基于社会工程学的密码破解技术综述

沙晖杰[1]，唐　晶[2]，冯世伟[3]，姚金皓[1]，赵明利[1]
（1. 网络空间部队信息工程大学，河南　郑州　450000；2. 西藏某部，西藏　昌都　854000；
3. 中软信息系统工程有限公司，北京　102209）

摘　要：密码安全作为信息安全的第一道防线，当前面临着日益复杂的威胁，密码加盐可以增强密码存储安全性，抵御彩虹表、暴力破解等技术攻击，但无法防范社会工程学手段直接获取原始密码的行为。系统综述了基于社会工程学的密码破解技术。首先梳理了社会工程学攻击的理论基础，其核心在于绕过技术防护，通过利用人类心理弱点和挖掘个人信息来操纵目标，从而高效破解密码。其次，分析了针对性字典构建、技术性诱导攻击及人工智能增强的新型攻击这三类主流破解技术，梳理了各类技术的原理、模式与攻击流程，并通过近年来的典型案例进行了实证分析。最后，从技术防护、非技术防护两个层面探讨了针对社会工程学密码破解技术的防御手段，并展望了未来社会工程学密码攻击与防御的发展趋势。

关键词：社会工程学；密码破解；针对性字典构建；人工智能；网络安全
中图分类号：TP309；TN918.1　　**文献标志码：**A　　**DOI：**10.19358/j.issn.2097-1788.2026.07.001

中文引用格式：沙晖杰，唐晶，冯世伟，等. 基于社会工程学的密码破解技术综述[J]. 网络安全与数据治理，2026，45(7)：1-8.
英文引用格式：Sha Huijie，Tang Jing，Feng Shiwei，et al. Review of social engineering-based password cracking techniques[J]. Cyber Security and Data Governance，2026，45(7)：1-8.

Review of social engineering-based password cracking techniques

Sha Huijie[1]，Tang Jing[2]，Feng Shiwei[3]，Yao Jinhao[1]，Zhao Mingli[1]
（1. Information Engineering University，Zhengzhou 450000，China；
2. One Ministry of Xizang，Changdu 854000，China；
3. China Software Information System Engineering Co.，Ltd.，Beijing 102209，China）

Abstract：As the first line of defense in information security，password security is currently facing increasingly complex threats. Password salting could enhance password storage security and resist technical attacks，such as rainbow tables and brute force cracking. However，it cannot prevent social engineering methods from directly obtaining the original password. This paper provides a systematic review of password cracking techniques based on social engineering. It begins by outlining the theoretical foundations of social engineering attacks，whose core lies in bypassing technical protections by exploiting human psychological weaknesses and mining personal information to manipulate targets，thereby cracking passwords efficiently. Subsequently，it analyzes three mainstream cracking techniques：targeted dictionary building，technology-induced attacks，and AI-enhanced attacks. The principles，modes，and attack processes of each technique are elaborated，supported by empirical analysis of typical cases from recent years. Finally，the paper discusses defense strategies against social engineering password cracking from both technical and non-technical perspectives，and concludes with an outlook on future trends in social engineering password attacks and defenses.
Key words：social engineering；password cracking；targeted dictionary building；artificial intelligence；cybersecurity

0　引言

社会工程学攻击已成为密码破解领域最具威胁性的方法之一，其核心在于利用人性弱点而非单纯依靠技术漏洞获取用户敏感信息。传统密码强度评估方法往往只关注密码的技术特性（如长度、复杂度），而忽视了其与个人信息的关联度，因此随着网络安全技术的不断进步，传统密码破解方法如暴力破解或字典攻击的效率和成功率逐渐下降，而社会工程学攻击却

因其对人性的精准把握而在破解准确率和效率方面逐渐超越传统密码破解方法，即使用户设置符合“强密码”标准的密码也可能被社会工程学手段破解[1]。社会工程学已成为当代黑客获取密码的首选策略。

社会工程学攻击之所以在当代社会中成功率较高，主要归因于其对人性弱点的精准把握。心理学研究表明，人们倾向于信任权威、回报他人善意、遵循社会规范、喜欢与相似的人互动[2]。攻击者利用上述这些人类共性心理特性，通过精心设计的欺骗手段，绕过技术防护措施，直接或间接地获取密码或密码相关敏感信息，从而实现对密码的有效攻击。而人工智能的高速发展则给社会工程学破解技术带来了全新的挑战。

