Computer Science and Application 计算机科学与应用, 2020, 10(3), 477-482
Published Online March 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.103050

Hans汉斯

Social Engineering Practice and Reflection Based on Social Network Services

—Take the Social Account Security of an Undergraduate as an Example

Feng Liu[1,2*#], Qiyi Huang[1*], Songyang Zhang[1], Qunkai Wu[1], Yu Sun[1]

[1]Binjiang College, Nanjing University of Information Science and Technology, Wuxi Jiangsu
[2]Institute of Artificial Intelligence and Progress Management, Shanghai University of International Business and Economics, Shanghai
Email: [#]lsttoy@163.com

Received: Feb. 25th, 2020; accepted: Mar. 9th, 2020; published: Mar. 16th, 2020

Abstract

Today's popular social engineering frameworks are more oriented towards real social applications. Frequent social worker vulnerabilities in social network services are often ignored. Therefore, this article focuses on the common social worker vulnerabilities and human weaknesses in social network services. The academic framework extends the theory. A social worker attack on undergraduate students in a school was used to verify the validity of the extended theory. Finally, reflected on the results and accumulated some experience for SNS users and institutions.

Keywords

Social Engineering, Personal Information Security, Christopher Hadnagy, Social Network Services, Humanity Vulnerabilities

基于社交网络服务的社会工程学实践与反思

——以某大学本科生社交账户安全为例

刘　峰[1,2*#]，黄祺熠[1*]，张松洋[1]，吴坤凯[1]，孙　钰[1]

[1]南京信息工程大学滨江学院，江苏 无锡
[2]上海对外经贸大学人工智能与变革管理研究院，上海
Email: [#]lsttoy@163.com

收稿日期：2020年2月25日；录用日期：2020年3月9日；发布日期：2020年3月16日

[*]共一作者。
[#]通讯作者。

文章引用: 刘峰, 黄祺熠, 张松洋, 吴坤凯, 孙钰. 基于社交网络服务的社会工程学实践与反思——以某大学本科生社交账户安全为例[J]. 计算机科学与应用, 2020, 10(3): 477-482. DOI: 10.12677/csa.2020.103050

摘　要

现今流行的社会工程学框架更偏向于现实社交方面应用，社交网络服务中频现的社工漏洞却常被忽略，因此本文主要聚焦于社交网络服务中常见的社工漏洞与人性弱点，对基础的社会工程学框架进行理论的延伸。通过对某校在校大学生进行社工攻击，来验证延伸理论的正确性。最后针对结果进行了反思，积累一些经验给SNS用户和机构。

关键词

社会工程学，个人信息安全，Christopher Hadnagy，社交网络服务，人性漏洞

1. 背景

社交网络服务(Social Networking Services, SNS)日益成为互联网用户间用来分享意见、见解、经验和观点的工具和平台。基于 WEB2.0 的发展，SNS 赋予了使用者更多的主动权，和更人性化，更多元化的互动模式，吸引用户愿意在互联网上发表见解和展示自己的生活。因此为社会工程人员给予了可趁之机。

根据 Christopher Hadnagy [1]的社会工程学框架,我们可以知道社会工程学(Social Engineering)入侵是利用人的弱点而不是计算机系统漏洞来突破信息安全防御措施的入侵手段，在近年发生的信息安全案例中，这种手段被大量采用。在这样的形势下，研究社会工程学对信息安全的威胁具有积极的意义[2]。人们在关注信息安全的时候更在意以计算机为基础的进攻和防御，但却不了解人在安全防御系统中起到了至关重要的作用。攻击者通过操控就能利用人性天性中的好奇、贪婪、情感共鸣以及心理弱点和本能反应使本应无懈可击的安全防御系统形如虚设。从已有研究来看，SNS [3]已成为黑客进行社会工程学攻击的重灾区。攻击者只需要进行一定量的信息收集，就可以利用信息不对称，轻而易举地获取目标的信任，并套取大量的私密信息。

