社工概念演化分析

王作广[1,2], 朱红松[1,2], 孙利民[1,2]

[1] 中国科学院大学 网络空间安全学院 北京 中国 100049
[2] 中国科学院信息工程研究所 物联网信息安全技术北京市重点实验室 北京 中国 100093

摘要 社工是黑客社区一种非常流行的攻击方法, 对网络空间安全造成了严重的危害。然而, 社工的概念定义作为理解社工威胁、开展社工研究的基础, 却并不一致、明晰, 而且随着概念的演化逐渐显现模糊、泛化、消解的趋势, 影响社工安全研究与防护工作的开展。本文对社工概念演化进行了体系化的研究, 同时也分析了社工攻击威胁的特性及态势, 梳理了社工实现方式/技术的发展和趋势, 总结了社工概念定义存在的问题及面临的挑战, 并对社工概念重新定义问题进行了讨论, 以期为社工安全研究提供参考、促进社工安全防护研究。

关键词 社会工程学; 社交工程; 社工; 概念; 演化; 定义; 安全; 威胁; 攻击; 防护
中图法分类号 TN915.08 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2021.03.02

The Concept Evolution Analysis of Social Engineering

WANG Zuoguang[1,2], ZHU Hongsong[1,2], SUN Limin[1,2]

[1] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[2] Beijing Key Laboratory of IoT Information Security Technology, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract Social engineering is a very popular attack in the hacker community, and has brought severe damage to cyber security. However, the concept of social engineering is not consistent and clear, despite its fundamental role in social engineering research. Furthermore, there is a tendency to be obscure, overgeneralize and decompose in the concept evolution of the social engineering. These phenomena impede the security research and defense on social engineering. This paper studies the concept evolution of social engineering, and analyzes the problems and challenges faced by the concept. It ends with a discussion on the concept redefinition, to promote the future research on social engineering.

Key words social engineering; concept; evolution; definition; security; threat; attack; defense

1 引言

1.1 领域界定与术语使用说明

迄今为止, Social Engineering 主要有两个不同领域的概念。

在社会科学领域, Social Engineering 通常被译作“社会工程”。社会工程是解决社会问题的工程技术, 是改造社会、建设社会和管理社会的科学体系, 如降低社会运行成本、规范社会活动、提高工作效率、控制社会发展风险, 并对社会的发展进行预测、规划、设计和评估等[1]。社会工程师(Social Engineer)就是处理社会问题的个人或群体。

社会工作者(Social Worker), 有时也简称“社工”, 是指在社会福利、社会救助、社会慈善、残障康复、优抚安置、医疗卫生、青少年服务、司法矫治等社会服务机构中从事社会服务工作的专业技术人员。

在网络空间安全领域, Social Engineering 在国内通常翻译最多的为“社会工程学”“社交工程”“社会工程”“社工”等名词。其中“社会工程学”作为传统字面翻译一直被国内沿用下来, 而“社交工程”的翻译则从字面直接体现了社交互动的一面。

为交流的方便性与意涵的全面性起见, 本文统一采用 Social Engineering 的中文翻译简写“社工”进行论述, 特殊之处仍用英文原词“Social Engineering”或其简写“SE”进行论述。“Social Engineer”译作“社工师”, 意指实施社工攻击的攻击者。正文中无特别指明处, “社工”均指网络空间安全范畴中的 Social Engineering 概念, 而非社会科学领域中社

通讯作者: 朱红松, 博士, 研究员, Email: zhuhongsong@iie.ac.cn。
本课题得到国家重点研发计划(No.2017YFB0802804); 自然基金青年项目(No.61702503)资助。
收稿日期: 2019-03-19; 录用日期: 2019-04-23; 定稿日期: 2020-12-21

会工作者的简称。

1.2 研究问题与论文结构

社工在全球信息安全史上已成为一种严重的现象[2], 构成了人、机、物全方位、多层次安全威胁态势, 但社工安全威胁却并没有引起工业界和学术界应有的关注和研究。在现实生活中, 社工作为黑客社区非常流行的攻击手段, 社工威胁的却被多数人忽视, 这持续增加了个人和组织遭受社工攻击的风险。

社工作为一种或一类网络空间安全攻击方法, 其大致的概念是“使用影响和说服, 通过让人们相信社工师所冒充的身份或通过操纵来欺骗人们, 利用人来获取信息”[3]。这里之所以称其为“大致的概念”, 是因为社工在黑客社区和学术研究领域, 至今并没有一个清晰精确、普遍接受的概念定义。而且根据本文的分析, 随着概念的演化, 各种各样的社工概念被描述, 其中一些概念是不一致、甚至矛盾的, 与此同时, 一些非社工攻击方法不断被涵盖形成对社工概念的侵蚀。社工概念逐渐呈现出模糊、泛化、消解的趋势。

这种现状和趋势严重影响了社工现象的理解、社工攻击事件的分析、社工安全研究与交流、社工防护工作的开展。

为此, 本文在第 2 章中对社工威胁的特性和现状进行了分析总结, 以期唤醒用户对社工威胁的安全意识, 引起工业界和学术界对社工安全领域的关注; 第 3 章通过文献调查研究, 追溯“Social Engineering”术语和概念的起源, 对社工概念的演化、特点和问题等进行了体系化的分析; 第 4 章总结了当前社工概念存在的问题和面临的挑战, 并对重新定义社工概念进行了讨论; 第 5 章对全文做了总结。

2 社工攻击威胁特性与现状

从社工威胁影响的视角来看, 社工威胁具有严重性、普遍性、持续性等特点。然而, 在用户和防护应用视角下, 社工风险经常被组织和用户忽略和低估, 而且缺少安全研究的关注和防护应用的投入。而在攻击者看来, 社工攻击是一种低投入、高回报、低风险、简单易用、难防御的, 具有绕过性、高效性、普适性等特点的攻击方法(章节 3.5), 是许多场景下优选的攻击手段。

2.1 社工是严重、普遍、持续的网络安全威胁

2.1.1 社工威胁的严重性与增长性

文献[4]在 2011 年对在美国、英国、加拿大、澳大利亚、新西兰和德国的 853 名 IT 专业人员进行的全球调查显示, 社工攻击造成的损失非常严重, 特别是对于大型组织中: 在过去的两年中有 48%的大公司和 32%的全部规模公司都经历超过 25 次的社工攻击, 将近 1/3 的大公司表示每个社工攻击事件的损失超过 10 万美元。文献[5-6]显示 2016~2018 年期间组织每年面临最多的安全威胁是社工攻击。文献[7]调查显示, 2018 年 85%的组织都经历过社工攻击, 比一年前增加了 16%, 2018 年每个组织平均由社工攻击造成的损失已经超过 140 万美元, 比上年增长了 8%。社工攻击已经形成了越来越严重的安全威胁。

另外, 安全技术的发展和和网络防护应用的改进成为黑客攻击的障碍, 攻击者利用技术上的漏洞变得越来越困难。社工作为一种绕过性的攻击方法, 通常并不与防御措施正面对抗, 而是利用人这个安全链中的薄弱环节达成目的。而且从技术上讲社工攻击的实施可能非常简单[8], 有时可能只需要打一个电话冒充一个内部人就能套取想要的信息, 随着社工工具的传播和社工攻击的进化, 更自动、更高级的社工已经成为可能。社工攻击的这种绕过性与简易性可能吸引更多的攻击者, 导致更多的社工攻击事件, 加重社工威胁的态势。

2.1.2 社工威胁的普遍性

社工威胁的普遍性源自网络安全中人因素(Human Factor)的不可避免性。任何计算机系统, 无论设计和安全设置多么好, 没有一个是不依赖于人的。这种普遍存在的人因素不仅是脆弱的, 而且它脆弱到损害大多数其他安全措施的程度[9]。这意味着这个安全弱点是普遍的, 是独立于平台、软件、网络、或设备年代的, 社工关注的就是网络安全链中人这个最薄弱的环节。

Kevin 在 RSA 会议上曾说, “你可以花一大笔钱从 RSA 会议的每个参展商、发言人和赞助商那里购买技术和服务, 但你的网络基础设施仍然很容易受到老式操纵的影响”[10]。经常有观点认为不插电的计算机是唯一安全的计算机, 事实上你可以说服一个人插电并开机, 这意味着即使关机的计算机也是脆弱的[11]。

尽管许多组织认识到拥有强大内部控制的重要性和价值, 但对一个组织信息安全来说, 最大的威胁是社工师对雇员的操纵[12]。报道[13]称, 前美国国家安全局(NSA)雇员斯诺登(Edward Snowden)向媒体泄露的一部分机密材料中, 可能是他通过说服美国国家安全局位于夏威夷的区域运营中心内的 20~25 名同事向其提供用户名和密码获得的, 借口是他的工作需要这些信息。

2.1.3 社工威胁的持续性

社工在历史上以很多形式已经存在了很久, 而且将继续存在[14]。文献[15]认为试图愚弄决策者的社工, 实际上只不过是中国几千年前为了类似目的而使用的计谋(Stratagem)的更新术语。要消除社工的破坏实际上是几乎是不可能的[16], 即使是安全意识培训, 也不太可能将这种脆弱性降低到零[17]。这是因为攻击主要利用的是人的脆弱性(Human Vulnerability)而不是计算机系统的缺陷, 我们可以保证计算机严格按照预定的流程运算, 但我们无法保证人不犯错。普遍存在的人的脆弱性伴随我们的一生的成长直至死亡, 只要人类种族延续, 这种脆弱性就不会消失[18]。人因素的不可控性是社工防护工作难以处理的, 而且社工攻击常以出乎意料的形态利用人的脆弱性。

而且, 随着技术的发展、环境的变化、应用的革新, 新的社工攻击方法会不断涌现, 各种各样新的社工攻击方法只受限于攻击者的想象力与创造力[19-20]。

2.2 社工是安全关注缺失的领域

尽管保护敏感信息的安全措施在增加, 但人仍然是安全链中最薄弱的环节[21-22]。对公司安全的最大威胁不是计算机病毒、一个关键程序的未修补漏洞、或者一个部署很糟糕的防火墙, 事实上, 最大的威胁可能是我们自己[23]。社工是一种被低估的安全风险, 很少在员工培训项目或公司安全策略中得到解决[24]。

社工威胁经常被用户忽略和低估, 文献[25]显示在人们知道要进行网络安全测试的情况下, 仍然有 3/4 的人出于好奇等原因, 将捡到的测试团队制作的恶意 USB 设备插入办公网计算机。此外, 普通职员普遍相信组织的系统和网络被设计、部署的非常安全, 而且有专门的安全人员负责, 所以不需要关注安全威胁。而且人性中普遍存在的乐观偏见(Optimism Bias)让人们相信, 自己并不会成为社工攻击的目标, 因为自己并不是重要人物, 或者认为自己具有超过平均水平的信息安全知识, 相对于大多数同事更有可能发现或抵御攻击。淡薄的安全意识与的不恰当安全认知导致更多的安全风险。

过去几十年, 安全防护的焦点一直集中在数字技术领域。20 世纪 70 年代我们被告知, 如果我们安装了访问控制包就有了安全性, 80 年代我们被鼓励安装有效的反病毒软件, 以确保我们的系统和网络安全。90 年代我们被告知防火墙将引导我们走向安全。安全技术在不断改进, 现在我们有了更多的选择, 入侵检测系统、入侵防御系统、软件脆弱性分析工具、生物因素认证、公钥基础设施、更强的加密算法等。然而, 在每一次迭代中, 人自身所引起的社工风险都没有被重视。企业将其年度信息技术预算的很大一部分用于高科技计算机安全(防火墙、保管库、锁和生物识别), 却被攻击者利用不知情或未受监控的用户绕过[26]。对于组织的整体安全防护, 如果轻视社工攻击, 对软件硬件安全措施(如软件补丁、硬件升级)的投入都将失去意义。

