第3章

心理学和可用性

人类无法安全地存储高质量的加密密钥,并且在执行加密操作时,他们具有无法接受的速度和准确性。（它们也很大,维护起来很昂贵,难以管理,而且它们会污染环境。令人惊讶的是,这些设备仍在继续制造和部署。但它们非常普遍,我们必须围绕它们的局限性来设计我们的协议。）

– KAUFMANN、PERLMAN 和 SPECINER [1025]

只有业余爱好者才会攻击机器;专业人士以人为目标。

– 布鲁斯施耐尔

梅特涅一直在撒谎,从来没有欺骗过任何人;塔列朗从不说谎,欺骗了全世界。

托马斯·麦考利

3.1 简介

许多真正的攻击至少与技术一样利用心理。我们在上一章中看到了一些在线犯罪如何涉及操纵愤怒的暴民,而财产犯罪和间谍活动都大量使用网络钓鱼,受害者被电子邮件引诱登录到看似真实但实际上是设计的网站窃取他们的密码或让他们安装恶意软件。

与类似的现实世界欺诈相比,网络钓鱼等在线欺诈通常更容易实施,但更难阻止,因为许多在线保护机制既不像现实世界的同类机制那样易于使用,也不像它们那样难以伪造。对于骗子来说,创建一个通过随意检查的假冒银行网站比在购物街建立一个真正的假冒银行分行要容易得多。

数百万年来,我们已经进化出社会和心理工具来帮助我们应对面对面的欺骗行为,但当我们收到一封要求我们做某事的电子邮件时,这些工具就不太有效了。为理想的技术,好好利用

会比糟糕的使用更容易。我们在现实世界中有很多这样的例子:土豆削皮器比刀更容易用于削土豆皮,但用于谋杀却难得多。但是对于计算机系统,我们并不总能做到这一点。

我们在日常业务中所依赖的好与坏之间的大部分不对称不仅仅取决于正式的交流 这可以很容易地自动化 而是取决于物理对象、人们的判断和支持的社会协议的某种组合。因此,随着我们与雇主、银行和政府的关系通过在线交流变得更加正式,并且我们失去了物理和人文背景,这些交流的伪造风险变得更大。

各种欺骗现在是用来破坏在线安全的主要机制。它可用于获取密码、泄露机密信息或直接操纵金融交易。恶作剧和欺诈总是发生,但互联网让其中一些变得更容易,并让其他人以可能绕过我们现有控制(无论是个人直觉、公司程序甚至法律)的方式重新包装。

基于社会工程学的攻击激增的另一个驱动因素是人们越来越擅长技术。随着设计人员学习如何预防更容易的技术攻击,对系统用户或操作员的心理操纵变得越来越有吸引力。因此,安全工程师绝对必须了解基本心理学,这是胜任处理从密码到验证码,从网络钓鱼到一般社会工程的一切事物的先决条件;对风险误解和危言耸听的有效认识对于理解愤怒的在线暴徒背后的机制以及社会对从恐怖主义到流行病的紧急情况的反应也是必要的。因此,正如安全经济学的研究导致本书第一版和第二版之间的视角发生真正的转变一样,安全心理学的研究也在很大程度上改变了我们在第二版和这一版之间看待世界的方式。

在本章的其余部分,我将首先调查相关的心理学研究,然后研究我们如何应用这些原则来使密码身份验证机制更强大地抵御攻击、更普遍的安全可用性,以及除此之外的良好设计。

3.2 心理学研究的启示

心理学是一门庞大的学科,从神经科学到临床主题,并延伸到从哲学到人工智能再到社会学的同源学科。虽然它的研究时间比计算机科学长得多,但我们对心智的理解远不完整:大脑要复杂得多。有一个核心问题 意识的本质 我们根本不了解。我们知道“头脑就是大脑所做的事情”,但构成我们自我意识和个人历史基础的机制仍然模糊不清。

尽管如此,人们对心智和大脑的功能知之甚少,而且我们一直在学习有趣的新事物。在什么

接下来,我只能提供直升机游览与我们的行业非常相关的三个心理学研究主题:认知心理学,研究诸如我们如何记忆以及我们犯了什么样的错误等主题;社会心理学,研究我们如何与群体中的其他人和权威建立联系;和行为经济学,它研究导致我们做出在可衡量和可利用方面始终不合理的决定的启发式和偏见

方法。

3.2.1 认知心理学

认知心理学是该学科的经典方法 建立在 19 世纪早期的实证研究基础上。它涉及我们如何思考、记忆、做出决定甚至做白日梦。 Ulric Neisser 等 20 世纪的先驱者发现,人类的记忆不像录像机那样工作:我们的记忆存储在大脑的网络中,它们可以从中重建,因此它们会随着时间的推移而变化并且可以被操纵 [1427] .有许多众所周知的结果。例如,更容易记住经常重复的事物,并且更容易在上下文中存储事物。其中许多见解被营销人员和诈骗者使用,但被大多数系统开发人员误解或忽略。

例如,我们大多数人都听说过 George Miller 的结果,即人类的短期记忆可以处理大约七个(正负两个)同时选择 [1317],因此,许多设计师将菜单选择限制在大约五个。

但这不是正确的结论。人们首先通过回忆要看的地方,然后通过扫描来搜索信息;找到相关菜单后,扫描十个项目仅是扫描五个项目的两倍。菜单大小的真正限制是屏幕大小,它可能会给你十个选择,而对于语音菜单,普通用户很难处理超过三个或四个 [1544]。在这里,米勒的洞察力也被误用了,因为空间结构记忆与回声记忆不同。这说明了为什么像 7+/-2 这样的广泛概念可能是危险的;你需要看细节。

近年来,该领域的重心已经从应用认知心理学转移到人机交互 (HCI) 研究社区,因为大量的实证知识不仅来自实验室实验,还来自现场系统的迭代改进。

因此,HCI 研究人员不仅对人类表现进行建模和测量,包括感知、运动控制、记忆和解决问题;他们还了解了用户的系统心智模型如何工作,它们与开发人员的心智模型有何不同,以及我们可以用来探索人们如何学习的技术(例如任务分析和认知演练)使用和理解系统。

安全研究人员需要找到将这些犁头变成剑的方法(坏人已经在研究它)。有一些唾手可得的果实;例如,安全研究界投入了大量精力来研究人们在操作设备时所犯的错误 [1589]。据说“人都会犯错”,错误研究证实了这一点:可预测的各种人为错误植根于认知的本质。使我们能够识别人、声音和概念的图式或心智模型

比电脑好得多,当错误的模型被激活时,也会让我们变得脆弱。

操作设备时发生的人为错误大致分为三类,具体取决于它们在“堆栈”中发生的位置:技能层面的失误、规则层面的错误以及认知层面的误解。

- 执行的动作往往成为一项技能问题,但当手动技能失败时,我们可能会失误 例如,按错按钮 我们也可能在使用错误技能时失误。例如,当您打算在下班回家的路上去超市时,您可能会错误地走回家的路,如果这是您大部分时间所做的(这也称为捕获错误)。错误被域名仿冒者利用,他们注册与流行域名相似的域名,收割打字错误的人;其他攻击利用了这样一个事实,即人们接受过单击“确定”弹出框来完成工作的培训。因此,在设计系统时,您需要确保危险操作(例如安装软件)需要与常规操作完全不同的操作顺序。错误也通常伴随着中断和感知混乱。

  一个例子是完成后的错误:一旦他们完成了他们的直接目标,人们很容易从整理行动中分心。越来越多的人把卡留在自动取款机里,自动取款机先给他们钱,然后再取回卡。

- 当人们遵循错误的规则时,他们按照规则采取的行动很容易出错。各种情况 例如信息过载 会导致人们遵循他们所知道的最强规则或最普遍的规则,而不是最好的规则。网络钓鱼者使用许多技巧让人们遵循错误的规则,从使用 https(因为“它是安全的”)到以冒充银行名称开头的 URL,如 www.citibank.secureauthentication.com 对大多数人来说,寻找一个name 是比解析其位置更强大的规则。

- 第三类错误是人们出于认知原因所犯的错误 他们要么根本不理解问题,要么假装理解,而忽略建议以完成工作。关于安全可用性的开创性论文 Alma Whitten 和 Doug Tygar 的“Why Johnny Can t Encrypt”证明了加密程序 PGP 对大多数大学生来说太难使用了,因为他们不理解私有加密与加密加密的微妙之处公钥、加密和签名性质 [2018]。人们越来越认识到,许多安全漏洞的发生是因为大多数程序员也不会使用安全机制。

  访问控制机制和安全 API 都难以理解且难以使用;安全测试工具通常也好不了多少。

  即使以非常错误的方式使用保护机制,程序也常常看起来能正常工作。然后,工程师们互相复制代码,并从在线代码共享站点复制代码,因此误解和错误被广泛传播 [11]。他们通常知道这很糟糕,但没有时间做得更好。

这一切背后都有一些重要的科学依据,这里仅举两个例子。詹姆斯·吉布森 (James Gibson) 提出了行动可能性或规则的概念:对于动物而言,物理环境可能是可攀爬的、可坠落的或可下的,类似地,一个座位是可坐的。人们在创造诱使他人以特定方式行事的环境方面已经发展出高超的技能:我们建造楼梯和门口,我们使物体易于携带或抓握;我们制造笔和剑 [762]。通常,感知是由规则组成的,这些规则可能比价值或意义更基本。以完全相同的方式,我们设计软件制品来训练和调节用户的选择,因此我们使用的系统的规则可以以各种方式影响我们的思维方式。我们还可以为粗心的人设计陷阱:将陷阱误认为坚实地面的动物有麻烦了。

Gibson 还提出了光流的概念,并由 Christopher Longuet-Higgins [1185] 进一步发展。当我们的眼睛相对于环境移动时,由此产生的光流场让我们能够解读图像,了解其中物体的大小、距离和运动。有一个优雅的光学视差数学理论,但我们的眼睛处理它的方式不同:它们包含对该流场特定方面的接收,假设其中的物体是刚性的,这使我们能够解决旋转和平移分量.光流使我们能够独立于双眼视觉了解周围物体的形状。我们将它们用于一些关键任务,例如降落飞机和驾驶汽车。

简而言之,认知科学为如何设计系统界面提供了有用的见解,以便使某些行动过程变得简单、困难或不可能。它越来越多地与计算机人机交互研究联系在一起。通过使错误变得简单或困难,您可以或多或少地犯错误;在第 28.2.2 节中,我给出了导致涉及医疗设备和飞机的严重事故的可用性故障的真实示例。然而,如果我们有一个可以引发可利用错误的有感知力的攻击者,那么安全性可能比安全性更难。

防御者可以期望攻击者做什么?他们将使用效果可预测的错误,例如捕获错误;他们会利用不正当的a or 舞蹈;它们将扰乱安全运行所依赖的流动;他们会在用户的系统心智模型与其实际逻辑之间寻找或创造可利用的不协调。要查找这些,您应该尝试通过认知走查来识别攻击点,就像代码走查可用于搜索软件漏洞一样。攻击者还通过实验学习并相互分享技术,并开发工具来有效地寻找已知攻击。因此,了解已经奏效的攻击非常重要。 (这是本书的功能之一。)

3.2.2 性别、多样性和人际差异

许多女性死亡是因为医学测试和技术假设患者是男性,或者因为工程师在设计汽车时使用男性碰撞测试假人;防护装备,从运动服到防弹背心再到宇航服,默认为男性量身定制 [498]。那么我们的信息系统也有问题吗?它们是由男性设计的,而且是年轻的极客男性,但超过一半的用户可能是女性。这种认识导致了对

性别 HCI 关于应如何设计软件以便女性也能有效使用它 。早期的实验是从行为研究开始的:实验表明,女性更多地使用周边视觉,而且事实证明,更大的显示器可以减少性别偏见。对美国女性程序员的研究表明,她们的修修补补比男性少,但更有效 [202]。但是自然有多少,后天有多少?社会因素很重要,编程的美国女性似乎更体贴,但自尊心较低和风险厌恶程度较高导致她们使用的功能较少。

性别已经成为心理学研究中一个有争议的话题。在 2000 年代初期,关于男性在计算机科学方面的能力的讨论有时是根据 Simon Baron-Cohen 的分析得出的,该分析给人们分别打分,分别是系统化者(擅长几何和某些符号推理)和移情者(善于直觉他人的情绪和一般的社会智力)[176]。大多数男性在系统化方面得分更高,而大多数女性在同理心方面做得更好。对应关系不准确;少数男性更善于共情,而少数女性更善于系统化。

Baron-Cohen 的研究领域是阿斯伯格综合症和自闭症谱系障碍,他认为这是男性大脑的一种极端形式。这个理论在极客中获得了一些支持,他们看到了为什么我们经常性格内向,更善于理解事物而不是理解人的解释。如果我们生来就是这样,那不是错。它还可以解释为什么极客夫妇经常生孩子。

这是否可以解释为什么男性比女性对计算机科学更感兴趣,而在美国和英国,女性一直占据大约六分之一的 CS 名额?但是在这里,我们遇到了麻烦。在波兰、罗马尼亚和波罗的海国家等前共产主义国家,女性占 CS 学生的三分之一,而印度的这一比例接近相等。男性主导软件也是一个相当新的现象。当我在 1970 年代开始工作时,女性程序员几乎和男性一样多,而且许多先驱者是女性,无论是在工业界、学术界还是政府。这表明相关的差异更多是文化上的,而不是遗传或发育上的。 Daphna Joel 及其同事等人的工作逐渐削弱了“男性大脑/女性大脑”解释的论点,他们通过广泛的神经影像学研究表明,虽然大脑中存在可识别的男性和女性特征,但个体的大脑是两者的镶嵌[985]。

尽管这些特征在成像中可见,但这并不意味着它们在出生时就已形成:我们的大脑具有很大的可塑性。与我们的肌肉一样,我们锻炼的组织也会变大。考虑到我们周围所见的性别认同、性偏好、攻击性、同理心等方面的差异,也许没有其他事情是可以预料到的。

其他研究表明,新生儿不存在性别表现差异 ,并在 6-7 岁左右出现,此时儿童早已学会区分性别并适应周围的社会线索,这在发达国家得到加强受到蓝色/粉色性别玩具和营销的海啸影响。 (一些人认为,女性在印度从事计算机工作更快乐,因为印度在 1980 年代摆脱了家用电脑的繁荣及其向游戏的演变。)这一点在童年后期和青春期被性别刻板印象所强化,她们将这些刻板印象内化为她们的一部分身份;

在女孩不应该擅长数学或对计算机不感兴趣的文化中,对“擅长数学”的赞美会引起刻板印象威胁（害怕确认对自己所属群体的负面刻板印象）。

也许因此,男性对个人表扬反应更好（“你真聪明！”）,而女性更容易受到表扬（“你一定付出了很多努力”）。因此,我们看到女性在赞美天才的学科（例如数学)中出现不足并不奇怪。更重要的是,类似的机制似乎是被标记为非学术的族群较差的学业成绩的基础。简而言之,人们不仅生来不同 ;我们学会与众不同,受到权力、文化态度、期望和机会的影响。基因和具有涌现行为的文化之间存在多个层次,包括细胞和回路。因此,如果我们想要在从学校到大学再到专业发展的过程中进行更有效的干预,我们需要更好地了解潜在的神经和文化机制。有关这方面的调查,请参见 Gina Rippon [1605]。

性别在堆栈的许多层面都很重要,从产品应该做什么到如何做。例如,汽车应该更快还是更安全?这与社会价值观纠缠在一起。男人是更好的司机是因为他们赢得了赛车比赛,还是女人是更好的司机是因为她们的保险索赔更少?

