第 1 篇　黑客文化篇

神话——WEB 蛛网迷宫

《网络迷情》中连接的纵横交错的光缆。黑客帝国中光怪陆离的空间。

在现实中也真的很像一个数字迷宫：不同的网络组成；功能繁多的服务；数之不尽的 WEB。网页之间的内容完全不同，之间的切换就像从一扇门走入了另一个天地，就算我们耗尽一生也难踏遍这个虚拟世界的每一个门。

更可怕的是我们所看到的并不一定是真实的信息。也许平常的信息下面隐藏着无数的秘密，这还不是最大的威胁。在神话中，迷宫存在着一种巨大的牛面人身的怪物，随时，都准备吞噬送到嘴边的祭品。在网络中可以说也存在着这样的怪物，虽然他们不是牛面人身，也不能真的吃掉你，却能破坏你视如珍宝的数据和偷走你的个人隐私。有人管这样的人叫做黑客。谜一定是存在的，但黑客是不是谜，这是个值得思考的问题。我们把这种思考放在后面章节中。现在，先来认识一下这个“谜”和我们都已经不能离开的这个网络迷宫。

迷宫的构造—— 网络与建筑

迷宫是一种建筑，而且是一种复杂的建筑。

如果说网络真的是一座迷宫的话，那它也应该是一座庞大而辉煌的建筑。就像古希腊轩昂的庙宇或者中世纪欧洲高大的城堡。

巧合的是，很多时候人们也经常把网络和建筑相提并论。例如在网络中电子商务就被称作鼠标和水泥的工作，将网络上一些特殊的路由器叫做防火墙。

网络的建设者们也喜欢用建筑的结构来构建网络。建筑是有层次、错落有致的。而与建筑一样，网络也是分层的。在标准的图纸上，网络是一个七层的建筑。而在实际的互联网中采用的是五层建筑。熟悉网络的人都知道我指的是 OSI 的 7 层协议和 TCP/IP 四层协议。在每一个层次中，就像建筑卧室和大厅一样，人们通过划分不同的服务提供不同的网络功能。就这样，人们通过这 7 层建筑的图纸，按照图纸最上层的程序文本，用最下层数字世界里的水泥——bit位，构建了网络这样辉煌的建筑。这座超大规模的建筑宏伟之处丝毫不输给现实中的金字塔、万里长城、阿耳忒迷斯神庙以及美国的帝国大厦。更神奇的是，这座建筑还在不断地扩大。

如果有人认为这还不够，那我们不妨把网络与建筑学做个类比。会发现二者有更多的相通之处。

1. 实用性 不论是网络还是建筑，第一目的都是为了使用。建筑是为了住宿，而网络是为了通信。所以二者的发展最终方向都是使人们的生活变得更加舒适和便捷。这些是

建设者们必须遵从的规则。那些对我们生活来说多余的、有害的设置必将被淘汰。非常值得强调的是 网络开始建设时,这不是很重视安全性,这不是‘ 建设者们 ’疏忽了,而是当时为了通信性而牺牲了安全性。这也是在一个时期内突出实用性的表现。未来安全先进的智能家居和智能网络也必然是技术复杂而使用方便。

2. 个性化：在不影响实用性前提下，建设者个人的审美角度甚至是个人习惯都会很容易影响到使用者的风格,形成‘ 个性化 ’的建筑风格。“ 个性化 ”的建筑可以表现在很多方面,又比如,建筑的外观造型上,既体现区域文化的特征又风格各异 比如,在环境设计方面强调‘ 均好性 ’理念,彻底摈弃传统的‘ 四菜一汤 ’模式 再比如,在户型设计方面,根据消费者的需求‘ 量体裁衣 ”,重新定义传统上的厅、卫、厨……。“ 个性化 ”的开发来源于创新。而在互联网上，许多门户网站提供一些 “ 以用户为中心 ” 的个性化服务。可以使用户在服务提供商的服务器上存储自己的电子邮件地址、住址和喜好等等个人的个性化信息。当用户访问服务提供商的网站时,只需登录一次,就可以在不同的网址、不同的服务器,甚至不同合作伙伴的网站上畅行无阻，这些个人信息将时刻紧密相随。除了门户网站给注册用户一个虚拟的私人空间外，互联网服务的个性化还表现在诸多购物服务、在线订票服务、在线付账单和价格比较服务之中。例如订飞机票，由于大多数用户只对从自己居住地出发的往返票感兴趣，网站就通过存储用户的地址、电话、信用卡等信息方便用户多次订票,与此同时,网站已‘ 悄悄 ’把用户分类为商业旅行用户和娱乐旅行用户等等,并不失时机的在用户浏览的网页上添加一些旅行社促销等相关广告内容。有的网站允许用户自己设计商品,不论是样式还是图案、尺寸,若是在 10 年前，想要购买一双超过 45 码的鞋,搜遍全北京也可能毫无结果，即使能找到一家，也往往就此一家绝无分号。