只要人们继续与计算机相关联, 人就会成为一个安全弱点, 无论技术怎样变化, 社工攻击将继续发生, 必须在所有的安全决策中考虑[27-28]。希望这些社工威胁特性和严重的社工威胁态势可以唤起人们对社工威胁的安全意识, 引起工业界和学术界对社工安全领域的关注研究。

3 社工概念演化分析

许多文献[29–31]认为术语“Social Engineering”是 Kevin Mitnick 在 2002 年 *The Art of Deception* 中提出的。本文经过概念溯源发现, “Social Engineering”作为一个 Phrack(Phreak 与 Hack 的合成词)术语早在 1984 年就开始在黑客 BBS 及刊物上使用, 而社工概念在 1974 年就产生于信息安全领域。

在社工概念溯源之外, 本文系统地分析了社工概念演化历程, 根据社工概念演化的特点将演化历程划分为 5 个阶段, 并详细阐释每个阶段的演化内容, 以期为社工研究领域提供一个体系化的概念演化参考。图 1 描绘了社工概念的起源及演化历程的整体视图, 图中箭头代表了社工的演进趋势, 箭身宽度代表了社工概念外延范围的大小, 箭身内部的图形描述了社工概念内涵及概念结构张力(即社工概念在不同方向上多个向外的力, 它可能导致概念的不稳定和消解, 详见章节 3.4)的大小(不规则程度), 图中文字标注了每个演化阶段的主要方面或特性。

社工概念演化分析概述如下:

(1) 第一阶段(1974~1983)

社工概念起源于 1974 年左右, 1974~1983 年期间主要在 phone phreak 社区流行。此时期社工主要作为一种针对电话公司交换中心操作员, 通过电话交谈, 采用假托、冒充、说服等方式, 有效获取信息或帮助的手段存在。

(2) 第二阶段(1984~1995)

1984 年社工开始在 *2600: The Hacker's Quarterly*、黑客 BBS 等媒体上传播, 并在 Phrack 社区流行。至 1995 年社工演化的 10 年间, 社工攻击针对的目标群体、实现方式、攻击目的等都在概念上都有

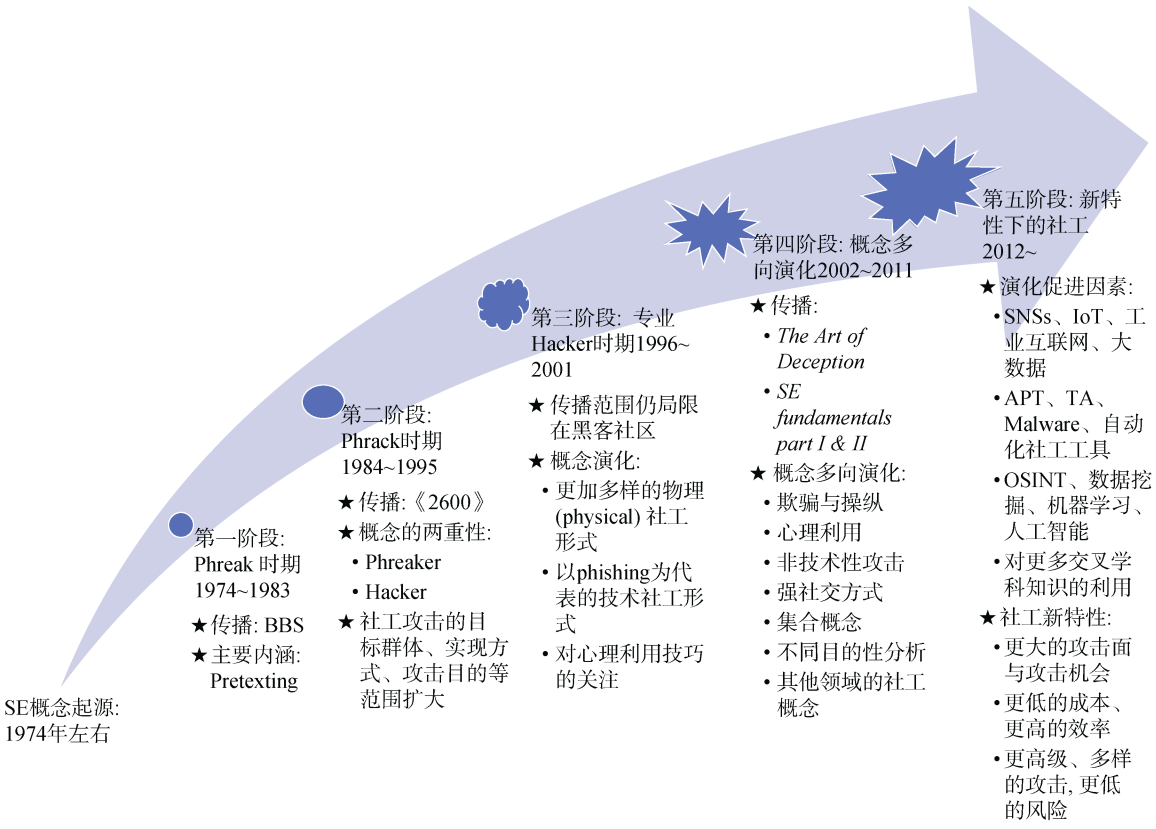

图 1　社工概念演化历程

Figure 1　The Concept Evolution of Social Engineering

了扩大, 社工也被用来描述黑客通过欺骗、操纵谈话、垃圾搜索、应聘保洁员等方法, 获取目标计算机系统的相关信息。社工表现出概念上的两重性, 既体现 Phreak 的一面, 又体现 Hack 的一面。

(3) 第三阶段(1996~2001)

这一时期社工在物理实现方式上更加多样。随着技术的演进, 网络钓鱼、木马等技术攻击方式开始进入社工的概念。另外, 社工心理学方面的特有属性开始被讨论, 如社会影响、说服理论、心理操纵等。

虽然此时期的社工攻击虽然造成了巨大的损失, 但社工仍然作为专业黑客社区的攻击方法而存在, 并没有进入大众的视野, 这可能与社工事件上报与响应、社工概念传播有关。

(4) 第四阶段(2002~2011)

2002 年前后, 以 *The Art of Deception*[32-33]、*Social Engineering Fundamentals, Part I & II*[8,34]为代表的社工研究相继发表, 社工概念的传播与社工威胁的增大, 逐渐引起人们对社工的关注与探索。

社工概念从此进入多方向演化阶段, 出现大量各种各样的社工概念描述, 通过对该时期社工概念的收集、汇总、聚类, 对人的欺骗与操纵、对人心理脆弱性的利用、非技术绕过性攻击、利用社交方式的攻击、社工集合概念等 5 类社工概念被识别, 这些多向演化的概念一直被沿用至今。另外, 本文分析了该时期社工概念在攻击目的方面的不同规定性, 并探索了社工在其他领域的概念应用情况。

此时期许多新的社工攻击方法不断扩大了社工概念的外延, 与此同时, 不少非社工攻击方法被涵盖, 侵蚀社工概念的内涵。另外, 这些不同类别的社工概念各自体现了一个概念演化方向, 这种多向演化的局面下众多的社工概念中许多是不一致的, 一些概念甚至是矛盾对立的。

这些演化特性催生社工内涵与外延的不对等, 导致社工概念边界模糊、术语使用泛化。不同方向的概念演化趋势产生的结构张力, 逐渐导致社工概念的分化和消解。

(5) 第五阶段(2012~)

2012 年左右起始, 社工演化除了对上一阶段多种类型概念的继承与延续外, 社工攻击在社交网络(Social Networking Sites, SNSs)、物联网(Internet of Things, IoT)、工业互联网、大数据等新环境, 高级持续性威胁(Advanced Persistent Threat, APT)、针对性攻击(Targeted Attack, TA)等新威胁形式, 自动化攻击工具, 数据挖掘、开源情报(Open Source Intelli-

gence, OSINT)处理、机器学习、人工智能(Artificial Intelligence, AI)等新技术, 以及对更多交叉学科知识的利用下等诸多因素的影响下, 社工攻击体现更多新的特性。综合演化过程, 社工已经演变为一种低投入、高回报、低风险、简单易用、难防御的, 具有绕过性、高效性、普适性等特点的攻击方法, 是许多场景下优选的攻击手段。构成了人、机、物多层次、全方位、严重的安全威胁。

这种多向演化背景下社工攻击呈现的新特性, 继续增加了社工概念演化的结构张力, 增加了对社工概念重定义的需求。

3.1 社工概念溯源与 Phreak 时期社工概念

3.1.1 “Social Engineering”名词溯源

根据本文对大量社工相关文献的研究, 发现“Social Engineering”最早出现于 1984 年开始刊行至今的 *2600: The Hacker's Quarterly* 第 1 卷 9 月份刊发的文章 *More on Trashing*[35]中, 该文献详细描述了利用垃圾搜索的方式收集信息的具体方法及建议, 并指出电话电信公司的垃圾箱中有许多有价值的信息材料, 如员工笔记本、系统说明、操作手册、员工名单、网络故障及维护报告、专业术语材料等, 这些信息可以用于**社工**(…notebooks with the Bell logo… printouts… directories list employees of Bell, goot to try **social engineering** on. Manuals… Maintenance reports… lists of abbreviations…)。

1984 年 10 月 *2600: The Hacker's Quarterly* 刊发的一个匿名文献 *Switching Centers and Operators*[36]对社工描述为“Also, they are more likely to be persuaded to give more information through the process of **'social engineering'**”, “In my experiences, these operators know more than the DA operators do and they are more susceptible to **'social engineering'**”。随后该杂志 1985 年的文献[37]描述社工为“One interesting thing to try is to pose as a phone company employee for **social engineering** purposes”。

可见, 此时期的 Social Engineering 概念主要为采用假托的方法, 来说服特定目标(如交换中心的部分操作员, 他们更易受社工的影响)提供更多信息的过程。而且, 文献[36]中对 Social Engineering 使用了双引号, 说明此时的 Social Engineering 有时作为引用名词或专有名词, 或有特指意涵。

3.1.2 Phreak 时期社工概念

概念的起源往往早于概念的传播, 根据文献调查分析, 社工概念的起源时间也早于 1984 年。

2600: The Hacker's Quarterly 于 1984 年开始发行之前, *YIPL/TAP* 作为流行于 Phreaker 社区最早期的地下出版物并没有直接对社工进行讨论。早期著名黑客组织 LOD(Legion of Doom)也成立于 1984 年, 文献[38]显示 LOD 的 BBS 是最早对 Social Engineering 及垃圾搜索(Trashing)讨论的黑客 BBS, 而这个 BBS 比其组织创立的时间(1984)还要早。文献[39]表明 plover-NET BBS 作为 LOD 原始成员的聚集地, 在 1983 年就吸引了 500 名使用者, Lex Luthor 作为 LOD 的创始人也是 plover-NET BBS 的联合系统管理员。自从 1978 年 BBS 被创建就开始有地下 BBS, 1980 年创建的 8BBS 就是其中著名的一个[40]。当时著名的社工师 Roscoe 和 Susan Thunder 就活跃在 8BBS 上[39]。可见, 社工概念的产生可能早于 BBS 的创立。

