一个真实的故事  
  
　　几年前的一个早晨，一群陌生人走进了一家大型远洋运输公司并控制了该公司的整个计算机网络。他们是怎么做到的?是通过从该公司的许多不同的员工那里一点点的获得帮助来达到目的的。首先，他们在实地踩点的两天之前已经对该公司进行了研究了解。例如，通过给人力资源部门打电话获得了公司重要员工的姓名列表。然后，他们在大门前假装丢失了钥匙让别人开门放他们进去。最后在进入三楼的安全区域时他们又故伎重演，这次他们丢失的是他们的身份标志，而一名员工面带微笑的为他们开了门。  
  
　　这群陌生人知道该公司的CFO那时不在公司，所以他们进入了他的办公室并从他没有锁定的个人电脑中获取了财务信息。他们将公司的垃圾堆翻了个遍，找到了各种有价值的文档。他们获得管理垃圾的门房的帮忙使他们可以将这些东西顺利的带出了公司。这些人同样学会了模仿CFO的声音，所以他们可以在电话中冒充CFO的身份装作很焦急的样子来询问网络密码。自此，他们最后终于可以使用常规的黑客手段来获取系统的超级用户权限。  
  
　　在这个案例中这些陌生人所扮演的角色是CFO请来对自己的计算机进行安全检查的网络安全顾问，而公司的员工对此都不知情。他们可以在没有从CFO那里获得任何权利的情况下运用社会工程学让自己畅通无阻(这个故事是Kapil Raina讲述的，他目前是Verisign的一名安全专家，并且和别人合作了mCommerce Security: A Beginner‘s Guide， 这本书也主要是他先前工作中的实际经验的总结。)  
  
　　定义  
  
　　我所读到的大多数介绍社会工程学的文章都有类似这样的开头“一种让他人遵从自己意愿的科学或艺术” (Bernz 2)，“一个外来的黑客使用心理学手段来欺骗合法的计算机系统用户，以获得他所需要的信息来访问该系统” (Palumbo)，或者是“从他人那里获取需要的信息(例如密码)而不是通过闯入目标系统实现” (Berg)。实际上，这些对社会工程学的解释都可以说是对的，关键在于你所处的角度问题。但是至少有一点是可以达成共识的:那就是黑客对人类天性中更趋于信任的倾向的聪明利用。黑客的目标是获得信息让他/获得那些重要系统的未授权的访问路径来获取该系统中的某些信息。  
  
　　信任是一切安全的基础。对于保护与审核的信任一般被认为是整个安全链中最薄弱的一环，人类那种天生愿意相信其他人的说辞的倾向让我们大多数都容易被这种手段所利用。这也是许多很有经验的安全专家所强调的。不论现在出版了多少关于网络安全漏洞，补丁和防火墙的刊物，它们对于安全所能起到的作用还是很有限的。  
  
　　目标和攻击手段  
  
　　社会工程学的基本目标和其他黑客手段基本相同:都是为了获得目标系统未授权访问路径或是对重要信息进行欺骗，网络入侵，工业情报盗取，身份盗取，或仅仅是扰乱系统或网络。常见的目标包括电话公司和应答服务机构，著名的大公司和金融组织，军事和政府机构以及医院。现在对那些网络公司的社会工程学攻击也开始出现了，但是仅限于那些较为出名的公司。  
  
　**想找一个很好的社会工程学真实案例是很难的**。一般成为攻击目标的机构都不愿意承认他们曾经是社会工程学攻击的受害者(不仅仅是因为承认机构基本安全设施存在缺陷是一件很尴尬的事，更重要的在于这会大大影响机构的形象)并且记载这类攻击的文档也很少见，所以没有人可以肯定他能够完全辨别出正在发生的社会工程学攻击。  
  
　　为什么机构总是成为社会工程学的目标呢?这是因为相对于许多技术上的黑客手段非法获取帐号来说社会工程学是一种更简单的手段。***即使对于那些技术很高的人，只是仅仅拿起电话向别人询问密码要比通过技术手段进入系统要容易。***并且实际上这也是黑客所经常做的。  
  
　　对于所发生的社会工程学类的攻击可以分为两个层次来进行分析:物理上的和心理上的。首先我们对攻击发生的物理地点进行讨论:**工作区，电话，你公司的垃圾堆，甚至是在网上。**对于工作区来说，黑客可以简单的只是走进来，就像电影上的那样，然后开始冒充被允许进入公司的维护人员或是顾问。入侵者悠闲的把整个办公室逛个遍直到他或是她找到了一些密码或是一些可以稍后在家里对公司的网络进行攻击，利用的资料之后就会从容的离开。另一种获得审核信息的手段就是简单的站在工作区那里观察公司雇员如何键入密码并偷偷的记住。  
  