深入挖掘,我们发现了对风险的性别和文化态度。在美国的调查中,白人和男性认为风险较低,仔细研究后,这是因为大约 30% 的白人男性认为风险极低。这种偏见在广泛的危害中是一致的,但对于手枪、二手香烟烟雾、多个性伴侣和街头毒品尤其强烈。亚洲男性对某些危险（例如机动车)表现出同样低的敏感性。

白人男性更信任技术,而不是政府 [693]。

我们工程师当然必须与世界共事,而不是如果我们的教育体系和我们的文化没有那么多偏见的话;但我们必须警惕计算机系统存在歧视的可能性,因为它们是男人为男人建造的,就像汽车和宇航服一样。例如,我和 Tyler Moore 做了一个实验,看看银行向客户提供的反网络钓鱼建议是否更容易让男性比女性更容易接受,我们发现确实如此 [1337]。似乎没有人在性别和安全可用性方面做过很多工作,所以这是一个机会。

但问题要广泛得多。许多系统将继续由白人或亚裔的年轻聪明直男设计,他们可能不会认真思考或根本不会思考他们没有直接遇到的各种形式的偏见和残疾。您需要认真考虑如何减轻影响 。仅仅让开发团队中的极客女孩测试您的新产品是不够的;你还必须考虑受教育程度较低的人和弱势群体 包括老年人、儿童和逃离虐待关系的妇女（关于这些我稍后会详细说明）。你真的必须考虑整个堆栈。多元化在公司治理、市场研究、产品设计、软件开发和测试中很重要。如果你不能修复开发中的不平衡,你最好在别处弥补。你需要了解你的用户 ;了解权力和文化如何助长失衡也很好。

由于许多与群体行为相关的因素都是社会起源的,我们

接下来转向社会心理学。

3.2.3 社会心理学

这试图解释个人的思想、感受和行为如何受到他人实际、想象或暗示存在的影响。它有很多方面，从人们从属于群体（无论是性别、部落、团队、职业甚至宗教）中获得的身份，到我们通过与他人比较获得的自尊。将它放在地图上的结果是三篇早期论文，它们为理解滥用权力及其与宣传、审讯和侵略的相关性奠定了基础。紧随其后的是关于旁观者效应的工作，这也与犯罪和安全高度相关。

3.2.3.1 权力及其滥用

1951 年，所罗门·阿希 (Solomon Asch) 表明，人们可以被诱使否认自己亲眼所见的证据，以便从众。受试者在听到其他小组成员的错误意见后判断线条的长度，这些小组成员实际上是实验者的走狗。大多数受试者屈服并服从，只有 29% 的人抵制假多数 [135]。

斯坦利·米尔格拉姆 (Stanley Milgram) 受到 1961 年对纳粹战犯阿道夫·艾希曼 (Adolf Eichmann) 的审判的启发，调查了有多少实验对象准备对扮演“学习者”角色的演员实施严重电击，而该演员应实验者的要求扮演“老师”的角色 即使“学习者”表现出剧烈疼痛并请求受试者停止。这个实验旨在衡量有多少人会服从权威而不是他们的良心。大多数人做了 米尔格拉姆发现，如果被告知，超过 60% 的受试者会做出彻头彻尾不道德的事情 [1312]。这个实验现在是有争议的，但对学科的发展产生了真正的影响。

第三个是斯坦福囚犯实验，它表明即使没有命令，正常人也可以做出邪恶的行为。 1971 年，实验者菲利普·津巴多 (Philip Zimbardo) 在斯坦福大学设立了一座“监狱”，其中 24 名学生被随机分配到 12 名看守和 12 名囚犯的角色。该实验的目的是发现监狱虐待的发生是否是因为看守（可能还有囚犯）是自我选择的。然而，扮演看守角色的学生很快变成了虐待狂独裁者，实验在六天后因道德原因而停止 [2073]。这个实验现在也有争议，今天重复进行不太可能获得伦理批准。但是，如果您正在为企业设计运营安全措施，滥用权力，无论是真实的还是表面上的，都是一个真正的问题。

在 1995 年至 2005 年期间，一名自称“Ocer Scott”的电话骗子命令美国 32 个州超过 68 家商店和餐馆（包括至少 17 家麦当劳商店）的经理以涉嫌盗窃和脱衣舞的罪名拘留一些年轻员工。搜索他们。下令进行其他各种降级，包括殴打和性侵犯 [2033]。前狱警

因冒充警察而受审,但被宣告无罪。至少有 13 名服从来电者并进行搜查的人被指控犯罪,其中 7 人被定罪。麦当劳因未对门店经理进行适当培训而被起诉,甚至在恶作剧电话模式确立多年后也是如此； 2007 年 10 月,陪审团命令他们向其中一名受害人支付 610 万美元,该受害人在她还是 18 岁雇员时曾被脱衣搜身。这是一个恶劣的案件,因为她被店长留在男友的监护下,男友随后对她进行了进一步的非礼。男友被判五年,经理承认非法拘禁她。麦当劳辩称,她要为没有意识到这是一场骗局而遭受的任何损失负责,而且店长没有运用常识。肯塔基州陪审团不买账,命令麦当劳赔钱。商店经理也提起诉讼,声称是公司疏忽警告她这个骗局的另一个受害者,并获得了 110 万美元 [1088]。因此,如果美国雇主未能培训员工抵制滥用职权,他们现在将面临严重损失的风险。

3.2.3.2 旁观者效应

1964 年 3 月 13 日,一位名叫 Kitty Genovese 的年轻女士在她位于纽约皇后区的公寓外的街道上被人刺死。媒体报道称,虽然袭击持续了将近半小时,但 38 名不同的目击者没有提供帮助,甚至没有报警。尽管后来发现这些报道被夸大了,但这一罪行导致了全国范围内的 911 紧急求助电话,并且还研究了为什么旁观者往往不介入。

约翰·达利 (John Darley) 和比伯·拉坦 (Bibb Latan´e) 在 1968 年报告了关于哪些因素会影响旁观者帮助看似癫痫发作的人的可能性的实验。他们发现,一个孤独的旁观者在 85% 的情况下会提供帮助,而认为其他四个人可以看到受害者的人在 31% 的情况下会提供帮助;群体规模主导了所有其他的影响。

另一个旁观者是男性、女性还是具有医学资格的人基本上没有区别 [513]。责任的分散在许多其他情况下都有明显的影响。如果你想完成某件事,你会发邮件给一个人询问,而不是三个人。当然,安全通常被视为与其他人打交道的事情。

然而,如果你发现自己处于危险之中,真正的问题是是否至少有一个旁观者会提供帮助,而最近的研究在这方面更为积极。 Lasse Liebst、Mark Levine 和其他人调查了过去十年中几个国家发生的一些公共冲突的闭路电视录像,发现在十分之九的情况下,一名或多名旁观者进行了干预以缓和冲突,并且越多的旁观者干预,他们就越成功[1163]。所以假设旁观者通常从另一边经过是错误的;所以旁观者效应的名称相当具有误导性。

3.2.4 欺骗的社会脑理论

我们的第二个大主题,也符合社会心理学,是对欺骗的研究越来越多。欺骗是如何运作的,我们如何检测和衡量它,以及我们如何阻止它?

现代方法始于 1976 年的社会智力假设。在那之前,人类学家一直认为我们进化出更大的大脑是为了制造更好的工具。但考古证据并不支持这一点。在整个旧石器时代,当我们的大脑从黑猩猩大小进化到人类大小时,我们使用的是同样简单的石斧。它们在新石器时代变得更加复杂,那时我们的祖先在解剖学上已成为现代智人。那么,尼克·汉弗莱 (Nick Humphrey) 问道,如果我们还不需要大脑,为什么还要进化出大脑呢?受到笼养和野生灵长类动物行为观察的启发,他的假设是智力的主要功能是社交。我们的祖先进化出更大的大脑并不是为了制造更好的工具,而是为了更好地使用其他灵长类动物作为工具 [934]。现在,越来越多的证据支持这一点,并将心理学转变为一门学科。

在那之前,社会心理学一直是一个贫穷的乡下表亲,并不被视为严谨;从那以后,人们意识到这可能是认知进化的驱动力。几乎所有的智能物种都是在社会环境中发展起来的。

(章鱼是个例外,但即使是它也必须了解捕食者和猎物的反应。)

灵长类动物学家安迪·怀腾 (Andy Whiten) 随后收集了很多关于战术欺骗的早期证据,并将社会智能重塑为马基雅维利大脑假说:我们变得聪明是为了欺骗他人,同时也是为了检测欺骗行为 [360]。并非所有人都完全同意这种描述,因为同理心等社会化的积极方面也很重要。但 Hugo Mercier 和 Dan Sperber 最近收集了大量证据,证明现代人脑比其他任何东西都更像是一台争论机器 [1294]。

我们的目标是说服而不是真相;修辞是第一位的,逻辑是第二位的。

来自社会智力假说的第二条线索是心智理论,这是 David Premack 和 Guy Woodru 于 1978 年提出的一个想法,但由 Heinz Wimmer 和 Josef Perner 在 1983 年的一个经典实验中发展起来,以确定儿童何时第一次能够告诉某人被骗了[2029]。在这个名为莎莉-安妮测试的实验中,一个孩子在安妮和孩子的注视下看到莎莉藏在杯子下面的糖果。然后安妮离开了房间,莎莉将糖果换到了另一个不同的杯子里。然后安妮回来,孩子被问到安妮认为糖果在哪里。正常的孩子从五岁左右就能得到正确答案;这是他们获得辨别他人信仰和意图的能力的时候。 Simon Baron-Cohen、Alan Leslie 和 Uta Frith 随后表明,阿斯伯格综合症/自闭症谱系中的儿童获得这种能力的时间要晚得多 [177]。

许多计算机科学家和工程师在某种程度上似乎属于这种范围,而且我们通常不像神经质的人那样善于欺骗。这有各种各样的含义!我们在政治、高级管理人员和市场营销方面的代表性不足。哦,在地下市场将可以编写恶意代码的极客与可以将其用于邪恶目的的骗子和间谍聚集在一起之前,网络犯罪要少得多。极客也更有可能成为告密者;我们不太可能为了取悦他人而对令人不安的事实保持沉默,因为我们不太重视他们的意见。但这是一个复杂的领域。一些知名的网络不法之徒比其他任何人都更倒霉;加里麦金农声称已经侵入五角大楼以发现飞碟的真相

并没有预料到联邦调查局的反应如此凶猛。许多犯罪都涉及其他类型的移情缺陷。其他有性格同理心缺陷的人包括精神病患者,他们无视他人的感受,但足够了解他们以操纵他们,而许多人的缺陷是情境性的,包括尼日利亚骗子,他们认为任何上当受骗的白人都是活该因为他们必须是种族主义者,所以士兵和恐怖分子认为他们的对手不是人,或者在道义上应该死。我将在后面的第 26.4.2 节中更详细地讨论激进化。

第三条线索是自欺欺人。罗伯特·特里弗斯 (Robert Trivers) 认为,我们已经进化出欺骗自己的能力,以便更好地欺骗他人:“如果欺骗是动物交流的基础,那么必须有强大的选择来发现欺骗,而这反过来又应该选择一定程度的自我欺骗,使一些事实和动机成为无意识的,以免通过自我知识的微妙迹象背叛正在实施的欺骗”[904]。我们忘记了不便的事实,并将我们想要相信的事情合理化。从诚实的极客到拥有完全相信其产品的神奇能力的伟大推销员,自欺欺人的能力很可能各不相同。但这是有争议的,而且在很多层面上。例如,如果托尼·布莱尔在2003年劝说英国开战时真的相信伊拉克拥有大规模杀伤性武器,那么这到底是不是谎言?你如何定义真诚?你怎么能测量它?如果您预计他们无法对您撒谎,您甚至会选出一位国家领导人吗? [904] 中有一个冗长的讨论,并且辩论与其他关于动机推理的工作有关。 Russell Golman、David Hagman 和 George Loewenstein 对人们如何避免信息进行调查研究,即使信息是免费的并且可能导致更好的决策:有患病风险的人避免进行医学检查,管理人员避免可能表明他们做出错误决定的信息,当市场下跌时,投资者较少关注他们的投资组合 [781]。这方面的研究一直追溯到西格蒙德弗洛伊德,他描述了否认不愉快信息的各个方面,包括我们试图尽量减少对我们所做的坏事的内疚感,并为此责怪他人的方式.

它还与社交媒体上的过滤气泡效应相关联。人们更喜欢听别人证实他们的信念和偏见,这可以用信息的享乐价值来分析。人们认为自己是诚实的,并试图避免因偏差而导致的道德失调[172];犯罪学家使用中和一词来描述规则破坏者使用的策略,以尽量减少他们对自己行为的内疚感(过滤效应和自欺欺人有重叠)。进一步的联系是 Hugo Mercier 和 Dan Sperber 关于大脑作为论证机器的工作,我在上面提到过。

第四个线程是意图。在我们祖先的进化环境中,检测敌意是一件大事;在前国家社会中,也许四分之一的男人和男孩死于他杀,更早以前,我们的许多祖先都是被动物捕食者杀死的。因此,我们似乎已经进化出对声音和动作的敏感性,这些声音和动作可能表明人、动物甚至神的意图。

结果,我们现在在防御涉及敌对意图的威胁(例如恐怖主义)方面花费过多,而在防御

导致更多人死亡的流行病,或可能导致更多人死亡的气候变化。

我们可能想要更仔细地考虑意图还有其他原因。在密码学中,我们使用置信逻辑来分析认证协议的安全性,并处理诸如“Alice 相信 Bob 相信 Charlie 控制着密钥 K”这样的陈述;我们将在下一章中谈到这一点。现在我们意识到人们使用心智理论来相互理解,哲学家们也参与其中。丹·丹尼特从哲学中推导出意向立场,认为我们在推理时使用的命题态度 信念、欲望和感知 归结为人和动物的意图。

一个相关的问题是社会动机推理:如果问题被置于社会角色中,人们的逻辑会好得多。在 Wason 测试中,受试者被告知他们必须检查一些卡片,卡片的一面是字母等级,另一面是数字代码,并给出一个规则,例如“如果学生的卡片正面有 D 级,那么背面必须标有代码 3”。向他们展示四张显示(比如)D、F、3 和 7 的卡片,然后询问“您必须翻开哪些卡片来检查所有卡片是否标记正确?”大多数受试者都弄错了;在最初的实验中,96 名受试者中只有 48% 的人答对了 D 和 7。然而进化心理学家 Leda Cosmides 和 John Tooby 发现,如果将规则改为“如果一个人正在喝啤酒,他must be 20 years old and the persons are a beer drinker, a coke drinking, a 25-year-old and a 16-year old.现在四分之三的受试者推断保镖应该检查啤酒饮用者的年龄和 16 岁的饮料 [483]。 Cosmides 和 Tooby 认为,我们的逻辑能力,或许还有算术能力,是作为监管社会交流的一种手段而进化而来的。

下一个因素是合理化或最小化 人们为不良行为辩护或使他们的伤害看起来更小的过程。我提到了尼日利亚的骗子,他们认为上当受骗的白人一定认为非洲人很愚蠢,所以他们活该;诈骗者将外国目标视为公平游戏的例子还有很多。犯罪学家唐纳德·克雷西 (Donald Cressey) 提出了欺诈三角理论来解释导致欺诈的因素:除了动机和机会外,还必须有一个合理化。人们可能会觉得他们的雇主支付给他们的工资过低,因此有理由捏造开支,或者当他们偷税漏税时,国家在福利上浪费金钱。

最小化在网络犯罪中非常普遍。经营 DDoS 出租服务的孩子们互相保证提供“网络压力器”服务是合法的,并在他们的网站上表示该服务只能用于合法目的。因此,破坏最小化可以作为打击犯罪的工具。英国国家犯罪局购买了谷歌广告,以确保任何搜索网络压力服务的人都能看到 DDoS 是一种犯罪的官方警告。 2018 年 1 月至 6 月期间仅花费 3,000 英镑就抑制了需求增长; DDoS 收入在英国保持不变,而在美国有所增长 [454]。

最后,社会背景的丧失是网络去抑制的一个因素。人们在网上更坦率地说话,这既有积极的影响,也有消极的影响 。害羞的人可以找到伙伴,但我们也看到恶性的口水战。 John Suler 将这些因素分析为匿名性、隐形性、异步性以及权威和地位象征的丧失;此外还有与心理界限相关的影响

和自我想象,导致我们放松警惕,表达我们通常出于社会原因而控制的从喜爱到攻击的感受 [1845]。

所有这些导致在线欺骗的性质和规模可以通过适当的交互设计来调节。没有人像他们在 Facebook 上表现的那样快乐,没有人像他们在 Instagram 上表现的那样有魅力,也没有人像他们在 Twitter 上表现的那样愤怒。他们放松了对 WhatsApp 支持的封闭团体的警惕,这些团体既不提供名人来激发绩效,也不提供匿名来促进拖钓。然而,人们在封闭的群体中不那么挑剔,这使得他们更适合传播阴谋论和激进化 [523]。

3.2.5 启发式、偏见和行为经济学

自 2000 年代中期以来,安全研究人员应用的一个心理学领域是决策科学,它位于心理学和经济学的边界,研究人们在做出决策时使用的启发式方法以及影响他们的偏见。它也被称为行为经济学,因为它研究人们的决策过程偏离经济学家建模的理性行为的方式。 Herb Simon 是早期的先驱,他既是早期的计算机科学家,也是获得诺贝尔经济学奖的经济学家,他指出,经典理性意味着无论选择的计算有多难,都会做任何使您的预期效用最大化的事情。那么,在有限理性的现实世界中,人们会如何行事呢?从那以后,人类理性的真正局限性得到了广泛探索,丹尼尔·卡尼曼 (Daniel Kah neman) 因其在该领域的重大贡献（与已故的阿莫斯·特沃斯基 (Amos Tversky) 一起)于 2002 年获得诺贝尔经济学奖 [1004]。

