SP	65.3 (± 12.62)	—
CC-v2	—	63.90 (± 15.51)
CC-RP	—	73.70 (± 14.92)

Table 6.17: Average (± Std) SUS scores of the participants in MTurk and Student studies

6.8 Usability

We have also asked users questions at the end of our second session. We hypothesized that the user's perception of the implicit learning training technique will be better than control group. We have asked users several questions to our participants in the end of our study. We used the SUS (System Usability Scale) questionnaire to gauge participants' reactions to the system during our usability test [61]. A SUS score higher than 68 is considered above average, while anything below 68 is considered below average[62].

MTurk Study As shown in **Table** 6.17, CC has comparatively more SUS scores than the Control group.

Student Study We found that CC-RP and RP performed better among students. However, CC-v2 had the lowest score.

6.9 Exit survey

Our post-study questionnaire in session two asked users about their experience in this study. We have used emergent coding to analyze the free-form, self-reported data from our questionnaire and categorize participants' comments from our Student Study. We primarily categorized coding as positive and negative. Positive had - used own mnemonics, Positive sentiment, Easy to use and System is useful. On the other hand, Negative had - Hard to recall, Confused about CC background. Many students found system-assigned PIN hard to recall. One student suggested, "Please do not assign PINs to students". However, some students use their own memorization strategies, One student from the control group mentioned using a mental mind trick to remember the PIN. Some students were confused about the CC-v2 background. Still, many students gave positive sentiments for CC-v2 saying. "It was an interesting exercise" and "Very cool system". Moreover, some students highlighted the system's ease of use and utility.

Table 6.18: Student Study: Emergent coding on Students' feedback

Code	**Type**	**Comment**	**Group**	**Frequencies**
Used own mnemonics	Positive	I used a mental mind trick to remember so I didn't find it too hard Regardless of training I found my PIN easy to remember due to the visual and numerical pattern	Control CC-RP	2.1%
Hard to recall	Negative	Assigning a single random PIN seems easy to forget. Maybe give multiple PINs for user to pick from Please don't assign PINs to students	CC-v2 CC-RP	2.8%
Confused about CC background	Negative	I didn't understand the orange highlights over various digits on the PIN pad after every digit. Not hard; I wish it said that yellow tiles weren't a "gotcha"	CC-v2 CC-v2	1.4%
Positive sentiment	Positive	It was an interesting exercise. Very cool system and experiment.	CC-v2	2.8%
Easy to use	Positive	The system is not hard to use The system is very easy to use.	CC-RP RP	2.1%
System is useful	Positive	Hint to access PIN or code. I surprisingly remembered the code the next day because I thought I would forget it by then.	CC-v2	2.1%

Chapter 7

Discussion

The results of our study show that current PIN rules have significantly improved over earlier ones, particularly in terms of training times, login times, and recall rates. This is strong proof that the PIN training techniques we created—CC-RP, RP, and CC-v2—offer important benefits for user experience and operational effectiveness. Through our Student study (which had a higher return rate), we found that our training designs improved login times so users were significantly faster at inputting their PIN. Two of the designs (CC-RP and RP) also had improved user perceptions (as measured by SUS scores). These results, combined with the positive results for CC-v1 in the pilot (MTurk) study, suggest that our CC design as implemented in CC-RP and CCv1 takes a valuable step towards improving the usability of system-assigned PINs. The training sessions for each of these designs take less than 16 to 34 seconds. Schechter et al. [5] conducted an experiment in which they observed the training times for two different PIN policies: a Second-PIN policy and a Mapping policy. Their training for the second-PIN policy, required up to four days of 25 times of logins and on average 120.8 seconds of interaction (calculated from Figure 3.3). Our own study, however, exhibited more promising results. We recorded median training times for our CC-RP and RP training techniques around 20 and 16 seconds, respectively. For our CC-v2 training technique, the median training time was around 34 seconds. Overall training time has been taken for around 16 to 34 seconds. These results indicate that our PIN training techniques significantly outperform those proposed by [5] in terms of training time.

Furthermore, another study by Huh et al. [6] indicated that the login time for a 6-digit PIN with a chunking policy was 41.7 seconds and 40.7 seconds without chunking. In contrast, our study found that the login times for our CC-v2, CC-RP, and RP policies were markedly lower, at 8.19, 7.52, and 6.77 seconds, respectively. In terms of recall rate, their study showed that a 4-digit PIN (without a chunking policy) had a recall rate of 74%, a 6-digit PIN with chunking had a recall rate of 57%, and a 6-digit PIN without chunking had a recall rate of 55%. These results underline the superior efficacy of our policies, which prioritize both efficiency and recall.