本文旨在系统性地梳理基于社会工程学的密码破解技术研究现状，分析其工作原理、技术分类和实战效果，并探讨有效的防御策略。通过全面综述这一领域的发展，为密码安全研究和实践提供参考。

1 社会工程学与密码安全的理论基础

社会工程学攻击之所以能够屡屡穿透层层技术防线，根本原因在于它精准地击中了信息安全链条中最薄弱且最不可预测的环节——人类本身。本节将从理论层面剖析社会工程学的概念，分析其对密码破解工程的作用机制。

1.1 社会工程学概念

传统的信息安全模型，如“CIA”三元组（保密性 Confidentiality、完整性 Integrity、可用性 Availability），其防护焦点集中于技术资产本身，譬如硬件、软件以及数据等。综合应用防火墙、入侵检测系统、加密算法等技术手段构成了信息安全防御的主要屏障[3]。然而，社会工程学攻击并不着眼于攻破这些技术屏障，而将攻击目标直接指向系统的用户、管理员或其他掌握访问权限的人员。其核心定位是一种非对称的、以人为中心的攻击方法。其本质是对人类间信任的利用与开发。攻击者并非破解复杂的加密算法，而是诱导目标自愿或无意识中泄露密码、重置凭证或执行其他危及安全的操作[4]。

从攻击目标来看，密码作为最普遍应用的身份验证凭证，自然成为应用社会工程学的首要攻击目标。攻击者追求的并非是密码这一串字符本身，而是其背后所代表的访问权限与信任关系。因此，社会工程学与密码安全的关系，并非单纯的攻防对抗，更是一种心理博弈。攻防的战场从服务器、网络协议以及漏洞后门，转移到了人的认知、情感和社交习惯之中。表 1 对比了传统技术攻击与社会工程学攻击的差异。

表 1 传统技术破解与社会工程学破解的模式对比

对比维度	传统技术破解	社会工程学破解[5]
攻击目标	软件漏洞、协议缺陷、加密强度	人类心理、认知偏差、组织流程
攻击路径	逻辑的、确定性的	心理的、高度可变的
防御重点	代码审计、补丁管理、网络隔离	安全意识、制度流程、行为监控
可预测性	相对较高，可通过扫描发现	极低，依赖于破解者创意和目标状态
攻击成本	往往需要较高的技术成本与工具	可高可低，最低一封邮件或一通电话

1.2 社会工程学在密码破解领域的技术基础

基于社会工程学的密码破解技术根据其破解手段进行分类，可以分为信息收集技术、心理诱导技术、心理操纵技术三类。

1.2.1 信息收集技术

信息收集技术是社会工程学密码破解的公共基础，任何基于社会工程学的攻击方式必须建立在获取被攻击目标的信息基础上，否则攻击者难以获得被攻击目标的信任，也就无从谈起获取其密码等敏感信息[6]。信息收集技术主要包括以下几种：

（1）公开数据挖掘：利用搜索引擎（如百度、bing 搜索）、社交媒体平台（如小红书、微博等）、公开数据库等渠道收集目标的个人信息。例如通过搜索“某公司 IT 部门”的关键词获取员工姓名、联系方式等，继而通过招聘软件等获取组织架构和人员关系[7]。

（2）非公开信息窃取：通过物理手段获取敏感信息，如翻找垃圾桶获取废弃文件、窃听对话、观察行为习惯等。研究表明，企事业单位的垃圾堆中往往包含大量敏感信息，如电话本、机构表格、备忘录等。

（3）技术工具辅助：使用专业工具（如 SEToolkit、Theharvester、Maltego）收集目标信息。SEToolkit 支持鱼叉式网络钓鱼攻击、网页攻击、海量邮件攻击等多种自动化攻击模式；Theharvester 可用于收集邮箱地址、域名、主机名等；Maltego 则可用于绘制目标的社交网络图[8]。

1.2.2 心理诱导技术

诱导手段是社会工程学攻击的攻击通道技术，攻击者依靠线上或线下等多种方法建立起与被攻击者的联系，同时也在互动中识别出高价值目标，从而实现筛选被攻击者的目的[9]。心理诱导技术主要包括：

（1）线上诱导：如钓鱼邮件、钓鱼网站、恶意链接等。根据反网络钓鱼工作组（APWG）的报告，2024 年上半年，全球共计观察到超过 184 万次网络钓鱼攻击，其中面向企业的网络钓鱼攻击单次涉及金额平均高达 8.7 万美元，同比增长超过 50%[10]。

（2）线下诱导：如电话诈骗、USB 掉落攻击、物理窃听等[11]。例如，攻击者故意在公共场所掉落一个特制 USB 设备，利用捡到者的好奇心插入电脑，从而传播恶意软件。