3.2.5.1 前景理论与风险认知

Kahneman 和 Tversky 对人们在面对不确定性时如何做出决定进行了广泛的实验研究。他们首先开发了模拟风险偏好的前景理论:在许多情况下,人们不喜欢失去他们已经拥有的 100 美元,而不是他们更看重赢得 100 美元。将一项行动定义为避免损失可以使人们更有可能采取行动;网络钓鱼者通过发送诸如“您的 PayPal 帐户已被冻结,您需要单击此处解锁”之类的消息来诱骗他人。我们也不擅长计算概率,并使用各种启发式方法来帮助我们做出决定:

- 我们经常根据最初的猜测或比较做出判断,然后在需要时进行调整 锚定效应;
- 我们根据容易联想到的例子进行推论 可用性启发式,这对于 50,000 年前的狮子攻击是可行的,但当大众媒体用恐怖主义图像轰炸我们时却给出了错误的答案;
- 我们更可能对听到的事情持怀疑态度,而不是对看到的事情持怀疑态度,这可能是因为我们有更多的神经元处理视觉;
- 我们过于担心不太可能发生但影响非常大的事件
  结果;

· 我们更愿意相信自己解决的事情,而不是
比我们被告知的事情。

行为经济学不仅与计算人们点击网络钓鱼电子邮件中的链接的可能性有关,而且与更深层次的风险感知问题相关。许多人认为恐怖主义的威胁比流行病、道路交通事故甚至食物中毒要严重得多:这是错误的,但对行为经济学家来说不足为奇。我们高估了在恐怖袭击中死亡的小风险,不仅因为它很小,还因为 9/11 电视报道的视觉效果、记忆事件的容易程度、敌人袭击的愤怒以及效果否则我们会考虑并担心它。 （还有其他因素,我们将在第三部分讨论恐怖主义时探讨。）

对风险的误解是许多其他公共政策问题的基础。心理学家丹尼尔·吉尔伯特 (Daniel Gilbert) 在一篇题为“要是同性恋才导致全球变暖就好了”的挑衅性文章中,将我们对恐怖主义的恐惧与对气候变化的恐惧进行了比较。首先,我们进化到对敌对意图比对自然更加警惕； 100,000 年前,一个拿着棍子的人（或一头饥饿的狮子)比雷暴的威胁要严重得多。其次,全球变暖并没有侵犯任何人的道德感;第三,这是一个长期的威胁,而不是一个明确而现实的危险;第四,我们对环境的快速变化比缓慢变化更敏感 [764]。还有更多的风险偏见:当我们处于控制之中时,我们就不会那么害怕,比如开车时,而不是作为汽车或飞机上的乘客;我们更害怕不确定性,也就是说,当风险的大小未知时（即使它很小)[1671, 1675]。我们还沉迷于满足感,这意味着我们会寻求“足够好”的替代方案,而不是费力地尝试完美地计算出赔率,尤其是对于小额交易。 （这里的误解不是冒险者的误解,而是经济学家忽视了真实的人在他们的计算中包括交易成本这一事实。）

因此,从民间谚语“一鸟在手胜于二鸟在林”开始,我们可以开发出很多机器来帮助我们理解和模拟人们对风险的态度。

3.2.5.2 现时偏差和双曲线贴现

圣奥古斯丁有一句著名的祈祷:“主啊,让我贞洁,但还没有。”我们在应用安全更新时发现了类似的情绪,人们可能会更多地关注成本,因为它们在时间、存储和带宽方面是直接和确定的,而不是不可预测的未来收益。目前的这种偏见导致许多人拒绝更新,这是多年来在线技术漏洞的主要来源。软件公司的一种反击方式是允许人们延迟更新:Windows 具有“重启/选择时间/暂停”功能。提醒将忽略率从大约 90% 降低到大约 34%,并最终可能使整体合规性翻倍 [726]。更好的设计是让更新变得如此轻松,以至于它们可以成为强制性的,或者几乎是强制性的;这是现在一些网络浏览器和基于云的服务普遍采用的方法。

双曲线贴现是决策科学家用来量化当前偏差的模型。直觉推理可能会导致人们使用效用函数来大大降低未来的价值,以至于即时满足似乎是最好的行动方案,即使事实并非如此。这些模型已被用来试图解释隐私悖论 为什么人们在调查中说他们关心隐私,但在网上却表现得不一样。我在第 8.6.6 节中更详细地讨论了这一点:其他因素,例如风险的不确定性和隐私措施的有效性,也发挥了作用。总而言之,获得免费研究的直接和确定的积极效用超过了披露过多个人信息或将其披露给可疑网站的随机未来成本。

3.2.5.3 默认值和微调

这导致了默认值的重要性。许多人通常会选择最简单的方法并使用系统的标准配置,因为他们认为这已经足够好了。 2009 年,Richard Thaler 和 Cass Sunnstein 写了一本畅销书“Nudge”来探讨这一点,指出政府只需设定正确的默认值就可以在不侵犯个人自由的情况下实现许多政策目标 [1876]。例如,如果一家公司的员工默认参加了养老金计划,大多数人不会费心选择退出,而如果它是可选的,大多数人也不会费心选择加入。第二个例子是有更多的器官可供选择移植在西班牙,那里的法律允许使用死者的器官,除非他们反对,而不是在英国,捐献者必须主动同意。第三个例子是,让纳税人在开始填写表格时而不是最后填写时声明表格中的信息真实,可以减少逃税。人们必须做出的一系列选择、他们做出选择的顺序以及他们什么都不做时的默认设置,被称为选择架构。

Sunnstein 在奥巴马政府找到了一份工作,负责实施其中的一些想法,而 Thaler 则获得了 2017 年诺贝尔经济学奖。

默认值在安全方面也很重要,但它们通常是由对手设置的,目的是让你绊倒。例如,Facebook 默认为相当开放的信息共享,每当有足够多的人想出如何增加他们的隐私设置时,架构就会发生变化,因此您必须重新选择退出。这不仅利用了危险的默认设置,还利用了控制悖论 提供控制的错觉会导致人们分享更多信息。我们喜欢掌控一切;与让其他人驾驶我们乘坐飞机相比,我们驾驶自己的汽车感觉更舒服 即使后者安全一个数量级。 “隐私控制设置给了人们更多的上吊绳索,”行为经济学家乔治·洛文斯坦 (George Loewenstein) 说道。 “Facebook 已经解决了这个问题,因此他们为您提供了难以置信的精细控制。” [1533]

3.2.5.4 意向性的默认

行为经济学家遵循心理学的悠久传统,将心智视为由相互作用的理性和情感成分组成 “心”和“脑”,或“情感”和“认知”系统。发育生物学研究表明,从很小的时候开始,我们就有不同的心理处理系统来处理社会现象(例如识别父母和兄弟姐妹)和生理现象。

现象。保罗·布鲁姆 (Paul Bloom) 认为,它们之间的紧张关系解释了为什么许多人认为思想和身体基本上是不同的 [268]。孩子们试图用物理学来解释他们看到的东西,但当他们的理解力不足时,他们就会用有意的行为来解释现象。这对年轻人具有生存价值,因为它使他们倾向于从父母或其他成年人那里获得有关新奇自然现象的建议。布卢姆认为它有一个有趣的副作用 :它使人类倾向于相信身体和灵魂是不同的 ,从而为宗教信仰奠定了基础。这个论点可能不会压倒信徒(他们会反驳说布卢姆只是偶然发现了智能设计师创造的一种机制,使我们对他有信心)。但它可能与安全工程师有关。

首先,它在某种程度上解释了基本归因错误 人们经常犯错误,试图从意图而不是上下文来解释事物。其次,试图通过向用户传授互联网的血腥设计细节来遏制网络钓鱼 例如,告诉他们解析电子邮件中似乎来自银行的 URL 一旦他们感到困惑,其价值将是有限的。如果情绪被编程为在理性耗尽时接管,那么与网络钓鱼者进行技术指导和反指导的战争是不合理的,因为他们会做得更好。安全默认值会更好。

3.2.5.5 影响启发式

促使人们根据意图而不是机制来思考可以利用 Paul Slovic 及其同事 [1787] 探索的影响启发式。这个想法是,虽然人脑可以处理认知处理的多个线程,但我们的情绪仍然坚决保持单线程,并且它们在概率论方面的表现甚至不如我们大脑的理性部分。因此,通过突出情感,营销人员或欺诈者可以尝试让您使用情感而不是理性来回答问题,使用启发式而不是计算来回答问题。一个常见的技巧是问一个情绪化的问题(无论是“你上个月有多少次约会?”或者甚至是“你觉得特朗普总统怎么样?”)来让人们对概率不敏感。

因此,色情网站已被用来安装大量恶意软件,这不足为奇 教堂网站也是如此,这些网站通常维护不善且容易被黑客入侵。同样,引起恐惧的事件 从癌症到恐怖主义 不仅比赤裸裸的概率更能吓到人们,而且使这些概率更难计算,甚至阻止人们做出努力。

其他可以加强我们通过意图解释事物的倾向的因素包括认知超载,大脑的理性部分只会感到疲倦。我们的自我控制能力也容易疲劳,无论是身体上还是精神上;一些心算会增加我们拿起巧克力而不是苹果的可能性。因此,建立繁忙网站的银行可能会销售更多人寿保险,但也可能使其客户更容易受到网络钓鱼的攻击。

3.2.5.6 认知失调

社会心理学的另一个有趣分支是认知失调理论。
当人们持有不同的观点时,他们会感到不舒服;他们寻求能够证实他们对世界和他们自己的现有观点的信息,并试图拒绝与他们的观点相冲突或可能损害他们自尊的信息。一个实际的结果是,面对越来越多的事情已经出错的证据,人们非常能够坚持错误的行动方针 [1863]。向自己或他人承认你被骗了可能会很痛苦;骗子知道这一点并加以利用。安全专业人员应该“感受喧嚣” 也就是说,要警惕最近建立的社交线索和期望让您处于压力之下而“只做”您通常会有所保留的事情的情况。是时候退后一步,问问自己是否被占有了。但是训练人们认识到这一点已经够难的了,要让普通人打破社会潮流并说“停止!”很难。已经进行了一些实验,例如培训卫生服务人员不要在电话中透露健康信息,以及培训妇女自卫班的人员抵制要求提供额外个人信息的要求。将此类培训纳入主流的问题在于,可用于培训的资金比以吸引客户为商业模式的公司的营销预算要少几个数量级。

3.2.5.7 风险恒温器

关于人们如何管理他们的风险敞口,已经进行了一些有趣的实证研究。约翰·亚当斯 (John Adams) 研究了强制性安全带法律,并确定它们实际上并不能挽救生命:它们只是将伤亡从车辆乘员转移到行人和骑自行车的人 [20]。安全带让司机感觉更安全,所以他们开得更快,以便将他们感知到的风险恢复到之前的水平。他将此称为风险恒温器,该模型也在其他应用中得到证实 [19]。经验教训是测试需要具有生态有效性:您需要在尽可能现实的环境中评估拟议干预措施的效果。

3.3 欺骗实践

这使我们从理论走向实践。欺骗通常涉及滥用合规专业人员开发的技术 这些人的工作是让其他人做事。销售主管可能会向您提供度假公寓的财务计划,让您眼花缭乱;警察可能会在场时提醒您小心驾驶;公园管理员可能会告诉您小心扑灭篝火,不要喂熊,并且公司律师可能会威胁您从您的网站上删除某些内容。

行为经济学的先驱和“助推”的倡导者迪克·塞勒 (Dick Thaler) 将行为经济学的自私使用称为“污泥” [1875]。但奇怪的是,经济学家们曾认为这种技术的利他用途比自私的用途更为普遍。营销人员不仅要推动

最有利可图的选择而不是最佳价值,但他们也使用所有其他可用的技巧。斯坦福大学的说服技术实验室一直走在开发让人们沉迷于屏幕的技术的前沿,他们的一位校友、前谷歌员工特里斯坦哈里斯 (Tristan Harris) 已成为直言不讳的批评者。有时被称为“硅谷的良心”,他解释了技术如何通过操纵默认和选择来赚钱,并询问如何在道德上做到这一点 [867]。手机和其他屏幕显示菜单,从而控制选择,但不仅如此。屏幕成为主流的两种技术是赌场使用间歇性可变奖励来制造成瘾的技术(我们每天检查手机 150 次,看看是否有人给予了我们关注)和无底消息馈送(让我们即使在我们不再饿了)。但是有许多早于计算机的旧技术。

3.3.1 推销员和骗子

欺骗是营销的孪生兄弟,所以一个起点是关于销售技巧的大量文献。一位著名的作家是心理学教授罗伯特·西奥迪尼 (Robert Cialdini),他从事暑期工作,销售从二手车到家居装修和人寿保险的各种商品,以记录交易技巧。他的著作《影响力:科学与实践》被销售专业人士广泛阅读,描述了用于影响人们和完成销售的六大类主要技术 [424]。

这些是:

1. 互惠:大多数人觉得需要回报;

2. 承诺和一致性:如果人们觉得自己前后矛盾,就会出现认知失调;

3.社会证明:大多数人都希望得到别人的认可。这意味着在他们所属的群体中跟随他人,群体越小,压力越大;

4. 喜欢:大多数人都想做好看或讨人喜欢的事情
人问;

5.权威:大多数人都对权威人物恭敬(回想一下上面提到的米尔格拉姆研究);

6. 稀缺性:我们害怕错过,如果我们可能想要的东西可以
突然不可用。

所有这些都是心理现象,是持续研究的主题。它们也可以追溯到我们祖先进化环境中的压力,食物短缺是一个真正的威胁,陌生人可能是危险的,群体团结一致反对他们(以及提供食物和住所)是至关重要的。所有这些都在我们经常遇到的广告和其他消息中重复使用。

Frank Stajano 和 Paul Wilson 在此基础上分析了骗局背后的原理。威尔逊研究并出现在九季关于最常见骗局的电视节目中 “真正的骗局” 这些骗局将对毫无戒心的公众实施,然后他们会被退还他们的钱,听取汇报并请求视频许可在电视上使用的镜头。多年来在数千个标记上进行数百次欺诈试验的专业知识被提炼为以下七项原则 [1820]。

1. 分心 – 欺诈者将注意力集中在错误的事情上。这是大多数魔术表演的核心。

2. 社会合规 社会训练我们不要质疑看似有权威的人,让人们容易受到假装来自银行或警察的骗子的攻击。

3. 从众原则 当周围的每个人似乎都承担同样的风险时,人们就会放松警惕。这是三张牌骗局的中流砥柱,也是社交网络上越来越多的骗局。

4. 不诚实 如果标记做一些狡猾的事情,他们就不太可能抱怨。许多人被“你得到一笔好交易,因为它是非法的”这一想法所吸引,整个骗局家族 例如转售以欺诈手段获得的机票 都以此为契机。

5. 仁慈 这是不诚实的反面,是对 Cialdini 互惠原则的改编。许多社会工程诈骗都依赖于受害者的帮助,从尾随进入建筑物到打电话诉说悲伤的故事以要求重设密码。

6. 需求和贪婪 销售培训师告诉我们,我们应该找到某人真正想要的东西,然后告诉他们如何得到它。一个好的骗子可以帮助商标做一个梦,并以此来榨取他们的钱。

7. 时间压力 这会导致人们本能地行动而不是停下来思考。普通营销人员一直使用这个(“这个价格只剩下 2 个席位”);骗子也是如此。

与 Cialdini 原则的关系应该是显而易见的。愤世嫉俗者可能会说欺诈只是营销的一个分支;或者,随着营销变得越来越激进,它看起来越来越像欺诈。在调查在线住宿诈骗时,我们发现很难对检测器进行编码,因为许多房地产经纪人都使用相同的技术。事实上,Cialdini 的模型已经很好地描述了欺诈者的行为,除了骗子增加了对同情的诉求、建立自己可信度的论据以及处理异议的方式 [2062]。 (这些也可以在常规营销文献的其他地方找到。)

哦,我们在软件中也发现了同样的情况,非法恶意软件和几乎合法的“潜在有害程序”(PUP) 之间存在模糊的分界线,例如用不同的广告替换您的广告的浏览器插件。一个很好的区分点似乎是技术性的:恶意软件由许多小型

僵尸网络,因为有被捕的风险,而 PUP 主要由一个大型网络分发 [954]。但骗子也使用常规的营销渠道:Ben Edelman 在 2006 年发现,虽然在网络搜索中排名靠前的公司中有 2.73% 是糟糕的,但在搜索广告中出现的公司中有 4.44% 是糟糕的 [612]。不良公司也更有可能展示廉价的信任信号,例如他们网站上的 TRUSTe 隐私证书。同样,假房东经常向潜在租户发送推荐信甚至身份证复印件,而真正的房东绝不会这样做。