3. 艺术性：对于建筑，我们并不陌生，应该说建筑是一种艺术，可以说很多建筑上的风格、流派、观念,都源于对艺术的探索与思考。而目前,当代艺术史已把建筑列为极其重要的艺术，甚至可以说，这个世界上所剩的最最经典的艺术是建筑。微软认为建立网络和管理网络都是一种艺术，互联网不但是技术的结晶，也是人类艺术的结晶，网络上的主页更是全人类艺术的载体。曾几何时，艺术创作一直是少数人的特权，因为任何艺术创作都需要特定的工具，而掌握任何一种传统的艺术工具都是件费时费力费神的事。自从有了互联网，艺术高深莫测的时代一去不复返了。在个人主页这一平台上，艺术回归大众。个人主页本身就是一种全新的艺术形式，它集传统艺术、行为艺术、装置艺术于一身。先锋而不晦涩,前卫而不腐朽,通俗而不庸俗。

4. 时空变换性：建筑是动态的，是随着时空的变化而变化的。人类有过什么样的思想,经历过什么样的时代,一定会在建筑中体现出来,建筑是时代的烙印。农业文明时代，房子的功能是混合的，即多功能的。而在工业文明时代，住宅功能趋向细化，居住和工作区域分离，整个工业文明的发展就是专业化和逐渐细分的过程。随着信息时代的到来，工作和生活追求效率，这又需要一种融合，这种融合却是一种升华，是效益的提高和整个社会的进步。如果以 1993 年浏览器诞生为起点，互联网这十年的发展虽然波澜壮阔、历经沧桑，但是在历史长河中，互联网革命仅仅完成了初级阶段。当然，推动这种变化的是其内在创作的精神，就像一个著名 IT 厂商的广告一样“：土木只是外表,网络才是世界的经脉 ”。这也是建筑师与网络技术工程师的区别。可以说建筑师也是一种黑客，反之亦然。

第1章 罗马城的建设

如果说网络很像一个超大型的建筑，那么它绝对不是一日建成的。那么是谁建立了最初这个罗马城？网络——黑客最大的贡献。这句话听起来类似“网络——计算机最重要的应用”。

黑客本来就是计算机革命的主角和英雄。是的，我们现在的网络最初是由最顶尖级的黑客所构造的，实际上早期的个人计算机也如此。

1.1 网络奠基人黑客

早期的计算机黑客是一群非常独特的人。据说他们中的许多人不善交际，也不懂人情世故，是一批只知道工作的书呆子。作为一个群体，他们的商业意识十分薄弱，政治意识更是匮乏，是一些地地道道的技术人员。到了 20 世纪 60 年代末期，在美国，一批新的计算机黑客开始崭露头角，他们中有许多是西海岸反越战运动的活跃分子。命运注定了他们要戏剧性地确立计算机的新形象，赋予 IBM 和其他大公司所从未赋予的色彩。

开始 Hacker 的发展都是以 MIT 的人工智能实验室为中心的，但斯坦福大学人工智能实验室(简称 SAIL)与稍后的卡内基梅隆(简称 CMU)也快速成长起来。三个都是大型的信息科学研究中心及人工智能领域的权威，聚集着世界各地的精英，不论在技术上或精神层次上，对早期黑客文化都有极高的贡献。另一个黑客重镇是 XEROX PARC 公司的 Palo Alto Research Center。从 1970 年初期到 1980 年中期这十几年间，PARC 不断出现惊人的突破与发明，不论质或量，软件或硬件方面，现代的鼠标－视窗－图标风格的软件就在那里发明。

在新泽西州的郊外，另一股神秘力量积极侵入黑客社会，终于席卷整个 PDP－10 的传统。1969 年，在 ARPANET 成立的同一年，有个在 AT&T 贝尔实验室的年轻人 Ken Thompson 发明了一种新的操作系统——后来名彻整个电脑世界的 Unix。Ken Thompson 很喜欢 Multics，他因为写了一个游戏 Star Travel 没有电脑可玩，就找到实验室里一台报废的机器 PDP－7，编写了一个操作系统，该系统在设计上有从 Multics 抄来的也有他自己的构想。他同事 Brian Kernighan 非常不喜欢这个系统，嘲笑 Ken Thompson 说：“你写的系统真差劲，乾脆叫 Unics 算了(Unics 发音与太监的英文 Eunuchs 一样)。”就这样，Thompson 的系统就叫了这个名字，只不过稍微改动了一下，叫 Unix。他的同事 Dennis Ritchie，发明了一个新的计算机语言 C语言，于是他与 Thompson 用 C 把原来用汇编语言

写的 Unix 重写一遍。C 的设计原则就是好用，非常自由弹性很大。就这样 UNIX 和 C 完美地结合成为一个统一体，C 与 Unix 很快成为互联网世界的主导。

在 TCP/IP 和 OSI 之争中，UNIX 专家约依改变了这一切。程序员们喜欢 UNIX 的灵活性和可移植性。大约在 1981 年，一个叫比尔·约依的 UNIX 计算机黑客取得了阿帕网络的资助，把 TCP/IP 协议编写进了 UNIX 之中。然后，在 1982 年，约依和两个斯坦福商学院研究生一起开办了“太阳微系统公司”，第一批“太阳”牌计算机安装完全以 TCP/IP 协议为规范的 UNIX 系统。这一软件在互联网发展史上写下关键一笔。“太阳”公司把网络软件作为机器的一部分安装在它所出售的计算机内而不单独收费，上网人数骤然增多，以 TCP/IP 协议为基础的互联网长势旺盛。欧洲的大学里也兴起了使用 TCP/IP 协议的地下运动。这个事件推动了事态的发展，为 TCP/IP 和 OSI 之争分出了胜负。TCP/IP 协议已无所不在，那么多人依赖于它，以致要想遏止它的势头用别的什么东西来替代它是不可能的。凭借无声而凶猛的冲击，TCP/IP 协议战胜了官方颁布的 OSI 标准。OSI 终于在大众的力量面前败退，在黑客面前败退。