在信息安全领域，学者们已经对大多数存在的问题展开研究和探讨。其中在 2018 年在 SNS 环境下档案信息服务存在的问题,从档案信息服务的整体战略构想、具体服务内容和档案信息安全三个层面，展开了一定的思考，提出了治理框架[4]，而在 2019 年就对当前信息时代可能产生的信息安全问题在社会伦理层面作了详细的总结[5]，则是对 web 应用中的系统漏洞展开讨论，但是并没有提及在社会工程学框架下的人性漏洞[6]。根据《2018 中国社交媒体影响报告》的数据显示，早在 2018 年底，我国使用 SNS 的用户规模就已经达到 8 亿人，其中微信月活覆盖率维持在 97%，由此可见，SNS 在互联网服务中占据着重要地位。然而在社交网站流失用户原因的调查中，认为占用时间而放弃继续使用的用户占 45.8%，因为健康影响而离开的用户占比 40.4%，余下的原因如垃圾信息太多，网站无用等原因均与安全性无直接联系。即用户目前不会因为安全性而大规模离开某个 SNS，这就导致了国内互联网企业对反社工机制的不重视。再加上我国在社工领域和反社工意识上普遍落后于国外，使得很多应用在设计时都更注重用户体验，从而削弱了必要的反社工机制，这大大减小了攻击者完成前期必要的信息收集工作所支付的代价。

因此本文就对于 SNS 中的一些常见的社会工程学漏洞和人性在信息安全领域的重要性展开研究，并

对已有的社会工程学框架在 SNS 方面的应用进行延伸，同时就一些实际生活中大学生的社交网络服务中潜藏的系统性社工漏洞与人性漏洞问题进行洞察，最后在社会工程学相关理论指导下进行实践，并归纳出若干经验。

2. 理论分析与方法

2.1. 对国内主流 SNS 的反社会工程学措施评价及分析

参考张成[7]的观点，当前国内主流的 SNS 都设计有强化陌生用户之间社交互动的系统，将爱好，婚姻状况，生日，星座等隐私信息透露出来，鼓励有其需要的用户拓展自己的人际交往圈，以此来维持在此 SNS 的用户粘性。当然此系统也很大程度上减少了信息获取的难度，为黑客创造出了一些社工漏洞，危害性较大。一些较大的 SNS 已经开始重视这个问题，将敏感信息进行局部隐藏，以此来达到反社工的目的。遗憾的是国内并没有一个规范化的 SNS 隐藏信息标准，导致很多敏感信息隐藏形同虚设。例如电话号码，身份证号等可以通过对同一个目标的多个 SNS 甚至是接触目标本人进行社工渗透，从而拼凑出隐藏的部分，从而绕过了反社工系统。

2.2. 针对人性漏洞的常见社工框架

考虑到 Christopher Hadnagy [1]与廖双[8]的社会工程学框架还是以现实为基准进行讨论的，很多例如微表情、肢体语言解读等现实社会工程学论点是不适用于 SNS 上的社会工程学入侵的。因此我们对该理论进行进一步延伸拓展，总结出以下六点适用于 SNS 上的人性漏洞(如下表 1)：

Table 1. Social engineering framework for SNS
表 1. 适用于 SNS 方向的社会工程学框架

潜在漏洞的攻击方式	手段	目的	优势
a) 渗透判断	观察目标行动，利用信息收集进行综合性判断	掌握目标在 SNS 中的使用习惯，使用规律	借助密码生成字典，破解效率高
b) 伪装欺骗	传播木马信息，伪造电子邮件，制作钓鱼网站	植入 webshell 准备长期渗透，或直接套取隐私信息	适用于网络安全意识较差的用户
c) 假托说服	用利益诱导目标，使目标为自己服务	以技术手段诱导目标泄露信息	双方利益不冲突时，效益较大
d) 信息威胁	冒充权威机构散布虚假信息	制造心理压力，增强目标的信任度	成本小，覆盖面广，可信度高，适合大面积，无差别式攻击
e) 投其所好	讲究说话的艺术，利用人的友善和同情心	以非技术手段诱导目标主动透露信息	易获取目标用户的信任，较难防范
f) 反向社会工程学	人为制造网络或计算机故障，并向目标提出解决方案	骗取目标信任，诱导目标泄露信息	较隐蔽，危害较大，不易防范，适用于领域内专业性较强的人群

以上六点改进的重点是我们一般进行实操之时常用的方法论。以此为基准开始进行社会工程学的实际操作。

3. 社会工程学的实操理论分析和执行回顾

对于进入社会工程学的实操过程之后，我们一般会先设计好全过程的计划和大概步骤。往往一般还是从初步的非接触式信息搜集、工具基本分析、接触性信息搜集、目标及其目标环境的信息识别与搜集、信息整理与框架分析法比对、个性化密码破解等步骤。具体步骤如图 1 所示。