（3）混合诱导：结合线上和线下手段，形成多维度攻击。例如，先通过社交媒体获取目标信息，再通过电话或邮件进行针对性诱导。

1.2.3 心理操纵技术

心理操纵技术是社会工程学攻击的核心心理攻击手段，其目的是采用各类社会工程学方法获取目标信任，从而实现对目标进行指挥。心理操纵手段主要包括：

（1）信任利用[12]：攻击者伪装成权威角色（如同事、上级领导）骗取信任关系。典型场景为：攻击者冒充公司高管对财务发送伪装电子邮件，从而造成交易密码泄露。

（2）恐惧制造：通过制造虚假的紧急情况迫使被攻击者做出错误判断。近几年，电信诈骗中常采用该手段，攻击者谎称被攻击者银行账号及密码已泄露，以此套取私密信息。

（3）利益诱惑：利用人类的贪欲，提供虚假利益诱使被攻击者泄露信息。例如，攻击者通过电话或邮件方式，告知被攻击者中奖但需要验证个人信息领奖。

（4）好奇心激发：利用人类的好奇心，诱导其点击链接或下载附件。例如，攻击者通过发送高诱惑性标题的邮件，引起被攻击者的猎奇心理并触发点击，从而进行木马攻击。

（5）情感操控[13]：利用同情心、恐惧等情绪，控制目标的思想和行为。例如，攻击者通过 AI 生成的亲属语音信息，声称家中出现意外情况需要转账救助，骗取被攻击者敏感密码信息。

1.3 社会工程学在密码破解领域的应用基础

社会工程学之所以能有效应用于密码破解领域，主要基于以下几个应用基础。

对信任机制的利用是社会工程学破解密码的核心基础。在密码学中，信任是身份认证的基础，而社会工程学攻击正是通过破坏或操纵这种信任机制来获取密码。例如，当用户完全信任某个人或机构时，有可能会轻易提供密码，而无需考虑其真实身份。这种对信任机制的直接利用，使得破解者能够绕过绝大多数基于密码复杂度的技术防护措施，直击密码认证逻辑的源头。

对认知偏差的利用是社会工程学破解密码的心理学基础。根据罗伯特·西奥迪尼的劝说心理学[14]，人们会因为互惠、承诺一致性、社会认同、权威、喜欢和稀缺性被社会工程学突破。例如，人们倾向于服从权威人物，即使他们被要求做违反规定的行为。攻击者理解并利用了这些根深蒂固的认知偏差，从而创造了高效的心理操纵攻击点。

对信息不对称的利用是社会工程学破解密码的信息基础。成功的社会工程攻击建立在深度的信息侦察基础之上。攻击者利用开源情报、社交媒体、数据泄露库等渠道，构建关于目标的详细档案，包括个人喜好、社交关系、行为习惯以及潜在的密码线索（如生日、宠物名）。研究表明，用户在设置密码时普遍存在规律性，如使用个人信息、采用常见模式或在多个平台复用密码[15]。攻击者利用这些规律，结合自动化工具生成高命中率的针对性密码字典，将盲目的暴力破解转化为精准的智能猜测，极大地提高了密码破解效率。

技术与心理的结合是社会工程学破解密码的实践基础。现代社会工程学攻击极少依赖单一手段，而是已经形成融合了技术工具与心理操纵的复合攻击链。例如，攻击者可能先通过搜索引擎收集目标信息，再使用 SEToolkit 生成钓鱼邮件，最后利用中间人攻击获取密码[16]。这种结合使得攻击者能够针对不同场景和目标人群，采取最有效的攻击手段，提高密码破解的成功率。

2 基于社会工程学的密码破解技术分类

2.1 针对性字典构建技术

与传统暴力破解相比，基于社会工程学的密码破解更加精准高效，其核心手段之一是构建针对性密码字典。这类技术通过收集目标的个人信息，生成具有高命中率的个性化密码字典，大幅提升破解效率。

常见用户密码分析器（Common User Passwords Profiler，CUPP）工具是针对性字典构建的典型代表。该工具基于社会工程学与心理学原理，通过系统收集目标的个人信息，智能生成高命中率的密码字典。相比传统暴力破解工具，CUPP 能实现“精准推测”，在渗透测试中表现出色。CUPP 常见的破解流程如图 1 所示。