1.2 贡献

黑客们最大的贡献：改变生存的方式，而且花费如此之小。

本来传统的通信技术可以扮演这个角色，可是自身商业性使之拱手让人。而黑客的奉献精神则使我们如此轻易地尝到这顿迟来的免费午餐。

电脑化空间的出现，使人类的时空概念发生了根本性的改变，对人及其所生存的环境都产生了巨大的冲击和影响。物理空间曾经对人具有非同寻常的意义。以往的人们终其一生，活动的区域可能不会超过居所附近步行可及的范围。后来，火车、汽车、轮船和飞机带来了人的流动性；现在，我们终于走到了大陆的尽头。我们曾经幻想会有永无止境的“边疆”等待我们去发现，但当我们从太空中俯瞰过地球之后，这种幻想被击得粉碎。开发殖民地的时代已彻底成为过去。这一方面使得土地的价格飞涨，另一方面表明，人类已经进入了一个需要依靠自身创造力来获得不断增长的时期，在这一时期里，财富和权力的聚集应该发生在另外的层面。

现在，惟一可供我们的文明继续扩张的领土——惟一真正的边疆——就是电脑化空间。它是人类赖以相互交往、发展经济、进行社会和政治谋划的新场所。

虽然电脑化空间并不是“真实”的物理空间，但也并不全然虚幻 在其中发生的事情会带来“真实”的后果。以电话来推论，人们已同这样的空间相处了上百年。一些人凭借在这一空间里的努力变得富有而闻名。一些人游乐于其中而流连忘返。一些人严肃地思考它的意义，一些人力图限制它的发展，还有一些人在国际场所围绕它作艰苦的谈判。当然，从一开始，一些人就在里面制造犯罪。

近 20 年，这一空间拓展疆土的步伐异乎寻常地迅速。电话开始与计算机杂交繁育，巨大的电子蜘蛛把整个世界织成了一张网。尽管电脑化空间仍然虚无缥缈，但却开始具有某种奇怪的“实感”了——把电脑化空间作为一种独立的存在来讨论，已不值得大惊

小怪。

因为人们开始进驻这个空间。不是一小撮人，不是少数技术怪杰，而是成千上万的普通人。也不是只在那里逗留片刻，而是几小时、数星期乃至经年累月。电脑化空间不仅体积扩大了,而且重要性也空前上升。

现在，无数人在电脑化空间里开创事业。人们在那里相遇甚至相爱，建立自己的社区,聊天,说长道短,筹划事情,互致信件,交换大量有价值的数据,姑且不论这些数据合法还是非法。

例如,在国际互联网上,人们可以足不出户,用电脑收发电子邮件,到银行存取款,调阅图书馆的藏书和当天的报纸,参加国际会议,看电影和听音乐,等等。简而言之,就是人们平时在现实空间环境里的工作、学习、娱乐，在电脑化空间里都可以做到。对于许多互联网的忠实用户来说，电脑化空间一点也不比现实空间更加虚幻，或者说，电脑化空间就是现实空间！

美国哥伦比亚大学原计划用 2 000 万美元修建新的图书馆大楼，经过比较，改用了一套电脑装置，把计划中的图书馆变成了一个用电脑网络访问的电脑图书馆。在此，电脑的虚幻空间打败了实体的建筑空间。

这种事例今后会越来越多：非物质的、无固定场所的虚拟空间将替代、或部分替代现有的物质实体空间。有人描述说,将会出现许多虚拟的商场、银行、图书馆、美术馆、大学，等等。它们的形象就是电脑屏幕窗口里的一个个设计精美的小小图标，你用鼠标轻轻一点，就进入到那虚拟的迷宫般的电脑化空间里去了。城市的概念也将发生改变，实体城市外，还将有虚拟城市；交通网络被形象高速公路所取代，交通法规变为电脑软件使用规范，公共场所成为虚拟的电子广场。在这个城市里，人们不受空间距离的限制，可以用光速访问政府某首脑，去美术馆查看印象派著名画家的不知名的作品，或与朋友聊天和游戏，等等。

到那时，所谓的信息时代的建筑和城市将会出现，而实体建筑和城市形象也将大大改变。城市不再有多种多样的建筑形式和种类,现在林立的办公楼、商场、邮局、银行等多种建筑将会变得寥寥无几，取而代之的是一组组的居住小区，每一个小区都有和全球通信系统相联系的网络；家居的外形可能十分简洁，而内部则布满了各种敏感元件，电子插座开关等 电视、音响、电话等家用电器都由一台隐藏在墙壁里的电脑所取代 唱片、磁带、报纸将在物质上消亡，转而通过信息网络来发行；人们很少需要出门，每个人都可以自由自在地支配自己的时间,坐在自己家中办公、上课、读报、看电影、或上虚拟商场购物、上虚拟饭馆点菜等等。当然买的和吃的都是实实在在的东西，而非电子商品和虚拟的京酱肉丝。