Our results point towards possibilities for even further improvements. We found that most of the CC-RP errors were due to incorrect order despite remembering the correct 4 digits. Our CC-v2 design aimed to reduce such errors but the design seemed to distract users from the PIN pad and interfere with the intended training.

Limitations. As we have conducted our study in 2 different populations, we have encountered different challenges in collecting useful data. In our MTurk Study, we found that many MTurk users have multiple accounts. This, along with a low return rate, resulted in a smaller-than-expected data pool. Although we solved our return rate problem in our Student study, this study had an unusually high recall rate for the Control group. This result may be due to the fact that students are frequently more careful and committed in this kind of research study. It also can be called as "Demand Characteristics" [63]. Our results should be considered in light of these population differences. In particular, our inability to detect significant differences in recall and storage rates could be due to these reasons. Future research should aim for larger and more diverse participant samples.

Chapter 8

Conclusion and Future Work

In this chapter, we review the conclusion of this thesis and future work. In Section 8.1 we present the overall summary of our research and in Section 8.2 we discuss future directions of our work.

8.1 Overall Summary

Our work takes a valuable step towards improving the usability of system-assigned PINs. Our designs involve a single short (16-34 seconds) training session and two of them significantly improve login times and user perception. All designs seem comparable for memorability, although there are some indicators that memorability might be stronger in CC-v2 and CC-v1/CC-RP (incorrect login analysis, storage rates, and recall rates). More study is needed with larger samples.

8.2 Future Directions

Future work includes personalizing the training, as some people may benefit from more repetitions. To determine whether training times might be useful in predicting users who will not recall their PIN, we have also analyzed the training times for users who remembered the PINs vs. who did not. To summarize, we found that users who forgot the PINs, took more time to take the training than the users who remembered their PINs. This might point towards a way to improve training by providing more repetitions until the repetition time decreases as expected.

Given that most login errors were due to digits being out of order, future designs might also focus on solving that problem. This is what CC-v2 aimed to do, but appeared too distracting as indicated by higher training times, lower SUS scores, and also some users commented that they thought their assigned digits should be orange (and were surprised when they were not). Future designs should take a different approach than CC-v2. For example, it might be possible to use a background image or pattern behind the digits, so that the interface looks different but does not imply that people need to interact with the parts that differ. We also want to see if our methods can help older people remember better. We're curious to find out if these learning techniques work just as well for older people as they do for younger ones. By looking at these different age groups, we can learn a lot from our study.

References

[1] P. R. Center, *Demographics of mobile device ownership and adoption in the united states — pew research center*, https://www.pewresearch.org/internet/fact-sheet/mobile/, (Accessed on 08/11/2023), Apr. 2021.

[2] B. Martınez-Pérez, I. De La Torre-Dıez, and M. López-Coronado, "Mobile health applications for the most prevalent conditions by the world health organization: Review and analysis", *Journal of medical Internet research*, vol. 15, no. 6, e120, 2013.

[3] S. Davidson, *Rbc refuses to refund ontario woman $8,772 because of pin — ctv news*, https://toronto.ctvnews.ca/ontario-woman-warns-about-choosing-credit-card-pin-after-rbc-refuses-to-refund-8-772-1.5895738, (Accessed on 01/14/2023), 2022.

[4] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? the security of customer-chosen banking pins", in *Proceedings of the International Conference on Financial Cryptography and Data Security*, Springer, 2012.

[5] S. Schechter and J. Bonneau, “Learning assigned secrets for unlocking mobile devices”, in *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*, 2015.

[6] J. H. Huh, H. Kim, R. B. Bobba, M. N. Bashir, and K. Beznosov, “On the memorability of system-generated PINs: Can chunking help?”, in *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS 2015)*, Ottawa: USENIX Association, Jul. 2015, ISBN: 978-1-931971-249.

[7] D. He, M. Naveed, C. A. Gunter, and K. Nahrstedt, “Security concerns in android mhealth apps”, in *AMIA annual symposium proceedings*, American Medical Informatics Association, vol. 2014, 2014, p. 645.

[8] A. Nisbet and M. Kim, “An analysis of chosen alarm code pin numbers & their weakness against a modified brute force attack”, 2016.

[9] Bay Alarm Company, *How to set a secure pin code for your burglar alarm system*, `https://www.bayalarm.com/home-security/burglar-alarm-systems-home-security/how-to-set-a-secure-pin-code-for-your-burglar-alarm-system/`, Accessed: 2023-02-01, 2020.

[10] S. G. Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, “Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication”, in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2020, pp. 268–285.