然后是“合法”企业的欺骗性营销做法。仅举众多研究中的一项,Arunesh Mathur 及其同事在 2019 年对 11,000 个购物网站进行了爬取,发现了 1,818 个“黑暗模式”实例 操纵性营销行为,例如隐藏订阅、隐藏成本、压力销售、潜入购物篮策略和强制开户。其中至少有 183 个明显具有欺骗性 [1242]。更重要的是,不良网站名列前茅;也许您访问的网站中有四分之一到三分之一(按流量加权)试图催促您。这种来自刚好接近欺诈起诉门槛的诈骗的持续压力通常会对信任产生寒蝉效应。如果安全警告与营销混在一起,或者以任何方式带有营销的味道,人们就不太可能相信它们。我们甚至看到对软件更新失去了一些信任;人们在调查中说,与安全补丁相比,他们不太可能应用安全增强功能升级,尽管有关升级的现场数据(还)没有显示出任何差异 [1591]。

3.3.2 社会工程学

通过操作系统的人入侵系统并不新鲜。军事和情报机构总是以对方的工作人员为目标 ;旧苏联的大部分情报成就都是这种类型的[118]。私人调查机构也不甘落后。

20 世纪下半叶,调查记者、私家侦探和诈骗犯将虚假电话发展成为一种介于工业流程和艺术形式之间的东西。工业过程的一个例子是私家侦探如何追踪英国的人。鉴于该国拥有每个人都已注册的国家医疗服务体系,诀窍是给你认为目标所在地区有权访问行政系统的人打电话,假装是医疗服务部门的其他人,然后询问。1996 年,我的同事在英国进行了一项实验,他们培训当地卫生部门的工作人员识别和报告此类呼叫1。

他们每周检测到大约 30 次虚假借口电话,这将增加到每周 6000 次或整个英国每年 300,000 次。这最终得到了某种程度的修复,但花了十多年的时间。真正的解决办法不是隐私法的执行,而是管理员只是停止接听电话。

另一个来自 20 世纪的古老骗局是窃取某人的 ATM 卡,然后假装来自银行打电话给他们,询问他们的卡是否被盗。听到它有,骗子说 我们认为是这样。请

1本书第二版第 9 章详细讲述了这个故事,可在线免费获取。

现在就告诉我你的密码,这样我就可以进入系统并取消你的卡。最近增长最快的变种是“授权推送支付”，骗子再次假装来自银行,并说服客户转账到另一个账户,通常是通过让客户对银行的身份验证程序感到困惑，这最反正顾客觉得很神秘2。

至于艺术形式,有史以来最令人不安的安全书籍之一是凯文·米特尼克 (Kevin Mitnick) 的“欺骗艺术”。米特尼克因闯入美国电话系统而被捕并被定罪,他在出狱后讲述了他几乎所有的攻击都涉及社会工程。他典型的技巧是向电话公司的员工假装他是同事,并寻求“帮助”,例如密码。通过公司总机并赢得人们信任的方法是销售培训课程的主要内容,而黑客则直接应用这些内容。自称是 CEO 的私人助理的人会因为一些琐碎的事情打电话给一个受到骚扰的系统管理员一两次;一旦这个想法被接受,来电者就会要求老板提供一个新密码。米特尼克成为使用此类技巧来破坏公司安全程序的专家,他的书讲述了一系列引人入胜的攻击[1325]。

社会工程学在 2006 年 9 月成为世界头条新闻,当时惠普女董事长帕特里夏邓恩聘请了私家侦探,这些私家侦探使用借口获取她怀疑的其他董事会成员和她认为有敌意的记者的电话记录。

她被迫辞职。这些侦探被判犯有欺诈性有线通信罪,并被判处社区服务 [138]。同年,英国隐私当局起诉了一家私人侦探机构,该机构为顶级律师事务所提供借口工作 [1138]。

随着对社会工程学的宣传越来越多,2007 年财政部税务总监察长对 IRS 进行了一次审计,其工作人员打电话给 102 名 IRS 各级员工,询问他们的用户 ID,并告诉他们更改密码以已知值； 62 人这样做了。更糟糕的是,尽管在 2001 年和 2004 年进行了类似的审计测试,但这种情况还是发生了 [1673]。从那时起,许多审计公司提供了社会工程服务;他们对他们的审计客户进行网络钓鱼以表明这有多么容易。自 2010 年代中期以来，人们开始反对这种做法,因为它会在不改变行为的情况下给员工带来很多困扰 。

社会工程不仅限于窃取私人信息。它也可以是关于让人们相信虚假的公共信息。本章开头 Bruce Schneier 的话出现在一篇关于股票骗局的报告中,一篇虚假的新闻稿称一家公司的首席执行官已经辞职,其收益将被重述。几家通讯社转告了此事,股价下跌了 61%,直到骗局被曝光 [1670]。这种假新闻一直存在,但互联网让它更容易传播,社交媒体似乎也让它无处不在。当我在第 26.4 节讨论审查制度时,我们将重新讨论这个问题。

2在极少数情况下,客户会使银行感到困惑； 2019 年的一项创新是“callham mer”攻击,有人反复打电话来“纠正”“他的名字”的拼写,并将其一次一个字符更改为另一个字符。

3.3.3 网络钓鱼

虽然基于电话的社会工程是 20 世纪最受欢迎的策略,但在线网络钓鱼似乎已取代它成为 21 世纪的主要策略。
操作员包括间谍和骗子,而目标是您的员工和客户。训练你的员工已经够难的了;培训普通客户就更难了。他们会假设您在试图哄骗他们,忽略您的警告,只是想出最简单的方法来从您的系统中获得他们想要的东西。你不能简单地为平均水平设计。如果英语说得不好、有阅读障碍或有学习障碍的人使用您的系统不安全,那么您就是在自找严重的法律麻烦。因此,使用您的系统最简单的方法最好是最安全的。

“网络钓鱼”一词出现在 1996 年的 AOL 密码被盗事件中。到那时,试图破解电子邮件帐户以发送垃圾邮件的尝试已经非常普遍,以至于 AOL 在其网页上有一个“报告密码请求”按钮;第一次提到“密码钓鱼”是在 1990 年,人们通过修改终端固件来收集 Unix 登录密码 [443]。同样在 1996 年,Tony Greening 报告了一项系统的实验研究:向悉尼大学的 336 名计算机科学专业的学生发送了一封电子邮件,要求他们提供密码,借口是在疑似破解后需要“验证”密码数据库-在。其中 138 个返回了有效密码。有些人表示怀疑:30 人返回了一个看似合理但无效的密码,而超过 200 人在没有官方提示的情况下更改了密码。

但他们中很少有人向当局报告了这封电子邮件 [812]。

七年后的 2003 年,针对银行的网络钓鱼攻击开始了,据报道有六次尝试 [441]。早期的攻击模仿银行网站,但既粗暴又贪婪;攻击者要求提供各种信息,例如 ATM PIN,他们的电子邮件也是用糟糕的英语写的。大多数顾客闻到了老鼠的气味。到 2008 年左右,攻击者学会了使用更好的心理;他们经常重复使用真正的银行电子邮件,只是更改了 URL,或者发送一封电子邮件,上面写着类似“感谢您向您的 PayPal 帐户添加新电子邮件地址”之类的内容,以激起客户登录并抱怨他们没有这样做。当然,使用提供的链接而不是输入 www.paypal.com 或使用现有书签的客户将被清空他们的帐户。到那时,国家行为者也开始使用网络钓鱼;我在第 2.2.2 节中描述了中国情报部门如何在 2008 年奥运会期间侵入达赖喇嘛的私人办公室。他们使用了最初由俄罗斯欺诈团伙使用的犯罪软件工具,他们似乎认为这让他们事后可以推诿。

欺诈损失迅速增长,但到 2015 年左右稳定下来。一些反措施帮助控制了事情,包括更复杂的登录方案(使用双因素身份验证,或其低成本表亲,要求密码中的一些随机字母);转向能更好地过滤垃圾邮件的网络邮件系统;以及寻找提现模式的后端欺诈引擎。竞争格局很严峻,因为网络钓鱼者会在每个国家/地区随时攻击最容易的目标,无论是窃取客户凭证还是使用他们的账户洗钱。集中损失导致目标醒来并采取行动。从那时起,我们看到了大

对亚马逊等非金融公司的大规模攻击;在 2000 年代后期,骗子会更改您的电子邮件和街道地址,然后使用您的信用卡订购宽屏电视。大约从 2016 年开始,活动就以礼券形式出现。

正如我们在上一章中提到的,网络钓鱼还被僵尸网络大师大规模使用,以招募新机器到他们的僵尸网络,并且被针对特定个人或公司的骗子以及情报机构以有针对性的方式使用。大规模攻击之间存在很大差异 ,在这种攻击中,从经济学角度来看,为僵尸网络招募一台新机器的成本最多可能只有几美分,而在有针对性的攻击中,间谍可能会花费数年时间试图破解手机竞争对手的政府首脑或精明的骗子可能会花费数周或数月的时间跟踪首席财务官,以期获得巨额回报。使用的诱饵和技术是不同的,即使安装在目标笔记本电脑或手机上的犯罪软件来自同一个稳定的。 Cormac Herley 认为,有针对性的犯罪和大规模犯罪的经济学之间的鸿沟是网络犯罪并不比现在严重得多的原因之一 [887]。毕竟,鉴于我们依赖计算机,所有计算机都是不安全的,而且攻击无时无刻不在,文明怎么还没有崩溃呢?网络犯罪并不总是像看起来那么容易。

另一个因素是创新的开发和传播需要时间。我们注意到,坏人用了七年时间才赶上 Tony Greening 1995 年的网络钓鱼工作。作为另一个例子,Tom Jagatic 及其同事在 2007 年发表的一篇论文展示了如何使用从目标社交网络中挖掘的上下文自动个性化每个网络钓鱼,从而使网络钓鱼更加有效 [971]。我在本书的第二版中引用了这一点,并且在 2016 年我们在野外看到了它:一个团伙向在公司财务部门工作的个人发送了数十万个带有美国和澳大利亚银行木马的网络钓鱼,并附上他们的姓名和职位显然是从 LinkedIn [1297] 中删除的。这似乎很粗鲁,并没有真正流行起来,但一旦坏人发现了这一点,我们将来可能会看到大规模的鱼叉式网络钓鱼,想想我们会如何应对是很有趣的。我们看到的其他个性化批量诈骗是勒索尝试,受害者收到电子邮件声称他们的个人信息已被泄露,并包括密码或信用卡号的最后四位数字作为证据,但此类诈骗的收益似乎很低.

在我撰写本文时,犯罪团伙越来越多地使用鱼叉式网络钓鱼来对安装勒索软件、窃取礼券和发起其他诈骗的公司进行有针对性的攻击。 2020 年,一群年轻人入侵了 Twitter,超过 1000 名员工可以使用内部工具控制用户帐户;该团伙从比尔·盖茨、巴拉克·奥巴马和埃隆·马斯克等知名用户的账户发送比特币诈骗推文 [1292]。

他们似乎已经在 SIM 交换欺诈方面磨练了鱼叉式网络钓鱼技巧,我将在后面的 3.4.1 和 12.7.4 节中讨论。这种“可转移技能”在骗子中的传播在许多方面类似于主流技术的采用。

3.3.4 操作安全

让你的员工抵制外人通过电话或在线诱使他们泄露机密的企图,这在军事界被称为操作安全或 Opsec。保护真正有价值的秘密,例如未公布的财务数据、尚未获得专利的工业研究和军事计划,取决于限制可以访问的人数,以及关于可以与谁讨论什么以及如何讨论的原则。仅仅存在规则是不够的;你必须培训有权访问的员工,解释规则背后的原因,并将他们融入组织中。在我们的医疗隐私案例中,我们对医疗服务人员进行了有关借口电话的教育,并制定了严格的回拨政策:他们不会在电话中讨论医疗记录,除非他们拨打了从医疗服务内部电话簿中获得的号码,而不是来自来电者。一旦工作人员检测到并打败了一些假借口电话,他们就会谈论它,并且信息会嵌入每个人的工作方式中。

另一个例子来自一家大型硅谷服务公司,当外人尾随员工进入校园建筑物时,该公司遭到入侵企图。

用机场式的身份证检查,甚至刷卡激活的十字转门来阻止这种情况,会改变氛围并与文化发生冲突。解决方案是创建并嵌入一个社会规则,即当有人为您打开大楼门时,您向他们展示您的徽章。与虚假电话一样,关键因素是社会嵌入,而不仅仅是培训。

最难教育的人往往是资历最深的人;一家咨询公司向 500 家上市公司的财务总监发送了一个 USB 记忆棒,作为匿名邀请的一部分,上面写着“让您有机会参加终生难忘的聚会”,其中 46% 的人将其放入他们的计算机中 [1031]。根据我自己在银行业的经验,你无法培训的是那些薪水比你高的人,比如交易室的交易员。

一些操作安全措施是常识性的,例如不要将敏感文件扔进垃圾桶。不太明显的是需要培训您信任的人。令人尴尬的电子邮件泄露似乎来自英国首相托尼·布莱尔的办公室,最初被归咎于“黑客”,结果被一名私人侦探从他私人民意测验专家家中的垃圾桶中捞出 [1208]。

人们以他们必须的方式操作系统,这通常意味着为了完成他们的工作而打破一些规则。研究表明,公司员工只有这么多的合规预算,也就是说,他们只准备每年将这么多时间投入到显然不能帮助他们实现目标的任务上 [196]。你需要弄清楚这个预算是多少,并明智地使用它。如果有一些信息你不希望你的员工被欺骗泄露,那么设计系统更安全,这样他们就不能泄露它,或者至少让披露涉及与其他员工交谈或跳过其他篮球。

但是公司的客户呢?网络钓鱼者有很大的空间可以简单地命令银行客户泄露他们的安全数据,而且这种情况会大规模发生,针对零售和企业客户。还有许多

客户在发现您的业务流程中存在漏洞时尝试进行的小骗局。我将在有关银行业务和簿记的章节中进一步讨论这两种类型的欺诈。

3.3.5 欺骗研究

最后,谈谈欺骗研究。自 9/11 以来,政府投入了大量资金试图寻找更好的测谎仪,欺骗研究人员获得了大约五个不同的心理学分支学科的资助。

测谎仪通过心率和皮肤电导测量压力;它自 1920 年代以来一直存在,并被美国一些州用于刑事调查,以及被联邦政府用于筛选人员以获得绝密许可。关于其有效性的证据充其量是零散的,并且由 Aldert Vrij [1970] 进行了广泛的调查。虽然它可以成为熟练审讯者手中的有效道具,但关键因素是技能而不是道具。当在实验室环境中由不熟练的人使用时,针对说低风险谎言的实验对象,它的输出比随机好不了多少。除了通过皮肤电导测量压力外,您还可以通过眼球运动测量分心,通过上半身运动测量负罪感。在与 Sophie van der Zee 合作的一个研究项目中,我们使用了身体动作捕捉服以及 Xbox 中的手势识别摄像头,得到的结果略好于测谎仪 [2063]。然而,此类技术充其量只能增强审讯者的技能,声称它们运作良好应被视为垃圾科学。值得庆幸的是,政府想要一个有效的审讯机器人的梦想在某种程度上已经实现了。

处理欺骗的第二种方法是根据真实客户行为训练机器学习分类器。这就是自 1990 年代后期以来信用卡欺诈引擎一直在做的事情,最近的研究也已扩展到其他领域。例如,Noam Brown 和 Tuomas Sandholm 创造了一个名为 Pluribus 的扑克游戏机器人,它在为期 12 天的 10,000 手德州扑克马拉松比赛中击败了十几名专家玩家。它不使用心理学,而是使用博弈论,与自己对弈数百万次,并追踪对本可以带来更好结果的出价的后悔。它可以在没有获得对手的面部表情或肢体语言等“信息”的情况下始终击败专家,这本身就说明了问题。使用统计机器学习而不是生理监测来处理欺骗也可能被认为较少侵犯隐私。

3.4 密码

密码管理为可用性、应用心理学和安全性提供了一个有指导意义的环境。也许自 1970 年代以来,密码一直是安全工程师面临的最大实际问题之一。事实上,正如可用性研究员 Angela Sasse 所说,鉴于我们对人类记忆的了解,很难想到比密码更糟糕的身份验证机制:人们无法记住不常使用或经常更改的项目;我们不能忘记按需;回忆比识别更难;没有意义的词更难理解。

为了将问题放在上下文中,大多数要求您设置的密码都不是

为了你的利益,但为了别人的利益。现代媒体生态系统由寻求最大化其页面浏览量和注册用户群的网站驱动,以便在出售时最大化其价值。这就是为什么当你看到一篇令人讨厌的新闻文章时,你觉得你必须发表评论,你发现你必须注册。点击,出现一页广告。使用电子邮件地址填写表格并提交。验证码错误,所以再做一次,看到另一页广告。单击电子邮件链接,然后查看带有另一个广告的页面。现在您可以添加一条没人会读的评论。在这种情况下,您最好输入随机垃圾并让浏览器记住它;或者更好的是,不要打扰。即使是主要的新闻网站也使用密码来违背读者的利益,例如限制您每月获得的免费页面浏览量,除非您使用不同的浏览器再次注册。Ryan Holiday [913] 详细描述了这个生态系统。