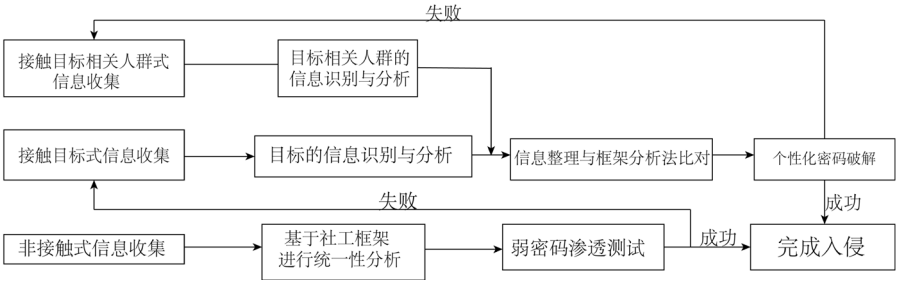

Figure 1. Flow chart of social engineering method
图 1. 社会工程学方法流程图

在做好准备工作后，首先进行该目标对象的初步分析阶段。在分析场景下该目标对象为校学生会宣传墙的 QQ 公众号，攻击者使用 56 个安全强度低的弱密码尝试登入公众号邮箱的方式失败了，说明该公众号的防范意识较强，使用的密码应该为与持有者关联性较强的密码。根据[8]中对被调查人密码来源比例统计图中显示：密码来源与自身相关的占比和相关信息生成的占比分别为 22.9%和 74.4%。故攻击者根据数据进行合理推测，做出密码大概率应为与管理人或者与大学关联性较强的密码的结论，在此结论的基础上攻击者打算从管理者的私人账号入手。攻击者首先想从点赞人群中找到该公众号的管理者，基于 SNS 的社工框架，攻击者判断这 27 人中存在管理者私人账号的可能性极高。故使用基于 Python 的爬虫技术[9]爬取了该公众号最早发布的说说下对此点赞的 27 人空间的详细信息。基于此判断，攻击者以“校学生会新人”的名义加入了校学生会新生群。因群内并没有设置实名验证环节，群管理也并没有对陌生账号起到应有的防备，攻击者可以很轻松以此名义收集到很多关键信息。攻击者初步了解到校学生会的成员管理体系，结合之前最早点赞的 27 人，判断出公众号的疑似管理者为 3 位同学，并添加了这 3 人的私人账号，通过空间和接触目标性的信息收集，利用伪装背景攻击者顺利收集到了目标 3 人的零散信息，并排除了两位疑似管理者，因此公众号管理者的身份基本确定。

在促成攻击者成功的根本原因还是如[10]所述，目标用户缺乏个人隐私和他人隐私的保护意识。但最后锁定的管理者设置的空间处于攻击者不可见状态，使得管理者本人的关键信息并没有被攻击者顺利获取到，这将导致攻击者的密码生成器生成的密码不完全。基于社工框架，攻击者迅速确定了与此人关系密切的多位目标，以话术诱导的方式套取信息，最终获取到了目标的关键隐私信息和密码设置习惯，例如目标和相关者生日、目标和相关者姓名、昵称、网名、星座、弱密码组合等。参考了刘建[11]在中所述的字典密码组合破解方法，利用密码生成器进行尝试，第一次通过泛式测试 234 条大字典密码没有成功，随后二次测试将范围缩小至 3 组，每组 48 条的小字典密码，成功登入。目标的密码设置格式为大学全称的拼音首字母+管理者姓名的拼音首字母+生日数字。整个过程费时 13 天。具体流程图如图 2 所示：

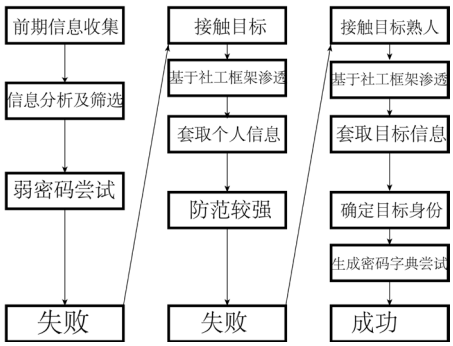

Figure 2. Flow chart of practical operations aimed at college students
图 2. 以在校大学生为目标的实际实操流程图