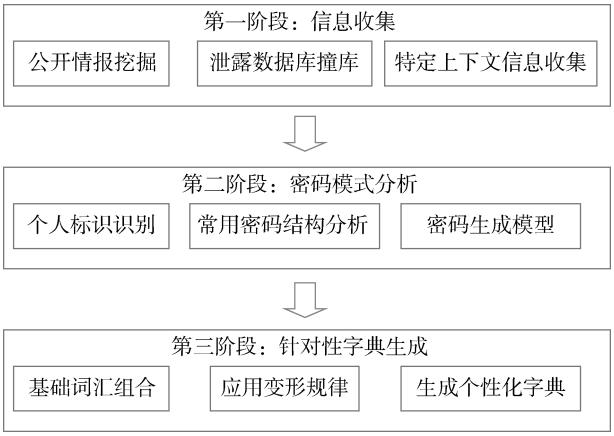

图 1　针对性字典构建方法破解流程

多源信息收集：这是构建针对性字典的基础。破解者综合利用公开来源情报（Open Source Intelligence，OSINT），从目标的社交媒体（如微博、小红书）、论坛、招聘网站等渠道，获取其姓名、昵称、生日、宠物名、兴趣爱好、职业信息等多维度信息。此外，从其他已泄露的数据库中关联获取目标曾使用的密码（即撞库攻击），能为分析其个人密码习惯提供关键样本。同时，近年来研究成果表明，同省份、同行业、同公司的密码设定具有一定规律性，这即是基于个人上下文的信息收集。

密码模式分析与规则提取：在获得原始信息后，下一步是分析并推断目标的密码设置习惯。研究表明，用户倾向于使用与自身密切相关的信息来构造易记密码，如“姓名缩写+生日”“宠物名+特殊符号”等[17]。进阶方法则进一步采用概率计算模型，如分析大量泄露密码集，利用马尔可夫模型或概率上下文无关文法（PCFG）来学习和概括用户群体的密码构造概率规则[18]。对于特定目标，还需结合其个人上下文（如近期关注的事件、喜爱的球队、就读学校名称）来生成相关密码规律。

针对性字典生成：基于提取的规则和个人信息，使用专用工具自动生成密码字典。在 CUPP 工具中，它通过与使用者交互，引导输入目标的各项个人信息，随后按照常见的密码组合逻辑（如拼接、大小写变换、添加数字后缀等）自动生成一份高度定制化的密码列表。相比包含数百万通用密码的庞大字典，这种针对性字典体积小，但尝试顺序更合理，命中率更高。

2.2　技术性密码诱导破解

在基于社会工程学的密码破解领域，技术性诱导破解指的是，通过结合或模仿信息技术流程、工具和通信渠道，来实施心理操纵以获取密码的破解方法。这类手段的核心在于，破解者并非直接利用软件漏洞、密码猜解，而是精心设计一个看似合法的交互场景，诱使目标主动执行危险操作或泄露敏感信息。这类方法由于其高效性、特异性已经成为社会工程学密码破解的主流方法，且已经形成了流程化的破解链。其典型破解流程如图 2 所示。

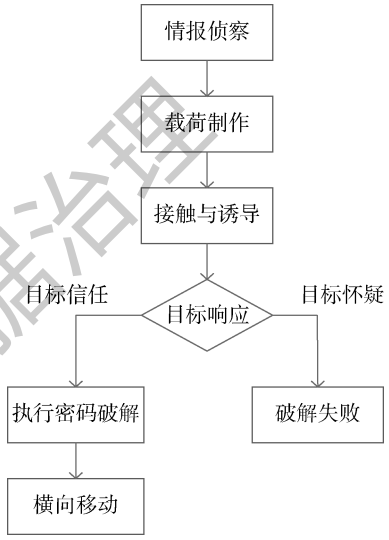

图 2　技术性诱导破解流程

阶段一：情报侦察

与字典构建类似，技术性密码破解始于对目标的全面信息收集，即 OSINT 侦察。破解者会系统性地搜索目标的社交媒体资料、公司网站、论坛发言等公开信息，以获取可用于定制攻击的个人信息、组织架构、技术术语和项目详情。例如，通过招聘软件获取员工的职位、上下级关系、公司体系，通过 GitHub、CSDN 等网站了解其技术栈，为后续冒充领导、同事、支持人员提供可靠的依据。

阶段二：载荷制作

在此阶段，破解者基于侦察信息，制作用于信息诱导的技术性载荷。这类载荷包括伪造钓鱼网站、恶意软件以及包含精心设计的剧本的双方通信内容。

阶段三：接触与诱导

破解者通过选定的渠道向目标传递恶意载荷，并运用心理学原理对目标进行诱导。常见的接触渠道包括：电子邮件与网络钓鱼、虚假电话、短信诈骗、搜索引擎诱导、恶意广告等[19]。

