计算机科学
COMPUTER SCIENCE

助记口令创建策略综述

陈佳敏, 蒋惠萍

引用本文

陈佳敏, 蒋惠萍. 助记口令创建策略综述[J]. 计算机科学, 2024, 51(11A): 240300100-11.

CHEN Jiamin, JIANG Huiping. Overview of Mnemonic Password Creation Policies[J]. Computer Science, 2024, 51(11A): 240300100-11.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240300100

助记口令创建策略综述

陈佳敏　蒋惠萍
中央民族大学信息工程学院　北京 100081
(22302049@muc.edu.cn)

摘　要　口令身份验证因其简单性和可部署性而成为当今最常见的身份验证方式。随着口令猜测攻击算法的不断改进,对口令强度的要求也越来越高。强口令虽然能够提高安全性,但往往难以记忆,而易记口令则容易受到破解的威胁,因此选择既强大又易于记忆的口令成为一项挑战。随着每个用户的账户数量不断增加,需要记住的口令数量也在增加,这给人类记忆带来了明显的压力,因此寻找生成易记强口令的方法成为必须。在过去的二十多年里,许多研究者提出了基于不同助记工具的助记口令创建策略。故对现有的助记口令创建策略进行综述,首先针对口令创建背景、口令强度进行概况总结,其次根据助记工具的特点,将其分为基于句子、基于单词、基于键盘和其他特殊类型4类,并对每种类型进行了深入综述;最后,对助记口令创建策略进行了总结和展望,并指出了未来的研究方向和发展趋势。

关键词:助记口令;口令强度;口令策略;可记忆性;安全性
中图分类号　TP309

Overview of Mnemonic Password Creation Policies

CHEN Jiamin and JIANG Huiping
School of Information Engineering,Minzu University of China,Beijing 100081,China

Abstract　Password authentication is the most common authentication method today due to its good simplicity and nice deployability. As algorithms for password guessing attacks continue to improve,the requirement for strong passwords is also increasing. Strong passwords,while improving security,are often difficult to memorize,while easy-to-remember passwords are vulnerable to cracking threats,making it a challenge to choose passwords that are both strong and easy to remember. As the number of accounts per user continues to grow,so does the number of passphrases that need to be memorized,placing a noticeable strain on human memory and making it necessary to find ways to generate strong passphrases that are easy to remember. Over the past two decades,many researchers have proposed strategies for creating mnemonic passphrases based on different mnemonic tools. Therefore,a review of existing mnemonic password creation strategies is conducted. Firstly,an overview is summarized for the background of password creation and the strength of the password. Secondly,according to the characteristics of mnemonic tools,they are categorized into four types:sentence-based,word-based,keyboard-based and other special types,and each type is reviewed in depth. Finally,the strategies for creating mnemonic passphrases are summarized and outlooked,and future research directions and development trends are pointed out.

Keywords　Mnemonic passwords,Password strength,Password strategy,Memorability,Security

1　引言

口令认证技术,以其低要求、简易部署及广泛适用性等特性,展现出其他认证方式所无法比拟的优势。因此,在未来可预见的时间内,口令身份验证将继续在身份验证系统中占据重要地位[1-2]。然而,强口令的复杂性往往导致用户难以记忆,进而促使他们选择易于记忆但安全性较低的口令,从而增加了口令泄露的风险[3-5]。为应对此问题,众多服务提供商采用口令组合策略,旨在引导用户选择更为安全的口令[6-7]。这些策略通常对口令的创建提出明确要求,如设定最小字符数、包含大写字母或数字,以及避免使用常见字典词汇等[8]。研究显示,这些策略确实有助于用户生成更为安全的口令[9],但过于严格的创建要求也可能引发用户的反感[10]。用户往往会采取某些策略以迎合这些要求,从而导致口令模式的可预测性增强[6,8]。此外,部分用户因无法记住复杂的口令而不得不将其记录下来,这无疑增加了安全风险[11]。这一困境的核心在于用户生成的口令在安全性与可记忆性之间存在固有的矛盾。在严格的口令策略下,用户难以同时实现口令的安全性与可记忆性。随着口令可用性的降低,用户倾向于重复使用同一口令,从而加剧了口令重用的问题[12]。

众多在线服务,包括微软和谷歌等,已采取措施将常见的简单口令列入黑名单,并禁止用户使用,旨在降低口令被猜测的风险[13]。为提高口令的易用性,多家机构和研究人员提出了各种记忆辅助方法,如口令短语[14-15]和助记符策略[16-17],以优化口令的可用性。例如,亚马逊的支付短语系统要求用户注册至少包含两个单词的短语以完成支付授权。Bonneau等的研究表明,与传统口令相比,多词短语在提升安全性方面具有显著优势[14]。Yan等则对比了基于句子的助记口令与

通信作者:蒋惠萍(jianghp@muc.edu.cn)

随机口令的安全性和可记忆性，指出两者在安全性上相当，但助记口令在可记忆性方面更胜一筹[17]。

本文第1章详细探讨了用户设置口令的常见行为，并对口令强度进行了概述；第2章综述了当前流行的基于句子的助记口令创建策略，并对各种方法的优缺点进行了深入分析和比较；第3章则聚焦于基于单词的助记口令创建策略，对不同方法生成的口令在强度和长度方面进行了比较和分析；第4章介绍了基于键盘的助记口令创建策略，并对各种创建策略的安全性和可记忆性进行了比较和分析；第5章则分析了其他特殊助记口令创建策略的特点；最后总结全文并展望未来。

2 背景知识

2.1 用户设置口令行为

身份验证作为计算机安全体系的核心要素，文本口令的使用已受到广泛而深入的研究。然而，这种传统的身份验证方法存在若干局限性。为了在安全性与用户友好性之间取得平衡，研究者们提出了图形密码、基于位置的认证等多种替代方案[18-20]。尽管这些新方法提供了多种选择，但它们并未完全超越传统键盘字符键入方式在身份验证中的简洁性与经济性优势[2]。因此，可以预见，在未来的一段时间内，基于文本的口令仍将是网络身份验证的主流形式[21]。

基于文本的密码，即口令，其认证技术以其低要求、简易部署和广泛适用性而显著优于其他认证方式。然而，就其实用性而言，基于口令的身份验证存在若干不足。一个理想的口令需兼具“易于记忆且难以预测”的特性[22]。口令常因遭受攻击而构成信息系统安全的主要风险点[23]。这种脆弱性主要源于用户的使用习惯与不当操作，而非口令系统固有的问题。这些问题多因口令的可记忆性需求而引发，诸如口令的重复使用、共享以及弱口令的选择等，均在口令认证研究领域受到广泛探讨，并被归类为“人为因素问题”[21,24]。

常见的“人为因素问题”往往与用户的个人信息紧密相关，例如姓名、昵称、住址或出生日期等[25]。口令破解工具能够轻易识别出包含字典中的常见单词[26]，以数字序列为后缀的真实词汇[26]、名人姓名[27-28]以及类似于“qwert”的键盘布局模式[29]的口令。除口令创建过程中的问题外，用户在使用口令时也存在安全隐患，如重复使用相同口令[27]、将口令记录在纸上[25]，或将口令置于显眼位置等[11,25,27,30]。Horowitza[30]估计，多达20%的用户会采用在显示器上粘贴便签的方式记录口令。

尽管大多数人认识到选择强大口令对信息保护的重要性，但用户往往缺乏具体指导来创建难以破解的口令。通常建议口令应由多种字符组成，而非仅限于字典中的词汇[17]。然而，尽管这些建议广泛存在，许多用户并未遵循这些最佳实践，导致安全性较低的弱口令被广泛使用。研究表明，由于口令泄露事件的普遍性以及用户对强口令创建规则的不了解，用户往往没有充分意识到使用弱口令所带来的风险[26,31]。

2.2 口令强度

使用强口令可以有效降低被猜测或破解的风险[32]。口令的强度主要依赖于其长度和复杂度，而复杂度则由口令中字符的随机性决定[33]。为提升口令复杂度，一种策略是规定口令必须至少包含3种类型的字符：小写字母、大写字母、数字和特殊符号。

密钥空间，即所有潜在密钥（例如口令）值的集合大小，是衡量系统安全性的关键指标[34]。以四位数PIN码为例，若每位数字均可在0－9之间选择，则其密钥空间为10^4，即拥有10000种可能的组合[35]。而一个由95个不同字符组成的八位口令，其密钥空间则高达95^8，约等于$7 * 10^{15}$，即存在约7万亿种潜在的口令组合。随着密钥空间的扩大，通过暴力破解法穷举所有可能组合所需的时间将显著增加[33]。