在互联网步入商业化的过程中，到处可以看到最初“黑客”的影子。黑客缔造了反商业软件的民主王国——开放源代码世界。

商业软件使得一批软件公司暴富起来，真正出现富可敌国的巨型企业，但这一切并没有给黑客们真正想要的。有人认为，黑客文明开始失去真正能够繁衍的土壤，真正黑客的名声开始为一些系统入侵者替代，人们开始渐渐忘怀那些能够自己写出整个操作系统软件的真正黑客。在每个人都认为黑客文化覆灭的时候，奇迹又出现了，黑客文明没有衰亡，相反，倒是在一片商业软件的海洋里，陡然崛起。因为那是人类生生不息的文化命脉

所在。

1993 初，一个悲观的观察家撰文指出，已经有理由认为 UNIX 的传奇故事连同他带有的黑客文明将一同破产。许多人预测，从那时起 UNIX将在六月内死亡。他们很清楚,十年的 UNIX 商业化,使自由跨平台的 UNIX 梦以失败告终。UNIX 允诺的跨平台可移植性,在一打大公司专有的 UNIX 版本之间不停地斗嘴中丢失，一个完美的操作系统最终沦为多种版本的一团乱麻，这应该说是人类文明史上的一个重大悲剧。在专有软件社会中,只有像微软一样的‘集权制,大教堂’生产方式才能成功。那个时代的人悲观地相信，技术世界的个人英雄主义时代已经结束，软件工业和发展中的互联网络将逐渐地由像微软一样的巨型企业支配,再也没有‘佐罗’;世界是恺撒大帝的世界,计算机文明将进入黑暗的帝国时代。黑客已经死了，自由不复存在。

第一代的 UNIX黑客似乎垂垂老矣，衣食不饱(Berkeley 计算机科学研究组在 1994 丢失了自己的基金）。这是一个压抑的时代。专有的商业 UNIX 的结果证明那么沉重、那么盲目、那么不适当,以致微软能够用那技术等次的 Windows 抢走他们生存的空间，拿走他们的干粮。幸运的是，在新闻报道看不见的地方甚至是大多数的黑客看不见的地方，一种全新的黑客文化正贪婪地吸吮着 INTERNET 的雨露,顽强地开始生长,在软件帝国时代里，一个带者宿命的俄狄普斯正在网络世界的角落里，在羽翼的阴凉中发出低低地呼喊。最后，这些文化将采取一个全新的方向而得到梦想不到的成功。

如果没有 GNU 出现,没有划时代的人物偏执狂 Stallman 出现,黑客的世界也许会同朋客一样，永远的被打上失落一代的标签永远封藏,Stallman 是黑客世界的黑格尔。他使黑客超越‘我思故我在’的个人精神主义,把黑客‘面死而在’的技术精粹主义带到人类社会，让黑客的精神划破沉闷的电脑时空的束缚，在商业社会的天空激荡起绚烂的火光。Linus 创造了 LINUX，成为继比尔盖茨之后软件世界最有影响力的软件世界灵魂人物。但是相同,如果没有 Stallman 理论和精神的指引，Linus 思想的成果只能是黑客世界的一个传奇而已,同凯文·米克尼克没有本质的不同，更谈不上去撕破盖茨微软帝国的层层烟幕，让自由的阳光重新回阴蠢的软件世界。

黑客自觉的意识同黑客自主的精神理论碰撞的时候，伟大的奇迹就诞生了。那就是反商业软件的民主王国—— 开放源代码世界。

第2章 历史和发展

2.1 黑客文化的发展

由于 ARPANET 的迅速发展，使得各地研究人员能以史无前例的速度与弹性交流资讯，超高效率的合作模式开始出现。ARPANET 另一项好处就是把全世界的黑客们聚在一起，不再像以前孤立在各地形成一股股的短命文化，网络把他们汇流成一股强大力量。开始有人感受到黑客文化的存在，于是动手整理了有关术语放到了网络上，在网上发表讽刺文学与讨论黑客所应有的道德规范（Jargon File 的第一版出现在 1973 年）。黑客文化在已经接上 ARPANET 的各大学间快速发展。

一开始，整个黑客文化的发展以麻省理工学院的人工智能实验室为中心，但斯坦福大学的人工智能实验室（简称 SAIL）与稍后的 Carnegie-Mellon University（简称 CMU）快速崛起。三个都是大型的资讯科学研究中心及人工智慧的权威，聚集着世界各地的精英，不论在技术上或精神层次上，对黑客文化都有极高的贡献。

在 1975 年 SAIL 就第一次发布了由 Raphael Finkel 编写的“Jargon File”。加利福尼亚 Homebrew 电脑俱乐部的绰号为‘伯克利蓝’的 Steve Jobs 和绰号为‘橡树皮’的 Steve Wozniak 开始制作“蓝盒子”，并用这种装置成功侵入了电话系统。他们后来创建了苹果电脑公司。在 BASIC 软件成功的鼓舞下，Bill Gates 毅然从哈佛大学退学，于 1975 年 7 月在阿尔伯克基竖起了 MicroSoft（简称 MS）公司的大旗。Bill GATES 为公司制定了目标：“每一个家庭每一张桌上都有一部微型电脑运行着我们的程序！”从此，这家由青年学生创办的公司将大步走向世界，成长为全球最大的电脑软件公司。成功推出了非常著名的 Windows 系列操作系统和 Internet Exploler 网络浏览器等应用软件。