[11] C. Rathgeb and A. Uhl, “Two-factor authentication or how to potentially counterfeit experimental results in biometric systems”, in *Image Analysis and Recognition: 7th International Conference, ICIAR 2010, Póvoa de Varzin, Portugal,*

June 21-23, 2010, Proceedings, Part II 7, Springer Berlin Heidelberg, 2010, pp. 296–305.

[12] K. Hafner, *Fernando corbató, a father of your computer (and your password), dies at 93 - the new york times*, `https://www.nytimes.com/2019/07/12/science/fernando-corbato-dead.html`, (Accessed on 06/24/2023), Jul. 2019.

[13] S. H. Islam and G. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography", *Mathematical and Computer Modelling*, vol. 57, no. 11-12, pp. 2703–2717, 2013.

[14] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks", *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646–1656, 2012.

[15] S.-Q. Wang, J.-Y. Wang, and Y.-Z. Li, "The web security password authentication based the single-block hash function", *IERI Procedia*, vol. 4, pp. 2–7, 2013.

[16] B. MacRae, A. Salehi-Abari, and J. Thorpe, "An exploration of geographic authentication schemes", *Proceedings of the IEEE Transactions on Information Forensics and Security*, 2016.

[17] W. Jeon, Y. Lee, and D. Won, "An efficient user authentication scheme with smart cards for wireless communications", *International Journal of Security and Its Applications*, vol. 7, no. 4, pp. 1–16, 2013.

[18] H. Imtiaz and S. A. Fattah, “A face recognition scheme using wavelet-based local features”, in *2011 IEEE Symposium on Computers & Informatics*, IEEE, 2011, pp. 313–316.

[19] P. Wang, C.-C. Ku, and T. C. Wang, “A new fingerprint authentication scheme based on secret-splitting for enhanced cloud security”, *Recent Application in Bio-metrics*, pp. 183–96, 2011.

[20] X. Wang, F. Guo, and J.-F. Ma, “User authentication via keystroke dynamics based on difference subspace and slope correlation degree”, *Digital Signal Processing*, vol. 22, no. 5, pp. 707–712, 2012.

[21] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes”, in *2012 IEEE symposium on security and privacy*, IEEE, 2012, pp. 553–567.

[22] V. Woollaston, *Pin number inventor recalls how created the security system on its 50th anniversary — daily mail online*, `https://www.dailymail.co.uk/sciencetech/article-3568688/PIN-man-hails-eureka-moment-50-years-ago.html`, (Accessed on 06/28/2023), May 2016.

[23] S. Brocklehurst, *The man who really invented the cash machine - bbc news*, `https://www.bbc.com/news/uk-scotland-40416025`, (Accessed on 06/28/2023), Jun. 2017.

[24] DataGenetics, *Pin number analysis*, `https://www.datagenetics.com/blog/september32012/index.html`, Accessed: 01/13/2023, 2012.

[25] T. Guardian, *The most common pin numbers: Is your bank account vulnerable? — debit cards*, `https://www.theguardian.com/money/blog/2012/sep/28/debit-cards-currentaccounts`, Accessed: 01/13/2023, 2012.

[26] R. Veras, J. Thorpe, and C. Collins, “Visualizing semantics in passwords: The role of dates”, in *Proceedings of the 9th International Symposium on Visualization for Cyber Security*, ser. VizSec, 2012.

[27] H. Khan, J. Ceci, J. Stegman, A. J. Aviv, R. Dara, and R. Kuber, “Widely reused and shared, infrequently updated, and sometimes inherited: A holistic view of pin authentication in digital lives and beyond”, in *Annual Computer Security Applications Conference*, 2020.

[28] D. Wang, Q. Gu, X. Huang, and P. Wang, “Understanding human-chosen pins: Characteristics, distribution and security”, in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017.

[29] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, “Do users’ perceptions of password security match reality?”, in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’16, San Jose, California, USA: Association for Computing Machinery, 2016, ISBN: 9781450333627. DOI: `10.1145/2858036.2858546`.

[30] J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords”, in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, IEEE, 2012.

[31] V. Taneski, M. Heričko, and B. Brumen, “Password security—no change in 35 years?”, in *Proceedings of the 37th International Convention on Information*

and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2014.

[32] A. V. Oppenheim and R. W. Schafer, “From frequency to quefrency: A history of the cepstrum”, *IEEE signal processing Magazine*, 2004.

[33] R. Veras, J. Thorpe, and C. Collins, “Visualizing semantics in passwords: The role of dates”, in *Proceedings of the 9th International Symposium on Visualization for Cyber Security*, ser. VizSec ’12, 2012.

[34] A. M. De Alvaré, “How crackers crack passwords or what passwords to avoid”, Lawrence Livermore National Lab., CA (USA), Tech. Rep., 1988.