口令复杂性的提升与其可能组合数的增长呈正相关，特别是当口令长度增加时，这种增长更为显著[36]。例如，一个四位数的口令，若字符集从26个字母扩展至95个字符，其密钥空间将扩大近200倍；而若口令长度从4位增加至12位，即使字符集仅包含26个字母，其密钥空间也将增加超过2000亿倍。尽管复杂性和长度均是抵抗暴力破解攻击的关键因素，但口令长度通常被视为决定其强度的主导因素[37]。允许口令长度在一定范围内变化（如8～15个字符）将进一步扩大密钥空间[38]。然而，限制口令长度的范围可能限制用户的选择，例如，6～8个字符的范围可能显著限制用户不采用口令短语的可能性；当口令长度为20且字符集包含数字、大小写字母及标准键盘上所有符号时，其密钥空间可达$4 * 10^{39}$[33]。这代表了理论上所有可能的口令组合。然而，在实际情境中，用户创建口令时往往遵循特定模式，如选择尽可能短的长度、固定位置使用大写字母或数字等，这些模式虽满足复杂性和长度要求，但显著降低了密钥空间的实际大小，因此攻击者可利用这些模式进行针对性破解[39]。类似地，采用简单口令短语的用户亦面临类似问题，尽管其长度可能较长，但由于结构简单，实际熵值较低，使得这些口令更易被猜测[39]。在信息系统中，熵是衡量系统无序性或随机性的关键指标，低熵值的口令更易受暴力破解攻击[37]。

在设定口令长度和复杂度限制时，系统需权衡最大可能密钥空间与实际管理可行性[40]。为提升用户记忆口令的便利性，系统可倾向于推荐较长而非复杂度过高且难以记忆的口令[33]。

3 基于句子的助记口令创建策略

基于句子的助记口令创建策略是一种提高口令可记忆性和安全性的创新方法[41]。此策略倡导用户采用易于记忆的句子，如喜爱的名言、歌曲歌词或个人口头禅，并将其转化为高强度的口令。实施过程如下：首先，用户需选定一个熟悉且不易被他人猜测的句子；随后，利用句子中每个单词的首字母、缩写或其他形式来构造口令；最后，为增强口令的复杂性，可添加数字、特殊字符或实施大小写转换。通过这种方式生成的口令，既保证了足够的复杂性以满足安全需求，又易于记忆，便于用户管理和使用。此方法不仅丰富了口令的多样性，降低了用户遗忘口令的风险，还作为一种实用高效的口令管理策略被广泛采用[42]。该策略得到了NIST[33]的推荐。根据句子与口令出现的顺序可以将策略细分为以下两类。

3.1 先句子后口令

Yan等[43]提出了一种备受推崇的口令生成方法——“passphrase”方法。该方法通过提取短语中每个单词的首字母来构造口令，与采用众所周知的短语如“An apple a day keeps the doctor away”（“Aaadktda”）不同。它建议采用更具

个性化特征的短语,例如“My brother Bob is 23 years old”,并据此生成如“MbBi23yo”这样的口令。此方法的目的在于提升口令的安全性,因为使用个人化短语能够增加口令的复杂程度,同时保持较高的记忆友好性。通过避免使用广为人知的短语,用户能够有效保护其账户和信息免受未经授权的访问。

Vu 等[44]对一种旨在提升口令召回率和安全性的口令生成方法进行了评估,即基于句子的助记口令创建策略。该策略的核心在于将句子中每个单词的首字母组合成口令,同时句子和口令的设计需遵循一系列严格的标准,以保障口令的复杂性和安全性。首先,句子必须至少包含 6 个单词,以确保口令的长度足够。其次,句子需具有实际意义,以便于用户记忆。此外,每个账户的句子和口令必须独一无二,以增强口令的独特性。另外,句子和口令的设计还需包含特殊字符(如@或#)和数字,以增加口令的复杂性。以句子“Ming and I once planted a rose bush”为例,生成的口令可能为“ming&ioparb1”。这种方法的综合性限制和要求旨在创建既强大又易于记忆的口令,同时确保每个账户的句子和口令独一无二,以避免口令重用问题[41]。

经过三年的深入研究,Vu 等[40]再次对基于句子的助记口令创建策略进行了评估,并在原有基础上引入了一系列新的限制,以进一步提高口令的安全性。这些新限制包括:1)口令必须包含至少一个大写字母,以增加字符集的多样性;2)口令必须包含至少一个小写字母,以提高大小写混合的难度;3)口令不得包含用户的用户名或其任何变体,以防止口令与用户信息关联。这些改进使得策略更加符合各大网站对口令的安全性要求,并在设计中充分考虑了个人隐私的保护。改进后的策略示例如下:给定句子“Ming and I once planted a rose bush”,生成的口令可能是“M&Ioparb1”。这种更新后的策略通过引入更多元素的要求,增强了口令的强度,禁止了用户相关信息的出现,保护了个人隐私,从而更好地应对当今网络安全的挑战。

Zhang 等[45]提出了一种基于中文句法的口令生成策略,该策略充分利用了中文语言的独特性,包括其特有的声母、韵母和音调,以及一字多音的现象。以“卜”字为例,它拥有“bǔ”“bo”和“pú”等多个读音[46],为口令的生成提供了丰富的可能性。基于这一特性,该策略制定了以下具体的口令设置规则:1)用户需选择一个至少包含 8 个汉字的助记句,该句应对用户个人具有意义。2)每个汉字将按照特定的规则替换为字母、单词、数字和特殊字符,替换规则为:

(1)提取汉字声母首字母,例如,将“我”替换为“W”。

(2)将汉字翻译为英文单词,再提取字母,例如,将“走”替换为“go”。

(3)将汉字转换成相似的特殊字符或者字母,例如,将“卜”替换为“|\”。

(4)将汉字转换成谐音字符,例如,将“爱”替换为“2”。

(5)将汉字转化为常用符号标记,例如,将“非”替换为“!”。

整个助记句在转换为口令时至少需使用两种替换规则。以“我和小明曾经种过一丛玫瑰”为例,按照此策略,生成的口令可能是“W&XMcjzg1cMG”,该口令利用了上述规则中的(1),(4)和(5)进行转换。这种策略不仅体现了中文句法的特点,而且通过多样化的替换规则,增加了口令的复杂性,从而提高了口令的安全性。

2021 年,Komiya 等[47]提出了基于日语句法的口令创建策略。该策略充分利用了日语字符的多样性,包括平假名、片假名和汉字[48]。其中,平假名和片假名代表音节,每个字符对应一个特定的音节[49],而汉字作为表意文字,承载着丰富的意义[50]。在日语中,这些字符的灵活组合可以形成富有意义的句子。考虑到汉字在日语中的特殊读法,即音读和训读[51],该策略能够生成比原始句子更长的助记符口令。具体的口令设置规则如下:1)用户需构思一个包含 6～8 个字符的日语句子,并确保句子中至少有一半字符为汉字。2)用户需选择汉字读音的顺序,即先音读后训读或先训读后音读。3)提取句子中每个字符的首个字母。4)选择两个数字,一个置于口令开头,另一个置于末尾。

以谚语“雨降って地固まる”为例,汉字读音顺序选择“先音读后训读”,数字选择“1”和“3”;雨→音读:ame,训读:ame;降→音读:kou,训读:fu;っ→tsu;て→te;地→音读:chi,训读:ji;固→音读:ko,训读:katameru;ま→ma;る→ru。则生成的口令为“1aakfttcjkkmr3”。尽管该口令仅包含小写字母和数字,可能不符合某些网站的口令要求[52]。但仅由 8 个字符组成的句子能够生成长达 14 位的口令,这显示了基于日语句法的口令生成策略在增加口令长度方面的优势。

3.2 先口令后句子

随着用户需记忆的口令数量持续增长,生成既安全又易记的助记符对用户而言愈发困难。基于句子的助记口令的安全性,很大程度上取决于用户所选择的句子内容[53]。根据 Kuo 等[16]的研究,用户生成的助记符口令相较于随机生成的口令,其安全性并不高。然而,人类对于一系列完全不相关项目的记忆能力相对有限[54]。因此,提升口令的安全性与记忆便利性之间的平衡成为一项重要挑战。