现在转向更诚实的用途,一个大公司使用的密码系统
现代服务公司有许多组成部分。

1. 可见部分是登录页面,注册时会要求您选择一个密码,并可能以某种方式检查其强度。以后每当您登录时,它都会要求您提供此密码。

2. 将有恢复机制使您能够处理忘记的 10 个密码甚至被盗用的帐户,通常是通过询问进一步的安全问题,或通过您的主要电子邮件帐户,或通过向您的手机发送短信。

3. 这背后是密码检查的技术协议机制,通常是当您在笔记本电脑或手机上输入密码时对密码进行加密的例程,然后将其与本地加密值进行比较,或将其带到远程服务器进行检查。

4. 通常有跨多个平台同步密码的协议机制,所以如果你在笔记本电脑上更改密码,你的手机将不允许你使用该服务,直到你在那里输入新密码。

   这些机制可以让您将被盗手机列入黑名单,而无需为它能够访问的所有服务重置密码。

5. 如果您的某个密码被用在不该用的地方,将会有入侵检测机制传播警报。

6. 许多网站都使用单点登录机制,就像您使用 Google 或 Facebook 帐户登录报纸一样。

让我们从底部开始。开发功能齐全的密码管理系统可能需要大量工作,而且为密码恢复提供支持也需要花费金钱(几年前,英国电话公司 BT 的密码重置中心有 200 名员工)。因此,外包“身份管理”具有商业意义。此外,入侵检测在规模上效果最好:如果有人在秘鲁的一家网吧使用我的 gmail 密码,而谷歌知道我在苏格兰,他们会向我的手机发送短信进行检查,而小型网站无法做到这一点.企图滥用密码的主要原因是一家公司遭到黑客攻击,泄露了数百万个电子邮件地址和密码,这很糟糕

伙计们去别处试试;大公司很快发现这一点,而小公司则不会。大公司还通过提醒您从新设备或陌生地方登录来帮助他们的客户保持态势感知。同样,如果您是一个小型网站或人们不常访问的网站,则很难做到这一点。

至于在设备之间同步密码,只有设备厂商才能真正做好;下一章将讨论加密传输到验证密码的服务器的密码的协议机制。这将我们带到密码恢复。

3.4.1 密码找回

2010 年代的经验是,随着大型服务公司的规模扩大以及人们大量转向智能手机,密码恢复通常是身份验证中最难的方面。如果您认识的人(例如您的员工)忘记了密码,您可以让他们与认识他们的管理员或经理互动。但对于您不认识的人(例如您的在线客户)来说,这就更难了。由于一家大型服务公司每天要恢复数以万计的帐户,因此在绝大多数情况下,您需要某种无需人工干预的方法。

在 1990 年代和 2000 年代,许多网站使用“安全问题”来恢复密码,例如询问您最喜欢的球队、您宠物的名字,甚至是您母亲的娘家姓。这种近乎公开的信息通常很容易被猜到,因此与猜测密码本身相比,它提供了一种更容易侵入账户的方法。每个人都问同样的问题,这让情况变得更糟。对于名人 或被前亲密伴侣虐待 可能没有可用的秘密。这在 2008 年被公之于众,当时一名学生通过密码恢复问题 她的出生日期和她第一所学校的名称 入侵了美国副总统候选人莎拉佩林的雅虎电子邮件帐户。这两个都是公开信息。从那时起,骗子就学会了在可能的时候使用安全问题来抢劫帐户;在美国社会保障局,一个常见的欺诈行为是为过去通过普通邮件处理养老金的养老金领取者开设一个在线账户,并将付款重定向到不同的银行账户。这在 2013 年达到顶峰;解决这个问题的对策是始终通过蜗牛邮件将帐户变更通知受益人。

2015 年,五位谷歌工程师发表了对安全问题的全面分析,其中许多被证明是极其脆弱的。例如,攻击者可以针对“最喜欢的食物?”获得 19.7% 的成功率。用英语讲。大约 37% 的人提供了错误的答案,在某些情况下是为了让他们变得更强大,但有时却不是。整整 16% 的人的答案是公开的。除了不安全之外,“安全问题”被证明很难使用:40% 的美国英语用户在需要时无法回忆起答案,而使用短信重置代码可以恢复帐户的人数是其两倍 [291] .

鉴于这些安全性和可记忆性问题,大多数网站现在都允许您通过向您最初注册时使用的地址发送电子邮件来恢复密码。但是,如果有人破坏了该电子邮件帐户,他们也可以获得您所有的依赖帐户。电子邮件恢复对于网站来说可能就足够了

在妥协影响不大的情况下,但对于重要的账户 例如银行和电子邮件本身 现在的标准做法是使用第二个因素。
这通常是通过短信发送到您手机的代码,或者更好的是使用可以加密代码并将其绑定到特定手机的应用程序。许多允许电子邮件恢复的服务提供商正在促使人们尽可能使用此类代码。谷歌研究表明,SMS 阻止了机器人的所有批量密码猜测、96% 的批量网络钓鱼和 76% 的针对性攻击 [574]。

但这取决于电话公司对谁可以获得重新放置的 SIM 卡的照顾,而许多人则没有。 2020 年的问题是基于拦截 SMS 验证码的攻击快速增长,其中大多数似乎涉及 SIM 交换,攻击者假装是您到您的移动电话公司并为您的帐户更换 SIM 卡。 SIM 交换攻击于 2007 年在南非开始,成为尼日利亚银行欺诈的主要形式,然后在美国流行起来 最初是作为接管有价值的 Instagram 账户的一种手段,然后是在比特币交易所抢劫人们的账户,然后是为了银行欺诈更普遍 [1092]。我将在 12.7.4 节中更详细地讨论 SIM 交换攻击。

攻击者还利用 SS7 信令协议远程窃听目标的手机并窃取代码 [489]。我将在有关电话和银行业务的章节中更详细地讨论此类攻击。军备竞赛的下一步是将客户从用于身份验证和帐户恢复的短信转移到应用程序;同样的谷歌研究表明,这将最后两个数字提高到 99% 的批量网络钓鱼和 90% 的针对性攻击 [574]。至于有针对性的攻击,Ariana Mirian 与加州大学圣地亚哥分校和谷歌的同事进行的其他研究接触了在网上宣传“黑客雇佣”服务并要求他们钓鱼 Gmail 密码的团伙。其中三个团伙成功了,通过中间人攻击击败了基于 SMS 的 2fa;取证随后发现,在 2018 年 3 月至 10 月期间,从相同的 IP 地址对 Gmail 用户进行了 372 次其他攻击 [1322]。这仍然是一个不成熟的犯罪市场,但要阻止此类攻击,应用程序或身份验证令牌是必经之路。它还引发了有关帐户恢复的进一步问题。如果我在 Gmail 上使用硬件安全密钥,我是否需要在保险箱中使用第二个密钥作为恢复机制? （大概。）

如果我在手机上使用一个应用程序进行银行业务,而另一个应用程序用作身份验证器,我是否遵守双因素身份验证规则? （参见关于银行业务的章节中的第 12.7.4 节。）

默认情况下,电子邮件通知不仅会告诉人们可疑的登录尝试,还会告诉人们在代码的帮助下成功登录了新设备。这样,如果有人在您的手机上植入恶意软件,您就有机会检测到它。那么受害者如何康复是下一个问题。如果一切都失败了,服务提供商可能最终会让他们与真人交谈。

但是在设计这样一个系统时,永远不要忘记它的强大程度取决于最弱的回退机制 无论是与您无法控制的电子邮件提供商的恢复电子邮件循环、容易受到 SIM 卡交换或移动恶意软件攻击的电话代码,还是对社会工程学持开放态度的人。

3.4.2 密码选择

许多帐户因猜测 PIN 或密码而受到威胁。正如我在 2.3.1.4 中所述,有僵尸网络不断通过猜测密码和密码恢复问题侵入在线帐户,以便使用电子邮件帐户发送垃圾邮件和招募机器到僵尸网络。随着人们发明新服务并为其设置密码,密码猜测者找到了新的目标。最近的一个例子是加密货币钱包:一个匿名的“比特币强盗”通过尝试使用以太坊钱包的大量弱密码成功窃取了 5000 万美元 [809]。与此同时,由于忘记密码,价值数十亿美元的加密货币已经丢失。所以密码很重要,基本上有三个广泛的问题,按重要性和难度的升序排列:

1. 用户是否会以足够高的概率正确输入密码?
2. 用户会记住密码,还是必须写下密码
   还是选择一个容易被攻击者猜到的?
3. 用户将密码泄露给第三方是否会破坏系统安全,无论是无意的、故意的还是欺骗的结果?

3.4.3 可靠密码输入难点

第一个人为因素问题是,如果密码太长或太复杂,用户可能难以正确输入。如果他们尝试执行的操作很紧急,这可能会带来安全隐患。如果客户在输入软件产品激活码时遇到困难,这可能会给您的支持台带来昂贵的呼叫费用。 2010 年代从笔记本电脑到智能手机的转变使得诸如“至少一个小写字母、大写字母、数字和特殊字符”之类的密码规则变得非常繁琐和烦人。这是促使人们采用更长但更简单的秘密的因素之一,例如三四个单词的密码。但是人们能够在不犯太多错误的情况下输入它们吗?

对许多欠发达国家用于售电的 STS 预付费电表进行了一项有趣的研究。客户将一些钱交给销售代理,并在收据上打印出一个 20 位数字。他们将这张收据带回家,在仪表的键盘上输入数字,然后灯亮了。 STS 的设计者担心,由于很多人是文盲,而且人们可能会在输入数字时中途迷路,因此系统可能无法使用。但文盲不是问题:即使是不识字的人也不会对数字感到困难(正如一位工程师所说,“每个人都可以使用电话”)。最大的问题是输入错误,这些是通过将 20 位数字打印成两行来解决的,第一行中有三组四位数字,然后是第二行中的两个 [93]。我将在 14.2 节中对此进行详细描述。

一个完全不同的应用是美国核武器的发射代码。
这些仅包含 12 个十进制数字。如果使用它们,操作员将承受极大的压力,并且可能使用即兴或过时的通信渠道。实验表明,12 位数字是最大的

在这种情况下可以可靠地传送。我将讨论这在 15.2 中是如何演变的。

3.4.4 密码难记

我们的第二个心理问题是人们经常发现密码很难记住 [2076]。 12 到 20 位数字可能很容易从电报或电表票中复制,但是当客户需要记住密码时,他们要么选择攻击者容易猜到的值,要么将它们写下来,或者两者兼而有之。事实上,标准的密码建议可以概括为:“选择一个你不记得的密码,也不要把它写下来”。

问题不仅限于计算机访问。例如,法国的一家连锁经济型酒店引入了自助服务。你会出现在酒店,在接待机器上刷你的信用卡,然后得到一张带有数字访问密码的收据来打开你的房间门。为了降低成本,房间没有连接浴室。一个常见的失败模式是你半夜起床去洗手间,忘记了你的访问密码,并意识到你没有带收据。所以你必须睡在浴室地板上,直到第二天早上工作人员到达。

密码可记忆性可以在五个主要标题下进行讨论:天真选择、用户能力和培训、设计错误、操作失败和社会工程攻击的易受攻击能力。

3.4.4.1 天真的选择

自 20 世纪 80 年代中期以来,人们研究了人们选择的密码类型,发现他们使用配偶的姓名、单个字母,甚至只是按回车键给出一个空字符串作为密码。对 1980 年 Unix 系统磁带的密码分析表明,在先驱中,丹尼斯·里奇使用了“dmac”(他的中间名是 MacAlistair);后来的谷歌董事长埃里克施密特使用了 wendy!!! (他妻子的名字)和 Brian Kernighan 使用了 /.,/., [795]。 Fred Grampp 和 Robert Morris 1984 年关于 Unix 安全性的经典论文 [805] 报告说,在强制密码长度至少为六个字符且至少有一个非字母的软件可用后,他们制作了一个文件,其中包含 20 个最常见的女性名字,每个后跟一个数字。在这 200 个密码中,他们检查的几十台机器中的每一台都至少使用了一个。当时,Unix 系统将加密的密码保存在所有系统用户都可以读取的文件 /etc/passwd 中,因此任何用户都可以验证对其他用户密码的猜测。其他研究表明,要求非字母只是将最流行的密码从“password”更改为“password1”[1672]。

1990 年,Daniel Klein 收集了 25,000 个 Unix 密码,发现根据 [1056] 中投入的努力量,可以猜出 21-25% 的密码。字典词占 7.4%,常用名占 4%,用户名和帐户名的组合占 2.7%,依此类推,如科幻小说中的词 (0.4%) 和体育术语 (0.2%) .其他密码猜测使用的模式,例如通过使用属于用户“Daniel V. Klein”的帐户“klone”并尝试密码,例如 klone、klone1、

klone123、dvk、dvkdvk、leinad、neilk、DvkkvD 等。次年,Alec Muett 发布了“破解”软件,该软件会尝试使用字典和通过一组修改规则派生的模式来暴力破解 Unix 密码。

据我所知,最大的密码选择学术研究是由 Joe Bonneau 完成的,他在 2012 年分析了泄露的密码文件中的数千万个密码,并且还在雅虎实习,他对登录系统进行了检测,以收集有关密码选择的实时统计数据。7000万用户。他还制定了用于密码猜测的最佳指标,无论是在独立系统中还是在攻击者使用从一个系统获取的密码来破解另一个系统的帐户的情况下 [289]。这项工作为密码强度检查器的设计和大型服务公司的其他当前实践提供了信息。

3.4.4.2 用户能力与培训

有时您可以培训用户。密码检查器训练他们使用更长的数字和字母密码,这种效果会蔓延到不使用它们的网站 [444]。但是你不想把顾客赶走,所以营销人员会限制你能做的。事实上,研究表明,密码规则的执行不是风险价值的函数,而是网站是否垄断的函数。此类网站通常有非常烦人的规则,而具有竞争对手(如亚马逊)的网站则更有用,更加依赖后端入侵检测系统。

在企业或军事环境中,您可以强制执行密码选择规则或密码更改规则,或发布随机密码。但随后人们将不得不把它们写下来。因此,您可以坚持以与保护数据相同的方式对待密码:银行主密码会在一夜之间进入保险库,而军事“绝密”密码必须密封在信封中、保险箱中、锁着的房间里无人居住,在有警卫巡逻的建筑物中。你可以派守卫在晚上巡逻,清理所有的桌子,把所有没有上锁的东西都扔进垃圾箱。但如果你想雇用和留住优秀人才,你最好仔细考虑一下。例如,一家硅谷公司制定了一项政策,即每台机器的 root 密码都将写在一张卡片上,并放入一个贴在机器侧面的信封中 这是对密码一视同仁的更人性化的版本方式作为他们保护的数据。国内相当于你的wifi路由器背面的卡,上面有密码。

在撰写本书的第一版时,我找不到任何关于训练人们选择密码的实验,这些实验可以根据应用心理学的标准(即具有足够统计能力的随机对照试验)站得住脚。我发现最接近的是对各种类型密码的召回率、遗忘率和猜测率的研究 [345];这并没有告诉我们为用户提供各种建议的实际效果。因此,我们决定看看通过培训可以取得什么成果,并从我们的一年级理科学生中选出了三组大约一百名志愿者 [2055]:

· 红色(控制)组得到了通常的建议(密码至少六个字符长,包括一个非字母)

- 要求绿色组想一个密码短语并从中选择字母来构建密码。所以“现在是中午 12 点,我饿了”会给出“I S12&IAH”

- 黄色组被告知从我们给他们的表格中随机选择八个字符（字母或数字）,将它们写下来,并在他们记住密码后一两周后销毁这张便条。

我们期望发现的是,红色组的密码比绿色组的密码更容易猜到,而绿色组的密码又比黄色组的密码更容易猜到;黄色组最难记住他们的密码（或者被迫更频繁地重置密码）,其次是绿色组,然后是红色组。但这不是我们发现的。

大约 30% 的对照组选择了可以使用 Alec Muett 的“破解”软件猜出的密码,而其他两组的这一比例约为 10%。
因此,密码短语和随机密码似乎同样有效。
当我们查看密码重置率时,三组之间没有显着差异 。当我们询问学生是否觉得密码难以记住（或记下来)时,黄色组的问题明显多于其他两组;但红色和绿色之间没有显着差异 。