[35] R. V. Yampolskiy, “Analyzing user password selection behavior for reduction of password space”, in *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology*, IEEE.

[36] C. W. Munyendo, P. Markert, A. Nisenoff, *et al.*, ““the same pin, just longer”: On the (in)security of upgrading pins from 4 to 6 digits”, 2022.

[37] M. Keith, B. Shao, and P. J. Steinbart, “The usability of passphrases for authentication: An empirical field study”, *International journal of human-computer studies*, vol. 65, no. 1, pp. 17–28, 2007.

[38] J. Nicholson, L. Coventry, and P. Briggs, “Age-related performance issues for pin and face-based authentication systems”, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013.

[39] M. N. Al-Ameen, M. Wright, and S. Scielzo, “Towards making random passwords memorable: Leveraging users’ cognitive ability through multiple c‘ues”,

in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015.

[40] J. H. Huh, S. Oh, H. Kim, K. Beznosov, A. Mohan, and S. R. Rajagopalan, “Surpass: System-initiated user-replaceable passwords”, in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.

[41] M. Cardaioli, S. Cecconello, M. Conti, S. Milani, S. Picek, and E. Saraci, “Hand me your pin! inferring atm pins of users typing with a covered hand”, *arXiv preprint arXiv:2110.08113*, 2021.

[42] S. Schneegass, A. Saad, R. Heger, S. Delgado Rodriguez, R. Poguntke, and F. Alt, “An investigation of shoulder surfing attacks on touch-based unlock events”, *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. MHCI, pp. 1–14, 2022.

[43] A. De Luca, M. Denzel, and H. Hussmann, “Look into my eyes! can you guess my password?”, in *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009.

[44] A. Saad, M. Chukwu, and S. Schneegass, “Communicating shoulder surfing attacks to users”, in *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia*, 2018.

[45] K. Renaud and M. Volkamer, “Exploring mental models underlying pin management strategies”, in *Proceedings of the 2015 World Congress on Internet Security (WorldCIS)*, 2015.

[46] J. Bonneau and S. Schechter, "Towards reliable storage of 56-bit secrets in human memory", in *Proceedings of the 23rd {USENIX} Security Symposium ({USENIX} Security 14)*, 2014.

[47] J. Blocki, S. Komanduri, L. Cranor, and A. Datta, "Spaced repetition and mnemonics enable recall of multiple strong passwords", *arXiv preprint arXiv:1410.1490*, 2014.

[48] S. B. Kaufman, C. G. DeYoung, J. R. Gray, L. Jiménez, J. Brown, and N. Mackintosh, "Implicit learning as an ability", *Cognition*, vol. 116, no. 3, pp. 321–340, 2010.

[49] C. A. Seger, "Implicit learning.", *Psychological bulletin*, vol. 115, no. 2, p. 163, 1994.

[50] T. Denning, K. Bowers, M. Van Dijk, and A. Juels, "Exploring implicit memory for painless password recovery", in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011.

[51] C. Castelluccia, M. Dürmuth, M. Golla, and F. Deniz, "Towards implicit visual memory-based authentication", in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2017.

[52] C. M. Mooney, "Age in the development of closure ability in children.", *Canadian Journal of Psychology/Revue canadienne de psychologie*, vol. 11, no. 4, p. 219, 1957.

[53] H. Bojinov, D. Sanchez, P. Reber, D. Boneh, and P. Lincoln, "Neuroscience meets cryptography: Crypto primitives secure against rubber hose attacks", *Communications of the ACM*, 2014.

[54] M. M. Chun, “Contextual cueing of visual attention”, *Trends in cognitive sciences*, vol. 4, no. 5, pp. 170–178, 2000.

[55] S. Dehaene, L. Naccache, G. Le Clec’H, *et al.*, “Imaging unconscious semantic priming”, *Nature*, vol. 395, no. 6702, pp. 597–600, 1998.

[56] M. M. Chun and Y. Jiang, “Contextual cueing: Implicit learning and memory of visual context guides spatial attention”, *Cognitive psychology*, vol. 36, no. 1, pp. 28–71, 1998.

[57] J. J. Katz and J. A. Fodor, “The structure of a semantic theory”, *language*, 1963.

[58] Z. Joudaki, J. Thorpe, and M. V. Martin, “Reinforcing system-assigned passphrases through implicit learning”, in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018.

[59] T. P. McNamara, *Semantic priming: Perspectives from Memory and Word Recognition.* Psychology Press, 2005.

[60] M. B. Donnellan, F. L. Oswald, B. M. Baird, and R. E. Lucas, “The mini-ipip scales: Tiny-yet-effective measures of the big five factors of personality.”, *Psychological assessment*, 2006.