为应对这一挑战,Jeyaraman 等[55]设计、开发并评估了一种基于文本语料库自动生成与给定口令相关的记忆助记符句子的系统。该系统首先随机生成包含大小写字符、特殊字符和数字的复杂口令。为增强口令的语义内容,系统采用自然语言句子,这些句子多源自新闻报道或故事,因富含信息而更易于吸引读者注意并留下深刻印象[56]。在替换过程中,系统对小写字母采用与首字母相同的字母进行替换,对数字则利用年份或形似字母进行转换,如将“0”替换为“o”,“1”替换为“l”等。对于大写字母,系统选择人名或地名进行替代。对于特殊字符,系统采用两种策略:一是将 ASCII 字符集中的特殊字符数量缩减至 26 个以内;二是使用两个小写字符的序列表示单个特殊字符,如将“%”表示为“aa”,“#”表示为“bb”。尽管这样的替换策略可能在一定程度上增加了记忆负担,但 Jeyaraman 等认为,相较于在没有助记符的情况下记忆复杂口令,记住这些替换规则的成本相对较低。通过创新性地结合语义内容生成助记符,该系统不仅提高了口令的安全性,还降低了用户的记忆负担,为口令管理提供了一种更为高效、安全的方案。

4 基于单词的助记口令创建策略

基于单词的助记口令创建策略,作为一种创新性的口令安全增强方法,其核心原理在于以单个单词为起点,通过实施

变形、转换、插入和删除等操作，衍生出更为强化的口令[57]。该策略的关键优势在于，运用单词作为口令的基础，能够有效避免包含易于识别个人信息的元素，如姓名、生日等常见个人标识，从而保护用户隐私。通过对单词进行巧妙处理，该策略不仅提升了口令的复杂性和独特性，增强了口令的防御能力，也有效降低了针对个人信息实施的攻击风险。

Forget 等[58-59]提出了一种轻量级的口令创建机制，即说服性文本口令(PTP)。该机制旨在通过鼓励用户采用更安全的口令策略，提高口令的整体安全性。说服技术(PT)[60]，作为一种通过互动计算系统改变用户态度和行为的技术，被有效地整合到 PTP 系统中。在 PTP 系统中，用户在创建口令时，系统会随机在用户输入的单词口令中插入一些字符，以此增强口令的安全性(具体过程见图 1 和图 2)。这种结合了随机性元素和用户互动的方法，显著提高了口令的复杂度，使其更难以被破解。Alain 团队的这一创新成果为用户创建更安全的口令提供了一种新颖且轻量级的解决方案，对提升口令安全性具有重要意义。

图 1 在应用有说服力的改进之前创建 PTP 口令[58]

Fig. 1 Creating a PTP password before applying persuasive improvements[58]

图 2 应用 Insert-2 说服性改进后的 PTP 口令创建[58]

Fig. 2 PTP password creation after applying Insert-2 persuasive improvement[58]

为了深入探究提高单词口令安全性的策略，Forget 及其团队设计并实施了多种 PTP 的变体。首先，团队提出了一种名为“预加载”的变体。在此变体中，用户在构建口令之前会接收到系统预置的字符。这些预置字符被随机放置在口令的前八个字符槽中，用户需根据这些预设字符创造自己的口令。其次，团队开发了“替换”版本。在此版本中，用户首先选定一个单词，随后系统随机替换口令中的部分字符。最后，团队还设计了“插入”变体。在此变体中，用户选定一个起始单词后，系统会在口令的随机位置插入额外字符，以扩展口令的长度。如图 2 所示，插入过程包含系统选择的两个字符。这些变体的设计旨在通过引入随机性和提高用户参与度，来增强口令的安全性，并为用户提供多样化的口令保护选择[61]。Forget 团队的这些探索为口令安全领域提供了更加灵活和多样的解决方案。

Yıldırım 等[62]提出了一种可靠的解决方案，鼓励用户自主创建口令公式。在他们的研究中，详细阐述了 3 种基于单词的口令记忆策略，旨在指导用户创造出既个性化又易于记忆的口令。这些策略如下所述：

1)用数字控制单词大小写

(1)选择一个单词，例如，“computer”成为简单的口令基础。

(2)指定一个数字，如 236，将单词“computer”和数字“236”结合。

(3)根据数字，将单词“computer”中指定位置的字母转换为大写，如第二、第三和第六个字母，形成“cOMpuTer”。

(4)在每个大写字母后添加对应的数字，形成“cO2M3puT6er”。

(5)通过调整每个数字的值，如增大或减小，生成新的口令，如“cO4M5puT8er”，以增加口令的复杂性。

2)单词与字符和数字交叉

(1)选择一个由普通数字组成的字符串，例如“12345”。(更推荐其他的数字，例如圆周率的前五位”31415”等。)

(2)指定一个由字母和特殊字符组成的序列，如“lo_ve_”。

(3)将数字字符串与字母和特殊字符序列交替组合，形成如“1l2o3_4v5e_”的强口令。

3)多个单词结合

若用户希望使用有意义的单词和短语，可以将多个单词结合，并添加字母、数字和其他特殊字符，形成长口令。例如，结合“monkey”“zoo”和“banana”，形成“monkeyzoobanana-size3”，其中特殊符号可根据喜好替换。

这 3 种口令创建方法各具特色，适用于不同用户群体和安全需求。第一种方法通过插入随机字符和大小写变换，提高了口令的复杂性。用户可以通过调整数字和变换规则，生成多个强口令，增强了灵活性。然而，若用户选择单词和数字的方式不当，可能导致口令的可预测性增加[63]。第二种方法利用数字和字符的交替组合，增强了口令的复杂性，可有效抵御简单猜测攻击。但用户需谨慎选择数字和字符组合，以确保口令的强度和可记忆性[64]。第三种方法允许用户构建包含有意义单词和短语的长口令，结合多种字符元素，提高了口令的安全性和可记忆性。但用户需注意，过长的口令可能增加记忆负担[65]。同时，文献[36]指出，由多个词典单词组成的口令可能存在熵值较低的问题，因此，在创建口令时，应更加注重单词后的设计和组合方式。

Umejiaku 等[66]针对用户需创建多个口令或频繁更改口令的挑战，设计了多种策略来增强口令的强度和安全性，旨在提升口令的随机性[67]或利用模式化助记符块来辅助记忆。其中，符合单词口令使用条件的策略如下：

1)元音替换法

该策略用预定义的字符替换单词口令中的所有元音，从而增加口令的复杂性和安全性。例如，单词“password”可以被转换为“p@ssw0rd”。

2)高频元音替换法

此方法涉及使用预定义的字符替换单词口令中出现频率最高的元音，进一步提升了口令的复杂性和安全性。例如，单词“experience”可以被修改为“1xp2ri3nc4”。

3)元音删除法

该策略通过移除单词口令中的所有元音，来进一步增加口令的复杂性和难以预测性。例如，单词“environment”可以简化为“nvrnmnt”。

上述3种口令增强策略在设计上各有优势,但同时也存在一定的潜在风险。策略一通过替换元音提高了口令的复杂性,使得口令更难猜测,且由于替换规则相对简单,用户更易记忆。然而,某些替换字符可能仍较为常见,因此选择时需谨慎。策略二通过替换单词中最常出现的元音,增加了口令的复杂性和多样性,提高了安全性。对于用户而言,该策略可能更易记忆,但仍需适应替换规则,可能增加使用难度[68]。策略三通过删除所有元音彻底改变了口令结构,使其更难猜测,但同时大大降低了口令的可读性,可能导致用户记忆困难[69]。

综上所述,这些方法均能在一定程度上提升口令的安全性。用户在选择时应根据个人偏好和记忆能力进行权衡。在实际应用中,用户应综合考虑这些方法的优缺点,选择最适合自己的口令增强策略[70]。

5 基于键盘的助记口令创建策略

基于键盘布局的助记口令创建策略充分利用了键盘字符排列的固有特性[70],以增强用户的记忆效果。一种常见的做法是利用键盘上的特定行或列作为口令生成的基础。在此方法中,用户可以选择键盘上的一行字母,并按照特定的序列或规则构造口令[72],确保口令包含大小写字母、数字和符号的混合。这种策略为用户提供了一种直观的记忆框架,使用户能够凭借对键盘布局的熟悉性[73],轻松回忆起口令的生成逻辑。这种直观性有助于用户在需要时快速而准确地输入口令,从而提高了口令的实用性和用户的使用体验。