作为 Phone Phreaker 大师, John Draper (Captain Crunch)描述社工为“与电话公司的内部工作人员交谈, 让他们相信你是电话公司的工作人员”[41]。文献[42]显示根据 John Draper (Captain Crunch)的回忆, Social Engineering 这个术语是他在 70 年代中期引入 phreaker 社区的, 用来描述这种假冒(Impersonation)攻击, 他当时并未意识到社会学科领域有这个术语, 也不曾从先前其他的用法采用/改编而来。

文献[43]显示 Social Engineering 是在 80 年代中期开始在 Phreaker/Hacker 社区开始流行, 根据 Bill Acker 的回忆 Social Engineering 这个术语最早是在 1974 年左右开始使用, 此前的术语是 Pretexting(假托), 即“打电话给某人, 用假托的方法获取信息, 或说服他们为你做一些事情”, 而 Pretexting 这个术语是由 FBI 创造用来辅助调查工作的。

通过对这些文献的分析与比较基本可以确定 Social Engineering 概念是在 1974 年左右产生于信息安全领域。而且, 此时期术语 Social Engineering 基本就是 Pretexting 的代名词。

综上所述, 社工从概念萌生开始在 1974~1983 年 phone phreak 盛行的 10 年间, 可以被描述为一种针对电话公司交换中心操作员, 通过电话交谈, 采用假托、冒充、说服等方式有效获取信息或帮助的手段。

3.2 Phrack 时期社工概念的两重性

自 1984 年社工开始在黑客 BBS、刊物上出现后, 一方面, 社工作为初始意义上电话飞客(Phreaker)领域的概念内涵逐渐扩大, 除冒充、假托、说服外, 也体现了欺骗的特性。文献[44]认为社工是“利用对话在虚假的伪装下交换信息, 例如冒充电信员工以获取对不同电话网络系统更多的知识和了解”, 文献[45]认为社工是通过冒充电话员工或供应商, 对电话行

业的服务人员欺骗性的利用。也有文献简单地认为社工就是胡说(Bullshitting)[46]、欺骗和谎言[47], 以获取信息。

另一方面, 社工作为 Phrack 社区获取计算机相关信息、绕过安全障碍的方法, 社工的优点逐渐被更多地认识。正如文献[44,48]所言, 初始意义上的黑客行为被认为是日夜持续的密码暴力破解, 但社工作为另辟蹊径的方法让刚开始了解它的人们感到震惊。而对于黑客来说, 相对于攻击计算机系统, 攻击人和规程更容易、更少风险[49]。文献[50]认为社工是企图对与计算机系统相关的帮助台及其他支持服务人员的利用。文献[48]认为社工是与系统用户交谈, 假装也是系统的合法用户, 并在交谈过程中操纵讨论以便用户能够透露密码、有助于突破安全障碍或其他有用信息的行为。文献[51]显示社工作为黑客社区的术语, 用以描述通过社交的方式获取关于受害者计算机系统信息的过程; 它给黑客提供了一个有效的捷径, 可以在许多其他方法不可行的情况下促进攻击。

社工攻击的目标群体范围有所扩大, 不仅限于电话公司交换中心操作员。对于社工的实现方式, 文献[35,52]都体现了垃圾搜索(Dumpster Diving)可以发现有价值的信息, 文献[49]指出公司对垃圾的处理是对社工的第一道防护线。文献[50]对逆向社工(Reverse Social Engineering)进行了描述。逆向社工是一种通过制造网络故障等方法, 让目标主动与攻击者交互进而泄露信息的社工方式[53]。

可见, 1984~1995 年期间社工作为 Phrack 领域的概念, 既有“针对电话公司员工实施的假托、冒充、说服、欺骗, 获取对电话网络系统更多的知识和了解”, 体现 Phreak 的一面, 又有“通过直接或间接社交的方式, 采用欺骗、操纵谈话、逆向社工、垃圾搜索、应聘保洁员等方法, 获取入侵目标计算机系统相关信息”, 体现 Hack 的一面。社工攻击针对的目标群体、实现方式、攻击目的等都在概念上都有了扩大。

3.3 专业 Hacker 时期社工概念

1996~2001 的 6 年间, 是信息安全领域开始迅速发展的时期[10], 也是社工概念演化的重要阶段, 主要体现在三个方面: (1)社工在物理实现方式上更加多样; (2)随着技术的演进, 网络钓鱼、木马等技术攻击方式开始进入社工的概念; (3)社工心理学方面的特有属性(如社会影响与说服、对信任的操纵)开始被讨论, 人作为计算机安全链最薄弱的环节的重要性逐渐被认识到。

3.3.1 物理(Physical)社工攻击方面

文献[8]认为社工攻击可以发生在两个层面上: 物理层面和心理层面(Physical and Psychological Levels)。对于物理层面的攻击, 入侵者可以冒充维修工人或顾问等有访问权限的人走进工作场所, 搜寻垃圾桶、搜寻办公室内记在显眼处的密码, 或者站在附近窥探员工输入的密码。文献[54]认为“(对攻击者来说)最重要的可能是社工能力, 如通过冒充让目标泄露密码、垃圾搜索(Stealing Garbage)、肩窥(Shoulder Surfing)等”。

文献[55]认为物理渗透(Physical Penetration)是一种高级的社工, 因为通常的社工不是面对面的交互, 并介绍了在上班或午饭的时间混入人群进入办公楼, 穿戴带类似于目标建筑物的徽章通过门卫, 应聘临时清洁工深入目标内部, 安装 KeyGhost 硬件键盘记录器以窃取信息等物理渗透方式和攻击场景。

文献[34]总结了冒充、说服、非授权物理访问、肩窥、垃圾搜索、溜空门、安装/移除信息窃取装置等社工攻击方式。文献[19]对社工攻击的类型进行了论述, 如垃圾搜索, 肩窥, 使用伪造的名片, 收买安保人员、酒店员工、保洁人员, 冒充(冒充技术支持人员打电话给用户, 冒充电话公司的员工, 冒充学生采访商务技术人员)等。

3.3.2 技术社工攻击方面

第一个网络钓鱼(Phishing)攻击在 1996 年被设计用来窃取 AOL(America Online)的用户密码, 攻击者发送看似来自 AOL 支持服务的虚假的电子邮件和即时消息, 许多毫无疑心的受害者泄露了他们的信息[21]。这也引起了社工网络欺诈的风险, 文献[56]认为社工最初被用来获取密码或对长途电话的访问, 后来社工被用来获取信用卡号和其他金融数据, 向金融欺诈发展。文献[19]将伪造电子邮件作为一种社工攻击类型。文献[18]将伪装、垃圾搜索(Dumpster Diving)、直接的心理操纵等作为社工及其威胁的一类, 并基于一些安全从业人员对“由心理操纵造成的威胁范围扩大”的认识, 将垃圾邮件(Spam)、部分病毒的传播、特洛伊木马等也包含在社工的语境下。

至此, 以网络钓鱼、木马等网络技术为代表的攻击方式开始进入社工的概念。文献[19]对早期的社工概念简单的总结认为社工很难定义和描述, 有效的社工是灵活和开放的, 也许社工最好的定义是“通过技术或非技术的方式获取信息的行为”。

3.3.3 社工的社会心理学方面

文献[18]显示此时期社工也经常被描述为通过心理利用(Psychological Subversion)来窃取密码。文献[56]将社工定义为一个黑客欺骗他人泄露在某种程度上使黑客受益的、有价值的数据的过程, 认为社工的成功源于心理技巧的应用, 应加强对社会心理学的研究, 并讨论了社会心理学内容(说服路径、一致性错觉、说服与影响技巧等)在社工网络欺诈中的应用场景。文献[8]认为, 社工的本质是对人类信任这种自然倾向的操纵。

文献[11]从心理学的角度, 认为社工是使人遵从攻击者期望的艺术和技术, 它虽然不是思想控制, 让人完成超出自身正常行为外的任务, 但也不是极其简单的技术, 社工关注的就是计算机安全链中这一最薄弱的环节。

这一时期值得注意的一个现象是, 此时的社工攻击虽然造成了严重的损失[56], 但仍然作为专业黑客社区的攻击方法而存在, 并没有进入大众的视野。这既有被攻击组织碍于声誉受损影响经营, 不承认社工攻击的发生[8]的原因, 也有大众安全意识薄弱、社工概念并没有在大众媒体上广泛传播的原因。

3.4 社工概念的多向演化

2002 年前后, *The Art of Deception*[32-33]、*Social Engineering Fundamentals, Part I & II*[8,34]等社工研究相继发表, 详细的社工举例及对早期社工的论述, 让人们对所谓“世界头号黑客”的“核心技术”——社工——开始有了直观而具体的了解, 社工概念的传播与社工威胁的增大逐渐引起人们对社工的关注。另外, 社会心理学、社会信任、语言心理学、表情与情绪等交叉学科在社工应用方面的作用开始被更多地探索, 如文献[57-58]讨论了微表情训练工具[59](2002 年被开发)在社工欺骗和操纵中的应用与识别。

相对于之前的阶段, 这一时期对社工的研究与讨论显著增多。从此, 社工概念进入多方向演化阶段, 出现大量各种各样的社工概念描述, 其中一部分被沿用至今。一方面, 其他学科知识在社工领域的应用、网络信息技术的发展和社工攻击方法的演进, 许多新的社工攻击形式被创造, 社工概念的外延不断扩大。与此同时, 不少非常明显的非社工攻击方法被描述为社工, 甚至出现了将社工定义为一个涵盖性术语的社工集合概念(章节 3.4.5)。另一方面, 这些不同类别的社工概念各自体现了一个概念演化方向, 这种多向演化的局面下众多的社工概念中, 许多概念是不一致的, 一些概念甚至是对立的。如文献[60]认为社工是通过说服或欺骗来获取信息系统访问权限的技术, 文献[27]则认为“在社工的性质上, 它总是心理上的, 有时是技术性的”。社工的技术性与非技术性相对立的观点也非常多, 如章节 3.4.3 的分析。肩窥、垃圾搜索等在大量文献中都作为一种社工攻击方法出现, 但文献[61]明确将其排除在社工概念在外。文献[24]认为“任何社工都涉及到利用某人的信任”, 而文献[62]对其评述认为社工攻击“并不总是需要与目标建立信任关系”。不同程度唯目的论及对目的规定不恰当的概念, 也存在相互矛盾之处, 如章节 3.4.6 的分析。

这产生了两个问题: (1)这些演化特性催生社工内涵与外延的不对等, 导致社工概念边界模糊、术语使用泛化; (2)不同方向的概念演化趋势产生的结构张力, 逐渐导致社工概念的分化和消解。

本文对这一时期的社工概念进行收集汇总, 并根据概念的特性进行聚类, 以下是聚合的不同类别及其内容分析。

3.4.1 社工是对人的欺骗与操纵

Kevin Mitnick[63]将社工定义为“社工是使用操纵、影响和欺骗来让一个人、一个组织内可信的人, 来顺从一个请求, 从而披露信息或者执行一些对攻击者有利的行动。这可能是一件简单的事情, 如通过电话交谈, 也可以复杂, 如让一个目标访问一个网站, 利用网站的一个技术缺陷让黑客接管电脑”, 并在 *The Art of Deception*[3,33]将社工描述为“Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.”。文献[27]将信息技术社工(Information Technology Social Engineering)定义为“一种利用欺骗和操纵等社交手段来获取对信息技术访问的攻击”。Wikipedia 和牛津词典对社工的定义也属此类: 在信息安全的语境中, “社工指的是为了让他人执行行为或泄露机密信息的心理操纵[64]”, 是“使用欺骗手段来操纵他人泄露机密或私人信息, 这些信息可能被用于欺诈[65]”。后续的研究[66–68]等都继承了这类定义。