　　使用电话进行的社会工程学攻击  
  
　　最流行的社会工程学手段是通过电话进行的。黑客可以冒充一个权利很大或是很重要的人物的身份打电话从其他用户那里获得信息。一般机构的咨询台容易成为这类攻击的目标。黑客可以伪装成是从该机构的内部打电话来欺骗PBX或是公司的管理员，所以说依赖于对打电话的人身份的确认并不是很安全的做法。以下就是一个Computer Security Institute曾经提到的典型PBX伎俩:“嗨，我是你的AT&T维修员，我现在正在工作，但是需要你帮我按几个键。”  
  
　　还有更聪明一些的手段:“他们会在半夜打电话给你:“六小时之前你是不是打过电话到埃及去了?”“没有啊。”然后他们会说，“我们现在查询到刚才发生的一次有效呼叫，使用的是你的电话卡并且该电话是打往埃及的。所以你得支付$2000的电话费帐单虽然可能如你所说这实际上是别人使用的费用记到了你的账上”他们接着会说，“我现在可以帮你把这$2000的电话帐单消除，但是需要你告诉我你的AT&T卡号和密码。”然后大多数人都会落入这个圈套中。” (Computer Security Institute)。  
  
　　**咨询台之所以容易受到社会工程学的攻击是因为他们所处的位置就是为他人提供帮助的**，因此就可能被人利用来获取非法信息。咨询台人员一般接受的训练都是要求他们待人友善并能够提供别人所需要的信息，所以这就成为了社会工程学家们的金矿。大多数的咨询台人员所接受的安全领域的培训与教育很少，这就造成了很大的安全隐患。  
  
　　一名在计算机安全机构中工作的专家曾经做过这样的实验来揭示咨询台所隐藏的安全漏洞。他“打电话到一家公司的前台。“请问今晚值班负责人是谁?”“是Betty。”“我有事情需要和Betty讲。”[他的电话被转接到了Betty那里]“嗨，Betty，今天很倒霉是吧?”“不啊，为什么这样说呢?”“你的系统停掉了。”“我的系统没有关闭啊，运行情况很好啊。”他说:“你最好退出登录一下。”她退出登录。然后他说，“现在重新登录。”她重新登录。“可是我这里一点变化也没有啊。”他说“再重新退出看看。”她还是很听话的照做了。“Betty，看来我得从这里将你直接登录来看看究竟你的帐号出了什么问题。现在把你的帐号和密码都告诉我。”然后Betty就会通过咨询台把自己的帐号和密码告诉他。”  
  
　　另一种黑客的电话攻击的战术是通过站在付费电话或ATM机旁边偷看实现的。黑客可以简单的通过这种方式获得信用卡号和密码。(恰好我的一个朋友在一个大机场就遇到了这种情况)在机场里面很多人都站在电话的旁边，所以在这种公共地方你应该特别小心。  
  
  
　　进入垃圾堆  
  
　　翻垃圾是另一种常用的社会工程学手段。因为企业的垃圾堆里面往往包含了大量的信息。The LAN Times列出了下列可能在垃圾堆中找出的危害安全的信息:“公司的电话本，机构表格，备忘录，公司的规定手册，会议时间安排表，事件和假期，系统手册，打印的敏感信息或是登录名和密码，打印出来的源代码，磁盘和磁带，公司的信件头格式以及备忘录的格式，以及废旧的硬件。  
  
　　这些资源可以向黑客提供大量的信息。电话本可以向黑客提供员工的姓名与电话号码来作为目标和冒充的对象。机构的表格包含着信息可以让他知道机构中的高级员工的姓名。备忘录中的信息可以让他们一点点的获得有用信息来帮助他们扮演可信任的身份。企业的规定可以让他们了解机构的安全情况如何。日期安排表更是重要，黑客可以知道在某一时间有哪些员工出差不在公司。系统手册，敏感信息，还有其他的技术资料可以帮助黑客闯入机构的计算机网络。最后是关于废旧硬件的问题，特别是硬盘:黑客可以对它进行恢复来获取有用信息。(我们会在下来的第二篇文章中进行相关讨论)  
  
　　在线的社会工程学  
  
　　国际互连网是使用社会工程学来获取密码的乐园。这主要是因为许多用户都把自己所有账号的密码设置为同样的一个:Yahoo, Travelocity, Gap.com…………。所以一旦黑客拥有了其中的一个密码以后，他(或者是她)就获得了多个账号的使用权。黑客所常用的一种手段是通过在线表格进行社会工程学攻击。他可以发送某种彩票中奖的消息给用户然后要求用户输入姓名(以及电子邮件地址——这样他甚至可以获得用户在机构内部使用的帐户名)以及密码。这种表格不光可以以在线表格的方式发送，同样可以使用普通邮件进行发送。况且如果是使用普通信件这种方式的话这些表格看上去就会更加像是从合法的机构中发出的，欺骗的可能性也就更大了。  
  
　　黑客在线获得信息的另一种方法是冒充为该网络的管理员通过电子邮件向用户索要密码。这种方法并不是十分有效，因为用户在线的时候对黑客的警觉性比不在线时要高，但是该方法仍然是值得考虑的。进一步来说，黑客也有可能放置弹出窗口并让它看起来像是整个网站的一部分，声称是用来解决某些问题，诱使用户重新输入账号与密码。这时用户一般会知道不应当通过明文来传输密码，但是即使如此管理员也应当定期的提醒用户防范这种类型的欺骗。如果想做到进一步的安全的话，系统管理员应当警告用户任何时候除非是与合法可信网络工作员工进行面对面交谈的情况下才能公开自己的密码。  
  