Ye等[74]对4种常见的助记口令创建技术的安全性和可用性进行了深入评估。其中,键盘更改(KbCg)方法是一种独特且有效的策略。其核心思想在于选取一个易于记忆的基础口令,通过改变键盘上一个或多个键的位置(如左上、右上、左下或右下),生成最终的口令。用户仅需记住基础口令和键位移动的方向,无需记忆最终生成的复杂口令。以"elephant"为例,若将所有键向左上方移动,最终生成的口令为"3o30yqh5"。实验结果表明,这种口令在安全性上与随机生成的口令相近,但在可记忆性上表现更佳。

这种创新的口令生成方法充分利用了人类对空间和方向记忆的优势[75]。用户仅需记忆基础口令和键位移动的方向,即可轻松恢复完整的口令。相较于传统的口令创建方法,该策略在提升口令安全性的同时,显著降低了用户的记忆负担。因此,KbCg方法在平衡口令的安全性和用户记忆便利性方面取得了显著成效。

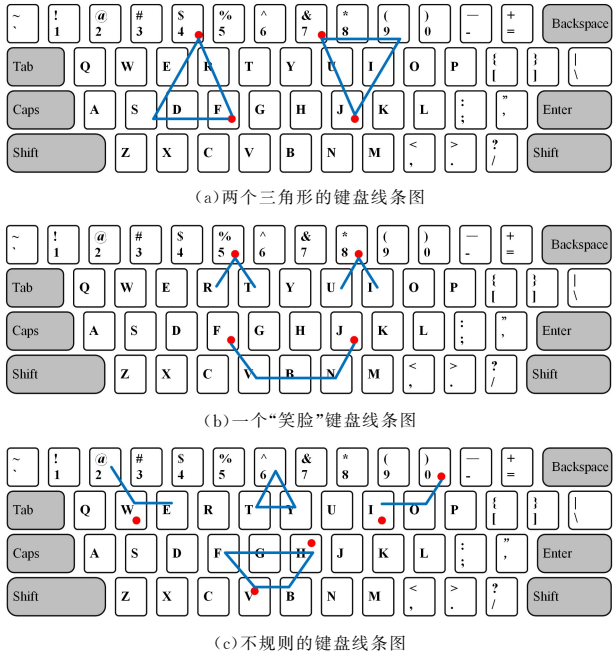
Guo等[76]进一步提出了Optiwords策略,这是一种基于图片优势效应[77]的创新文本口令创建方法。它引导用户在键盘上绘制简单的线条图案(称为"口令图案"),并根据自定义的顺序从这些线条中选取字符,组合成最终的文本口令。为增强口令的安全性,Optiwords设定了3个核心规则。

1)口令构成规则:要求口令至少包含8个字符,且必须涵盖大写字母、小写字母、数字和特殊符号中的至少3类。这一准则确保了口令的复杂度,可有效抵御多种口令破解技术。

2)字符顺序规则:允许用户根据偏好选择字符在口令图案中的排列顺序,如水平或垂直排列。这种灵活性使得用户可以根据自己的记忆习惯定制口令。

3)字符位置规则:Optiwords还允许用户决定是否将字符直接放置在口令图案的线条上。例如,在绘制四边形图案时,用户可以选择是否沿图形边缘排列字符。这一选项进一步丰富了口令的多样性。

基于上述规则,一个键盘图案可以生成多个不同的文本口令。图3展示了Optiwords图案的3个示例。图中的点表示该字符是通过"Shift"键输入的。在图3(a)中,根据从左到右、从上到下的顺序,生成的口令可以是"$esdFr&uJi98"。若选择从右到左、从上到下的顺序,则口令为"98&uJi$esdFr"。若用户仅选择左三角形上的顶点字符,口令则为"$sF&89iJu"。类似地,图3(b)和图3(c)中的图案按一定顺序生成的口令可以是"r%tu*iFvbnJ"和"2We6ty)oIfgHbV"。



(a)两个三角形的键盘线条图

(b)一个"笑脸"键盘线条图

(c)不规则的键盘线条图

图3 键盘线条图示例

Fig. 3 Examples of keyboard line drawings

Optiwords作为一种创新的口令创建策略,为用户提供了富有趣味性和创新性的口令生成方式。然而,在推广过程中需关注用户的记忆能力和使用工具的便捷性,以确保其在实际应用中的有效性。

在Optiwords策略中,用户需记忆所选形状。使用复杂形状虽能提高口令安全性,但也增加了记忆难度。相反,简单形状虽易记但可能降低安全性[78]。为平衡可记忆性与安全性,Song等[79]随后提出了一种新的基于形状记忆的口令生成策略——Alphapwd。该策略基于字母和汉语拼音的书写笔划顺序,模拟字符在键盘上的书写过程,旨在帮助用户创建既安全又难忘的口令。

Alphapwd策略的核心思想体现在以下几个方面:首先,生成的口令需至少包含大写字母、小写字母、数字和符号中的两种类型的字符;其次,通过模拟键盘上字母的书写顺序,将按键对应的符号作为口令的组成部分;再次,用户可选择是否将所有密钥符号作为口令的一部分,或者选择性地使用部分符号,例如,每隔一段时间选择口令上的符号,但不影响字母的轮廓;最后,用户仅需记忆所选助记符及其在键盘上的起始位置,然后利用这些信息输入口令。

以英文单词"god"为例,展示Alphapwd口令生成的过程。根据图4所示的书写顺序,生成的口令为"resdrdxz6t

yiuhji9ij"(g→'resdrdxz',o→'6ty',d→'iuhji9ij'),该口令包含多种字符类型,呈现出随机字符串的外观。然而,通过暴力算法破解该口令,其搜索空间将达到 95^{20}。但用户仅需记忆3个助记符及其起始位置('g'起始位置为'r','o'起始于'6','d'起始于'i'),即可快速准确地输入口令。这种策略巧妙地平衡了记忆需求与安全性,提供了一种高效且用户友好的口令生成方式。然而,Alphapwd 的有效性受限于用户对键盘布局的熟悉程度,对于非经常使用键盘或使用不同键盘布局的用户,可能需要一定的适应期。

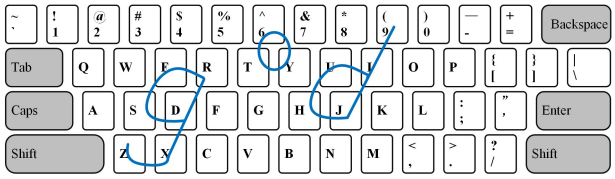


图 4 在键盘上模拟'g''o''d'

Fig. 4 Simulation of 'g''o''d' on keyboard

值得注意的是,Alphapwd 策略并未利用"Shift"键进行字符切换,这可能会导致口令中大小写字符无法并存,且无法使用与数字同键的特殊字符[80]。为增强口令字符类型的多样性,Lyu 等[81]在 2021 年提出了 AvoidPwd 策略,这是一种基于键盘转换的新型助记符口令生成方法。AvoidPwd 策略鼓励用户自定义"路线"绕过"障碍物",并选择路线上的字符作为口令。其中,"障碍物"为易记单词,其每个字母均为障碍;而"路线"则是通过障碍物的字符串,实现了键盘序列的可视化。

AvoidPwd 策略的基本思想如下:

1)用户首先选择一个易于记忆的单词(不限语言)作为"障碍物",并基于该"障碍物"设计一条"路径"作为口令。在输入时,用户利用"Shift"键敲击"障碍物"附近的键。"障碍物"在此充当记忆辅助工具,减轻了用户的记忆负担。

2)即使选择相同的"障碍物",用户也可以通过改变路径方向生成不同的口令。在需要更新口令时,用户仅需调整通过"障碍物"的路径即可。以下是一些建议的路径设计策略。

(1)全包围:适用于所有字符都集中在键盘上的"障碍物"。用户可以设计一条环绕"障碍物"的完整路径,并在末尾适当延伸。

(2)半包围:适用于大部分字符集中但有少数分散的"障碍物"。用户可以设计一条部分包围"障碍物"的路径,然后直接指向剩余部分。

(3)同方向绕行:适用于字符从"障碍物"向外延伸的情况。用户可以从"障碍物"外侧画出一条曲线作为路径。

3)AvoidPwd 策略建议用户在设计"路径"时,确保至少包含 8 个字符,并涵盖大写字母、小写字母、数字和符号中 3 种类型的字符。

综上所述,与传统的基于键盘的口令策略相比,AvoidPwd策略展现出了更高的灵活性。同一"障碍物"可以生成多个不同的口令。如图 5 所示,障碍物是一个英文单词"left"。红点表示该键与"障碍物"相邻,应使用"Shift"键键入。采用相同方向的方法绕过障碍物,可能的文本口令为"aSDR%∧Yhnm〈〉"。当用户需要定期更新口令时,可以选择不同的路径设计方法。