一些研究强调社工对人的欺骗, 如文献[69]认为“通常社工是欺骗人们提供(机密的、私人的或有特权的)信息或访问给黑客的过程”。社工是欺骗人们帮助攻击者达到他们的目的[70-71], 用于社工的技术和用于实施传统欺诈的技术之间并没有太大的区别[56], 他们之前被称作骗子, 现在被称为社工师[14]。文献[72]

认为社工“是一个欺骗人们放弃访问控制或机密信息的过程, 是网络安全的一个巨大威胁”。

一些文献强调社工是对人的操纵, 如文献[57]认为社工是“操纵目标人采取不一定符合他自身最佳利益的行为”。文献[73]认为社工是“一名社工师试图利用影响和说服, 来操纵受害者泄露机密信息或按照社工师的恶意目的执行”。文献[74-75]认为社工是一种“攻击者诱导受害者泄露信息或执行一项使攻击者能够破坏受害者系统的行动”的攻击方法。同类的观点还有, 社工是“利用人类行为来破坏安全的‘艺术’, 而不让参与者(或受害者)意识到自己被操纵了”[76], 是“对单个人或一群人, 技巧或非技巧性的心理操纵, 来产生一个需要的目标行为”[18]。后续研究[77–80]也持此类观点, 文献[79-80]认为“在本质上, 社工是指欺骗技术的设计和应用”。

一些文献认为社工是对信任的欺骗与操纵, 如文献[8,34,80]认为社工是“对人类信任这种自然倾向的操纵和利用”, 文献[24]认为“任何社工都涉及利用某人的信任”。

3.4.2 社工是一种对人心理的利用

文献[81]认为“社工攻击通常使用各种各样的心理技巧来让计算机用户给他们提供访问计算机或网络所需的信息”。文献[27]认为“在社工的性质方面, 我认为它总是心理上的, 有时是技术性的。例如冒充帮助台打电话给他人的假托通常被认为是非技术的、心理的; 通过电子邮件的假托是技术的、心理的, 社工的心理方面、而非技术方面促成了攻击”。文献[82-83]认为社工是攻击者对受害者的本能反应、好奇心、信任、贪婪等心理弱点实施诸如欺骗、伤害, 以期取得自身利益的手段。

此外, 一些文献关注社工对社会心理学中说服、影响的利用。如社工是让目标顺从攻击者期望的技术[11], 是一种说服的艺术[72]。文献[62]从“请求-说服-顺从”的角度将社工定义为“利用社交互动(Social Interaction)作为一种手段来说服个人或组织遵从来自攻击者的特定请求的科学, 其中社交互动、说服或请求涉及一个与计算机相关的实体”。文献[84]认为社工是“试图影响一个或多个人泄露信息或执行一个行为, 这些信息或行为可能导致一个信息系统的非授权的访问、网络非授权使用或数据的非授权泄露”。文献[85-86]认为“欺骗、说服或影响人们提供信息或执行有利于攻击者的行动被称为社工”。

3.4.3 社工是一种非技术性攻击

文献[87–89]认为“社工仍然是绕过安全性的流行方法, 因为攻击关注的是安全架构中最薄弱的环节, 即组织内的工作人员, 而不是直接针对技术控制, 如防火墙或认证系统”。文献[90-91]认为“社工作为一种策略, 被用来绕过计算机安全解决方案, 避免用暴力工具攻击系统的风险”。文献[92]认为“社工是主要通过非技术手段非法获取计算机系统信息”。文献[2,28]直接描述“社工是一种非技术类型的攻击”。

与此类概念相对立的观点认为社工可以是技术的, 甚至社工师需要掌握许多专业技术知识。如文献[61,93]显示越来越多的攻击者将新出现的技术与传统的社工方法融合在一起, 网络钓鱼、跨站请求伪造(Cross Site Request Forgery, CSRF)都是社工的一种形式。文献[3]认为“社工成功通常很大程度上也需要很多计算机系统和电话系统的知识和技术”。

3.4.4 强调社工社交特性的概念

文献[51,94]认为, 社工是通过社交手段获取关于目标人网络和系统信息的过程。文献[61]认为“尽管肩窥(Shoulder Surfing)、垃圾搜索(Dumpster Diving)帮助攻击者在准备阶段收集情报, 但它们不涉及与受害者任何形式的社会交互, 因此我们不把它们归类为社工攻击方法, 作为我们分类法的一部分”。文献[95]认为社工是通过使用社交方法来渗透信息系统。文献[16]认为社工可以被定义为通过与人的互动来欺骗他们破坏正常的安全规程。文献[96]认为在社工攻击中攻击者使用人类交互, 即社交技能来获取关于组织或其计算机系统的信息。文献[2]认为社工用来描述“强烈依赖人类交互的非技术类型入侵”。

3.4.5 社工是一个集合概念

与上述社工概念类型不同, 一些文献认为社工是一个集合概念, 即认为社工作为一个涵盖性的术语, 来指代一系列对他人欺骗、操纵以获取信息或实施入侵的方法。文献[97]认为, 社工是一组被攻击者用来操纵受害者做一些他们原本不会做的事情的伎俩。文献[98]认为, 社工是用来操纵人们执行行为或者泄露机密信息的一个技术集合。文献[99]显示, “在信息安全领域, 这一术语被广泛用于描述犯罪分子使用的一系列技术…”。文献[91,100]认为社工是一个涵盖了诸如网络钓鱼、假托、钓鱼(Baiting)、尾随(Tailgating)等许多恶意行为的术语。文献[101]认为“社工被用作涵盖性术语, 用于描述使用各种各样的攻击向量和策略来对用户进行心理操纵的、广泛的计算机攻击”。

社工集合概念一方面体现了社工攻击方法的多样性, “有许多类型的社工的攻击, 社工攻击的种类和范围仅受想象力的限制”[19-20]。另一方面, “最令

人困惑的是, 社工吸引了如此多的定义, 涵盖了诸如密码窃取, 从垃圾中搜寻有用信息, 恶意误导等一系列行为”[18]。

此类定义并不从社工概念的内涵属性角度出发, 而是从社工攻击方法这个外延视角出发来定义社工, 虽然避免了概念界定的麻烦, 但问题在于, 不少非常明显的非社工攻击方法被涵盖, 如信号劫持、网络监控、拒绝服务[20,102], 移动设备偷窃[102], 网页搜索[84], 网络嗅探[24], 搜索引擎毒化[61], 广告软件、流氓软件[101] 等, 在概念的模糊性中寻求语义的庇护[42]。随着社工概念的不断演化, 概念的边界会更加模糊, 最终导致术语多意、使用泛化、概念被侵蚀分解。

3.4.6 社工概念的不同目的性分析

多数社工概念强调社工的目的是信息收集, 如文献[14,19,26,81,103-104]等认为社工是“通过技术或非技术的方式获取信息的行为”, 这些信息通常是计算机网络或系统相关的信息, 甚至“即使不是十分有用的信息, 这些信息也可以用来了解目标环境, 指导社工的实施方法”[103]。

一些社工概念强调受害人对社工师的帮助行为, 如文献[105]认为“社工的目的是说服受害者提供帮助”, 文献[3]认为“社工师依靠的是他操纵人们提供帮助以达到目的的能力”。文献[70-71,77]等也认为社工是“使目标帮助攻击者实施攻击”。

此外, 有文献认为获取物理访问也是社工的目的。文献[97,106]认为社工的目的“通常是让受害者泄露敏感信息(如密码)、或者让攻击者非法访问建筑物、或进入受限制区域”, “有时, 社工指的是进入办公室, 四处寻找有关计算机系统的信息, 比如在显示器上贴着的密码”[107]。

另有一些文献则将社工的目的范围定义的非常宽泛, 文献[8,24,96]认为“社工的基本目标与一般的黑客行为是一样的: 为了进行欺诈、网络入侵、工业间谍活动、身份盗窃, 或者仅仅是破坏系统或网络, 获得对系统或信息的未经授权的访问”。

然而, 如果社工概念的目的被规定的不恰当, 将直接导致概念的缺陷, 如概念泛化。正如文献[27]所言, “对于‘社工的唯一目的是说服’这个定义, 一个人对他所做的入室盗窃撒谎, 来说服他的邻居建立一个安全围栏, 这将被归类为社工”, “在解释目的时考虑的非常广泛, 在这个定义下, 骗子借用他人的手表永远不归还, 构成了社工(攻击)”。从说服和操纵等角度出发, 且对社工目的范围规定过窄或过宽的定义均存在此类问题。如根据文献[62]的定义(见章节 3.4.2), “小男孩通过电脑与父母通信, 以吃午餐为由说服父母同意 5 美元的请求”这个例子符合作者的定义, 但这显然不是我们通常意义上要表达的“社工”。

3.4.7 社工在其他领域的概念

这一时期出现了与社工概念内涵非常相近的概念, 如认知攻击、语义攻击、反身控制(Reflexive Control)。

对于认知攻击, 2002 年文献[108]将其定义为“认知攻击是依赖于改变人类用户的感知和相应的行为来获得成功, 对计算机或信息系统的攻击”。“这种用户行为的改变, 受到了操纵用户对现实感知的影响”[109], “这种对感知的操纵或认知攻击, 超出了传统计算机安全领域的范畴(关注技术和网络基础设施)”[108], “当用户的行为受到错误信息的影响时, 就会发生认知攻击”[110]。

对于语义攻击, 文献[111]显示“Libicki 在信息战的背景下描述了语义攻击, 指软件媒介/代理(Software Agents)被敌方故意提供的错误的信息误导”。语义攻击“直接针对的是人机接口(Human-Computer Interface), 这是互联网上最不安全的接口”[112]。

由于认知攻击、语义攻击比较相近, 文献[111]将两者合并在一起讨论。文献[101]将语义攻击与社工结合, 定义语义社工攻击为“在社工的语境下, 语义攻击是操纵用户-计算机接口(User-Computer Interface)欺骗用户, 并最终破坏计算机系统安全”。

有研究认为这两种攻击都属于社工攻击, 文献[113]认为“认知攻击是社工的一种形式, 尽管它可能针对的是广泛的受众, 而不是特定的个体”。文献[101,42]认为语义攻击是一种特定类型的社工攻击, 它通过操作平台或系统应用等欺骗而不是直接攻击用户。

俄罗斯军方已经探索了将网络欺骗应用到一种被称为“反身控制(Reflexive Control)”的概念中[15], 它在激发敌方采取发起方所需的行为方面特别有效[114]。文献[115]将反身控制定义为“一种向合作伙伴或敌方传递特别准备的信息, 使他们自愿做出由行动发起人所期望的、预先确定的决策”。在战争中指挥官的首要目标之一就是干涉敌方指挥官的决策过程, 这个目标通常是通过使用虚假信息、伪装或其他策略与计谋来实现的, 对俄罗斯来说, 最主要的方法之一是使用反身控制理论, 这个理论很久以前就在俄罗斯发展起来并在信息战领域应用, 且仍在进行进一步的改进[115]。