阶段四：破解执行与横向移动

一旦目标信任了破解者所伪造的场景并执行操作（如告知密码、下载运行恶意程序），密码破解便进入

执行阶段。密码或系统口令被破解者直接捕获，随后，破解者利用获取的初始立足点，在企业内网、目标关系网内进行横向移动，通过窃取更多密码、口令、敏感信息提升自己的权限，最终控制核心系统或传播性地破解关系网内其他目标密码口令[20]。

2.3 人工智能增强的社会工程学密码破解

随着人工智能，特别是大语言模型和生成式人工智能的快速发展，社会工程学密码破解正在经历一场深刻的模式变革。人工智能技术已从辅助工具演变为密码破解的核心驱动力，在自动化程度、精准度、规模以及欺骗性等维度实现了全面的跃升。人工智能对社会工程学密码破解的赋能体现在以下几个方面：

（1）智能化情报侦察

攻击前的信息收集阶段因人工智能而变得空前高效。传统社会工程学依赖人工筛选公开信息，而现代破解者可以利用人工智能驱动的工具，自动从社交媒体、论坛、泄露数据库等多源信息中，快速整合并关联目标的碎片化数据，构建高精度的个人数字画像。现有研究已经能够做到基于文本写作风格的跨平台用户身份对齐，通过分析目标在不同平台的写作习惯，将多个匿名账号关联至同一真实个体，从而挖掘出更深层、更隐蔽的行为模式和社交关系[21]。这为后续的个性化攻击提供了丰富的情报基础。

（2）高度拟真的攻击载荷

在掌握目标画像后，生成式人工智能技术可被用于制作极具迷惑性的攻击载荷内容。如通过大模型技术生成个性化的钓鱼邮件。现有研究已经证明，ChatGPT 这类大模型可生成复杂的欺诈剧本，并能绕过现有的检测机制。这标志着密码破解从利用通用模板的广撒网模式，进化成针对目标定制的精准狙击模式。而深度伪造（Deepfake）技术的引入，更是将社会工程学密码破解推上了一个新的高度。破解者可伪造高度逼真的目标上司、同事或亲友的音频、视频，甚至可以实现实时通话，通过视频通话或语音指令直接索要密码或触发敏感操作[22]。

（3）自主化密码破解

人工智能的赋能不止于欺诈内容生成，更体现在攻击流程的全自动执行上。自主型人工智能代理（AI Agent）能够模拟密码破解者，自动执行从信息搜集、钓鱼邮件生成与发送到与目标进行多轮对话交互的完整攻击链。已有研究通过智能体成功模拟了在多轮对话中实施社会工程学密码破解的场景[23]。这意味着未来一定会出现完全由人工智能驱动的 7×24 小时不间断的、能根据目标反应实时调整话术的自动化攻击模型，这极大提升了密码破解的规模与效率。

3 社会工程学密码破解的典型案例分析

根据攻击的复杂度和目标范围，社会工程学密码破解主要呈现两种模式：高互动式破解以及大规模破解。高互动式破解通常针对特定高价值目标，破解者进行长期、深度的身份伪装和欺诈，通过语音、视频或复杂剧本建立高度的信任，目的在于窃取核心密码。大规模破解攻击则追求广泛影响，如利用搜索引擎、恶意广告等手段，通过伪造大量用户熟悉的界面诱导广泛目标群体执行恶意操作。

3.1 伪造开源软件站点的大规模密码破解

2025 年 5 月 20 日，知名网络安全公司唯思科技（WithSecure）公布了一起黑客组织通过篡改 KeePass 密码管理器窃取用户全部密码的案例[24]。

该密码破解事件是一次典型的多链条社会工程学攻击，属于上文中描述的典型大规模破解行动。破解者首先通过 Bing 搜索引擎恶意广告进行流量引导，将目标群体导向虚假网站。如图 3 所示，在目标下载并运行伪装成合法 KeePass 软件的恶意安装包后，恶意软件会在后台部署 Cobalt Strike 等高级攻击工具，建立远程控制通道。随后破解者利用该通道导出目标系统中存储的所有密码，并利用这些窃取的密码在网络内横向移动，最终在关键计算机、服务器、终端上部署勒索软件。