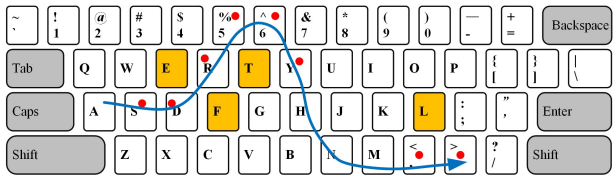


图 5 使用英语单词"left"作为障碍的例子

Fig. 5 Example of using the English word 'left' as an obstacle

综上所述,与传统的基于键盘的口令策略相比,AvoidPwd策略展现出了更高的灵活性。同一障碍物可以生成多个不同的口令。在图 5 中,障碍物为英文单词"left",采用同方向绕行策略,可能的文本口令为"aSDR%∧Yhnm〈〉"。当用户需要定期更新口令时,可以选择不同的路径设计方法。AvoidPwd 策略通过引入"Shift"键,有效解决了 Alphapwd 策略中口令字符类型不足的问题,从而提高了口令的安全性。用户只需记住障碍物和选择的路径,无需记忆具体的字符序列,即可轻松更新口令。然而,需注意的是,某些较弱的路径设置方法,如仅在水平方向上直线移动[82],不建议使用,因其易遭受破解攻击[83]。为提高口令强度,建议用户结合多种方法创建口令。此外,与 Alphapwd 策略相似,AvoidPwd 策略同样要求用户对键盘布局有一定的了解。

6 其他助记口令创建策略

除了基于句子、单词和键盘的助记口令生成策略外,一系列创新性的助记口令策略也应运而生。这些策略为用户提供了丰富多样的选择,使得用户能够根据个人偏好和习惯创建出既独特又安全的口令。

6.1 基于形状的助记口令创建策略

Weiss 等[84]提出了一种新颖的身份验证方法——PassShapes。该方法要求用户绘制由 8 种不同笔划的任意组合构成的简单几何形状,以此向计算系统验证身份。在 PassShapes 中,共定义了 8 种不同的笔划方式,如图 6 所示。

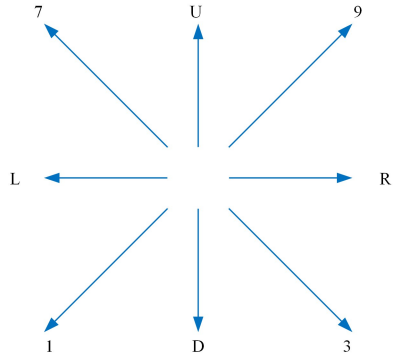


图 6 PassShapes 概念中使用的 8 种不同笔划

Fig. 6 Eight different strokes used in the concept of PassShapes

PassShapes 能够生成字母数字字符串作为口令,用于内部处理和存储。每种笔划都对应一个特定的字符表示,如图 6 所示,其中字母代表笔划的方向,如"L"代表"left"(左),"R"代表"right"(右)等;而数字则指示与标准数字键盘上位置相对应的方向(即"7"对应于"左上角")。提笔事件,即分隔两个笔划序列的动作,则用"X"进行标记。图 7 展示了一个包含两个笔划序列、共计 10 种笔划的 PassShape 示例。

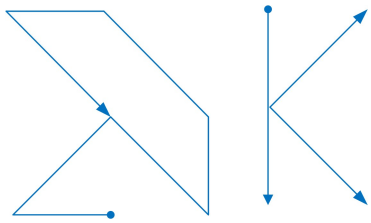


图 7　内部表示为 L93U7L3XD93 的 PassShape 示例

Fig. 7　PassShape example with the internal representation L93U7L3XD93

PassShapes 策略利用具体形状或图案的组合,显著提升了口令的可记忆性和安全性。该策略充分利用了人类大脑对图像和形状的记忆优势,使用户能够更轻松地记住复杂的口令。这种口令策略的一大优势在于提供了一种直观且高效的记忆辅助方式,因为人脑对视觉信息的处理速度更快,记忆更深刻[85]。同时,基于形状的口令有助于降低用户遗忘口令的风险,因为形状和图案通常更易于与个人生活经验相联系,从而增强了口令的记忆效果。

6.2　基于更改的助记口令创建策略

随机生成的口令虽然具有高度的安全性,但由于其复杂性和难以记忆的特性,其在实际应用中的采纳率受到一定的限制[39,86]。为了克服这一挑战,Huh 等[87]提出了一种与 Alain 等[58-59]的研究方向相悖的创新性口令方案,即"Surpass"。Surpass 策略旨在通过允许用户在随机生成的口令中替换部分字符,从而生成更加个性化的、易于记忆的口令。

初始口令由 94 种不同字符(包括数字、大小写字母和特殊符号)随机组合而成,共包含 8 个字符。系统提供了 4 种不同的 Surpass 策略,从 1-Change 到 4-Change,这些策略逐步放宽了用户可替换字符的数量,最多可替换原始口令的 50%。例如,表 1 列出了以"6^^V[af."为原口令的 4 种 Surpass 策略实例。

表 1　Surpass 规则

Table 1　Surpass policies

策略	详细描述	例子
1-Change	用户可以从给定的随机生成的 8 个字符的口令中替换最多 1 个字符	6^^V[af.→ 6^^V[a]
2-Change	用户最多可以替换 2 个字符	6^^V[af.→ 6^^v[a]
3-Change	用户最多可以替换 3 个字符	6^^V[af.→v^^v[a]
4-Change	用户最多可以替换 4 个字符	6^^V[af.→v^^v[1]

这种方法在保持口令安全性的同时,显著提高了其易用性,使得用户更易于接受和记忆口令。根据 Huh 等进行的用户研究表明,3-Change 和 4-Change 策略在可记忆性方面相较于原始口令展现出显著优势。具体而言,采用 4-Change 策略的口令在 8 天内的存活率相比原始口令提高了 44%。

然而,随着可替换字符数量的增加,口令的安全性也相应降低。从原始口令的 0% 破解风险,到 3-Change 策略的 1.21%,再到 4-Change 策略的 5.82%,口令被破解的可能性逐步上升。因此,在权衡随机生成的 8 个字符口令的选项时,Huh 等建议用户选择 Surpass 策略中的 3-Change 策略,以在口令的安全性和可记忆性之间寻求一个最佳的平衡点。

6.3　基于游戏的助记口令创建策略

McLennan 等[88]设计并验证了一种创新的口令记忆方法,该方法以游戏布局为基础来创建口令。研究者们开发了一种名为 Game Changer 的口令系统,该系统通过国际象棋棋盘上的棋子位置来生成口令。例如,如图 8 所示,将黑王(BK)放在 c7 位置、黑车(BR)放在 g6 位置、白骑士(WN)放在 b5 位置以及白卒(WP)放在 f2 位置,这些棋子的特定布局可以转换成一个口令,如"BKc7BRg6WNb5WPf2"。每个这样的布局都对应一个独特的口令组合。

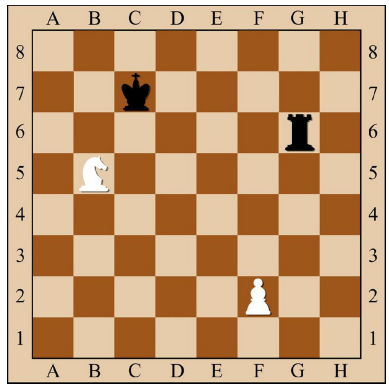


图 8　国际象棋口令:BK c7,BR g6,WN b5,WP f2

Fig. 8　Chess-based password:BK c7,BR g6,WN b5,WP f2

该方法使用国际象棋棋盘和棋子位置作为口令的基础,创造出的口令至少包含大写字母、小写字母和数字,且这 3 种字符穿插组成非常复杂且难以猜测的口令。同时,每个棋盘布局都对应一个独特的口令,因此可以生成大量不同的口令组合。

除了国际象棋,用户还可以选择以大富翁游戏的棋盘布局为基础来创建口令。这种方法通过以游戏元素为口令的创建增添了趣味性和独特性,有助于提高口令的记忆效果和安全性。然而,这种方法更适合对这些游戏有深入了解的用户,因为用户需要能够回忆起棋盘布局以及棋子的种类和摆放位置。