反身控制概念与社工概念非常相似, 不同的是, 反身控制通过精心定制或虚假的信息, 目的是欺骗、

操纵、干涉敌方在军事及信息战中的决策[115]。

3.5 新特性下的社工

2012 年左右起始, 新环境、新威胁、新技术等方面促进了社工进一步的演进。SNSs、IoT、工业互联网、可穿戴设备、移动设备的广泛应用和安全区域隔离的弱化, 在增加数据可访问性、提高服务质量和生产效率的同时, 形成了更大的社工攻击面和攻击机会, 也让攻击者可以轻易地同时接触和影响庞大的受害者群体。共享性、开放性的大数据环境为构建更可信的社工攻击提供了条件。社工工具的传播与开源让大规模社工攻击更简易。社工攻击对高级威胁形式(TA、APT)的吸收, 对新技术(OSINT 处理、机器学习、人工智能)的利用, 让高效率、针对性、智能化的高级社工攻击成为可能, 构成了人、机、物多层次、全方位、严重的安全威胁。

这种多向演化背景下社工攻击呈现的新特性, 放大了社工概念多向演化的结构张力, 加速了社工概念多向演化和消解的趋势。虽然有研究根据这些社工体现的部分新特性, 在不同的演化阶段(2008 年文献[116], 2016 年文献[117])冠以“社工 2.0”的名义, 但却没有给出新特性下社工的概念定义, 这继续增加了对社工概念重定义的需求。

3.5.1 更大的攻击面与攻击机会

1997 年 SixDegree.com 的出现被认为是 SNSs 的首次出现, 但此时的 SNSs 仍然是概念化的阶段, 并没有被广泛应用。自 2002 年开始, Friendster、LinkedIn、Facebook、Twitter、Google+等各种社交媒体相继创立发展, 越来越多的人被吸引到这些网站创建个人资料(Profile), 以一种新的方式与他人建立关系。2012 年社交媒体中 Pinterest 用户量超过 10 亿[118]。Facebook 的用户每月分享超过 300 亿条内容[85]。社交媒体用户量爆发式增长产生的海量数据, 标志着大数据时代的到来。而且个人却比以往任何时候都更加暴露[80]。许多用户在这些网站上发布关于他们的活动、人际关系、地点和兴趣的个人信息。这些数据包括电子邮件地址、电话号码、生日、工作地址、当前所在城市、学校名字等其他个人资料[119]。社交网络已经成为一个大的敏感数据池[120]。

物联网(Internet of Things, IoT)概念在 2011 年左右开始普及, 于 2014 年进入大众市场[121]; IPv6 的启动与应用, 给万物互联提供了地址空间的技术支持。2012 年美国通用电气公司提出工业互联网, 2013 年德国提出工业 4.0[122], 工业逐渐向开放化、全球化、互联化、定制化、数字化、智能化发展。移动设备、可穿戴设备被广泛应用, 传感器将无处不在, 可以植入几乎所有能想象到的互联设备, 许多人决定测量他们自己的一切状态, 包括睡眠数据、生理数据、位置、情绪、环境等。大量的互联的设备成为社工攻击的新资源、新目标、新传播渠道。在此之前一封来自电冰箱的欺骗性邮件或即时信息可能看起来很荒谬, 然而如今这个想法似乎并不可笑, 大量的智能电视、家庭路由器等物联网设备, 包括一台电冰箱被用来发送恶意电子邮件[123]。而 Stuxnet 事件已经说明了社工作为攻击的关键环节, 对国家关键基础设施安全构成了重大威胁。

现代社会中个人生活和职业生活之间没有分离, 社交网络被更广泛地应用到职业工作环境, 组织关系、家庭关系信息公开在社交网络上。组织内部的计算机处理私人事情(如求职), 家庭电脑处理公司工作的现象非常普遍, 而且不少行业的员工缺乏基本的安全知识, 家庭电脑连接在弱口令或初始口令的路由器下。甚至部分企业鼓励自带设备(Bring Your Own Device, BYOD)、远程家庭办公的工作模式。组织的信息安全边界变得模糊, 传统企业信任区的概念已经不存在, 或者失去了最初的意义。

社交网络、工业互联网、物联网的广泛应用在将全球用户、各种各样的设备互联互通、提高服务质量和生产效率的同时, 伴随着各种各种各样的脆弱性, 为攻击者实施社工攻击提供了更多的渠道和更大的攻击面, 构成对人、机、物全面的威胁。此外, 这些新环境中大量关于人和设备的敏感信息为社工攻击提供了易得的信息资源, 网络技术发展和人们对高效工作的追求, 弱化了不同安全级别区域的隔离, 给攻击者制造了更多的攻击机会。

3.5.2 更低的攻击成本与更高攻击高效率

用户低下的安全意识和易得的开源情报, 增加了社工攻击的简易性与有效性, 降低了社工攻击成本。文献[25]显示, 在人们知道要进行网络安全测试的情况下, 测试团队在人员经常出入的地方丢放 20 个恶意的 USB 存储器, 15 个被发现且全部被插入办公网计算机。文献[124]显示在社交网站中建立新关系时, 信任并不像面对面的接触一样必要, 一个虚假的 Facebook 用户发出 200 个好友请求, 87 个回复中 82 个用户泄露对身份盗窃有用的个人信息, 如电子邮件和家庭住址、出生日期、就业情况等。大数据环境与数据挖掘技术的发展, 让开源情报(Open Source Intelligence, OSINT)的利用更有效。任何在公开网站(Facebook、Twitter、Foursquare 等)上发布的信息都可能给犯罪分子提供一个线索, 告诉他们如何将你所在的位置和你的真实身份联系起来[99], 构

造更让人信服的社工攻击。2012 年, 文献[125]展示了如何使用开源情报对组织员工构造一次鱼叉式钓鱼攻击。软件工具 Maltego 被用来从目标公司网站、社交网站收集开源情报, 简单的网络钓鱼工具被用来根据员工兴趣创建钓鱼邮件。文献[126]显示聚合多个社交媒体网络(LinkedIn 和 Facebook)上发现的信息, 会导致社工攻击更加成功。文献[127]展示了利用 Google+、LinkedIn、Twitter、Facebook 4 个社交网站上公开信息自动识别组织员工的身份的可能性。

越来越多的社工攻击工具被开发, 这些工具如 SET、Maltego、Phishing Frenzy、Gophish 支持多种类型信息的自动化收集和多种社工攻击向量(Attack Vector)的创建, 为低成本、大规模自动化实施社工攻击提供了条件, 即使在成功率很低的垃圾邮件钓鱼场景下, 社工攻击仍然是经济可行的, 因为少数的受害者就可以有相对较高的回报, 毕竟在低成本条件下, 即使是大规模的攻击总投入也相对较小。SET(Social-Engineer Toolkit)作为社工渗透测试的代表性工具, 可以提供构建鱼叉式钓鱼攻击、网站攻击、基于 Arduino 的物理介质攻击、无线热点攻击形式等社工攻击向量, 使用者只需按照提示的步骤设置一些参数即可, 整个社工攻击测试流程中多数步骤都可以自动化完成。而且许多社工攻击工具是开源的, 如 SET(2012 年在 Github 上开源[128])、Phishing Frenzy、Gophish, 这也意味着普通黑客或脚本小子可以轻易构造一次半自动化的社工攻击。

另外, 社工攻击的效率和成功率不断被提高。受害人大量细节信息可以通过手动整理或通过自动化开源情报收集工具收集。大数据的背景下数据挖掘技术的应用促进了开源情报的利用。低价易得的目标(Low Value and Low Hanging Fruit)和大规模的 Spam Phishing 逐渐被放弃, 特殊和有经济价值的目标被仔细选择, 更可信的社工攻击被精心构造, 如鱼叉式钓鱼(Spear Phishing, Context Aware Phishing)。文献[70]的研究发现, SNSs 中的上下文元素(Contextual Elements)为攻击者提供了心理利用条件, 员工很容易在 SNSs 中被欺骗。攻击者发送 10 封钓鱼邮件, 有 90%的几率其中至少一个人成为受害者[129]。文献[130]的研究表明, 一个攻击者利用社交网络数据来增加网络钓鱼攻击的收益是非常容易、非常有效的, 如果被一个看似熟人的人所请求, 那么网络用户成为受害者的可能性是普通情况的 4 倍。

互联网、社交网络、移动通信的广泛应用, 让攻击者可以轻易地同时接触和影响庞大的受害者群体。社交网络的共享性、开放性、低信任需求等特点让社工攻击更简易, 社工工具的传播与开源为大规模实施社工攻击提供了条件。开源情报为社工攻击提供了易得的信息资源, 丰富的背景信息导致了更可信的社工攻击, 提高了攻击的成功率。社工攻击这种低成本、高效率特性可能诱发更多的社工攻击, 加重网络安全威胁态势。

3.5.3 更高级的攻击形式与更低的风险

APT(Advanced Persistent Threats)通常是国家之间为了军事、政治等利益, 投入巨大人力物力, 经过长期规划和精心设计编程的高级攻击威胁。2010~2012 年相继发生的 Stuxnet、Duqu、Flame 等 APT 攻击事件就是例证。社工在 APT 攻击的开始阶段, 作为建立攻击入口点的手段, 或在中间阶段用于解决传统攻击方法遇到的障碍。文献[131]描述了一个常见的 APT 攻击阶段模型, 其中社工作为模型的核心部分。Stuxnet、Flame APT 攻击中均使用社工(Baiting)方法作为突破物理隔离、传播恶意代码的手段, 不同的是 Stuxnet 用于破坏设备, Flame 用于监视目标[132]。

相对于 APT 攻击, 针对性攻击(Targeted Attack, TA)通常是由世界各地的黑客群体或黑客个体发起, 为了经济利益窃取财务信息, 实施金融诈骗或报复行为, 攻击对象主要是组织、企业、个人等。针对性社工攻击越来越流行, 一些恶意软件被精心设计来实施针对特定用户或组织的钓鱼攻击[117]。文献[133]显示, 社工恶意软件(Social Engineering Malware)将心理和技术策略结合, 诱惑用户执行恶意软件、对抗现存的防护措施, 越来越多的恶意软件用社工作为传播的手段, 并且这些社工恶意软件威胁体现出了广泛性与持续性的特点。

文献[134]的研究表明, 即使是那些认为自己了解社工技术的人, 一个精心策划和执行的社工攻击也可能成功。互联网及社交媒体上大量在线免费可得的数据, 为社工师调查特定的目标、发起针对性社工攻击提供了方便。文献[135]显示, 通过仔细的设计和在特定时间发布消息, 可以让几乎任何一个人点击一个链接, 因为任何一个人都会对某件事感到好奇, 或者对某个话题感兴趣, 或者发现自己处于一个符合信息内容和上下文的生活环境中。文献[136]讨论了攻击者在实践中如何滥用在线社交网络提供的推荐功能或朋友发现(Friend-Finding)功能, 激励受害者主动联系攻击者, 在社交网络上发起被动社工攻击。由于是受害者主动发起的好友请求, 这种攻击形式更少引起受害者的怀疑, 而且可以绕过一些针对主动请求(Unsolicited Request)的恶意行为检测。

文献[137-139,119-120,127]等分别在自动社工机器人(Automated Social Engineering Bot, ASE bot)方面进行了研究。自动社工机器人能够自动地收集目标的开源情报, 进行社交媒体关联分析, 通过结合适当的聊天逻辑和增强的智能与受害者对话, 进行自动化的社工攻击。文献[15]显示自动聊天机器人被用来说服聊天对象分享自己的身份或访问带有恶意内容的网站。越像人类的(Human-Like)ASE 攻击检测它就越困难[120]。文献[138]提出了一种利用聊天机器人对真实人类网络聊天进行中间人攻击的社工威胁, 这种利用真实人类对话的社工攻击非常难识别和检测, 实验显示被自动聊天机器人替换的链接点击率高达 76.1%。