我们得出的结论如下。

- 对于遵循说明的用户,基于助记词的密码提供了两全其美的方法。它们像天真选择的密码一样容易记住,又像随机密码一样难以猜测。

- 问题就变成了用户合规性问题之一。相当多的用户（可能是他们中的三分之一)只是不按照他们说的去做。

因此,当军队给士兵随机选择的密码时,它的价值来自于密码分配迫使用户遵守的事实,而不是密码是随机的（因为助记词也可以）。

但是集中分配的密码通常是不合适的。当您向公众提供服务时,您的客户希望您提供与竞争对手大致相同的界面。因此,您必须让用户选择他们自己的网站密码,并使用一些轻量级算法来拒绝“明显错误”的密码。
（GCHQ 建议使用在线密码转储中最常见的 100,000 个密码的“错误密码列表”。)在银行卡的情况下,用户期望银行发行的初始 PIN 以及之后将 PIN 更改为他们的密码之一的能力选择（尽管您可能再次阻止“明显错误”的 PIN,例如 0000 或 1234）。超过一半的持卡人保留随机 PIN,但大约四分之一的持卡人选择诸如儿童出生日期之类的 PIN,这些 PIN 的熵低于随机 PIN,并且在不同的卡上具有相同的 PIN。

结果是,如果小偷先在离线模式下然后在在线模式下尝试所有卡上最常见的 PIN,那么偷钱包或钱包的小偷可能有大约十一分之一的机会走运,所以他每次得到六次。

禁止流行选择（如 1234)的银行可以将几率增加到十八分之一左右 [295]。

3.4.4.3 设计错误

使密码易于记忆的尝试是严重设计错误的常见来源。如何不这样做的典型例子是询问“你母亲的婚前姓氏”。数量惊人的银行、政府部门和其他组织仍然以这种方式验证他们的客户，尽管现在它往往不是密码而是密码恢复问题。你总是可以试着告诉你的银行“Yngstrom”，告诉电话公司“Jones”，告诉旅行社“Gerghty”等等；但是数据在公司之间广泛共享，因此您很容易最终混淆他们的系统 更不用说您自己了。如果您尝试打电话给您的银行并告诉他们您已决定将您母亲的娘家姓从 Yngstrom 更改为 yGt5r4ad – 甚至是 Smith – 那么祝您好运。事实上，考虑到大量数据泄露事件，您不妨假设任何想要获取您所有常用密码恢复信息的人 包括您的地址、您的出生日期、您的第一所学校和您的社会安全号码，以及作为你母亲的处女

姓名。

一些组织使用上下文安全信息。我曾经使用过的一家银行向其商业客户询问他们账户中最后一张已清算的支票的价值。从理论上讲，这可能会有所帮助：如果有人无意中听到我在电话中进行交易，那么这不是一个长期的妥协。不过，细节值得关注。首次引入此系统时，我想知道我刚刚向其开具支票的供应商是否会冒充我，并得出结论，询问最后三张支票的价值会更安全。但是我们实际遇到的问题是出乎意料的。将支票簿交给我们的会计师进行年度审计后，我们无法与银行交谈。我也不喜欢窃取我的实体帖子的人也可以窃取我的钱的想法。

当今需要密码的应用程序数量之多超出了人类记忆的能力。 Dinei Flöencio 和 Cormac Herley 在三个月内对 50 万网络用户进行的一项 2007 年研究表明，普通用户有 6.5 个密码，每个密码在 3.9 个不同的网站上共享；有大约 25 个需要密码的帐户；平均每天输入 8 个密码。 Bonneau 在 2012 年发布了更广泛的统计数据 [289]，但从那以后，由于智能手机的出现，用户密码输入的频率已经下降。现代网络浏览器也会缓存密码。请参阅下面第 3.4.11 节对密码管理器的讨论。但许多人出于许多不同的目的使用相同的密码，并且没有制定特殊的流程来处理他们的高价值登录，例如他们的银行、他们的社交媒体账户和他们的电子邮件。因此，您必须预料到您刚刚设计的电子银行系统的客户选择的密码也可能为黑手党运营的色情网站所知。 （甚至还有一个网站 http://haveibeenpwned.com，它会告诉您哪些安全漏洞泄露了您的电子邮件地址和密码。）

最普遍和最持久的错误之一是强迫用户定期更改密码。当我在 1980 年代第一次遇到强制更改每月密码时，我观察到它导致人们选择密码，例如三月的“julia03”，四月的“julia04”等等，并在第一个（2001 年）) 本书的版本（第 3 章，第 48 页）。然而，在 2003 年，NIST 的 Bill Burr 撰写了密码指南，建议定期更新 [1096]。

这被四大审计师采用,并将其推广给所有审计客户3。同时,安全可用性研究人员进行了一项又一项调查,表明每月的变化并不是最理想的。 Yinqian Zhang、Fabian Monrose 和 Mike Reiter 对用户发明的密码转换技术的首次系统研究表明,在强制过期的系统中,超过 40% 的密码可以从以前的密码中猜出,强制更改并没有太大作用帮助那些选择弱密码的人,并且定期选择密码的努力也可能降低密码质量 [2070]。最后,可用性大师 Lorrie Cranor 在 FTC [492] 担任首席技术专家期间撰写了一份调查,并得到了一项学术研究 [1505] 的支持。

2017 年,NIST 放弃了;他们现在推荐仅在妥协时更改的长密码4。英国 GCHQ 等其他政府机构紧随其后,微软最终宣布从 2019 年 4 月起终止 Windows 10 的密码过期政策。然而,许多公司都受到信用卡发行机构制定的 PCI 标准的约束,这些标准尚未赶上并仍然规定三个月的变化;另一个问题是,审计员要求许多公司遵守规定,这无疑需要时间才能赶上。

在 2020 年,当前的时尚是邀请用户选择三个或更多随机字典单词的密码。这是由著名的 xkcd 卡通宣传的,它建议将“正确的马电池订书钉”作为密码。然而,实证研究表明,真实用户选择的多词密码短语的熵比他们真的从字典中随机选择时得到的熵要少得多;他们倾向于使用普通名词双字母组,而转向三个或四个单词会带来迅速递减的回报 [296]。电子前沿基金会现在提倡用骰子来选词;他们有一个包含 7,776 个单词的列表（65 个,所以掷五次骰子来选择一个单词）,并注意到一个包含 6 个单词的短语有 77 位的熵并且是令人难忘的 [290]。

3.4.4.4 运行故障

最普遍的操作错误是无法重置默认密码。自从 20 世纪 80 年代早期的拨号接入系统引起调皮的小学生的注意以来,这一直是一个长期存在的问题。一个特别糟糕的例子是系统具有无法更改的默认密码,由无法修补的软件检查。我们在物联网中看到越来越多这样的设备;它们在使用寿命期间仍然很脆弱。正如我在第 2 章中所描述的,Mirai 僵尸网络的出现是为了招募和利用它们。

显而易见的密码是另一个长期存在的问题,无论是在便签纸上还是在某些电子等价物上。一个著名的早期案例是 R v Gold 和 Schifreen,两名年轻的黑客在展览终端上贴的一张纸条上看到了 Prestel 开发版的电话号码,Prestel 是英国电信运营的早期公共电子邮件服务。稍后拨入,发现欢迎界面上显示了维护密码。他们试过这个

3我们大学的审计员连续三年在他们的年度报告中写道,我们应该每月强制更改密码,但无法提供任何证据来支持这一点,甚至不知道他们的政策最终来自 NIST。我们不为所动,要求审计委员会主席任命一批新的审计师,最终这件事发生了。

4NIST SP 800-63-3

在实时系统上也是如此,而且它有效!他们开始侵入爱丁堡公爵的电子邮件帐户,并将“来自”他的邮件发送给他们不喜欢的人,宣布授予爵士头衔。这一令人发指的罪行震惊了当权派,以至于当检察官未能说服法院对这些年轻人定罪时,英国议会通过了第一部《计算机滥用法》。

第三个操作问题是在不需要密码或出于不诚实的原因想要密码时要求输入密码,正如我在本节开头所讨论的那样。您被迫在网站上设置的大多数密码都是出于营销原因 获取您的电子邮件地址或让您感觉属于某个“俱乐部”[294]。因此,对于永远不打算再次访问该站点的用户来说,通过在密码字段中输入“123456”甚至更粗鲁的词来表达他们的愤怒是完全合理的。

第四个是残暴的密码管理系统:有些系统根本不加密密码,并且不时有报告称有进取心的黑客将后门走私到密码管理库 [427]。

但也许最大的运营问题是容易受到社会工程攻击。

3.4.4.5 社会工程攻击

细心的组织以各种方式传达安全上下文,以帮助员工避免犯错。例如,美国国家安全局有不同颜色的内部和外部电话,当房间里的外部电话挂断时,机密材料甚至不能在房间里讨论 更不用说在电话上了。

然而,尽管许多银行和其他企业保持一定的内部安全环境,但他们经常训练客户以不安全的方式行事。由于普遍存在的网络钓鱼,尝试通过单击电子邮件中的链接登录银行是不明智的,因此您应该始终使用浏览器书签或手动输入 URL。然而,银行营销部门会发送大量包含可点击链接的电子邮件。事实上,营销行业的大部分工作都致力于让人们点击链接。许多电子邮件客户端(包括 Apple、Microsoft 和 Google 的)都将纯文本 URL 设置为可点击,因此他们的用户可能永远不会看到不可点击的 URL。银行客户受过良好训练,不会做错事。

如果 Web 服务将他们定向到其他地方,谨慎的客户也应该保持谨慎 但银行系统会为其服务使用各种奇怪的 URL。来自美国银行的垃圾邮件将英国客户引导至 mynew card.com,但证书错误(用于 mynewcard.bankofamerica.com)。

还有更多大银行培训客户进行不安全计算的例子 通过无视域名、忽略证书警告和愉快地单击链接 [582]。因此,即使是安全专家也难以区分银行垃圾邮件和网络钓鱼 [443]。

通过电话向身份不明的来电者提供安全信息是不明智的 但我们都会接到要求提供安全信息的银行职员的电话。银行现在也用我们的手机打电话给我们,希望我们向整个火车车厢的陌生人提供安全信息,而不是让我们发短信

一个答复。 （我的一张卡被冻结了,因为银行保安人员在我开车时给我打电话;如果不是在免提模式下处理电话是违法的,而且没有安全的地方可以停下来。）将银行卡 PIN 码放入 ATM 或商店中的 PIN 输入设备 (PED) 以外的任何设备也是不明智的;花旗银行甚至要求客户不要理会并报告要求提供个人信息（包括 PIN 和帐户详细信息）的电子邮件。所以发生了什么事?你猜对了 它向澳大利亚客户发送了一封电子邮件,要求客户“作为安全升级的一部分”登录其网站并使用卡号和 ATM PIN [1087] 进行身份验证。在 2005 年的一个案例中,哈利法克斯向我们一名联系银行安全部门的学生的母亲发送了一封垃圾邮件,结果告诉她这是网络钓鱼。然后学生联系 ISP 报告滥用行为,发现 URL 和服务是真实的 [1241]。哈利法克斯在 2008 年的崩溃中消失了,考虑到他们自己的安全部门无法区分垃圾邮件和网络钓鱼,也许这是正义的（尽管这让我们纳税人损失了一大笔钱）。

3.4.4.6 客户教育

在网络钓鱼在 2000 年代中期成为网上银行的真正威胁之后,银行试图训练他们的客户在网站上寻找某些功能。这部分是降低风险,但部分是风险倾销 确保不理解或不能遵守指示的客户可以对由此产生的损失负责。一般模式是,一旦客户接受了遵循某些特定规则的培训,网络钓鱼者就会利用这一点,因为没有充分解释规则的原因。

一开始,建议是“检查英语”,所以坏人要么找到会写英语的人,要么干脆开始使用银行自己的电子邮件,但更改了 URL。然后是“寻找锁符号”,因此网络钓鱼站点开始使用 SSL（或者只是通过在其网页上放置锁符号图形来伪造它）。一些银行开始将客户帐号的最后四位数字放入电子邮件中;网络钓鱼者的回应是输入前四个（对于给定的银行和卡产品来说是不变的）。

接下来的建议是可以点击图片,但不能点击 URL;网络钓鱼者迅速放入看似图像但实际上指向可执行文件的链接。当时的建议是通过将鼠标悬停在链接上来检查链接的真正去向;然后,坏人要么在 URL 中插入一个非打印字符以阻止 Internet Explorer 显示其余部分,要么使用一个难以控制的长 URL（许多银行也是这样做的）。

这种军备竞赛最有可能使攻击者受益。反制措施变得如此复杂和违反直觉,以至于让越来越多的用户感到困惑 这正是网络钓鱼者所需要的。多年来,安全和可用性社区已经知道“责备和培训”不是处理不可用系统的方法 唯一真正的解决办法是首先设计安全可用性 [1451]。

3.4.4.7 网络钓鱼警告

部分解决方案是为用户提供更好的工具。现代浏览器通过一系列机制提醒您注意恶意 URL。首先,有反病毒和威胁情报社区整理的不良 URL 列表。

其次,有查找过期证书和其他合规性失败的逻辑(因为这些警报中的大多数都是误报)。

在工业界和学术界,已经有很多关于如何让人们注意警告的研究。我们看到了很多,大多数都是无关紧要的,而且很多都是为了将风险从别人转移给我们。那么人们什么时候关注呢?在我们自己的工作中,我们尝试了很多事情,发现当警告不是模糊和笼统(“警告 - 访问此网站可能会损害您的计算机!”)而是具体和具体(“您访问的网站将要访问已确认包含对您构成重大风险的软件,没有明显的好处。它会尝试用旨在窃取您的银行帐户和信用卡详细信息以欺骗您的恶意软件感染您的计算机)[1327]. Adrienne Porter Felt 和 Google 可用性团队的后续研究尝试了许多想法,包括使用面孔在心理上突出警告(这不起作用)、简化文本(这有帮助)以及使安全默认值既有吸引力又突出(这也有帮助) .优化这些因素可将依从性从约 35% 提高到约 50% [675]。但是,如果您想阻止绝大多数人点击已知的错误 URL,那么自愿遵守是不够的。

您要么必须在防火墙处阻止它们,要么在浏览器中阻止它们(就像 Chrome 和 Firefox 对不同类型的证书错误所做的那样 我们将在 21.6.1 中返回这个问题)。

3.4.5 系统问题

并非所有网络钓鱼攻击都涉及心理学。有些涉及与密码输入和存储有关的技术机制以及一些更广泛的系统问题。

正如我们已经指出的,一个关键问题是我们是否可以限制密码猜测的次数。如果猜测是有限的(如 ATM PIN),安全工程师有时将密码系统称为“在线”,如果不是,则称为“离线”(这最初意味着用户可以获取密码文件并将其带走尝试的系统猜测其他用户的密码,包括更多特权用户)。但这些术语不再真正准确。某些离线系统可以限制猜测,例如使用物理防篡改功能将您限制为三个 PIN 猜测的支付卡,而某些在线系统则不能。例如,如果您使用 Kerberos 登录,窃听线路的对手可以观察到您使用密码加密的密钥从服务器流向您的客户端,然后使用该密钥加密的数据在线路上流动;这样他们就可以花时间尝试所有可能的密码。这里最常见的陷阱是通常限制密码猜测的系统,但当它被黑客攻击并且单向加密密码文件连同加密密钥被泄露时,突然无法这样做。然后坏人可以在闲暇时针对每个帐户尝试他们的整个密码字典。

密码的可猜测性最终取决于所选密码的熵

词和允许猜测的数量,但这在特定威胁模型的上下文中发挥作用,因此您需要考虑您试图防御的攻击类型。概括地说,有以下这些。

针对一个帐户的有针对性的攻击:入侵者试图猜测特定用户的密码。他们可能会尝试在办公室猜测对手的登录密码,以便直接进行恶作剧。

试图渗透属于特定目标的任何帐户:敌人试图在任何地方破解您拥有的任何帐户,以获取可能有助于接管其他帐户或直接造成伤害的信息。

试图渗透目标系统上的任何帐户:入侵者试图以系统的任何用户身份登录。这是网络钓鱼者试图破解目标银行的任何账户以便通过该账户洗钱的典型案例。

尝试渗透任何系统上的任何帐户:入侵者只想要一个给定域中任何系统的帐户,而不关心是哪个帐户。例如,坏人试图猜测任何在线电子邮件服务的密码,以便他们可以从受感染的帐户发送垃圾邮件,以及目标攻击者想要登录到目标公司域中的任何随机机器作为滩头阵地。

尝试利用对一个系统的破坏来渗透到相关系统:入侵者已经占据了滩头阵地,现在想向内陆移动以捕获更高价值的目标。

服务拒绝攻击:攻击者可能希望阻止一个或多个合法用户使用系统。这可能针对特定帐户或系统范围。

这种分类有助于我们在评估密码系统时提出相关问题。

3.4.6 你能拒绝服务吗?