Game Changer 口令系统推出两年后,Brumen[89]对其进行了安全性评估,并提出了 5 项改进建议,旨在增强系统的安全性和提供更多的口令组合选项。改进建议如下:

1)增加棋子类型:建议在系统中增加更多的棋子类型,这将扩大口令的组合范围,使口令更加复杂和安全。

2)扩展位置选项:提议增加口令系统中使用的位置数量,以提高口令的多样性。增加位置选择可以提升口令的组合可能性,从而增强系统的防御能力。

3)引入多种颜色的棋格:建议在系统中使用多种颜色的棋格,这将增加口令生成时的选择元素,使口令更难被猜测和破解。

4)增加棋子颜色的多样性:提议引入多种颜色的棋子,以提升口令的多样性。通过增加棋子颜色的选择,可以进一步提高口令的复杂度和强度。

5)考虑棋子移动:鼓励在生成口令时不仅考虑棋子的位置,还要考虑它们的移动。将棋子的移动纳入口令生成过程,可以创造出更具变化性和难以预测的口令。

这些改进建议旨在使 Game Changer 口令系统更加灵活和安全,同时为用户提供更多样化的口令组合,以实现更强的口令保护。通过这些改进,该系统能够更好地满足用户对于口令记忆和安全性的需求。

6.4　基于公式的助记口令创建策略

Ye 等[74]深入研究了 4 种广受欢迎的助记口令创建

策略，其中包括一项颇具创意的 UsForm(使用公式)技术。该技术引导用户选定一个数学公式及一系列数字，随后依据此公式构建方程式，并借助替代性表达方式生成口令。这种创新的口令创建方法旨在同时增强口令的安全性和记忆便捷性。

以公式“2+3+5=10”为例，用户能够利用该公式创造出诸如“TWO+3+Five=10”或“Twoand3+5=Ten”之类的口令。在此过程中，用户需牢记所选公式、数字及替代表达方式。由于口令基于用户自定义的公式和数字组合，因此具有独特性且难以遗忘。

UsForm 口令创建策略的一大显著优势在于其个性化特点。用户可根据自身偏好选择易于记忆的公式，从而创造出具有鲜明个人特色的口令。同时，由于用户需记忆公式和数字，这也进一步提升了口令的记忆难度，从而增强了其安全性。

7 结语

7.1 论文总结

口令认证因其符合用户偏好、易于使用和明确的使用意图而在众多认证方法中脱颖而出[90]。并且由于口令认证的易用性、高速性和安全性，故成为目前使用最广泛的身份认证方式[91]。本文对助记口令创建策略进行了梳理，将其归纳为基于句子、基于单词、基于键盘和其他策略四大类。

在基于句子的助记口令创建策略中，可以进一步细分为先创建句子后生成口令和先生成口令后构建句子两种方法。先句子后口令的方法要求用户首先构思一个有意义的句子，并可通过添加个人独特的短语来增加口令的复杂度。这个句子至少应包含 6 个单词，并且生成的口令必须包含至少 3 种类型的字符：大小写字母、数字和特殊符号。目前，这种方法已经发展出多语言版本，通过根据语言特性进行微调，能够很好地适应不同的语言环境。而在先口令后句子的方法中，系统会生成一个包含字符和数字的口令，然后利用文本语料库中的语义内容来提供记忆助记符句子，从而减轻用户的记忆负担。这种创新方法通过引入语义内容来增强口令的安全性，并降低用户的记忆成本。随着大型语言模型的发展，预计先口令后句子方法中的替换难题将得到解决。

基于单词的助记口令创建策略以单词为基础，通过对单词进行变形、转换、插入和删除等操作，生成强化口令。这种方法的优势在于确保口令不包含与个人直接相关的信息，如姓名或生日。同时，通过对单词进行巧妙的处理，不仅增加了口令的复杂性和独特性，还提高了抵御个人信息攻击的能力。基于单词的助记口令策略提供了多种选择，允许用户根据个人需求灵活生成安全且易记的口令。在实际应用中，用户应权衡不同方法的优缺点，选择最适合自己的口令创建策略。

基于键盘的助记口令创建策略利用键盘布局的特点，帮助用户更容易地记住口令，因为口令的生成与键盘上的字符位置直接相关。这种方法生成的口令在安全性上与随机口令相近。然而，是否使用“Shift”键会影响口令中包含的字符种类。此外，这种策略的有效性依赖于用户对键盘布局的熟悉度。对于那些不常使用键盘或使用不同键盘布局的用户来说，可能需要额外的时间来适应。用户应根据自己的需求和使用习惯，评估这些基于键盘的策略的优缺点，以选择最适合自己的口令生成方法。

除了基于句子、单词和键盘的助记口令创建策略之外，还有其他创新性的方法为用户提供口令选择。基于形状的口令策略利用人脑对图像和形状的记忆能力，提高了口令的可记忆性和安全性；基于随机口令的更改策略通过建议优先选择 3-Change，实现了强度和可记忆性的平衡；基于游戏的口令策略提供了一种有趣且独特的口令生成方式，但这种方法更适合熟悉相关游戏的用户；基于公式的口令策略提供了个性化的口令生成方式，用户可以根据自己的喜好选择公式，创造出既独特又易于记忆的口令。这些助记口令创建策略为用户提供了广泛的选择，用户能够根据自己的需求和偏好创建出既个性化又安全的口令。

7.2 未来展望

在当前的口令安全领域，助记口令的创建策略正在不断演进，但仍然面临着一些挑战。以下是对未来研究方向的一些展望。

1)口令重用问题的解决：尽管已有研究探讨了如何在不同系统中设置不同口令的问题，但口令重用依然是一个普遍现象[92]。未来的研究需要更深入地研究如何有效防止用户在多个系统中重复使用同一口令，并设计出能够激励用户为每个系统创建既独特又安全的口令的策略。这可能包括开发智能提示系统，帮助用户为不同服务生成和记忆独特的口令，或者实施更严格的口令管理政策，确保用户遵循最佳实践。

2)跨设备口令输入的一致性：随着用户在多种设备和键盘布局之间切换，基于键盘的助记口令创建策略可能会面临输入上的挑战。研究者需要考虑如何设计出能够在不同设备和输入方法之间保持一致性的口令创建策略。这可能会涉及对现有助记口令系统的适应性改进，或者开发新的口令创建方法，使其不受特定键盘布局的影响。

3)助记口令策略的普及：为了提高用户对助记口令策略的接受度和使用率，研究者需要探索如何将这些策略有效地传达给用户，并确保它们易于理解和实施。这可能包括开发易于理解的教育材料、将辅助功能集成到现有的口令管理工具中，以及与操作系统和应用程序的紧密集成，以便用户在创建新账户时能够自然地采用这些策略。

4)口令策略的自动化和智能化：随着人工智能和机器学习技术的发展，研究者可以探索如何利用这些技术来自动化口令策略的制定和执行。例如，可以开发智能系统来分析用户的输入习惯，自动推荐合适的助记口令创建策略，并在用户尝试输入弱口令时提供即时反馈。

结束语 本文对助记口令创建策略进行了全面的综述，将其主要分为基于句子、基于单词、基于键盘和其他特殊类型的策略。主要分析了各种策略的优缺点，并探讨了它们在提高口令安全性和可记忆性方面的有效性。助记口令创建策略尽管取得一定进展，但仍面临挑战，如口令重用和跨设备一致性问题。未来研究需关注防止口令重用、适应多设备环境、普及助记策略和智能化口令管理。目标是开发更安全、易用、适应性强的口令助记策略。

参考文献

[1] BONNEAU J, HERLEY C, VAN OORSCHOT P C, et al. Passwords and the evolution of imperfect authentication[J]. Communications of the ACM, 2015, 58(7): 78-87.

[2] BONNEAU J,HERLEY C,VAN OORSCHOTP C,et al. The quest to replace passwords:A framework for comparative evaluation of web authentication schemes[C]// 2012 IEEE Symposium on Security and Privacy. IEEE,2012:553-567.

[3] UR B,NOMA F,BEES J,et al. I Added'!'at the End to Make It Secure:Observing Password Creation in the Lab[C]// Eleventh Symposium on Usable Privacy and Security(SOUPS 2015). 2015:123-140.