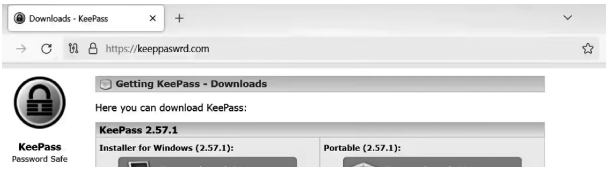

图 3 伪装的 KeePass 下载页面

该案例完美演绎了社会工程学中的信任转移理论。破解者利用了用户对知名开源软件 KeePass 和搜索引擎 Bing 的双重信任，将一个本应存储密码的保险箱变成了密码破解工具，从而绕过了所有安全防护措施，造成了大面积的密码泄露。

3.2 针对高价值目标的高互动式密码破解

2025 年 6 月，谷歌威胁情报小组和加拿大公民实验室的联合调查发现，一个名为 UNC6293 的黑客组织在 2024 年 4 月至 6 月间，利用谷歌邮箱的应用专用密码这一功能，成功绕过了邮箱的双因素认证机制，入

侵了多名知名学者的邮箱账户[25]。

破解者伪装成美国国务院的 ClaudieS. Weber，以邀请参加闭门政策讨论会为名，向目标发送欺诈邮件。虽然邮件来源于普通的谷歌个人邮箱，但是破解者在抄送行中添加了多个以“@ state. gov”为后缀的政府邮箱地址，增强了邮件的可信度。

当目标表现出兴趣但因时间冲突无法参与时，破解者进一步诱导其加入所谓的美国国务院宾客平台，声称这是一个能让外部人员参与会议的协作平台。随后，破解者发送了一份说明文件，详细说明了如何在谷歌账户中创建应用专用密码，并要求将生成的密码分享给自己，以便注册上文中的宾客平台身份。破解者从而得到了目标的谷歌账号的登录权限，完成了全部密码破解攻击。

该案例中破解者综合运用了权威伪装（冒充政府官员）、稀缺性与紧迫性（暗示机会重要）以及信任建立（长期专业沟通）。其高明之处在于并未直接索要密码，而是指导目标主动创建一个合法的、可绕过安全检测的强密码并交出，这使得传统网络安全观念中“不透露密码即是安全的”这一朴素防御认知完全失效。这是一起典型的高互动式密码破解案例。

4 防御策略

面对日益巧妙且种类繁多的社会工程学密码破解攻击，传统的单一防御手段已经无法有效保护用户的信息安全。因此，防御的核心理念必须从单纯的技术阻截转变为技术防御与心理防御深度融合的综合治理理念。

4.1 技术性防御措施

技术性防御的目标是通过强制性审查的技术手段，利用自动化工具进行实时检测与响应，在破解者的攻击链的各个阶段设置障碍，减少人为失误的可能性。面对日益精密的社会工程学密码攻击，采取多层次的技术防护措施能够有效降低大规模密码破解行动的成功率。

针对传统的钓鱼软件、钓鱼电话等社会工程学密码破解手段，应用多因素认证、零信任架构等手段可以有效降低高风险目标的被破解概率。多因素认证指用户登录系统或进行需要密码的操作时，不是仅仅依靠一串字符作为唯一的验证因素，而是需要提供两种或更多不同类型的验证因素，如密码、短信验证码、生物识别等。即使破解者获取到了用户的密码，也会被另外的验证因素所阻，导致无法达到窃取用户资产的最终目的。零信任架构则是采用“永不信任，始终验证”的原则，对所有访问请求进行持续验证和授权。如用户登录必须限定在特定的终端设备上，一旦用户登录环境发生了变化，即要求重新进行认证。这类方法虽然一定程度上降低了用户使用的体验感，但是能够有效避免用户遭受社会工程学攻击后密码遗失产生的后续损失。

上述两类方法主要解决了用户密码被破解后的登录权限控制问题，而近年来人工智能技术的引入，能够有效切断破解者在攻击载荷制作、目标交互触达这两个密码破解步骤中的成功率。引入人工智能检测模型能够有效识别钓鱼邮件、钓鱼电话内容，针对人工智能驱动的大规模密码破解行动具备非常好的防御效果。另一方面，针对目前 Deepfake 滥用产生的大量假冒视频、通话，防御者借由 FakeCatcher[26]等人工智能模型能够进行有效的识别，用人工智能防御去对抗人工智能欺诈，防御者才能够在效率上与破解者持平，而一般而言，防御者拥有的计算资源和网络资源是远远超过破解者的，这就能够大大降低破解者利用人工智能加持的社会工程学进行密码破解的可能性。