　　电子邮件同样可以被用来作为更直截获取系统访问权限的手段。例如，从某位有信任关系的人发来的电子邮件附件中可能携带病毒，蠕虫或者是木马。一个很好的案例是VIGILANTe提到的对于AOL的攻击:“在这个案例中，黑客打电话给AOL的技术支持中心，并与技术支持人员进行了近一个小时的谈话。在谈话中黑客提到他有意低价出售他的汽车。那名技术支持人员对此很感兴趣，于是黑客就发送了一篇带有表明为“汽车照片”附件的电子邮件给他。但是实际上，那不是什么汽车的照片，邮件执行了一个后门程序让黑客可以透过AOL的防火墙建立连接。  
  
　　说服  
  
　　黑客他们自己从心理学角度对社会工程学做的阐述中强调了如何调整出一个完美的心理状态去攻击。基本的说服手段包括:。不论是使用哪一种方法，主要目的还是说服目标泄露所需要的敏感信息，所以这时一个社会工程师实际上就是一个可以被信任并由此获得敏感信息的人。另一个很重要的地方在于不要一次询问太多的信息，而是每次从某个人获得少量的信息来维护良好的自身形象。  
  
　　扮演一般来讲是说构造某种类型的角色并按该角色的身份行事。并且角色应该是越简单越好。某些时候就仅仅是打电话给目标，说:“嗨，我是MIS的Joe，我需要你的密码，”但是这种方式并不是任何时候都有效。在其他情况下黑客会专心调查目标机构中的某一个人并在他外出的时候冒充他的声音来打电话询问信息。根据Bernz，一个在这方面发表了大量文章的黑客的说法，他们是使用某种小设备来伪装声音并且还要对他们扮演目标说话的方式与机构的组织结构进行大量的研究。但是我认为这种手段基本上不具备扮演攻击的特征，因为它需要大量的时间来进行准备，但是无论如何，这种攻击方式同样是存在的。  
  
　　在扮演攻击中经常采用的角色包括:维修人员，技术支持人员，经理，可信的第三方人员(例如总裁的执行助理打电话说总裁已经允许他对某些信息进行询问)，或者是企业同事。在一个大公司这点是不难实现的。因为每人不可能都认识公司中的每个人员而身份标识是可以伪造的。这些角色中的大多数都具有一定的权利，让别人会不由自主的去巴结。大多数的雇员都想讨好老板，所以他们会点头哈腰的对那些有权利的人提供他们所需要的信息。  
  
　　让他人服从是一种基于团体的行为，但是有时也可以利用来说服单一个体，告诉他所有人都已经提供了黑客现在所询问的同类信息，假设黑客现在扮演的是一名IT经理。黑客所需要做的就是让目标暂时对自己职责的不明确。  
  
　　还有一种比较有争议的社会工程学手段是仅仅简单的表现出友善的一面来套取信息。其理由是大多数人都愿意相信打电话来寻求帮助的同事所说的话，所以黑客只需要获得基本的信任就可以了。进一步来说，大多数的雇员会友善的作出回应，特别是对于女性的请求。稍稍恭维一下目标或是与他调情会让目标乐意进一步的合作，**但聪明的黑客在获取信息的时候分寸会把握得很好，不会让目标对任何的特别之处产生怀疑。**一个微笑(如果是在面对面的场合下)或者一句简单的“谢谢”都可以成为合作的开始。如果这个还不够的话，冒充新手同样可以达到目的:“我都糊涂了，(眨眼睛)你能帮帮我吗?”  
  
　　反向社会工程学  
  
　　获得非法信息更为高级的手段被称为“反向社会工程学”。黑客会扮演一个不存在的但是权利很大的人物让企业雇员主动的像他询问信息。如果深入的研究，细心的计划与实施的话，反向社会工程学攻击手段可以让黑客获得更多更好的机会来从雇员那里获得有价值的信息。但是这需要大量的时间来准备，研究以及进行一些前期的黑客工作。  
  
　　根据Rick Nelson所写的《黑客手段:社会工程学》中的说法，反向社会工程学包括三个部分:暗中破坏，自我推销和进行帮助。黑客先是对网络进行暗中的破坏让网络出现明显的问题，然后他就来对网络进行维修并从雇员那里获得他真正需要的信息。那些雇员不会知道他是个黑客，因为他们网络中出现的问题会得到解决，所有人都会很高兴(包括黑客在内^\_^)。  
  
　　结束语  
  
　　当然，任何一篇社会工程学的文章都不能不提到Kevin Mitnick,所以我也引用他在Security Focus发表的一篇文章中的一句话:“你可以花大价钱购买技术与服务……但是你的网络设施同样免不了受到老伎俩的侵害。”