[4] WASH R,RADER E,BERMAN R,et al. Understanding password choices: How frequently entered passwords are re-used across websites[C]// Twelfth Symposium on Usable Privacy and Security(SOUPS 2016). 2016:175-188.

[5] GUO Y,ZHANG Z. LPSE:Lightweight password-strength estimation for password meters[J]. Computers & Security,2018,73:507-518.

[6] KOMANDURI S,SHAY R,KELLEYP G,et al. Of passwords and people:measuring the effect of password-composition policies[C]// Proceedings of the Sigchi Conference on Human Factors in Computing Systems. 2011:2595-2604.

[7] WANG D,WANG P. The emperor's new password creation policies:An evaluation of leading web services and the effect of role in resisting against online guessing[C]// Computer Security—ESORICS 2015: 20th European Symposium on Research in Computer Security,Vienna,Austria,Part II 20. Springer International Publishing,2015:456-477.

[8] SHAY R,KOMANDURI S,KELLEY P G,et al. Encountering stronger password requirements: user attitudes and behaviors [C]// Proceedings of the Sixth Symposium on Usable Privacy and ecurity. 2010:1-20.

[9] WEIR M,AGGARWAL S,COLLINSM,et al. Testing metrics for password creation policies by attacking large sets of revealed passwords[C]// Proceedings of the 17th ACM Conference on Computer and Communications Security. 2010:162-175.

[10] INGLESANT P G,SASSE M A. The true cost of unusable password policies:password use in the wild[C]// Proceedings of the Sigchi Conference on Human Factors in Computing Systems. 2010:383-392.

[11] ADAMS A,SASSE M A. Users are not the enemy[J]. Communications of the ACM,1999,42(12):40-46.

[12] SEGRETI S M,MELICHER W,KOMANDURI S,et al. Diversify to survive:Making passwords stronger with adaptive policies[C]// Thirteenth Symposium on Usable Privacy and Security(SOUPS 2017). 2017:1-12.

[13] HABIB H,COLNAGO J,MELICHER W,et al. Password creation in the presence of blacklists[C]// NDSS Symposium 2017. 2017.

[14] BONNEAU J,SHUTOVAE. Linguistic properties of multi-word passphrases[C]// International Conference on Financial Cryptography and Data Security. Berlin,Heidelberg:Springer,2012:1-12.

[15] SHAY R,KELLEY P G,KOMANDURI S,et al. Correct horse battery staple:Exploring the usability of system-assigned passphrases[C]// Proceedings of the Eighth Symposium on Usable Privacy Snd security. 2012:1-20.

[16] KUO C,ROMANOSKY S,CRANOR L F. Human selection of mnemonic phrase-based passwords[C]// Proceedings of the Second Symposium on Usable Privacy and Security. 2006:67-78.

[17] YAN J,BLACKWELL A,ANDERSON R,et al. Password memorability and security:Empirical results[J]. IEEE Security & Privacy,2004,2(5):25-31.

[18] FORGETA. A world with many authentication schemes[D]. Ottawa:Carleton University,2013.

[19] GOLDBERG J,HAGMAN J,SAZAWALV. Doodling our way to better authentication[C]// Extended Abstracts on Human Factors in Computing Systems(CHI'02). 2002:868-869.

[20] THORPE J,MACRAE B,SALEHI-ABARI A. Usability and security evaluation of GeoPass:a geographic location-password scheme[C]// Proceedings of the Ninth Symposium on Usable Privacy and Security. 2013:1-14.

[21] HERLEY C,VAN OORSCHOT P C,PATRICK A S. Passwords:If we're so smart,why are we still using them? [C]// Financial Cryptography and Data Security: 13th International Conference,FC 2009,Accra Beach,Barbados,Revised Selected Papers 13. Springer Berlin Heidelberg,2009:230-237.

[22] WIEDENBECK S,WATERS J,BIRGETJ C,et al. Authentication using graphical passwords:Effects of tolerance and image choice[C]// Proceedings of the 2005 Symposium on Usable Privacy and Security. 2005:1-12.

[23] CARSTENS D S,MCCAULEY-BELL P R,MALONEL C,et al. Evaluation of the human impact of password authentication practices on information security [J]. Informing Science,2004,7:67-85.

[24] SUMMERS W C,BOSWORTH E. Password policy:the good,the bad,and the ugly[C]// Proceedings of the Winter International Synposium on Information and Communication Technologies. 2004:1-6.

[25] BARTON B F,BARTONM S. User-friendly password methods for computer-mediated information systems[J]. Computers & Security,1984,3(3):186-195.

[26] FLORENCIO D,HERLEY C. A large-scale study of web password habits[C]// Proceedings of the 16th International Conference on World Wide Web. 2007:657-666.

[27] DHAMIJA R,PERRIG A. Deja {Vu--A} User Study:Using Images for Authentication[C]// 9th USENIX Security Symposium(USENIX Security 00). 2000.

[28] GROVES J. Truffles—Myth or Strategic Plan?Sniffing out some bizarre and inspired ways of motivating people to remember their passwords[J]. Computer Fraud & Security,2002,2002(1):9-12.

[29] SCHWEITZER D,BOLENG J,HUGHES C,et al. Visualizing keyboard pattern passwords [J]. Information Visualization,2011,10(2):127-133.

[30] HOROWITZA S. Top 10 security mistakes[J]. Computer world,2001,35(28):38-38.

[31] ZHANG L,MCDOWELL W C. Am I really at risk? Determinants of online users' intentions to use strong passwords[J]. Journal of Internet Commerce,2009,8(3/4):180-197.

[32] KELLEY P G,KOMANDURI S,MAZUREK M L,et al. Guess again(and again and again):Measuring password strength by simulating password-cracking algorithms[C]// 2012 IEEE Symposium on Security and Privacy. IEEE,2012:523-537.