4.2 非技术防御措施

技术手段永远存在被绕过的可能，特别是面对高互动性的社会工程学密码破解攻击，破解者会根据用户的实际情况制定定制化的破解方案，致使技术手段已经无法进行有效的防御。而精心设计的流程和高度警觉的用户永远是密码安全的最后堡垒。非技术防御的核心目标就是构建一道强大的人类防火墙，将用户从最薄弱的环节转变为最坚定的防御者。这一目标的实现，依赖于持续的安全教育以及刚性的安全流程。

针对面向企业用户的社会工程学密码破解攻击，企业需要进行持续的、融入日常工作的安全培训活动。这包括定期安全意识培训、模拟攻击演练、心理意识与批判性思维培养等。定期安全意识培训旨在提高用户对社会工程学攻击的认识和防范能力，培训内容应包括识别钓鱼邮件、识别钓鱼电话、警惕可疑请求、不轻易透露密码等。模拟攻击演练旨在通过模拟钓鱼邮件测试、电话诈骗演练等，提升用户的识别能力。心理意识与批判性思维培养则是直接针对用户的心理弱点展开培训，系统讲解破解者如何利用权威、紧迫性、互惠、社会认同、喜好与稀缺性等社会工程学原理进行操控，培养用户的健康怀疑态度和验证本能，使他们在面对异常或高压请求时，能够本能地质疑和报告。

另一方面，刚性的安全流程则是面向破解者的最

后一道防线，如多人验证机制就是很好的一种防御手段。多人验证机制，即任何敏感操作，均需要大于等于2人相互验证后才能进行，包括对外界提供密码、提供敏感信息等。它确保即使单一个体被成功操纵，破解行为也会在流程层面被阻断。这不仅体现在企业用户中，如企业转账密码管控、企业核心服务器登录密码管控等，也体现在个人用户中，如敏感转账需要家庭成员进行同意认证等[27]。这额外的验证人员，往往是破解者尚未利用社会工程学进行攻击的人员，其心理防线的强度是显著高于目标个体的，这有利于对社会工程学破解的成功防御。

5 结论

本文系统论述了基于社会工程学的密码破解技术及其防御策略，揭示了其与传统技术攻击的区别与当前发展现状。社会工程学破解之所以高效且难以防御，根源在于其将攻击焦点从复杂的加密算法和系统漏洞，转移至信息安全链条中最薄弱且普遍存在的环节——人及其心理行为模式。通过对信任机制的利用、对认知偏差的操纵以及信息不对称的建立，破解者能够以较低成本实现高成功率的密码破解。

当前，社会工程学密码破解技术已呈现出精准化、自动化、智能化的显著趋势。从依赖个人信息构建针对性字典，到结合钓鱼、伪冒等多种手段形成复合攻击，再到如今大模型和生成式人工智能在情报侦察、内容生成、攻击流程自动化方面的全面赋能，破解攻击的逼真度、规模和效率均有了革命性的提升。面对上述挑战，任何单一的技术或管理措施都无法构成有效防御。未来的密码安全防护必然转向一种深度融合的协同防御模式。在技术层面，推行多因素认证、实施零信任架构并利用人工智能进行威胁检测，构筑自动化的主动防御体系；在非技术层面，则需通过持续、沉浸式的安全意识教育锻造用户心理防线，并通过建立强制验证等刚性流程来固化安全链条。唯有将技术手段与人员意识进行有机结合，才能构建起纵深安全防御体系。

展望未来，社会工程学密码破解攻击与防御的对抗必将持续升级。破解者将进一步利用人工智能模拟更复杂的人类互动与情感，防御者则将在行为识别、异常检测、可解释性人工智能安全等领域深化研究。在这场攻防对抗中，唯有人才是一切的根本。构建以人为本的防御体系，辅助以技术手段，加强用户心理防线的建设，是抵御社会工程学密码破解攻击的核心途径。