计算机革命浪潮开始了，商人来了，政客来了，更多的普通人来了，罪犯也来了。20 世纪 80 年代初期，主要就是软件公司开始崛起，包括受沃兹影响而成长起来的一代年轻黑客 John Harris、Richard Garriott 和 Jay Sullivan 等，他们创办了 Sierra On－Line、Broderbund 等软件公司。软件如同即兴的爵士乐一样，开始招来一夜间暴富的机会。有了巨大的钱眼，美国公司的商业文化开始大举入侵了。盖茨等‘反黑客’的价值观和行为，大举掠夺黑客们创造的成果，以精明商人的手段将这些创新兑换为“美元”。利润最大化的价值观开始颠覆黑客领土。是的，在 MIT 人工智能实验室中孕育出来的‘纯种’黑客，已经永远成为历史，随着 IT 应用的不断社会化，黑客的规模、特性和行为也越来越社会化。黑

客究竟是天才？是牛仔？是艺术家？是罪犯？是恶作剧者？也许，更准确的是黑客已经成为上述各类人物的混合体。

20 世纪 90 年代可以说是黑客的灾难和混乱时期，作为信息共享的产物，INTERNET 一方面为我们提供了极大的便利。另一方面，使用的人多了，林子一大，什么鸟都有，技术不再是少数人的专有权力，越来越多的人都掌握了这些技术，导致了黑客的概念与行为都发生了很大的变化。

在国内，黑客出现得比较多的应该从 1998 年开始。现在，国内网络上的“黑客”团体多不胜数，较大规模和实质内容的组织主要有“中国鹰派联盟”“安全焦点”以及在“中美黑客大战”中风头极盛的“中国红客联盟”等。

2.2 特点

黑客，从“妖魔”到“不速之客”，从个体到群体，其发展和演变十分神速。进入新世纪以来，有组织的黑客大战骤然升级，对抗次数频繁，其攻击手段和技术不断更新，阵容日渐壮大，其发展趋势愈来愈成为举世关注的“焦点”。他们的变化主要体现出如下特点：

群体联盟化

这是一个让网络安全执法部门比较头痛的问题，因为近期黑客的活动和行为，已不再局限于“个人主义”的信息盗窃和破坏，正在加速演变成一种社会模式，甚至形成具有政治化倾向的集团联盟。研究统计数字我们发现，2002 年总体攻击事件下降了，但网络犯罪造成的损失却持续增加。究其原因，正是普通的入侵攻击在执法部门的打击之下，开始从无序向有序发展，呈现群体联盟、分布协作的趋势。

地域全球化

黑客作为一种客观存在不是凭空产生的。近 20 年来，随着计算机及其网络的不断普及和延伸，地球似乎变成了一个“小村落”。上网已不再仅限于发达国家和地区，也不再是大中城市“网民”的特权和专利。一个黑客及其群体，只要拥有电脑、电话和调制解调器，就可以在世界任何一个地方上网，并向世界任何一点发起攻击，使人们防范黑客范围不断扩大，犯案认证更加困难。

构成社会化

黑客技术从一种所谓的精英文化正逐渐转向平民化。我国的黑客包括社会各个阶层的人，从无业“网民”到白领阶层，文化程度包括从初中生到研究生的几乎各个学历层次。

阵容年轻化

这一点我们的感受有时是令人震惊的。举一个最近的例子，我们曾经接到一个政府网络的报警，他们一台重要服务器被入侵，数据被完全毁坏。黑客同时留下邮件地址进行敲诈。我们在最初的分析中，认为这应该是一个能力很强，胆大妄为、经验老道的黑客，因为他所留下的邮件是虚假的，入侵留下的 IP 也是经过肉鸡跳转的，犯罪步骤有较强的逻辑性。然而最后真正抓住他时发现，他还只是一个高中的学生。在国外这类例子就更多。

这里要提醒各位读者的是，年轻化只是的一个表面现象。实际上，随着技术的简化，利用计算机犯罪的群体的年龄覆盖面越来越宽。

技术智能化

未来黑客程序都在开始向隐身、智能和可控化方向发展，其攻击力和潜在危害越来越大。一些狡猾的所谓“黑客高手”们开始成为武器制造和提供者。很多的自动攻击机、脚本化攻击程序,包括我们前面所说到的网络‘蠕虫’病毒,从应运而生到大规模泛滥,也正是由于这个原因。一些稚气的“脚本黑客”拿着这些武器将网络砸开缺口，而一些高级黑客在后面坐享其成。

手段多样化

黑客攻击手段和方法经历了由低到高的发展过程，并不断形成新的变种。在已掌握的 5000 多种黑客攻击手段中，新出现的黑客变种技术已增加到 60 多种。

动机“商业化”

黑客及其群体的类型和作案动机可以划分为多种。目前，该群体的作案动机一改往日那种以恶作剧、蓄意破坏、群体对抗和控制占有为主要目的，开始运用更高超的技术手段,采取更为隐蔽和欺骗的方法,通过因特网‘窃取’具有‘卖点’的软件专利产品,并将‘盗窃”来的软件产品改头换面，用以商业目的，牟取暴利。据报道，近期美国及西欧有关机构,相继破获黑客以赢利为目的的网上‘盗窃’案例,已查获黑客及其群体用以‘盗窃’的电脑 60 余台(套),据估算有关商家和公司因此所造成的经济损失高达 120亿美元。