[33] SCARFONE K,SOUPPAYA M. Guide to enterprise password

management (draft) [J]. NIST Special Publication, 2009, 800(118): 800-118.
[34] NIELSEN G, VEDEL M, JENSEN C D. Improving usability of passphrase authentication[C]// 2014 Twelfth Annual International Conference on Privacy, Security and Trust. IEEE, 2014: 189-198.
[35] MARKERT P, BAILEY D V, GOLLA M, et al. This pin can be easily guessed: Analyzing the security of smartphone unlock pins [C]// 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020: 286-303.
[36] NARAYANAN A, SHMATIKOV V. Fast dictionary attacks on passwords using time-space tradeoff[C]// Proceedings of the 12th ACM Conference on Computer and Communications Security. 2005: 364-372.
[37] WALIA K S, SHENOY S, CHENG Y. An empirical analysis on the usability and security of passwords[C]// 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI). IEEE, 2020: 1-8.
[38] GRASSI P, GARCIA M, FENTONJ. Digital identity guidelines [R]. National Institute of Standards and Technology, 2020.
[39] KEITH M, SHAO B, STEINBARTP J. The usability of passphrases for authentication: An empirical field study[J]. International Journal of Human-computer Studies, 2007, 65(1): 17-28.
[40] VU K P L, PROCTOR R W, BHARGAV-SPANTZEL A, et al. Improving password security and memorability to protect personal and organizational information[J]. International Journal of Human-computer Studies, 2007, 65(8): 744-757.
[41] NELSON D L, VU K P L. Effects of a mnemonic technique on subsequent recall of assigned and self-generated passwords [C]// Human Interface and the Management of Information. Designing Information Environments: Symposium on Human Interface 2009, Held as Part of HCI International 2009, San Diego, CA, USA, Part I. Springer Berlin Heidelberg, 2009: 693-701.
[42] ZHANG J, LUO X, AKKALADEVI S, et al. Improving multiple-password recall: an empirical study[J]. European Journal of Information Systems, 2009, 18(2): 165-176.
[43] YAN J, BLACKWELL A, ANDERSON R, et al. The memorability and security of passwords-some empirical results[R]. University of Cambridge, Computer Laboratory, 2000.
[44] VU K P L, TAI B L, BHARGAVA, et al. Promoting memorability and security of passwords through sentence generation [C]// Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Sage CA: Los Angeles, CA: SAGE Publications, 2004, 48(13): 1478-1482.
[45] ZHANG Y, XIAN H Q, YU A M. Chinese sentence-based password mnemonic strategy[J]. Science Technology and Engineering, 2019, 19(35): 253-258.
[46] CHEN X, SHU H, WU N, et al. Stages in learning to pronounce Chinese characters[J]. Psychology in the Schools, 2003, 40(1): 115-124.
[47] KOMIYA K, NAKAJIMA T. Memorability of Japanese Mnemonic Passwords[C]// Cross-Cultural Design. Experience and Product Design Across Cultures: 13th International Conference (CCD 2021), Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, Part I 23. Springer International Publishing, 2021: 420-429.
[48] IGARASHI Y. The changing role of katakana in the Japanese writing system[D]. Canada: University of Victoria, 2007.
[49] KUBOZONOH. Mora and syllable[M]// The Handbook of Japanese Linguistics. 2017: 31-61.
[50] SOTIROVA-KOHLI M, ROSEN D H, SMITH S M, et al. Empirical study of Kanji as archetypal images: understanding the collective unconscious as part of the Japanese language[J]. Journal of Analytical Psychology, 2011, 56(1): 109-132.
[51] WYDELL T N, PATTERSON K E, HUMPHREYSG W. Phonologically mediated access to meaning for kanji: Is a rows still a rose in Japanese kanji? [J]. Journal of Experimental Psychology: Learning, Memory, and Cognition, 1993, 19(3): 491.
[52] FURNELLS. An assessment of website password practices[J]. Computers & Security, 2007, 26(7/8): 445-451.
[53] BONNEAU J. The science of guessing: analyzing an anonymized corpus of 70 million passwords[C]// 2012 IEEE Symposium on Security and Privacy. IEEE, 2012: 538-552.
[54] MILLER G A. The magical number seven, plus or minus two: Some limits on our capacity for processing information[J]. Psychological Review, 1956, 63(2): 81.
[55] JEYARAMAN S, TOPKARA U. Have the cake and eat it too-infusing usability into text-password based authentication systems[C]// 21st Annual Computer Security Applications Conference (ACSAC'05). IEEE, 2005: 10 pp. -482.
[56] DOR D. On newspaper headlines as relevance optimizers[J]. Journal of Pragmatics, 2003, 35(5): 695-721.
[57] MALONE D, MAHER K. Investigating the distribution of password choices[C]// Proceedings of the 21st International Conference on World Wide Web. 2012: 301-310.
[58] FORGET A, BIDDLE R. Memorability of persuasive passwords [M]// Extended Abstracts on Human Factors in Computing Systems (CHI'08). 2008: 3759-3764.
[59] FORGET A, CHIASSON S, VAN OORSCHOT P C, et al. Improving text passwords through persuasion[C]// Proceedings of the 4th Symposium on Usable Privacy and Security. 2008: 1-12.
[60] FOGG B J. Persuasive technology: using computers to change what we think and do[J]. Ubiquity, 2002, 2002(December): 2.
[61] YEE K P, SITAKER K. Passpet: convenient password management and phishing protection[C]// Proceedings of the Second Symposium on Usable Privacy and Security. 2006: 32-43.
[62] YILDIRIM M, MACKIE I. Encouraging users to improve password security and memorability[J]. International Journal of Information Security, 2019, 18: 741-759.
[63] CLAIR L S, JOHANSEN L, ENCK W, et al. Password exhaustion: Predicting the end of password usefulness[C]// Information Systems Security: Second International Conference (ICISS 2006). Kolkata, India, Springer Berlin Heidelberg, 2006: 37-55.
[64] UR B, BEES J, SEGRETI S M, et al. Do users' perceptions of password security match reality? [C]// Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. 2016: 3748-3760.
[65] DENNING T, BOWERS K, VAN DIJK M, et al. Exploring implicit memory for painless password recovery[C]// Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2011: 2615-2618.
[66] UMEJIAKU A P, DHAKAL P, SHENG V S. Balancing Pass-

word Security and User Convenience:Exploring the Potential of Prompt Models for Password Generation[J]. Electronics,2023,12(10):2159.

[67] SHUKLA V,MISHRA A,AGARWAL S. A new one time password generation method for financial transactions with randomness analysis[C]// Innovations in Electrical and Electronic Engineering(ICEEE 2020). Springer Singapore,2021:713-723.

[68] SHAY R,KOMANDURI S,DURITY A L,et al. Designing password policies for strength and usability[J]. ACM Transactions on Information and System Security (TISSEC), 2016,18(4):1-34.

[69] BHANA B,FLOWERDAY S V. Usability of the login authentication process: passphrases and passwords[J]. Information & Computer Security,2022,30(2):280-305.

[70] FORGET A,CHIASSON S,BIDDLE R. Choose your own authentication[C]// Proceedings of the 2015 New Security Paradigms Workshop. 2015:1-15.

[71] ONSORODI A H H,KORHAN O. Application of a genetic algorithm to the keyboard layout problem[J]. PloS One, 2020,15(1):e0226611.

[72] SCHWEITZER D,BOLENG J,HUGHES C,et al. Visualizing keyboard pattern passwords [J]. Information Visualization, 2011,10(2):127-133.

[73] SANDNES F E,AUBERT A. Bimanual text entry using game controllers:relying on users' spatial familiarity with QWERTY [J]. Interacting with Computers,2007,19(2):140-150.

[74] YE B,GUO Y,ZHANG L,et al. An empirical study of mnemonic password creation tips[J]. Computers & Security,2019,85:41-50.

[75] SHELTON A L,MCNAMARA T P. Systems of spatial reference in human memory[J]. Cognitive Psychology,2001,43(4):274-310.

[76] GUO Y,ZHANG Z,GUO Y. Optiwords:A new password policy for creating memorable and strong passwords[J]. Computers & Security,2019,85:423-435.

[77] HOCKLEY W E. The picture superiority effect in associative recognition[J]. Memory & Cognition,2008,36(7):1351-1359.

[78] UELLENBECK S,DÜRMUTH M,WOLF C,et al. Quantifying the security of graphical passwords:The case of android unlock patterns[C]// Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communication Security. 2013:161-172.

[79] SONG J,WANG D,YUN Z,et al. Alphapwd:A password generation strategy based on mnemonic shape[J]. IEEE Access, 2019,7:119052-119059.

[80] FERGUSON D,DUNCAN J. Keyboard design and operating posture[J]. Ergonomics,1974,17(6):731-744.

[81] LYU S,YAO Q,SONG J. AvoidPwd:A mnemonic password generation strategy based on keyboard transformation[J]. China Communications,2022,19(10):92-101.

[82] CHOU H C,LEE H C,HSUEHC W,et al. Password cracking based on special keyboard patterns[J]. International Journal of Innovative Computing, Information and Control, 2012, 8(1):387-402.

[83] KOMANDURIS,SHAY R,CRANOR L F,et al. Telepathwords:preventing weak passwords by reading user's minds [C]// Proceedings of the 23rd USENIX Conference on Security Symposium(SEC'14). 2014:591-606.

[84] WEISS R,DE LUCA A. PassShapes:utilizing stroke based authentication to increase password memorability[C]// Proceedings of the 5th Nordic Conference on Human-computer Interaction:Building Bridges. 2008:383-392.

[85] FRAUNE M R,JUANG K A,GREENSTEIN J S,et al. Employing user-created pictures to enhance the recall of system-generated mnemonic phrases and the security of passwords[C]// Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Sage CA:Los Angeles,CA:SAGE Publications, 2013,57(1):419-423.

[86] BISHOP M. Password management [C]//COMPCON Spring'91 Digest of Papers. IEEE,1991:167-169.

[87] HUH J H,OH S,KIM H,et al. Surpass:System-initiated user-replaceable passwords[C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015:170-181.

[88] MCLENNAN C T,MANNING P,TUFT S E. An evaluation of the Game Changer Password System:A new approach to password security[J]. International Journal of Human-Computer Studies,2017,100:1-17.

[89] BRUMENB. Security analysis of game changer password system [J]. International Journal of Human-Computer Studies, 2019, 126:44-52.

[90] ZIMMERMANN V,GERBER N. The password is dead,long live the password-A laboratory study on user perceptions of authentication schemes[J]. International Journal of Human-Computer Studies,2020,133:26-44.

[91] WANG P,WANG D,HUANG X Y. Advances in Password Security[J]. Journal of Computer Research and Development, 2016,53(10):2173-2188.

[92] WOODS N,SIPONEN M. How memory anxiety can influence password security behavior[J]. Computers & Security, 2024, 137:103589.

CHEN Jiamin, born in 1999, postgraduate. Her main research interests include information security and machine learning.

JIANG Huiping, born in 1975, Ph. D, professor, is a member of CCF (No. 13453S). Her main research interests include artificial intelligence and machine learning.