当您检测到密码猜测时,基本上有三种方法来处理:锁定、节流和保护性监视。银行可能会在三个错误的 PIN 码后冻结您的卡;但是,如果他们在三次尝试输入错误密码后冻结了您的在线帐户,他们就会面临拒绝服务攻击。服务也可能意外失败;配置不当的系统可能会产生重复的失效凭据。现在很多商业网站都使用节流而不是锁定。在军事系统中,您甚至可能不希望这样,以防进入网络的敌人可能会通过大量错误登录尝试来干扰网络。在这种情况下,保护性监控可能是首选,并计划在危机中需要时放弃限速。 Joe Bonneau 和 Soren Preibusch 收集了有多少主要网站使用帐户锁定与各种类型的速率控制的统计数据 [294]。他们发现流行的、不断发展的、有能力的网站往往更安全,支付网站也是如此,而

内容网站做得最差。微软研究院的 Yuan Tian、Cormac Herley 和 Stuart Schechter 研究了如何正确进行锁定或节流;除其他事项外,最好惩罚对弱密码的猜测（否则攻击者会先猜测它们才能获得优势）,在保护选择弱密码的用户时更加积极,并且不要惩罚重复提交相同密码的 IP 或客户端密码错误 [1888]。

3.4.7 保护自己还是保护他人?

接下来,系统需要在多大程度上保护用户和子系统免受彼此的影响?在任何人都可以获得帐户的全球系统中 例如移动电话系统和自动取款机系统 你必须假设攻击者已经是合法用户,并确保没有人可以以他人的费用使用该服务。因此,知道一个用户的密码不会让另一个用户的帐户受到威胁。这既有个人方面,也有系统方面。

在个人方面,不要忘记我们在 2.5.4 中所说的亲密伴侣虐待:人们选择的密码通常很容易被他们的配偶或伴侣猜到,密码恢复问题也是如此:所以需要一些思考了解虐待受害者如何恢复安全感。

在系统方面,存在用于子系统之间相互认证的各种密码,在服务器-服务器环境中强制密码质量的机制很少,以及许多众所周知的问题（例如,Java 可信密钥库文件的默认密码是 改变 ）。开发团队经常共享最终出现在实时系统中的密码,即使在这种做法导致 3.4.4.4 节中描述的爱丁堡公爵的电子邮件被黑客入侵事件发生后 30 年也是如此。在一家大型服务公司内,您可以通过命名加密密钥并确保每个名称生成对底层硬件安全模块的调用来锁定 stu ;或者您甚至可以使用 SGX 等机制将密钥绑定到已知软件。但这需要花费真金白银,而钱并不是唯一的问题。企业系统组件通常托管在不同的服务公司,这使得采用更好的实践也成为一个困难的协调问题。因此,服务器密码通常出现在脚本或其他明文文件中,最终可能出现在 Dropbox 或 Splunk 中。因此,考虑最终用户之外的密码实践至关重要。在后面的章节中,我们将了解 Kerberos 和 ssh 等协议;现在,请回想一下 Ed Snowden 的评论,即对典型的大公司进行黑客攻击是微不足道的:只需对系统管理员进行鱼叉式网络钓鱼,然后用链条进入。本章的大部分内容都是关于“对系统管理员进行鱼叉式网络钓鱼”的部分;但不要忽视“锁链”部分。

3.4.8 密码输入攻击

密码输入通常保护不力。

3.4.8.1 界面设计

粗心的界面设计太普遍了。一些常见的提款机在头部高度有一个垂直键盘,这使得扒手很容易看到女人在从手提包中拿出钱包之前输入 PIN 码。键盘对于设计它们的男性来说可能处于合理的高度,但比女性矮几英寸的女性就会暴露在外。

在公共场所输入卡号或 PIN 码时,我通常会用身体或另一只手盖住打字的手 但您不能假设您的所有客户都会这样做。很多人都不愿意屏蔽 PIN,因为这是不信任的信号,尤其是当他们在超市排队时,朋友就站在附近。英国银行发现 20% 的用户从不屏蔽他们的 PIN [127] – 然后以此来指责客户的 PIN 被高架闭路电视摄像机泄露,而不是设计更好的 PIN 输入设备。

3.4.8.2 可信路径和虚假终端

可信路径是确保您通过不对窃听开放的通道登录到真实机器的某种方式。虚假终端攻击可以追溯到分时计算的初期。公共终端将运行一个攻击程序,该程序看起来就像通常的登录屏幕一样 要求输入用户名和密码。当毫无戒心的用户这样做时,它会保存密码,回复“对不起,密码错误”,然后消失,调用真正的密码程序。用户认为他们输入错误并再次输入密码。这就是 Windows 具有安全注意序列的原因;按 ctrl-alt-del 可以保证将您带到真正的密码提示。但最终,在 Windows 10 中,它被删除了,为 Windows 平板电脑铺平了道路,因为几乎没有人理解它。

ATM 盗刷器是安装在 ATM 喉管上的设备,可以复制卡的详细信息,并有一个摄像头来记录客户的 PIN。主题有很多变体。欺诈者也部署了错误的 PIN 输入设备,甚至因将密码窃取硬件连接到银行分支机构的终端而被判入狱。

我将在有关银行业务和簿记的章节中更详细地描述这个世界;长期的解决方案是从易于复制的磁条卡转向更难复制的芯片卡。无论如何,如果终端可能包含恶意硬件或软件,那么仅靠密码是不够的。

3.4.8.3 密码重试计数器的技术失败

许多孩子发现,按松动程度依次解开每个环,通常可以在几分钟内将自行车密码锁弄坏。同样的想法适用于许多计算机系统。 PDP-10 TENEX 操作系统一次检查一个字符的密码,并在其中一个字符错误时立即停止。这开启了计时攻击:攻击者会反复将猜测的密码放在内存中合适的位置,将其作为文件访问请求的一部分进行验证,然后等待查看被拒绝需要多长时间 [1129]。一个

第一个字符的错误几乎会立即报告,第二个字符的错误需要更长的时间报告,第三个字符的错误需要更长的时间,依此类推。所以你可以一个接一个地猜测字符,而不是从 A 字符的字母表中提取的 N 个字符的密码平均需要AN / 2 次猜测,它需要 AN / 2。 （请记住,三十年后,您今天正在构建的系统可能只剩下对其更具新闻价值的安全故障的记忆。）

在嵌入式系统领域,这些相同的错误正在重演。使用一个遥控车锁装置,一旦从遥控钥匙发送错误字节,接收器上的红色指示灯就会亮起。对于某些智能卡,可以通过尝试每个可能的输入值并查看卡的功耗来确定客户 PIN,然后在输入错误时发出重置信号。原因是错误的 PIN 导致 PIN 重试计数器递减,写入保存该计数器的 EEPROM 存储器导致几毫安的电流浪涌 这可以及时检测到,以便在写入完成之前重置卡 [1105]。

这些实施细节很重要。对于实现密码学的人来说,计时通道是一个严重的问题,我们将在下一章进行更详细的讨论。

最近一个引人注目的问题是 iPhone 中的 PIN 重试计数器。我的同事 Sergei Skorobogatov 指出,iPhone 将敏感数据加密保存在闪存中,并构建了一个适配器,使他能够保存加密的内存内容,并在多次 PIN 尝试后将它们恢复到原始状态。这使他能够尝试所有 10,000 个可能的 PIN,而不是 Apple 试图强加的 10 个 PIN 限制 [1777]5。

3.4.9 密码存储攻击

密码在存储的地方通常很容易受到攻击。在麻省理工学院的“兼容分时系统”ctss（Multics 的 1960 年代前身）中,曾经发生过一个人正在编辑当天的消息,而另一个人正在编辑密码文件。由于软件错误,两个编辑器的临时文件互换了,每个登录的人都收到了密码文件的副本！ [476]。

另一个可怕的编程错误在 1980 年代后期袭击了一家英国银行,该银行错误地向所有客户发放了相同的 PIN [54]。由于处理 PIN 的程序意味着银行中没有人可以访问除他们自己以外的任何人的 PIN,因此直到数千张客户卡发货后才发现该错误。大失误仍在继续:2019 年,这家安全公司使用 Biostar 和 AEOS 生物识别锁系统进行楼宇入口控制,其客户包括 83 个国家/地区的银行和警察部队,其在线数据库未受保护,其中包含超过 100 万人的 ID、明文密码、指纹和面部识别数据;通过 Internet 扫描发现此问题的安全研究人员能够将自己添加为用户 [1864]。

5这样做是为了削弱时任联邦调查局局长詹姆斯·康梅 (James Comey) 的论点,即 iPhone 是无法破解的,因此应该命令苹果公司进行操作系统升级,以创建一个后门;参见第 26.2.8 节。

审计提供了另一种危险。当系统尝试登录密码失败时,日志中通常包含大量密码,因为用户获取的“用户名、密码”序列不同步。如果日志没有得到很好的保护,那么看到使用不存在的用户名 e5gv*8yp 登录失败的审计记录的人只需要尝试将此作为所有有效用户名的密码。

3.4.9.1 单向加密

此类事件教会人们通过使用单向算法加密密码来保护密码,这是 Roger Needham 和 Mike Guy 的一项创新。
密码在输入时通过单向函数传递,只有当它与先前存储的值匹配时用户才会登录。然而,它经常被错误地实施。正确的方法是生成一个随机密钥,在这种情况下历史上称为盐;使用一种缓慢的、加密强度高的单向函数将密码与盐结合起来;并存储盐和散列。

3.4.9.2 密码破解

一些使用加密密码文件的系统使其具有广泛的可读性。 Unix 曾经是最好的例子 密码文件 /etc/passwd 对所有用户都是可读的。因此任何用户都可以获取它并尝试通过加密字典中的所有密码并将它们与文件中的加密值进行比较来破解密码。我们已经在 3.4.4.1 中提到了人们多年来为此目的使用的“破解”软件。

大多数现代操作系统都在某种程度上解决了这个问题。例如,在现代 Linux 发行版中,密码经过加盐处理,使用 5000 轮 SHA-512 进行哈希处理,并存储在只有 root 用户可以读取的文件中。但是仍然有密码恢复工具可以帮助您,例如,如果您使用忘记的密码加密了 Oce 文档 [1674]。拥有 root 访问权限的骗子也可以使用此类工具,并且仍然存在许多设计糟糕的系统,其中密码文件以其他方式易受攻击。

还有凭证刺痛:当一个系统被黑客攻击并且密码被破解(或者甚至被发现未加密)时,它们会在其他系统上被试用以抓住许多重复使用它们的人。这仍然是一个实时问题。

所以密码破解还是值得关注的。一种值得考虑的对策是欺骗,它可以在堆栈的所有级别起作用。你可以让蜜罐系统在有人登录时发出警报,系统上的蜜罐帐户,或密码金丝雀 真实帐户的伪造加密密码 [996]。

3.4.9.3 远程密码校验

许多系统远程检查密码,使用密码协议来保护传输中的密码,密码安全和网络安全之间的交互可能很复杂。本地网络通常使用一种称为 Kerberos 的协议,服务器会向您发送一个根据您的密码加密的密钥;如果你

知道密码,您可以解密密钥并使用它来获取使您能够访问资源的票证。我将在下一章的 4.7.4 节中讨论这个问题;它并不总能保护弱密码免受可以窃听加密流量的对手的攻击。 Web 服务器主要使用一种称为 TLS 的协议来加密来自手机或笔记本电脑上浏览器的流量;我将在下一章的 5.7.5 节中讨论 TLS。如果服务器被黑,TLS 不会保护您。

然而,有一种名为同时对等身份验证 (SAE) 的新协议,它旨在即使在密码可猜测的情况下也能建立安全会话,并且已从 2018 年开始在 WPA3 标准中采用以进行 WiFi 身份验证。我稍后也会讨论这个。

然后是 OAuth,一种允许访问委托的协议,因此您可以授予一个网站使用另一个网站提供的机制对您进行身份验证的权利。由 Twitter 于 2006 年开发,现在被谷歌、微软和 Facebook 等主要服务提供商使用,让您登录媒体和其他网站;授权服务器为此目的颁发访问令牌。我们稍后也会讨论这些机制。随之而来的风险是跨站攻击;我们现在(2019 年)看到 OAuth 被威权国家的国家行为者用来钓鱼当地的人权捍卫者。该技术是创建一个具有合理名称(例如“Outlook Security Defender”)的恶意应用程序,并发送一封据称来自 Microsoft 的电子邮件,请求访问权限。如果目标响应,他们最终会进入 Microsoft 网页,要求他们授权应用程序访问他们的数据 [46]。

3.4.10 绝对限制

如果您对保护密码的密码算法和操作系统安全机制有信心,那么密码猜测攻击成功的概率是密码熵的函数(如果密码是集中分配的)以及用户心理的函数(如果密码是集中分配的)允许选择它们。军事系统管理员通常更喜欢发布随机密码,因此可以控制密码猜测攻击的可能性。例如,如果 L 是最大密码寿命,R 是登录尝试率,S 是密码空间的大小,那么密码在其寿命期内被猜到的概率是 P = LR/S,根据美国国防部密码管理指南 [546]。

从攻击者的目标开始,这种“可证明的安全”原则存在问题。他们是想破解目标帐户,还是想破解任何帐户?

如果一支军队有 100 万个可能的密码和 100 万个用户,并且在对任何帐户尝试输入错误密码 3 次后警报响起,那么攻击者只需为每个不同的帐户尝试一个密码即可。如果你想阻止这种情况,你不仅要对每个账户进行速率控制,还要对所有账户进行速率控制。

举一个具体的例子,Unix 系统曾经限制为八个字符的密码,因此有 968种或大约252种可能的密码。一些英国政府系统过去常常使用固定的辅音、元音和数字模板随机选择密码,旨在使它们更容易记住,例如 CVCNVCCN(例如 fuR5xEb8)。如果密码不区分大小写,则猜测概率会大大降低,仅为214.52.102中的一个或大约229。因此,如果攻击者每秒可以猜出 100 个密码 也许

分布在网络上数百台机器上的 10,000 个帐户,以免发出警报 然后他们将需要大约 500 万秒或两个月才能进入。如果您要保护这样的系统,您可能会发现它谨慎进行速率控制:设置一个限制,比如每个用户帐户每 10 秒猜测一次密码,也许可以通过源 IP 地址。您还可以计算失败的登录尝试次数并对其进行分析:是否有一系列不断的猜测表明攻击者正在使用僵尸网络或其他一些入侵尝试?

一旦你注意到一个,你会怎么做?你会关闭系统吗?
欢迎回到拒绝服务的世界。

对于商业网站,由于用户密码选择不当,每秒 100 个密码可能会转化为每秒一个受损的用户帐户。

对于拥有 1 亿个帐户的 Web 服务来说,这可能不是什么大问题 但仍然值得尝试确定任何工业规模的密码猜测攻击的来源。如果它们来自少数 IP 地址,您可以阻止它们,但正确地做到这一点比看起来更难,正如我们在上面的第 3.4.6 节中提到的那样。如果自动猜测攻击持续存在,那么另一种处理它的方法是验证码,我将在第 3.5 节中描述。

3.4.11 使用密码管理器

自 1980 年代以来,公司一直在销售可以记住您的多个应用程序密码的单点登录系统,当浏览器在 1990 年代中期出现并且人们开始登录数十个网站时,密码管理器成为大众市场产品。浏览器供应商注意到了,并开始免费提供几乎相同的功能。

选择随机密码并让您的浏览器记住它们可能是一种务实的操作方式。浏览器只会将密码输入到具有正确 URL (IE) 或相同主机名和字段名 (Fire fox) 的网页中。浏览器允许您设置一个主密码,该密码加密所有单独的站点密码,您只需在浏览器更新时输入。

一般来说,密码管理器的主要缺点是您可能会忘记主密码;并且您的所有密码可能会立即泄露,因为恶意软件编写者可以想出如何破解普通产品。这是使用浏览器时的一个特殊问题,另一个是主密码并不总是默认设置,因此许多用户不设置主密码。 (这同样适用于您作为平台选项获得的其他安全服务,例如加密您的手机或笔记本电脑。)使用浏览器的一个优势是您可以在手机浏览器和笔记本电脑浏览器之间同步密码.

第三方密码管理器可以提供更多功能,例如为您选择长随机密码、识别多个网站共享的密码,以及为您管理密码收集的备份和恢复提供更多可控方式。 (对于浏览器,这归结为备份您的整个笔记本电脑或手机。)它们还可以帮助您跟踪您的帐户,这样您就可以查看您是否在已宣布存在漏洞的系统上设置了密码。缺点是许多产品真的很可怕,甚至一些硬件密码管理器都会明文存储您的所有秘密 [130],而排名前五的软件产品存在严重的系统漏洞,从自动完成到忽略子域 [389]].你怎么知道

任何给定的产品实际上是可靠的吗?