身份‘合法’化

目前，在西方甚至已有完全合法化的黑客组织、黑客学会等。在因特网上，黑客组织有公开的网站、信道和杂志，这些黑客经常召开黑客技术交流会。从 1998 年 11 月开始，每年在纽约召开世界黑客大会。在我国，由于专业安全技术人员稀缺，很多职业入侵者也加入到这个队伍,使黑客身份合法化,呈现出‘黑白不分’的状况。

“未来”军事化

世界各国试图招募和培养自己的网络战队伍。在有些国家，许多以前高级的网络罪犯摇身一变,成为炽热可手的安全顾问,通过运用‘以毒攻毒’的方式,采用了一系列黑客技术手段,来达到国家政治和军事目的。因此,有军事专家预言“利用国家支持的黑客组织,将是未来战场上不可忽视的重要军事力量。”

第3章 黑客精神的变迁

3.1 变迁

不管如何提纯黑客文化的精髓，或是将其中不知数量的破坏者划分出来，事实却是残酷的。传统的黑客精神正在变迁是不争的事实。随着信息技术的发展，黑客技术这项天生带有明显侵略性的技术就像被打开的潘多拉盒子，被越来越多的人们创造和利用，其中不乏混入许多不法之徒。

“近几日，最让全世界互联网企业和用户胆战心惊的一个消息就是网上黑客准备2003年7月6日在全球范围内发动一场入侵网站、篡改网页能力的大赛，据称黑客的目标是在6个小时内对6 000个网站进行破坏，遭受恶意破坏的网站数目有可能会达到两、三万个。这一行动有可能导致全球互联网瘫痪。美国政府对此发出警告，全球互联网企业都如临大敌。这一消息也引起了中国媒体的广泛关注，各大网站都纷纷进行报道，中国有关部门也提请互联网企业高度戒备。”

看到这则消息,脑子里立刻浮现出这样几个词汇 网上极端主义,网上恐怖主义,网上基地组织。这些黑客们理性的丧失和对“杀戮”的随意已经直逼真实世界的恐怖主义，甚至还会超过这些恐怖主义。因为真实世界的恐怖分子发动恐怖袭击时还有种种宗教、政治、经济、文化等方面的借口,网上黑客实施攻击根本就不要什么借口。

美国的这场‘全球黑客大赛’由一个叫 Defacers Challenge 的网站组织，并由第三方独立网站 zone-h.org来计算黑客得分情况。不料，zone-h.org 这个计分网站当天就被另一群黑客攻击，始终处于掉线状态。这场竞赛引起了媒体的极大关注，但是结果却是雷声大，雨点小。据后来的报道，只有几百个网站，而且大部分还是小企业的网站遭遇攻击。有专家认为，这样的攻击几乎每天都在进行，无法说明这次有什么与众不同。人们不禁要问，这大赛难道是一个骗局？

根据比赛的要求,要在6小时内攻破6 000个网站，也就是必须连续保持每分钟攻破17个网站。这种速度只能是利用程序漏洞扫描，这需要那些服务器本身就有明显的安全缺陷。比赛的奖励也近乎玩笑。况且，哪一次真正的黑客进攻前，会提前一个礼拜作广告？但如果是骗局，为什么又会受到这样的关注？仅仅是因为厂商要寻找商业的突破口，媒体要制造新闻事件，而一些十几岁的小黑客有多余的精力需要释放？

这个事件本身却恰恰蕴藏着整个世界的缩影。这个故事里头，有技术、有资本流动、

有全球化(全球黑客联动),俨然具备了 21 世纪的戏剧要素。黑客大赛夸口的目标亦宛如大规模杀伤性欺骗，它的威慑力使你不得不警惕，这是莫须有的名头。你不得不多买几台来自大洋彼岸的防火墙。你在明处,它在暗处 你是弱势,它是强势 你被攻击,必须交学费。你明知是祸躲不过，为此只有祸兮福兮，主动来提高企业的安全措施和技术储备。

另一方面，你并不因为被攻击而成为了弱势群体，而具备道德优势。相反，在全球化语境里，你将成为一个笑柄，攻击他人的黑客却成为当代的英雄和偶像，甚至据称黑客行为正在逐渐成为美国青少年的一种休闲娱乐方式。随后又被好莱坞的《黑客帝国Ⅱ》之类的文化霸权占据了 14 岁天才少年的心灵,你不但失去了现在,而且失去了未来。除非你接受这个丛林法则，认同这个我黑故我在的游戏。拒绝这个游戏就是等死，而玩这个游戏就是找死。

3.2 老黑客与新黑客

老辈学者曾经写文章说：现在世风日下，甚至连强盗的素质都在下降。在解放前，强盗绑票以后不是万不得已极少撕票，可是现在的强盗绑去人质以后动辄就撕票，甚至先把人杀了再勒索赎金。黑客也是黄鼠狼下老鼠，一代不如一代。

黑客原指热衷于计算机技术、水平高超的计算机专家，尤指程序设计人员。这些人的工作的出发点就是通过编写自由软件，促进信息与技术共享，使获取信息和计算机资源更为便利。他们富有社会良知，酷爱言论自由与隐私权，最反对对电子空间进行集权主义式的管理,所以他们要为此抗争。1990 年,黑客米奇·卡普和约翰·巴娄在旧金山创建了电子边疆基金会(EFF)，来促进网络空间的基本权利，他们把电子边疆基金会定义为“一个在计算机和互联网领域致力于公共利益，保护基本的公民自由，保护隐私权与言论自由的一种非盈利无党派组织。”从此我们可以看出，黑客们是在以一种理想主义的反叛姿态为计算机技术进步提供推动力量，他们希望通过自己的努力，创造一个更加开放的网络空间。