在人工智能(Artificial Intelligence, AI)技术应用方面, 文献[140]显示了利用 AI 技术创建有针对性的鱼叉式网络钓鱼攻击的可能性。文献[141]描述了一个利用递归神经网络的 AI 社工攻击, 它学会了在 Twitter 上发布针对特定用户的个性化钓鱼帖子。文献[142]描述了如何使用长短期记忆网络创建一种更好的钓鱼攻击的算法生成 Phishing URL, 来绕过基于递归神经网络的 Phishing URL 分类检测。文献[143]利用生成对抗网络构建一个基于深度学习的域名生成算法, 旨在有意绕过基于深度学习的检测器, 在一系列的对抗性迭代后, 生成器学习生成越来越难以检测的域名。

社工攻击对高级威胁形式(针对性攻击、APT)的吸收, 对新技术(OSINT 处理、机器学习、人工智能)的利用, 让社工攻击变得更高级、更有侵略性。另外, 社工攻击被认为是一种低风险的攻击方式。相对于入侵计算机系统, 利用人和规程的脆弱性更容易、更少风险[49]。现在高级的社工攻击, 关注小范围特定的目标, 不会惊动大范围的受害者, 更隐蔽地实施攻击, 减小了被检测到的风险。

3.5.4 新特性下社工概念的演化

文献[117,144]认为, 社工作为一种欺骗方法已经使用了很长时间, 技术、社交网络、网络犯罪的发展以及在线用户的天真行为这 4 个因素促成了社工的发展演变为一种多层面、复杂的新现象, 并称之为社工 2.0(Social Engineering 2.0, SE 2.0)。文献[144]认为社工 2.0 是一个复杂的领域, 涉及多种多样的技术和能力, 它与老式社工之间最大的区别在于更大的范围内自动社工攻击的可能性。事实上, 早在 2008 年文献[116]就使用了“社工 2.0”字样来体现社工的一些新特点。然而, 这些研究都没有给出社工 2.0 具体的概念及定义。

4 讨论

从概念演化的历程及问题分析可以发现, 当前的社工概念就处于这种延的续多向演化局面没有打破, 新特性下社工概念又没有形成的状态。社工概念边界模糊、术语使用泛化的现状和多向演化结构张力下概念分化消解的趋势, 对社工现象的理解、社工攻击事件的分析、社工安全研究与交流、社工防护工作的开展产生了严重的影响。

在此背景下, 如何清晰恰当地界定社工概念的内涵定义, 统一对社工的基本认识, 成为社工研究领域最急需、最重要的问题。

针对上述问题, 本文在对社工概念演化综合分析的基础上, 初步将社工概念重新定义如下: “社工是指通过(直接或间接、实时或非实时、主动或被动等)社交方式, 利用人(社会心理、认知、意识、思维、行为习惯、神经反射等方面)的脆弱性(Human Vulnerability), 利用或不利用技术手段、技术脆弱性, 针对网络空间安全实施危害的行为。”简而言之, 社工是通过社交方式, 利用人的脆弱性, 针对网络空间安全实施危害的行为。

为了进一步讨论该定义, 本文分别从目的论、性质轮、关系论等方面: (1)解释新概念定义过程中对社工目的属性的考虑; (2)说明新概念的共有属性、特有属性、本质属性, 分析新概念与演化过程中不同类别概念的关系; (3)分析社工攻击向量与其他攻击向量的关系。

4.1 社工定义的目的论分析

章节 3.4.6 论述了对社工概念目的属性不恰当规定导致社工定义过窄或过宽的问题及举例, 此处不再赘述。本文对社工攻击的目的限定为“针对网络空间安全实施危害的行为”, 这考虑了社工概念演化的历史性与演进性: (1)网络空间安全领的社工概念始终在网络空间安全领域内演化, 其主体意涵与社会科学领域中的社会工程(Social Engineering)、社工(Social Worker)存在明显区别。这种限定可以明确将网络空间安全领域的社工与社会科学领域中“社工”区分开。(2)这种限定既可以将概念演化过程中信息收集、网络入侵等常见目的涵盖, 同时又赋予社工概念目的属性更大的演化空间。

这样就避免了不同学科领域社工概念和术语的歧义与混淆, 也缓解了网络空间领域社工概念的泛化、社工术语的滥用, 如将章节 3.4.6 中提及的不涉及危害网络空间安全的财物盗窃、骗局等排除在社工概念之外。

4.2 社工定义的性质论分析

作为网络空间攻击方法的一种, 社工的共有属性, 如目的论分析所述, 是造成网络安全的违反, 如造成信息泄露、网络入侵、物理损坏等危害, 或机密性、完整性、可用性、可控性、可审查性等的违反。

社工相对于传统攻击方式(如密码穷举破解、软件漏洞利用等)的特有属性: (1)在主体攻击者角度体现为欺骗、操纵、说服、影响、诱导等方法的应用, 包含了多向演化中章节 3.4.1 所述概念的内涵(对人的欺骗、操纵)。这些属性体现了社工应用方法, 而且随着技术的发展、环境的变化、社工攻击场景的不同, 可能有更多种不同的应用方法, 但不是社工概念的本质属性反映。(2)在客体受害者角度体现为对人轻信、好奇、贪婪、懒惰、心理捷径、主观期望、固定行为模式等脆弱性的利用, 包含了多向演化中章节 3.4.2 所述概念的内涵(对心理脆弱性的利用)。对人脆弱性(Human Vulnerability)的利用反映了社工本质属性的一个方面。(3)在实现形式角度体现为直接或间接、单向或双向、主动或被动、强或弱的社交形式, 包含了多向演化中章节 3.4.4 所述概念的内涵(强社交特性)。社交特性反映了社工本质属性的另一个方面。(4)在技术属性方面, 本文对社工攻击中技术手段、技术脆弱性的利用不做规定, 技术的发展会重构社工的实现方法及形式, 章节 3.4.3 中认为社工是完全是非技术型攻击的观点没有从概念的本质出发, 是阶段性的认识。

基于以上对社工特有属性的说明与概念对比分析, 在网络空间安全的语境下: (1)社工区别于其他攻击方法的本质属性为“通过社交的方式, 利用人的脆弱性”, 这也是社工区别于其他网络攻击方法的判断标准。(2)因此, 社工的简洁定义为“通过社交方式, 利用人的脆弱性, 针对网络空间安全实施危害的行为”。这个定义包含了演化历程中社工概念内涵的主体(章节 3.4.1~3.4.4, 3.5.4), 体现了名词意涵, 限定了社工概念演化的领域范围(章节 3.4.6), 避免了集合概念导致的术语多意、使用泛化、概念被侵蚀分解的问题(章节 3.4.5, 3.4.6), 形成了相对稳定的概念内涵和清晰的概念边界, 并适当地扩大了概念演化的空间, 缓解了概念多向演化与新特性不断呈现的导致的结构张力。

4.3 社工定义的关系论分析

从攻击实施过程的视角, 社工作为一种攻击向量(攻击方法、攻击路径), 与其他攻击向量的关系体现为辅助、增强、连接、替代等, 即: 社工可用于辅助增强其他攻击向量、使其更简易、高效等; 社工可用于攻击的开始阶段以建立攻击切入点, 可用于攻击的中间阶段以衔接其他攻击向量组成完整的攻击链, 可用于攻击的最后阶段以完成攻击任务等; 社工也可作为替代其他攻击向量的优选方案或备选方案, 用以独立完成整个攻击过程。

最后, 上述社工概念定义并不成熟, 在这里初步提出, 是希望作为讨论内容, 以求指教; 同时也是对社工概念定义的一个观点, 以供参考。我们将在未来的工作中进一步研究并完善该定义。

5 结论

本文关注网络空间安全领域中的社工, 分析总结了社工攻击威胁特性与现状, 概述了安全意识、对社工安全防护的关注和投入的重要性。本文对社工概念起源与演化进行了体系化的研究, 将社工概念演化分为五个阶段, 并梳理了每个阶段社工概念的特点和社工实现方式/技术的发展; 同时, 分析了社工概念存在的问题, 找到了导致社工概念模糊、泛化、消解趋势的关键原因(即社工概念多向演化与社工新特性不断呈现导致的结构张力), 总结了社工概念面临的挑战。最后, 对重新定义社工概念进行了讨论, 以期为社工安全研究提供参考、促进社工安全防护研究。

参考文献

[1] Guo W. On Social Engineering[D]. Shenyang Normal University, 2012.
(郭维. 论社会工程师[D]. 沈阳师范大学, 2012.)

[2] Indrajit R E. Social Engineering Framework: Understanding the Deception Approach to Human Element of Security[J]. *International Journal of Computer Science Issues*, 2017, 14(2): 8-16.

[3] Mitnick K D, Simon W L. The Art of Deception: Controlling the Human Element of Security[M]. John Wiley & Sons, 2011.

[4] Dimensional Research. The Risk of Social Engineering on Information Security: A Survey of It Professionals. Technical report. Dimensional Research, 2011.

[5] Cybersecurity Snapshot: Cyberthreats, Regulations, Workforce Issues in 2016. https://www.isaca.org/pages/2016-cybersecurity-snapshot.aspx. Jan. 2016.

[6] Cyberthreats Increasing but Shifting, with Ransomware Attacks Down 17 Percent. ISACA. https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2018/cyberthreats-increasing-but-shifting-with-ransomware-attacks-down-17-percent. Jun. 2018.

[7] Ponemon Institute LLC, Accenture. Ninth Annual Cost of Cybercrime Study. Technical report. 2019.

[8] Granger S. Social engineering fundamentals, part I: hacker tactics[J]. *Security Focus,* December, 2001, 18.

[9] Nohlberg M. Social Engineering Audits Using Anonymous Surveys: Conning the Users in Order to Know if They Can Be Conned[C]. *4th Security Conference, Las Vegas, USA,* 2005.

[10] Kevin Mitnick. My first RSA Conference[J]. *SecurityFocus*, 2001. http://www.securityfocus.com/news/199.

[11] Harl. People Hacking: The Psychology of Social Engineering. http://www.textfiles.com/russian/cyberlib.narod.ru/lib/cin/se10.html. 1997.

[12] Brody R G, Brizzee W B, Cano L. Flying under the Radar: Social Engineering[J]. *International Journal of Accounting & Information Management*, 2012, 20(4): 335-347.

[13] Exclusive: Snowden persuaded other NSA workers to give up passwords. https://www.reuters.com/article/net-us-usa-security-snowden-idUSBRE9A703020131108. Nov. 2013.

[14] Thornburgh T. Social Engineering: The "Dark Art"[C]. *The 1st annual conference on Information security curriculum development - InfoSecCD '04*, 2004: 133–135.

[15] Timothy L. Thomas. Cyberskepticism: The Mind's Firewall. Technical report. FOREIGN MILITARY STUDIES OFFICE (ARMY) FORT LEAVENWORTH KS, 2008.

[16] Ghafir I, Prenosil V, Alhejailan A, et al. Social Engineering Attack Strategies and Defence Approaches[C]. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud*. 2016: 145–149.

[17] Van Mourik D-J. Targeted attacks and the human vulnerability[D]. The Hague : Cyber Security Academy, 2017.