[61] J. Brooke *et al.*, “Sus-a quick and dirty usability scale”, *Usability evaluation in industry*, vol. 189, no. 194, pp. 4–7, 1996.

[62] A. Smyk, *The system usability scale & how it’s used in ux*, `https://xd.adobe.com/ideas/process/user-testing/sus-system-usability-scale-ux/`, Accessed: 01/27/2023, 2020.

[63] K. Cherry, *What are demand characteristics in psychology research?*, `https://www.verywellmind.com/what-is-a-demand-characteristic-2795098`, (Accessed on 08/08/2023), Apr. 2020.

Chapter 9

Appendix

9.1 Wrong PIN distribution

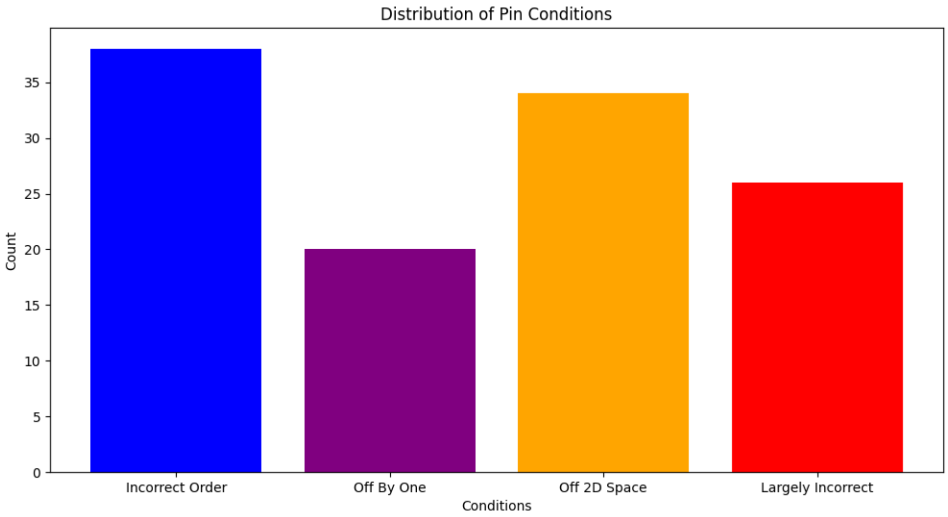


Figure 9.1: Wrong PIN distribution in CC group

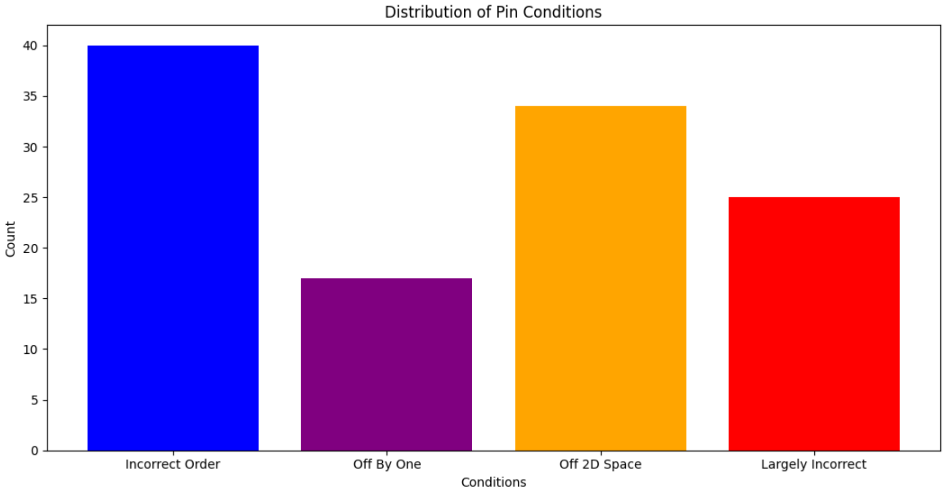


Figure 9.2: Wrong PIN distribution in Control group

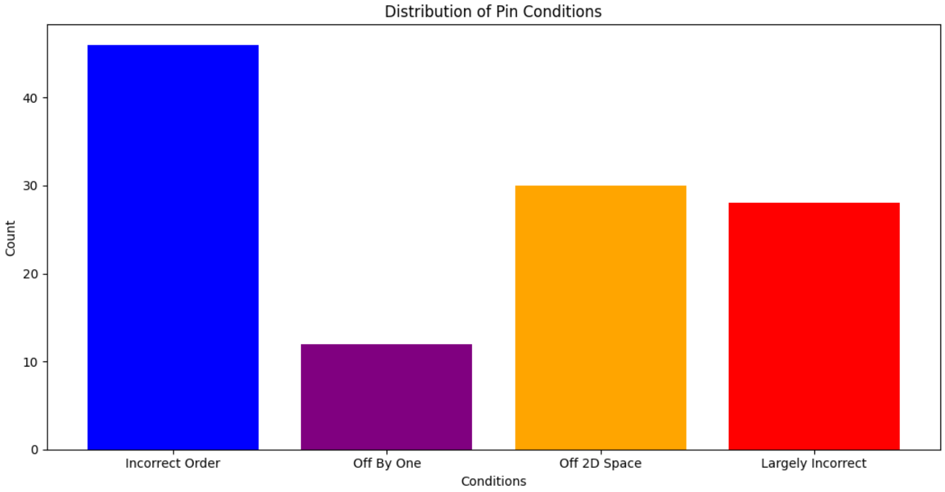


Figure 9.3: Wrong PIN distribution in CC-RP group

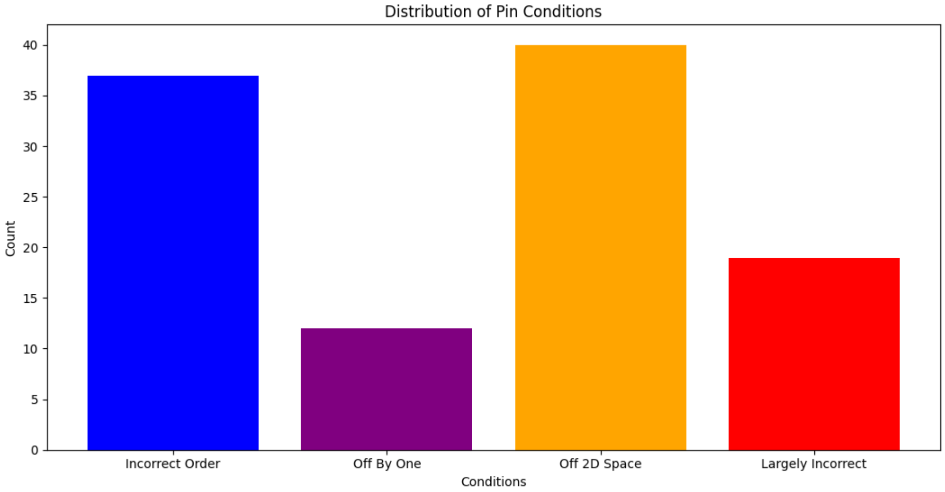
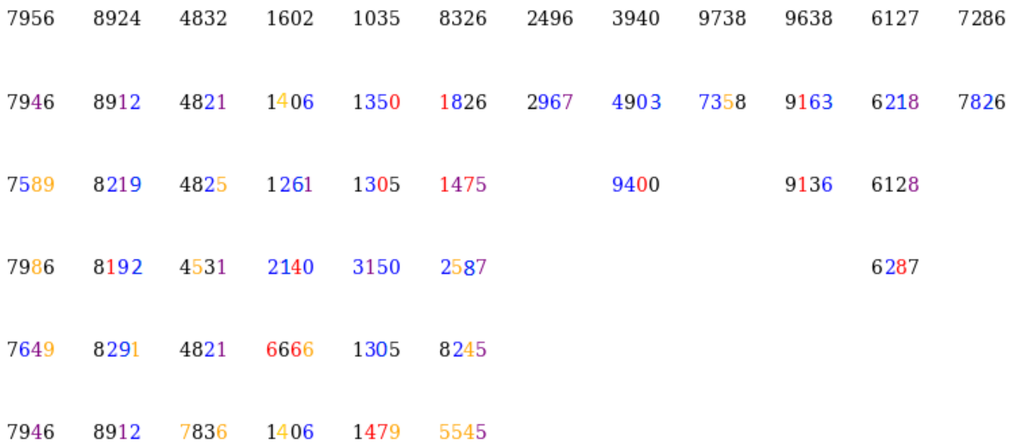
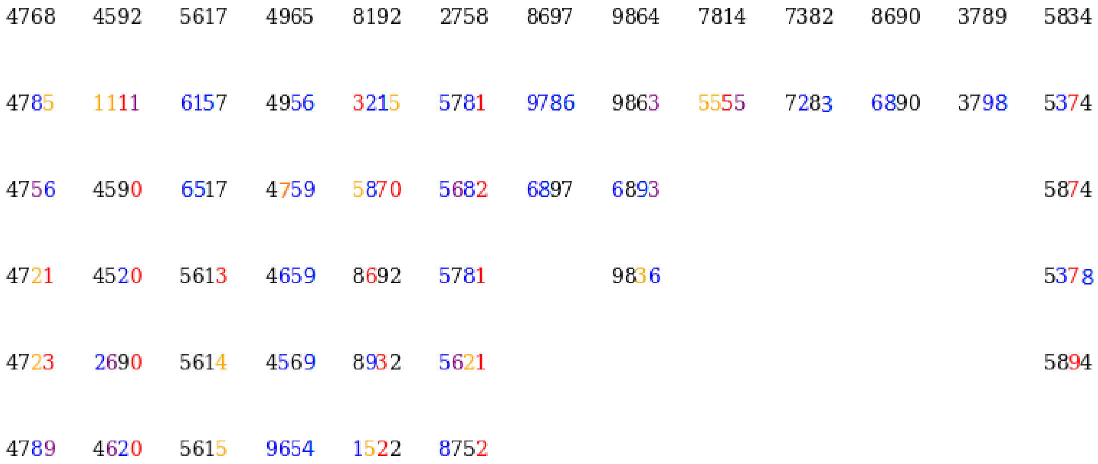