许多银行试图禁用存储,无论是通过在其网页中设置 autocomplete= off 还是使用其他阻止密码管理器的技巧。银行认为这可以提高安全性,但我一点也不相信。阻止人们使用密码管理器或浏览器自己的存储可能会使他们中的大多数人使用较弱的密码。银行可能会争辩说,关闭自动完成功能会使设备被盗后的妥协更加困难,并且可能会阻止恶意软件从您的浏览器或密码管理器的数据库中窃取密码,但该产品提供的网络钓鱼防御被禁用 这可能会使普通客户面临更大的风险风险 [1355]。这也不方便;由于客户的反应 [1278],第二天突然禁用密码存储的一家银行不得不让步。人们以各种方式管理风险。我个人为了不同的目的使用不同的浏览器 ,并让它们存储低价值的密码;对于电子邮件和银行等重要账户,我总是手动输入密码,并且总是通过书签而不是点击链接导航到它们。但大多数人不那么小心。并且一定要仔细考虑备份和恢复,并进行实践以确保它有效。

当您的笔记本电脑死机时会发生什么?你的手机什么时候没电了?当有人说服您的电话公司将您的电话号码链接到他们的 SIM 卡时?当你死了 或者当你生病而你的伴侣需要管理你的学习 ?他们知道在哪里可以找到主密码吗?如果您(和您的遗嘱执行人)只需要记住“第 169 页,远大前程”,就可以将它们写在一本书中。将它们写在随身携带的日记本上,写在写着“密码”的页面上,并不是很好。很少有人做对这一切。

3.4.12 我们会摆脱密码吗?

密码很烦人,所以很多人都在讨论摆脱它们,从笔记本电脑到手机的转变给了我们一个机会。没有键盘的物联网设备的激增将迫使我们出于某些目的而没有它们。一些公司试图完全摆脱它们。一个例子是在线银行 Monzo,它仅通过一款应用程序运营。他们让客户决定是使用指纹、图案锁、PIN 还是密码来保护他们的手机。然而,他们仍然使用电子邮件来提示人们升级,并对购买新手机的人进行身份验证,因此帐户盗用涉及手机盗用,或者猜测密码或密码恢复问题。使用短信而不是密码进行身份验证的最受欢迎的应用程序可能是 WhatsApp。我希望这会变得更加普遍;因此,我们将看到更多基于手机接管的攻击,从 SIM 交换到 Android 恶意软件、SS7 和 RCS 黑客攻击,再到简单的物理盗窃。在这种情况下,恢复通常意味着电子邮件循环,使您的电子邮件密码比以往任何时候都更加重要 或者打电话给呼叫中心并告诉他们您母亲的娘家姓。所以事情的变化可能没有看起来那么大。

Joe Bonneau 及其同事在 2012 年分析了这些选项 [292]。有许多标准可以用来评估身份验证系统,我们在这里研究了这些标准:对盗窃的弹性、对物理观察的弹性、对猜测的弹性、对恶意软件和其他内部危害的弹性、对来自其他验证者的泄漏的弹性、对网络钓鱼的弹性以及有针对性的模仿。其他因素包括容易

使用、易学性、是否需要携带额外的东西、错误率、恢复的难易程度、每个用户的成本，以及它是否是任何人都可以使用的开放式设计。他们得出结论，大多数涉及净收益的计划都是单点登录的变体 OpenID 确实变得很普遍，许多人使用谷歌或 Facebook 登录他们的报纸，尽管明显的隐私成本6。除此之外，任何安全改进都涉及放弃密码的一项或多项优势，即它们简单、有效且便宜。

Bonneau 的调查对 CAP 读卡器等实体身份验证给予了很高的安全评级，它使人们能够使用银行卡登录网上银行；银行监管机构已经在许多国家/地区强制执行双因素验证。使用与银行卡绑定的东西可以提供更传统的信任根，至少对于传统的商业银行来说是这样；客户可以走进一家分行并订购一张新卡7。成为国家级攻击者目标的公司，例如谷歌和微软，现在向其所有员工提供某种身份验证令牌 。

调查遗漏了什么吗？好吧，那句老话是“你拥有的东西，你知道的东西，或者你是的东西” 或者，正如西姆森·加芬克尔 (Simson Garfinkel) 引人入胜的说法，“你曾经拥有的东西，你忘记的东西，或者你曾经是的东西”。第三种选择，生物识别技术，自从高端手机开始提供指纹读取器以来就开始广泛使用。一些国家，如德国，向其公民发放包含指纹的身份证，这可能会在其他一切出现问题时提供替代的信任根。我们将在本书后面的单独章节中讨论生物识别技术。

令牌和生物识别技术仍然主要与密码一起使用，首先作为设备被盗时的后盾，其次作为安全恢复过程的一部分。因此，密码仍然是构建大部分信息安全的（不稳定的）基础。可能改变这一点的是越来越多的设备完全没有用户界面，因此必须使用其他机制进行身份验证。一种越来越普遍的方法是信任首次使用，也被称为“复活小鸭”，因为小鸭在孵化后看到的第一只移动的动物会产生联系。我们将在下一章讨论这个问题，也会在我们深入研究特定应用程序（例如车辆安全性）时讨论。

最后，您应该认真考虑如何验证客户或其他根据数据保护法行使其要求提供其个人信息副本的权利的人的身份。 2019 年，James Pavur 冒充他的未婚妻 [1886] 向公司发出了 150 份此类请求。 86家公司承认他们有信息

6政府为公共服务设置单点登录的尝试不太成功，英国的“验证”计划将于 2020 年关闭 [1392]。围绕加强政府在身份保证方面的作用的尝试存在很多问题，我将在生物识别学一章中进一步讨论，这些问题会蔓延到从在线服务到选举安全的问题。由于现有企业享有的网络效应，其他私营部门公司也很难与之竞争。然而在 2019 年，Apple 宣布将提供一种新的、对隐私更友好的单点登录机制，并利用其应用商店的市场力量迫使网站支持它。因此，提供的隐私的质量和性质正在成为为其他动机而进行的战斗的副作用。我们将在经济学章节中对此进行更深入的分析。

7这不适用于像 Monzo 这样的无网点银行；但他们确实会拍下你的视频
您注册以便他们的呼叫中心稍后可以识别您。

关于她的信息,许多人有意识地要求她的登录名和密码来验证她的身份。但大约四分之一的人准备接受电子邮件地址或电话号码作为身份验证;另有 16% 的人要求提供易于伪造的身份证件。他收集了关于她的全部个人信息,包括她的信用卡号、她的社会保险号和她母亲的娘家姓。一家她从未与之打过交道的威胁情报公司发送了一份她已被泄露的帐户和密码的列表。鉴于如果公司在 30 天内不遵守此类要求,将在欧盟面临巨额罚款,你最好提前想好如何应对,而不是让法律办公室的助理即兴发挥程序。如果您取消密码,而前客户声称他们的手机被盗,您会怎么做?如果您持有从未成为您客户的人的个人数据,您如何识别他们?

3.5 验证码

我们能否拥有利用大脑优势而非劣势的保护机制?该领域最成功的创新可能是 CAPTCHA “完全自动化的公共图灵测试来区分计算机和人类”。这些是您在发布博客、注册免费在线帐户或恢复密码时经常需要解决的小视觉难题。这个想法是人们可以很容易地解决这些问题,而计算机却很难解决。

CAPTCHA 于 2003 年首次大规模使用,以阻止垃圾邮件发送者使用脚本在免费电子邮件服务上开设数千个帐户,并使攻击者更难尝试对大量现有帐户中的每个帐户输入几个简单的密码。它们是由 Luis von Ahn 及其同事 [1969] 发明的,他们的灵感来自艾伦图灵提出的关于计算机是否智能的著名测试:你把一台计算机放在一个房间里,把一个人放在另一个房间里,然后邀请一个人来试着区分它们。测试被翻转,以便计算机可以分辨出人与机器之间的差异 。

早期版本开始使用 AI 中一个已知的“难题”,例如在嘈杂的背景下识别扭曲的文本。这个想法是,破解验证码等同于解决人工智能问题,因此攻击者实际上必须手工完成工作,或者在计算机科学领域进行真正的创新。人类擅长阅读扭曲的文本,而程序则不那么擅长。结果比看起来更难。许多针对验证码的攻击,甚至直到今天,都在利用实施细节。

一旦聪明人努力解决,早期系统提出的许多图像识别问题也被证明一点也不难。还有协议级的攻击; von Ahn 提到,理论上垃圾邮件发送者可以让人们解决这些问题,作为获得免费色情内容的代价 [1968]。这很快就开始发生了:垃圾邮件发送者创造了一个游戏,在这个游戏中,你通过一个接一个地解决验证码来脱掉女人的衣服 [191]。几年之内,我们看到市场上出现了商业验证码破解工具 [843]。在接下来的几年中,使用受人类视觉系统启发的信号处理技术的通用攻击在解决至少一个子集方面变得相当有效

大多数类型的文本 CAPTCHA [746]。地下市场的安全经济学研究表明,到 2011 年,该行动已转向使用人类;在每天收入几美元的国家,人们将以每 1000 人大约 50 美分的价格解决验证码问题。

从 2014 年起,CAPTCHA 被 Luis von Ahn 的另一项发明 ReCAPTCHA 取代。这里的想法是让一些用户做一些有用的工作,并相互检查他们的答案。该服务最初要求人们转录谷歌图书中混淆 OCR 软件的文本片段;最近你会得到一个包含八张图片的谜题,要求“点击所有包含店面的图片”,这有助于谷歌训练其视觉识别人工智能系统 8。它通过设置两三个多项选择题并花费数十秒来回击廉价劳动力攻击,而不是允许快速响应。

CAPTCHA 的实施通常是草率的,对于视力受损的用户来说存在可访问性问题。并尝试在葡萄牙支付道路通行费,网站会抛出一个验证码,要求您识别带有对象的图片,如果您对葡萄牙语的理解不够好,无法弄清楚您应该寻找什么!

3.6 总结

心理对安全工程师很重要,因为欺骗和可用性。现在大多数真正的攻击都以用户为目标。各种网络钓鱼是主要的国家安全威胁,是开发和维护网络犯罪基础设施的主要手段,也是对网上银行系统的主要威胁之一。其他形式的欺骗占网络犯罪生态系统其余部分的大部分,这在数量和价值上与遗留犯罪大致相当。

部分补救措施是安全可用性,但该领域的研究长期以来一直被忽视,被认为不如密码学或操作系统那么迷人。
这对我们来说是一个严重的错误,从 2000 年代中期开始,我们开始意识到让普通人更容易以安全的方式使用系统的重要性。自 2010 年代中期以来,我们也开始意识到,我们还必须让普通程序员的工作变得更轻松;许多破坏真实系统的安全漏洞都是工具太难使用的结果,从使用不安全默认值的加密 API 到 C 编程语言。获得正确的可用性还可以直接帮助业务发展:PayPal 通过提供更安全、更方便的在线购物方式建立了 1000 亿美元的业务 9。

在本章中,我们简要介绍了与欺骗和人们犯下的各种错误相关的心理学研究,然后将身份验证作为案例研究。许多关于安全可用性的早期工作都集中在密码系统上,这引发了许多有趣的问题。我们

8看到 ReCAPTCHA 说“点击所有包含直升机的图像”并且不想帮助军事 AI 研究的用户遭到了反对。谷歌自己的员工也对这项研究提出抗议,该项目被终止。但其他用户仍然反对免费为谷歌工作。

9完全披露:我为他们提供咨询。

现在有越来越多的数据,不仅涉及我们可以在实验室中测量的事物,例如可猜测性、可记忆性和用户可培训性,而且还涉及只能在现场观察到的因素,例如真实系统如何崩溃、真实攻击如何扩展和不同参与者面临的激励如何导致不安全的均衡。

在 2008 年第一届安全与人类行为研讨会结束时,心理学家尼克·汉弗莱 (Nick Humphrey) 总结了关于风险的长时间讨论。 “我们都同意，”他说，“人们对恐怖主义关注过多,而对网络犯罪关注不够。但对心理学家来说,这是显而易见的。如果你想让人们在机场更放松,拿走坦克和枪支,放上一些漂亮的沙发,用扬声器播放莫扎特,人们很快就会放松下来。如果你想让人们在网上更加谨慎,让每个人都使用 Jaws 作为他们的屏幕保护程序。但这种情况不会发生,因为计算机行业会竭尽全力让计算机看起来不像过去那么可怕。”当然,政府希望人们对恐怖主义感到焦虑,因为它会抬高警察预算并帮助政治家获得连任。所以我们给了人们错误的信号,也把钱花在了错误的事情上。了解心理学、经济学和工程学需求之间的许多紧张关系对于在全球范围内构建强大的系统至关重要。

研究问题

安全心理学是 2020 年的热门话题之一。在本书的第二版中,我注意到安全经济学的整个领域自 2001 年第一版以来如雨后春笋般涌现,并写道“我们还需要对安全经济学进行更多的基本思考”。心理与安全之间的关系”。安全可用性也已成为一门学科,每年一度的可用隐私和安全研讨会,我们一直在举办研讨会,将安全工程师与人类学家、心理学家、哲学家和其他研究风险以及人们如何应对风险的人聚集在一起。

我寻找研究主题的元算法是首先查看应用程序,然后再查看相邻学科。第一个例子是安全可用性:由于从汽车到医疗设备的安全关键产品不仅需要软件和互联网连接,还需要复杂的界面甚至它们自己的应用程序,我们如何设计它们才能使它们不会通过以下方式伤害人们意外,还是恶意?

第二个例子,也是安全与人类行为研讨会的主题,是我们可以从研究人们如何应对风险的学科中学到的东西,从人类学和心理学到社会学、历史和哲学。我们的 2020 年活动邀请了领先的犯罪学家。现在的大流行表明,也许我们也应该与建筑师合作。他们现在正在研究人们如何在身体上保持距离但又能参与社交,他们的技能是理解形式如何促进人类体验和人类互动。设计不仅仅是破解代码。

延伸阅读

Real Hustle 视频可能是关于欺骗的最佳教程； YouTube 上有许多剧集。与此同时,关于社会工程学的最佳书籍仍然是凯文·米特尼克 (Kevin Mitnick) 的《欺骗的艺术》[1325]。 Amit Katwala 撰写了一份关于欺骗检测技术的简短调查 [1024],而 Tony Docan-Morgan 则编辑了 2019 年关于欺骗研究状况的手册,其中包含 51 章的专家介绍的许多方面 [569]。

关于社会心理学如何在营销中被使用和滥用,必读的书是 Tim Wu 的“The Attention Merchants”,它讲述了广告的历史 [2050]。

在计算机科学文献中,James Reason 的“人为错误”或许是一个很好的起点,它告诉我们安全关键系统社区从多年研究其领域中的同源问题中学到了什么 [1589]。然后是标准的 HCI 文本,例如 [1544],而早期关于安全可用性的文章出现为 [493],关于网络钓鱼的文章出现为 [976]。

随着我们进入一个自主设备的世界,越来越多的研究表明我们如何通过迪士尼化让人们更加信任机器人例如,让图书馆机器人的眼睛跟随行进方向,并让它们快乐地唧唧喳喳当他们帮助客户时 [1687]。对自动驾驶汽车的类似研究表明,如果车辆具有一些个性,人们会更信任这些车辆,并且乘客会获得一些战略控制权,例如选择路线的能力,甚至只是命令汽车停下来。

至于行为经济学,我让我的学生阅读丹尼·卡尼曼 (Danny Kahneman) 的诺贝尔奖演讲。有关更多技术细节,请参阅 Danny 在此之前与 Tom Gilovich 和 Dale Grin 编辑的大量论文 [769],或者他后来撰写的通俗科学书籍“Thinking, Fast and Slow” [1005]。另一种观点给出了行为经济学的整个历史,是迪克塞勒 (Dick Thaler) 的“行为不端:行为经济学的形成”[1874]。对于该理论在政府和其他地方的应用,标准参考文献是 Dick Thaler 和 Cass Sunnstein 的“Nudge”[1876]。迪克后来对“污泥”的第二个想法是在 [1875]。

有关密码和相关机制的详细历史,以及许多实证结果和对测量可猜测性和召回率的统计技术的分析,我强烈推荐 Joe Bonneau 的论文 [289],其中许多章节最终成为我引用的论文以上。

最后,如果您对阴暗面感兴趣,Albert Biderman 和 Herb Zimmer 的“人类行为的操纵”报告了朝鲜战争后在美国政府资助下进行的审讯实验 [239]。

被誉为刑讯逼供者的圣经,描述了感官剥夺、药物、催眠、社会压力等在审讯和洗脑囚犯时的相对效果。至于如今使用的测谎仪和其他欺骗检测技术,标准参考文献是 Aldert Vrij [1970]。