许多杰出的黑客对计算机和互联网的发展做出了重大的贡献，他们在互联网上的天空中灿若群星，光耀千秋。如李纳斯·托沃兹发明了 Linux,史蒂夫·沃兹尼亚克制造了第一台真正的个人电脑,蒂姆·伯纳斯·李发明了万维网,桑迪·勒纳与别人共同发明了因特网路由器,伯勒尔·史密斯发明了苹果计算机。甚至连比尔·盖茨也被认为最初也是一个黑客，自他孩提时代起，电脑就是他的激情所在，他把所有能挤出的时间都花在当地的电脑中心公司的电脑上编程。因为他没有获得使用计算机的权力（MITS 牛郎星)就编写了第一个 BASIC语言的解释程序并使它运行成功，由此而颇受黑客们的尊敬。盖茨与保罗·艾伦创办微软的最初打算就是为个人电脑开发编程语言，这是一个典型黑客主义的出发点，因为只有黑客才会使用这些机器来编程。只是到了后来，攫取利润动机才压倒了他的激情。

今天的黑客，也享有着和古老的黑客的同一个词。但却是魔鬼撒旦。按照弗洛伊德的学说，人有毁灭自身的本能。如今的黑客或许是双重人格的体现，或许是被惯坏的一

代。他们也有五种乐趣：毁灭事物的乐趣；使别人有用的东西变为无用的乐趣；将木马扫描程序打开,看到它们居然在运行的乐趣 面对重复的任务,不断学习的乐趣 工作在单纯的思考中，如此易于被其他黑客们驾驭的乐趣。也有一种黑客，比弱智的使用工具的黑客要强，那就是病毒或者黑客软件制造者。他们没有更大的心力去创造未来，也不屑于毁灭现在。他们的目的就是多多制造点麻烦，反对能够反对的一切。

对照老黑客们的追求，现在的这一帮子黑客，哪里还有半点老黑客的影子？他们的行为哪里还有崇高？哪里还有道义？如果说过去一段时间黑客搞破坏还有一点炫耀技术、炫耀本领、进行恶作剧的影子,那么现在的黑客早就成了网上暴徒,只知道破坏,只知道发泄，早就成了为破坏而破坏的黑客，就像是精神空虚毫无寄托的暴徒，无缘无故深夜到大街上去砸商店的玻璃来寻求乐趣。他们做的事，既损人也不利己，但是他们看到网络正常运行就难受，就是想搞破坏。这是一种不折不扣的网上打砸抢行为，这种行为意味着黑客文化的彻底堕落。他们实际上就是一群身穿黑衣、骑着摩托的日本暴走族在信息高速公路上横冲直撞。

近年的黑客频频发动袭击说明互联网安全形势有持续恶化之势，网络安全事件层出不穷。每年的黑客兴风作浪都造成巨大的损失。网络的特性决定了防范这种黑客袭击比防范来自真实世界的恐怖袭击更为困难。假使恐怖分子放出风声要炸金门大桥的话，美国得到情报后只要多派海岸警卫队警察加强巡逻盘查、提高安全警戒的级别就行了，可现在网络袭击神不知鬼不觉的，即使 FBI 也无计可施。面对这样一种网络安全生态环境，我们无法不忧心忡忡。网络之路将伸向何方呢？

第 2 篇　黑客技术篇

第4章 黑客威胁

互联网的发展已经到了使人们的生活与其有着更多的直接联系。随着政府上网、企业上网、更多的网民触网，不远的将来互联网必将成为人民生活中不可或缺的一部分。因此，网络的安全和稳定就会成为关系国计民生的大事。黑客的对任一要害部门的破坏都有可能酿成大的社会问题，对任一大的企业的破坏都有可能造成严重的甚至无法挽回的经济损失。随着黑客攻击频率和危害程度的加大，已经引起了人们的广泛关注。不少人士提出了不少的办法来解决这个问题，如加强法制、加大打击力度，加强对青少年的教育等，无疑是好的。但在这里需要明确这样几点：

第一，黑客是互联网的伴生物，在现有社会制度和时代特征下不可能消除。只要真正彻底的共享不能实现，只要存在各种各样的利益差别，只要人性中的好奇心存在，黑客就会存在下去。所以，与黑客的斗争是长期的。

第二，黑客的数量会增大破坏力会加强。不管采取任何打击措施，随着互联网进入民众的日常生活，教育程度差异、利益冲突、意识形态不同，黑客因个人原因或群体、民族、国家原因都会增多而不会减少。只不过引起社会关注的是那些超级黑客，而一般的黑客因破坏力弱而不被注意。而超级黑客的破坏力是巨大的，一旦成功，后果有时难以预料或评估。因此，应该充分认识黑客行为的影响。

第三，黑客是独特的，感化他们的可能性极小。他们一般痴迷于技术而不谙世俗规矩 想法狂热、新奇 对于世界、社会、互联网的理解怪异 計算机和网络是他们的生命，不仅是电子高手，而且对电子理论的了解超乎常人，比一般人深刻得多，物理对他们来说很容易。这就需要组织力量对黑客的思想、心理、行为样式作科学的、细致的研究分析，对黑客有一个准确的了解，以便采取相应有力的措施。