Figure 9.4: Wrong PIN distribution in RP group



7956	8924	4832	1602	1035	8326	2496	3940	9738	9638	6127	7286
7946	8912	4821	1406	1350	1826	2967	4903	7358	9163	6218	7826
7589	8219	4825	1261	1305	1475		9400		9136	6128	
7986	8192	4531	2140	3150	2587					6287	
7649	8291	4821	6666	1305	8245						
7946	8912	7836	1406	1479	5545						

Figure 9.5: Wrong PIN entered by users in CC group. Here digits with Blue color= Digit is in incorrect order, Purple= Digit is off by one, Orange= Digit is off by 2D space, Red= Digit is largely incorrect

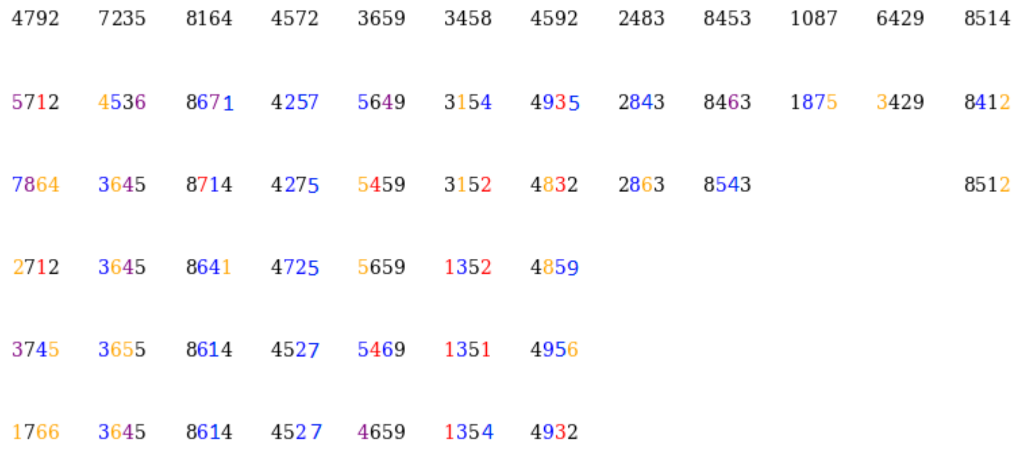


4768	4592	5617	4965	8192	2758	8697	9864	7814	7382	8690	3789	5834
4785	1111	6157	4956	3215	5781	9786	9863	5555	7283	6890	3798	5374
4756	4590	6517	4759	5870	5682	6897	6893					5874
4721	4520	5613	4659	8692	5781		9836					5378
4723	2690	5614	4569	8932	5621							5894
4789	4620	5615	9654	1522	8752							

Figure 9.6: Wrong PIN entered by users in Control group. Here digits with Blue color= Digit is in incorrect order, Purple= Digit is off by one, Orange= Digit is off by 2D space, Red= Digit is largely incorrect

7019	8216	4056	6214	5291	6140	4836	5276	3419	5726
7912	8691	4566	1212	5921	6142	4583	5706	3916	5762
7812	8571	4566	2961	5219	6142	4683	5726	3169	
7913	8171	4566	2361	5129	6426	4350	5267	3169	
7845	8971	4566	2231	5192	6426	4856	5627	3196	
7919	8671	4566	2222	5912	6041	4835	5627	3619	

Figure 9.7: Wrong PIN entered by users in CC-RP group. Here digits with Blue color= Digit is in incorrect order, Purple= Digit is off by one, Orange= Digit is off by 2D space, Red= Digit is largely incorrect