参考文献

[1] 张硕,吴瑕. 社会工程学视角下密码的设置与保管研究[J]. 智能计算机与应用,2020,10(10):59-64,70.
[2] 库尔特·P·弗雷, 艾登·P·格雷格. 人性实验:改变社会心理学的28项研究[M]. 2版. 白学军,译. 北京:中国人民大学出版社, 2021.
[3] 沈昌祥,张焕国,冯登国,等. 信息安全综述[J]. 中国科学(E辑:信息科学), 2007, 37(2):129-150.
[4] 戴玲,彭长根. 社会工程学攻击下的信息安全保密工作[J]. 保密工作, 2016(10):48-49.
[5] 宋艾米. 基于社会工程学的网络安全渗透检测模型研究[D]. 上海:东华大学, 2013.
[6] Mitnick K, Simon W. The art of deception: controlling the human element of security[M]. New York: John Wiley & Sons, Inc., 2003.
[7] Stringhini G, Hohlfeld O, Kruegel C, et al. The harvester, the botmaster, and the spammer: on the relations between the different actors in the spam landscape[C]//Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security. ACM, 2014:353-364.
[8] Kehkashan T, Abdelhaq M, Al-Shamayleh A S, et al. Explainable phishing website detection for secure and sustainable cyber infrastructure[J]. Scientific Reports,2025,15:41751.
[9] Muhanad A, Abuelezz I, Khan K, et al. On how cialdini's persuasion principles influence individuals in the context of social engineering: a qualitative study[C]//International Conference on Web Information Systems Engineering. Springer, 2024:373-388.
[10] Meurs T, Hoheisel R, Junger M, et al. What to do against ransomware? Evaluating law enforcement interventions[C]//2024 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2024:76-93.
[11] Fakih M, Dharmaji R, Mahmoud Y, et al. Invisible ears at your fingertips: acoustic eavesdropping via mouse sensors[C]//2025 IEEE Annual Computer Security Applications Conference. IEEE, 2025:583-597.
[12] Duben A J. Social engineering: how crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication[J]. Computing Reviews, 2022,63(7):182-183.
[13] Longtchi T, Xu S. Characterizing theevolution ofpsychological factors exploited bymalicious emails[C]//International Conference on Science of Cyber Security. Springer, 2025:158-178.
[14] Khadka K. Persuasion and phishing: analysing the interplay of persuasion tactics in cyber threats[J]. arXiv.org, 2024. DOI: 10.53735/cisse.v12i1.207.
[15] Hranicky R, Sirova L, Rucky V. Beyond the dictionary attack: enhancing password cracking efficiency through machine learning-induced mangling rules[J]. Forensic Science International: Digital Investigation, 2025, 52(Sup):301865.

[16] 张荣涛,岳珂玮,赵怡航,等. 基于社会工程学工具(setoolkit)的钓鱼网站攻击[J]. 电子工程学院学报, 2019, 8(11):285-286.
[17] 杨浩,朱志祥. 利用社会工程学进行密码猜解[J]. 西安文理学院学报(自然科学版), 2013, 16(4):100-103.
[18] 刘建. 基于专用字典的密码破解方法研究与应用[D]. 哈尔滨:哈尔滨工业大学, 2015.
[19] Beni R M. Social engineering attacks on the cyber-physical system: human cyber and physical impacts[C]//Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer, 2025:296-311.
[20] Nowakowski W. Social engineering analysis framework: a comprehensive playbook for human hacking[J]. IEEE Access, 2025, 13:18827-18849.
[21] 杨燕燕. 暗网多平台用户身份对齐方法研究[D]. 北京:中国人民公安大学, 2023.
[22] Ramaswamy M. AI-enhanced secure identity verification for financial services[J]. International Journal for Multidisciplinary Research, 2024, 6(6):1-12.
[23] Kumarage T, Johnson C, Adams J, et al. Personalized attacks of social engineering in multi-turn conversations: LLM agents for simulation and detection[J]. arXiv. 2503. 15552,2025.
[24] WithSecure Lab. Don′t drop password managers[EB/OL]. [2025-04-07]. https://labs. withsecure. com/content/dam/labs/docs/W_Intel_Research_KeePass_Trojanised_Malware_Campaign. pdf.
[25] Google Threat Intelligence Group. Creative phishing academics critics of Russia[EB/OL]. [2025-06-15]. https://cloud. google. com/blog/topics/threat-intelligence/creative-phishing-academics-critics-of-russia/.
[26] Ciftci U A, Demir I, Yin L. FakeCatcher: detection of synthetic portrait videos using biological signals[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2020, PP(99):1-1.
[27] 华为. 亲情防诈,守护家人用机安全[EB/OL]. [2025-10-20]. https://consumer. huawei. com/cn/support/content/zh-cn16071068/.

（收稿日期：2026-03-23）

作者简介：

沙晖杰（1995-），男，硕士，讲师，主要研究方向：信息安全、人才培养。

唐晶（1996-），女，硕士，助理翻译，主要研究方向：军事学。

冯世伟（1990-），男，硕士，高级工程师，主要研究方向：工程管理。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部