[18] Harley D. Re-floating the titanic: Dealing with social engineering attacks[C]. *European Institute for Computer Antivirus Research*, 1998: 4–29.

[19] Manske K. An Introduction to Social Engineering[J]. *Information Systems Security*, 2000, 9(5): 1-7.

[20] Mohd Foozy C F, Ahmad R, Abdollah M, et al. Generic Taxonomy of Social Engineering Attack[C]. *MUiCET*. 2011: 1–7.

[21] Dang H. The origins of social engineering[J]. *McAfee security journal*, 2008: 4–9.

[22] Thomas V. Measuring Effectiveness[M]. Building an Information Security Awareness Program. Amsterdam: Elsevier, 2014: 119-124.

[23] BBC NEWS. How to hack people. http://news.bbc.co.uk/2/hi/technology/2320121.stm. 14-Oct-2002.

[24] Bretschneider D E, (u S) N P S. Sea Level Variations at Monterey, California.[M]. Monterey, California: Naval Postgraduate School, 1980.

[25] Stasiukonis S. Social engineering, the USB way. Dark Reading. https://www.darkreading.com/attacks-breaches/social-engineering-the-usb-way/d/d-id/1128081. Jun. 2006.

[26] Lineberry S. The Human Element: The Weakest Link in Information Security[J]. *Journal of Accountancy*, 2007, 204(1): 44-49.

[27] Evans N J. Information Technology Social Engineering: An Academic Definition and Study of Social Engineering - Analyzing the Human Firewall[D]. Iowa State University, Doctor of Philosophy, 2009. DOI:10.31274/etd-180810-436

[28] Whiteman J R. Social Engneering: Humans are the Prominent Reason for the Continuance of These Types of Attacks[D]. New York: ProQuest LLC, 2017.

[29] Song A M, Cao Q Y. Research on Social Engineering Model Based on Objective Management[J]. *Computer Science*, 2012, 39(z3): 41-44.
(宋艾米, 曹奇英. 基于目标管理的社会工程学模型研究[J]. *计算机科学*, 2012, 39(z3): 41-44.)

[30] Xue C, Yang S P. Research on Invasion of Penetration Based on Social Engineering[J]. *Journal of Guizhou University (Natural Science)*, 2015, 32(1): 81-85.
(薛晨, 杨世平. 基于社会工程学的入侵渗透的研究[J]. *贵州大学学报(自然科学版)*, 2015, 32(1): 81-85.)

[31] Ma M Y. Research on The Defense Technology of Social Engineering Attacks[D]. Beijing University of Posts and Telecommunications, 2015.
(马明阳. 针对社会工程学攻击的防御技术研究[D]. 北京邮电大学, 2015.)

[32] Chenoweth J D. Book Review: The Art of Deception: Controlling the Human Element of Security[J]. *Journal of Information Privacy and Security*, 2005, 1(2): 69-70.

[33] Mitnick K D, Simon W L, Simon W L. The Art of Deception: Controlling the Human Element of Security[M]. Wiley, 2002.

[34] Granger S. Social engineering fundamentals, Part II: Combat strategies[J]. *Security Focus. Retrieved October*, 2002, 12.

[35] The Kid & Co., The Shadow. MORE ON TRASHING[J]. *2600: The Hacker's Quarterly*, 1984, Volume 1, Number 9. http://67.225.133.110/gbpprorg/2600/2600_01-9_p50.txt, (-or-) http://www.hackcanada.com/ice3/2600/2600_01-9_p50.txt.

[36] Anonymous. Vital Ingredients: Switching Centers and Operators[J]. *2600: The Hacker's Quarterly*, 1984.

[37] Shadow T. How to Run a Successful Teleconference[J]. *2600: The Hacker's Quarterly*, 1985.

[38] Unknown. The history of The Legion Of Doom[J]. *Phrack Magazine*, 1990, Three(Thirty-one, Phile #5 of 10). http://phrack.org/ issues/31/5.html.

[39] Zajac B. The Hacker Crackdown—Law and Disorder on the Electronic Frontier[J]. *Computer Fraud & Security Bulletin*, 1994, 1994(5): 18-19.

[40] Hu Y, Fan H Y. Hackers: cowboys of the computer age[M].

China Renmin University Press(CRUP), 1997.
(胡泳, 范海燕. 黑客: 电脑时代的牛仔: Hackers: cowboys of the computer age[M]. 中国人民大学出版社, 1997.)

[41] BlackOpsPro07. The Secret History of Hacking[M]. 2001. https://www.youtube.com/watch?v=PUf1d-GuK0Q.

[42] Hatfield J M. Social Engineering in Cybersecurity: The Evolution of a Concept[J]. *Computers & Security*, 2018, 73: 102-113.

[43] Lapsley P. Exploding the Phone: The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell[J]. *Choice Reviews Online*, 2013, 50(12): 50-6803-50-6803.

[44] Quittner J. Interview With Ice Man And Maniac[J]. *Phrack Magazine*, 1992, 4(14). http://phrack.org/issues/40/14.html#article.

[45] Kluepfel H M. In search of the cuckoo's nest [computer security][C]. *The 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*. 1991: 181–191.

[46] Social Engineering[J]. *Phrack Magazine*, 1988: 2(20). http://phrack.org/issues/20/8.html#article.

[47] Kluepfel H M. Foiling the wiley hacker: more than analysis and containment[C]. *The International Carnahan Conference on Security Technology*. 1989: 15–21.

[48] Fiery D. Secrets of a Super Hacker, The Knightmare, 1994: Secrets of a Super Hacker[M]. Bukupedia, 1994.

[49] Collinson H. Cracking a Social Engineer[J]. *Computers & Security*, 1995, 14(8): 700.

[50] Quann J. The hack attack - Increasing computer system awareness of vulnerability threats[C] *Applying technology to systems*, 1987: 155-155. https://ntrs.nasa.gov/search.jsp?R=19880038985.

[51] Winkler I S, Dealy B. Information Security Technology?...Don'T Rely on It: A Case Study in Social Engineering[C]. *The 5th Conference on USENIX UNIX Security Symposium*, 1995: 1-5.

[52] Anonymous. Telco Trashing Yields Big Rewards[J]. *Phrack Magazine*, 1992, 4(40). http://phrack.org/issues/40/2.html#article.

[53] Winkler I S. Social Engineering and Reverse Social Engineering. http://www.ittoday.info/AIMS/DSM/82-10-43.pdf. May 1998.

[54] Jordan T, Taylor P. A Sociology of Hackers[J]. *The Sociological Review*, 1998, 46(4): 757-780.

[55] Scott Higgins. Physical penetrations: the art of advanced social engineering. Technical report. SANS Institute, totse.com. 2001.

[56] Jonathan J. Rusch. The "social engineering" of internet fraud[C]. *Internet Society Annual Conference,* 1999:1-11.

[57] Hadnagy C. Social engineering: The art of human hacking[M]. John Wiley & Sons, 2010.

[58] Hadnagy C. Unmasking the Social Engineer: The Human Element of Security[M]. John Wiley & Sons, 2014.

[59] Ekman P. Microexpression Training Tool and Subtle Expression Training Tool. *Salt Lake City: A Human Face*, 2002.

[60] McClure S, Scambray J, Kurtz G. Hacking Exposed 5th Edition[M]. Mcgraw-hill, 2005.

[61] Ivaturi K, Janczewski L. A Taxonomy for Social Engineering Attacks[J]. *International Conference on Information Resources Management*, 2011, 1(2): 1-12.

[62] Mouton F, Leenen L, Malan M M, et al. Towards an Ontological Model Defining the Social Engineering Domain[M]. IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014: 266-279.

[63] A convicted hacker debunks some myths. CNN.com. http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html. Oct. 2005.

[64] *Wikipedia*. Social engineering (security). https://en.wikipedia.org/w/index.php?title=Social_engineering_(security)&oldid=885978090. 2019-3-5.

[65] social engineering | Definition of social engineering in English by Oxford Dictionaries. *Oxford Dictionaries | English*. https://en.oxforddictionaries.com/definition/social_engineering. 2019-3-5

[66] Nohlberg M, Kowalski S. The cycle of deception: a model of social engineering attacks, defenses and victims[C]. *HAISA*. University of Plymouth, 2008: 1–11.

[67] Gulenko I. Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness[J]. *Information Management & Computer Security*, 2013, 21(2): 91–101.

[68] Fan W, Lwakatare K, Rong R. Social Engineering: IE based Model of Human Weakness to Investigate Attack and Defense[J]. *SCIREA Journal of Information Science and Systems Science*, 2016, 1(2): 34–57.

[69] Gragg D. A multi-level defense against social engineering[J]. *SANS Reading Room, March*, 2003, 13: 1-21.

[70] Silic M, Back A. The Dark Side of Social Networking sites: Understanding Phishing Risks[J]. *Computers in Human Behavior*, 2016, 60: 35-43.

[71] Schaeken M. Information security awareness measuring & social engineering 2.0. Assessment of information security awareness (ISA) in the Belgian healthcare sector using an enhanced HAIS-Q.[D]. Msc Business Proces Management and IT, Open Universiteit Nederland, 2018.

[72] Hasan M, Prajapati N, Vohara S. Case Study on Social Engineering Techniques for Persuasion[J]. *International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks*, 2010, 2(2): 17-23.

[73] Huber M, Mulazzani M, Schrittwieser S, et al. Cheap and Automated Socio-technical Attacks Based on Social Networking Sites[C]. *The 3rd ACM workshop on Artificial intelligence and security - AISec '10*, 2010: 61–64.

[74] Nohlberg M. Securing information assets: understanding, measur-

ing and protecting against social engineering attacks[D]. Sweden: Department of Computer and Systems Sciences, Stockholm University, 2008.

[75] Best Practices for Social Engineering Attacks. Rapid7.com. https://www.rapid7.com/globalassets/external/docs/download/Metasploit_Best_Practices_for_Social_Engineering_Attacks.pdf. Jun. 2018.

[76] Gulati R. The threat of social engineering and your defense against it. Technical report. SANS Institute, www.sans.org, 2003. https://www.sans.org/reading-room/whitepapers/engineering/paper/1232

[77] Bullee J W. Experimental Social Engineering: Investigation and Prevention[D]. University Library/University of Twente, PhD, 2017. DOI:10.3990/1.9789036543972

[78] Stewart J, Dawson M. How the Modification of Personality Traits Leave one Vulnerable to Manipulation in Social Engineering[J]. *International Journal of Information Privacy, Security and Integrity*, 2018, 3(3): 187.

[79] Samani R, McFarland C. Hacking the Human Operating System: The role of social engineering within cybersecurity. Technical report. McAfee, 2015.

[80] Breda F, Barbosa H, Morais T. Social Engineering and Cyber Security[C]. INTED2017 Proceedings, 2017: 4204-4211.

[81] Peltier T R. Social Engineering: Concepts and Solutions[J]. *Information Systems Security*, 2006, 15(5): 13-21.

[82] Lu F. Social Engineering Leading Non-traditional Information Security[J]. *China Computer News*, 2006:1.
(卢凡. “社会工程学”主导非传统信息安全[J]. *中国计算机报*, 2006: 1.)

[83] Fan J Z. Hacker Social Engineering Attack[M]. Jinan Qilu Electronic Audio and Video Publishing House, 2008.
(范建中. 黑客社会工程学攻击[M]. 山东: 济南齐鲁电子音像出版社, 2008.)