4792	7235	8164	4572	3659	3458	4592	2483	8453	1087	6429	8514
5712	4536	8671	4257	5649	3154	4935	2843	8463	1875	3429	8412
7864	3645	8714	4275	5459	3152	4832	2863	8543			8512
2712	3645	8641	4725	5659	1352	4859					
3745	3655	8614	4527	5469	1351	4956					
1766	3645	8614	4527	4659	1354	4932					

Figure 9.8: Wrong PIN entered by users in RP group. Here digits with Blue color= Digit is in incorrect order, Purple= Digit is off by one, Orange= Digit is off by 2D space, Red= Digit is largely incorrect

9.2 Session 1 Questionnaire

Please answer the following questions by selecting the relevant answer:

1. What gender do you identify as?

□ Male

□ Female

□ Non-binary

□ Prefer not to answer

2. What is your age?

□ 18 – 25 years old

□ 26 – 35 years old

□ 36 – 50 years old

□ 50 +

□ Prefer not to answer

3. What is the highest degree or level of education you have completed?

□ High school

□ Bachelor's degree

□ Master's degree

□ PhD or higher

□ Prefer not to answer

4. What is your first language (i.e., mother tongue)?

□ English

□ French

□ Other . . . .

□ Prefer not to answer

5. What is your primary area of study or work?

□ Social Sciences and Humanities

□ Science

□ Health Science

□ Engineering

□ Law

□ Education

□ Business

□ IT

□ Other ————

□ Prefer not to answer

How much do you agree with each statement about you as you generally are now, not as you wish to be in the future? Please indicate your answer using the following 5-point scale where: (1. = Strongly Disagree, 2. = Somewhat Disagree, 3. = Neither Agree nor Disagree, 4. = Somewhat Agree, 5. = Strongly Agree and 6. = Prefer Not to Answer)

	How much do you agree with each statement about you as you generally are now, not as you wish to be in the future?	1	2	3	4	5	6
1	I am the life of the party						
2	I talk to a lot of different people at parties						
3	I don’t talk a lot						
4	I keep in the background						
5	I sympathize with others feelings						
6	I feel others’ emotions						
7	I am not really interested in others						
8	I am not interested in other people’s problems						
9	I get chores done right away						
10	I like order						
11	I often forget to put things back in their proper place						
12	I make a mess of things						
13	I have frequent mood swings						
14	I get upset easily						
15	I am relaxed most of the time						
16	I seldom feel blue						
17	I have a vivid imagination						
18	I have difficulty understanding abstract ideas						
19	I am not interested in abstract ideas						
20	I do not have a good imagination						

Thank you for your cooperation in completing this questionnaire. Kindly submit the questionnaire by clicking on the ‘Submit’ button.

9.3 Session 1 Post-study Questionnaire

	Please respond to the following questions for the following parameters (Strongly Disagree, Somewhat Disagree, Neither Agree nor Disagree, Somewhat Agree, Strongly Agree and Prefer Not to Answer)	1	2	3	4	5	6
1	I found the training phase (if there was any) boring						
2	I thought the training (if there was any) would help me to remember the PIN						
3	I prefer to use my own chosen PIN over this system-assigned PIN						

4. We are interested in any other comments you might have concerning the system and experiment. Please write in the space below any thoughts you’d like to share with us.

Thank you for your cooperation in completing this questionnaire. Kindly submit the questionnaire by clicking on the ‘Submit’ button.

9.4 Session 2 Questionnaire

Did you write down or record the assigned PIN? It's okay if you did.

□ Yes

□ No

□ Prefer not to answer

Please respond to the following questions for the following parameters (Strongly Disagree, Somewhat Disagree, Neither Agree nor Disagree, Somewhat Agree, Strongly Agree and Prefer Not to Answer)

	Please respond to the following questions for the following parameters (Strongly Disagree, Somewhat Disagree, Neither Agree nor Disagree, Somewhat Agree, Strongly Agree and Prefer Not to Answer)	1	2	3	4	5	6
1	I found the first part of the experiment, i.e., “training phase” boring						
2	I think it was difficult to remember the digits in the assigned PIN codes						
3	I think that I would like to use this system frequently in order to have a more secure authentication token						
4	I found the system unnecessarily complex						
5	I thought the system was easy to use						
6	I think that I would need more instructions to be able to use this system						
7	I thought there was too much inconsistency in this system						
8	I would imagine that most people would learn to use this system very quickly						
9	I found the system very complicated to use						
10	I felt very confident using the system						
11	I needed to learn a lot of things before I could get going with this system						

12. We are interested in any other comments you might have concerning the system and experiment. Please write in the space below any thoughts you'd like to share with us.

Thank you for your cooperation in completing this questionnaire. Kindly submit the questionnaire by clicking on the 'Submit' button.