第四，媒体的宣传应该加大黑客危害程度的报道。这里引用江海客对媒体看法的话：“回顾一下媒体的一些报道黑客和黑客事件的手法，我感觉有三个不好的倾向 神话、丑化和美化，有了过分神话出来的力量，过度丑化激发的恐慌和逆反心理，加上不恰当叫好的鼓励，一方面是越来越多的人把成为一名黑客当作理想，另一方面则是有些黑客放弃冰山下面的生活，渴望来到前台戴上红帽子。”

其实，黑客技术并不下流，也并不深奥。相反，黑客技术是网络安全技术的一部分。或者可以认为就是网络安全技术。从反面说就是黑客技术，从正面说就是网络安全技术。这种技术被不法之人用了，当然要遭到谴责。但如果因为这种技术会引来犯罪而不准研究和介绍，也是不正确的。我们应该推广介绍这些技术，这样才能使我们对网络安全有更深的理解，从更深层次提高网络安全。

我们要善用这种技术，加强对这些技术的研究。

4.1 黑客入侵的步骤

黑客们究竟为什么要入侵某一目标？除非本身就是怀着特定的目的外，一般是偶然的因素居多，但在这偶然的因素下面也有许多必然的原因，如系统本身存在一些安全漏洞或Bug等，让黑客有机可乘。黑客通常采用以下的几个步骤来实现入侵目标主机的目的。

第一步：寻找目标主机并分析目标主机。在Internet上能真正标识主机的是IP地址，域名是为了便于记忆主机的IP地址而另起的名字，只要利用域名和IP地址就可以顺利地找到目标主机。当然，知道了要攻击目标的位置还是远远不够的，还必须将主机的操作系统类型及其所提供服务等资料作个全面的了解，这样才能做到“知己知彼，百战不殆”。此时，黑客们常会使用一些扫描器工具，轻松获取目标主机运行的是哪种操作系统的哪个版本，系统有哪些账户WWW、FTP、Telnet、SMTP等服务器程序是何种版本等资料，为入侵作好充分的准备。

第二步：获取账号和密码，登录主机。黑客要想入侵一台主机，首先要有该主机的一个账号和密码，否则连登录都无法进行。这样常迫使黑客先设法盗窃账户文件，进行破解，从中获取某用户的账户和口令，再寻觅合适时机以此身份进入主机。当然，利用某些工具或系统漏洞登录主机也是黑客们常用的一种技法。

第三步：得到超级用户权限，控制主机。黑客如果有了普通用户的账号，便可以利用FTP、Telnet等工具进入目标主机。在进入目标主机后，黑客一般是不会就此罢手的，因为普通用户的权限实在有限，所以他们就要想方设法获得超级用户权力，然后做该主机的主人。

第四步：打扫战场，隐藏自己。在黑客真正控制主机后，就可以盗取甚至篡改某些敏感数据信息，同时也会更改某些系统设置、在系统中置入特洛伊木马或其他一些远程操纵程序，作为日后入侵该主机的“后门”。入侵目的任务完成后，便会清除日志、删除拷贝的文件等手段来隐藏自己的踪迹。之后，他就可以实现“远程办公”，更为方便地进出俘虏到的主机。

4.2 黑客技术的基本原理和方法

4.2.1 口令入侵

所谓口令入侵是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。获得普通用户账号的方法很多，如利用目标主机的Finger功能当

用 Finger命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上 利用目标主机的 X.500 服务 有些主机没有关闭 X.500 的目录查询服务，也给黑客提供了获得信息的一条简易途径；从电子邮件地址中收集：有些用户电子邮件地址常会透露其在目标主机上的账号；查看主机是否有习惯性的账号：有经验的用户都知道,很多系统会使用一些习惯性的账号 造成账号的泄露等等。

4.2.2 端口扫描

所谓端口扫描,就是利用 Socket编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而侦知目标主机的扫描端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等等。常用的扫描方式有 Connect)扫描、Fragmentation 扫描。

4.2.3 网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具（如 NetXRay for Windows95/98/NT、Sniffit for Linux、Solaries等）就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

4.2.4 放置特洛伊木马程序

特洛伊木马(Trojans)程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或执行了这些程序之后，它就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在你的电脑中，并在你的系统中隐藏一个可以在 Windows启动时悄悄执行的程序。当你连接到互联网上时，这个程序就会通知黑客你的 IP 地址及被预先设定的端口。黑客在收到这些资料后，再利用这个潜伏其中的程序，就可以恣意修改你的电脑设定、复制任何文件、窥视你整个硬盘内的资料等，达到控制你的计算机的目的。

4.2.5 电子邮件攻击

电子邮件攻击主要表现为向目标信箱发送电子邮件炸弹。所谓的邮件炸弹实质上就是发送地址不详，容量庞大的邮件垃圾。由于邮件信箱都是有限的，当庞大的邮件垃圾到达信箱的时候，就会把信箱挤爆。同时，由于它占用了大量的网络资源，常常导致网络塞车，它常发生在当某人或某公司的所做所为引起了某些黑客的不满时，黑客就会通过这种手段来发动进攻，以泄私愤。因为相对于其他的攻击手段来说，这种攻击方法具有简单、见效快等优点。

此外，电子邮件欺骗也是黑客爱玩的把戏。他们常会佯称自己是系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令有可能为指定的字