4. 结果

通过实施本次社会工程学实操，得出以下五点结论。

1) 本人利用了此 SNS 的社工漏洞。以网页邮箱为载体测试密码，绕过了此 SNS 的手机验证和安全系统。防止在测试密码期间 SNS 向目标用户发送安全警告导致密码被更改。本次渗透测试的结果已经表明，在网络环境如此复杂的今天，SNS 管理者对用户的安全保障在一定程度上仍有缺失。

2) 利用了与目标和目标关系者之间的信任关系。众所周知，一旦双方建立了信任关系，就意味着两者有了一定的信任基础。此时，对方会分享一些不同主题的信息，包括无意间谈到的一些我需要的信息。这种现实中常用的社会工程学攻击在 SNS 上也同样奏效。

3) 对方过于轻信社会工程人员的信息背景。这里攻击者与目标接触，伪造成想加入协会的新生，这样可以令目标快速放下戒心，进入攻击者想了解的话题。在这个环节中没有任何一个人对攻击者的信息背景产生怀疑，这是非常危险的。

4) 密码的设置。在这个案例中，公众号的密码设置的过于简单，以至于能被密码字典生成出来。因为公众账号的影响力高于个人账号，所以公众账号在被黑客入侵后的危害性也远大于个人账号，所以本人建议公众账号的密码设置至少要有一个大写字母和标点符号，这将大大提升账号的安全性和破解难度。

5) 爬虫的应用。基于 python 语言的网络爬虫在此次入侵中起到了关键作用，我们需要的信息在浏览器中由 HTML 代码构成的，攻击者通过爬虫获取这些内容，对 html 代码进行分析和过滤，从而在短时间内获取攻击者想要信息，大幅缩短了人工查找所需的时间。减少信息获取时间，降低目标对自己的怀疑程度，这一点在社会工程学攻击中尤为重要。

5. 讨论

本文通过实操可以看出在我国 SNS 以大学生为代表的网络用户在网络安全和反社工方面仍隐藏着较多安全漏洞。就结果来看安全意识不高，即便在校大学生是我国文化程度较高的一个群体，也存在容易被社工攻击成功渗透的可能。以此为基准进行推测，我国文化程度较低的其他群体是否存在更多的风险是下一步研究的内容。本文着重强调 SNS 程序编写时产生的社工漏洞和用户自身的社工漏洞，希望可以为研究网络安全提供参考，从而引起公众对个人隐私和网络安全的重视。同时下一步的工作着眼于对攻击过程中微观的分析及攻击流程优化以及相关社工工具的改进。

基金项目

本项目受上海对外经贸大学人工智能变革与管理研究院区块链技术与应用研究中心资助。项目号：SUIBE-ABC-2020-1。

参考文献

[1] Hadnagy, C. (2013) Social Engineering: The Art of Human Hacking.

[2] 王治, 范明钰, 王光卫. 信息安全领域中的社会工程学研究[J]. 信息安全与通信保密, 2005(7): 233-235.

[3] 刘慧康, 赵禹铭. 基于 SNS 隐私悖论的社会工程学研究[J]. 电脑知识与技术, 2018, 14(36): 13-15.

[4] 崔理华. 基于社交媒体的档案信息服务优化研究[J]. 当代旅游, 2018(7): 141-141.

[5] 吕耀怀. 大数据时代信息安全的伦理考量[J]. 道德与文明, 2019(4): 84-92.

[6] 卢志科, 康晓凤, 眭桢屹, 等. Web 应用漏洞扫描检测系统[J]. 软件导刊, 2019, 18(8): 196-190.

[7] 廖双. 浅谈网络安全下的黑客社会工程学攻击[J]. 计算机产品与流通, 2018(4): 73.

[8] 张弘, 石瑞民, 丁锰. 密码持有人信息与所使用密码关系的调查统计分析[J]. 中国人民公安大学学报: 自然科学版,

2013(1): 80-83.

[9] 钱程, 阳小兰, 朱福喜. 基于 Python 的网络爬虫技术[J]. 科学技术创新, 2016(36): 273-273.

[10] 孙瑜惠. 微信使用中的隐私信息泄露与保护研究[D]: [硕士学位论文]. 武汉: 武汉体育学院, 2017.

[11] 刘建. 基于专用字典的密码破解方法研究与应用[D]: [硕士学位论文]. 哈尔滨: 哈尔滨工业大学, 2015.