[84] Oosterloo B. Managing social engineering risk: making social engineering transparant[D]. Industrial Engineering and Management, University of Twente, 2008.

[85] Algarni A, Xu Y. Social engineering in social networking sites: phase-based and source-based models[J]. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 2013, 3(6): 456–462.

[86] Algarni A A M. The impact of source characteristics on users’ susceptibility to social engineering Victimization in social networks[D]. School of Electrical Engineering and Computer Science Science and Engineering Faculty, Queensland University of Technology, 2016.

[87] Hermansson M, Ravne R. Fighting Social Engineering[D]. University of Stockholm/Royal Institute of Technology, 2005.

[88] Nohlberg M. Social engineering: understanding, measuring and protecting against attacks. Technical report. University of Skövde, 2007.

[89] Bakhshi T, Papadaki M, Furnell S. A Practical Assessment of Social Engineering Vulnerabilities.[C]. *HAISA*. 2008: 12–23.

[90] Larson R E, Cockcroft L. Understanding Network Security Threats[M]. CCSP: Cisco Certified Security Professional Certification Exam Guide. Osborne: McGraw-Hill, 2003.

[91] Conteh N Y, Schmick P J. Cybersecurity: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks[J]. *International Journal of Advanced Computer Research*, 2016, 6(23): 31-38.

[92] Beckers K, Pape S, Fries V. HATCH: Hack and Trick Capricious Humans – a Serious Game on Social Engineering[C]. 2016: 1-3.

[93] Jakobsson M. Modeling and Preventing Phishing Attacks[M]. Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 89.

[94] Mills D. Analysis of a Social Engineering Threat to Information Security Exacerbated by Vulnerabilities Exposed through the Inherent Nature of Social Networking Websites[C]. 2009 Information Security Curriculum Development Conference on - InfoSecCD '09, 2009: 139–141.

[95] Tetri P, Vuorinen J. Dissecting Social Engineering[J]. *Behaviour & Information Technology*, 2013, 32(10): 1014-1023.

[96] Dhiman P, Wajid S A, Quraishi F F. A Comprehensive Study of Social Engineering - The Art of Mind Hacking[J]. *IJSRCSEIT*, India: Technoscience Academy, 2017, 2(6): 543–548.

[97] Hasle H, Kristiansen Y, Kintel K, et al. Measuring Resistance to Social Engineering[M]. Information Security Practice and Experience. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 132-143.

[98] Thapar A. Social Engineering: An Attack Vector most Intricate to Tackle. Technical report. CISSP 106841. Infosec Writers, 2007.

[99] Lab K. SOCIAL ENGINEERING, HACKING THE HUMAN OS. https://www.kaspersky.com/blog/social-engineering-hacking-the-human-os/3386/. 2013-12-20.

[100] Bisson D. 5 Social engineering attacks to watch out for. http://www.infosecisland.com/blogview/24410-5-Social-Engineering-Attacks-to-Watch-Out-For.html. Mar. 2015. https://www. tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/. Nov. 2019.

[101] Heartfield R, Loukas G. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks[J]. *ACM Computing Surveys*, 2016, 48(3): 1-39.

[102] Nyamsuren E, Choi H-J. Preventing social engineering in ubiquitous environment[C]. *Future Generation Communication and Networking (FGCN 2007)*. IEEE, 2007, 2: 573–577.

[103] Lafrance Y. Psychology: A precious security tool. Technical report. SANS Institute, www.sans.org, 2004.

[104] McAfee. Social Engineering in the Internet of Things (IoT). https://www.mcafee.com/blogs/other-blogs/executive-perspectives/social-engineering-internet-things-iot/. Mar. 2015.

[105] Pfleeger C P, Pfleeger S L. Security in Computing[M]. Prentice Hall Professional, 2003.

[106] Uebelacker S, Quiel S. The Social Engineering Personality Framework[C]. *2014 Workshop on Socio-Technical Aspects in Security and Trust*. 2014: 24–30.

[107] Winkler I. Corporate Espionage: What it Is, why It's Happening in your Company, what You must do about it[J]. *Edpacs*, 1999, 27(5): 1.

[108] Cybenko G, Giani A, Thompson P. Cognitive Hacking: A Battle for the Mind[J]. *Computer*, 2002, 35(8): 50-56.

[109] Cybenko G, Giani A, Thompson P. Cognitive hacking and the value of information[C]. *Workshop on Economics and Information Security*. 2002: 16–17.

[110] Cybenko G, Giani A, Heckman C, et al. Cognitive hacking: technological and legal issues[C]. *Law Tech 2002*. 2002:7-9.

[111] Thompson P. Cognitive Hacking and Intelligence and Security Informatics[C]. Defense and Security. *Proc SPIE 5423, Enabling Technologies for Simulation Science VIII*, Orlando, Florida, USA. 2004, 5423: 142-151.

[112] Schneier B. Semantic attacks: The third wave of network attacks. https://www.schneier.com/crypto-gram/archives/2000/1015.html#1. Oct. 2000.

[113] What is cognitive hacking? - Definition from WhatIs.com. https://whatis.techtarget.com/definition/cognitive-hacking. Aug. 2017.

[114] Thomas T L. Russia Military Strategy: Impacting 21st Century Reform and Geopolitics[M]. Foreign Military Studies Office, 2015.

[115] Thomas T. Russia's Reflexive Control Theory and the Military[J]. *The Journal of Slavic Military Studies*, 2004, 17(2): 237-256.

[116] Jakobsson M. Social Engineering 2.0: What's Next[J]. *McAfee security journal*, 2008: 13–15.

[117] E.Frumento, R.Puricelli, F.Freschi, et al. The role of Social Engineering in evolution of attacks. Technical report. 653618, CEFRIEL, 2016.

[118] Wikipedia. Pinterest. https://en.wikipedia.org/w/index.php?title=Pinterest&oldid=873992162. Dec. 2018.

[119] Boshmaf Y, Muslukhov I, Beznosov K, et al. The Socialbot Network: When Bots Socialize for Fame and Money[C]. *The 27th Annual Computer Security Applications Conference on - ACSAC '11*, 2011: 93–102.

[120] Kaul P, Sharma D. Study of Automated Social Engineering, Its Vulnerabilities, Threats and Suggested Countermeasures[J]. *International Journal of Computer Applications*, 2013, 67(7): 13-16.

[121] Why it is called Internet of Things: Definition, history, disambiguation. https://iot-analytics.com/internet-of-things-definition/. Dec. 2014

[122] Wikipedia. Industry 4.0. https://en.wikipedia.org/w/index.php?title=Industry_4.0&oldid=872950801. Dec. 2018.

[123] Gan D, Heartfield R. Social engineering in the internet of everything[J]. *Cutter IT Journal*, 2016, 29(7): 20–29.

[124] Haddadi H, Hui P. To Add or Not to Add: Privacy and Social Honeypots[C]. *2010 IEEE International Conference on Communications Workshops*. 2010: 1–5.

[125] Ball L D, Ewan G, Coull N J. Undermining-social engineering using open source intelligence gathering[C]. *KDIR 2012: The 4th International Conference on Knowledge Discovery and Information Retrieval*. 2012:1-6.

[126] Scheelen Y, Wagenaar D, Smeets M, et al. The devil is in the details: Social Engineering by means of Social Media. Technical report. A Project Report on System & Network Engineering, Universiteit van Amsterdam, 2012.

[127] Edwards M, Larson R, Green B, et al. Panning for Gold: Automatically Analysing Online Social Engineering Attack Surfaces[J]. *Computers & Security*, 2017, 69: 18-34.

[128] Trustedsec. trustedsec/social-engineer-toolkit. https://github.com/trustedsec/social-engineer-toolkit. 2018.

[129] Green B, Prince D, Busby J, et al. The Impact of Social Engineering on Industrial Control System Security[C]. *The First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy - CPS-SPC '15*, 2015: 23–29.

[130] Jagatic T N, Johnson N A, Jakobsson M, et al. Social Phishing[J]. *Communications of the ACM*, 2007, 50(10): 94-100.

[131] Frumento E, Puricelli R. An innovative and comprehensive framework for Social Driven Vulnerability Assessment[J]. *Magdeburger Journal zur Sicherheitsforschung*, 2014, 2: 493–505.

[132] Kushner D. The Real Story of Stuxnet[J]. *IEEE Spectrum*, 2013, 50(3): 48-53.

[133] Abraham S, Chengalur-Smith I. An Overview of Social Engineering Malware: Trends, Tactics, and Implications[J]. *Technology in Society*, 2010, 32(3): 183-196.

[134] Kvedar D, Nettis M, Fulton S P. The Use of Formal Social Engineering Techniques to Identify Weaknesses During a Computer Vulnerability Competition[J]. *J. Comput. Sci. Coll.*, 2010, 26(2): 80–87.

[135] Benenson Z, Gassmann F, Landwirth R. Unpacking Spear Phishing Susceptibility[M]. Financial Cryptography and Data Security. Cham: Springer International Publishing, 2017: 610-627.

[136] Irani D, Balduzzi M, Balzarotti D, et al. Reverse Social Engineering Attacks in Online Social Networks[C]. *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, Berlin, Heidelberg, 2011: 55–74.

[137] Huber M, Kowalski S, Nohlberg M, et al. Towards Automating Social Engineering Using Social Networking Sites[C]. *2009 International Conference on Computational Science and Engineering*. 2009, 3: 117–124.

[138] Lauinger T, Pankakoski V, Balzarotti D, et al. Honeybot, Your Man in the Middle for Automated Social Engineering[C]. *LEET*. USA: USENIX Association, 2010: 1–8.

[139] Balduzzi M, Platzer C, Holz T, et al. Abusing Social Networks for Automated User Profiling[C]. *Recent Advances in Intrusion Detection*. Springer, Berlin, Heidelberg, 2010: 422–441.

[140] Gallagher R. Where Do the Phishers Live? Collecting Phishers' Geographic Locations from Automated Honeypots[C]. *2016 ShmooCon*, 2016.

[141] Seymour J, Tully P. Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter[C]. *Black Hat USA 37*, 2016: 1-39.

[142] Bahnsen A C, Torroledo I, Camacho L D, et al. DeepPhish: Simulating Malicious AI[C]. 2018 APWG Symposium on Electronic Crime Research (eCrime), 2018:1-9.

[143] Anderson H S, Woodbridge J, Filar B. DeepDGA: Adversarially-Tuned Domain Generation and Detection[C]. *The 2016 ACM Workshop on Artificial Intelligence and Security*. New York, NY, USA: ACM, 2016: 13–21.

[144] Ariu D, Frumento E, Fumera G. Social Engineering 2.0: A Foundational Work: Invited Paper[C]. *The Computing Frontiers Conference*. New York, NY, USA: ACM, 2017: 319–325.

王作广 于2016年在解放军信息工程大学计算机科学与技术专业获得硕士学位。现于中国科学院大学、中国科学院信息工程研究所，网络空间安全专业，攻读博士学位。研究领域为社工安全、工业控制系统安全、安全脆弱性分析。
Email: wangzuoguang16@mails.ucas.ac.cn

孙利民 于1998年在国防科学技术大学计算机学院获得博士学位。现任中国科学院信息工程研究所研究员。主要研究方向为物联网及其安全、工业控制系统安全、网络空间安全。Email: sunlimin@iie.ac.cn

朱红松 于2009年在中国科学院大学计算所获得博士学位。现任中国科学院信息工程研究所研究员。主要研究方向包括物联网安全、网络空间测绘、社工安全。Email: zhuhongsong@iie.ac.cn