信息网络安全防范技术丛书

黑客与反黑客

HEIKE YU FANHEIKE

张斌主编

北京邮电大学出版社
www.buptpress.com

黑客与反黑客

主编　张　斌
编者　王　玮　王铭皓　张　华
　　黄　洪　谢朝海　尚旭光

北京邮电大学出版社
·北　京·

内 容 简 介

我国正处在互联网络的飞速发展的时代，由于网络规模不断扩大、复杂程度日益升高，以及黑客攻击技术越来越完善，导致我国信息安全形势非常严峻，网络犯罪猖獗。这些都为政府和企业部门网络安全防范工作提出了新的挑战。在本书中，作者深入分析了当今黑客常用的攻击技术，并根据工作实践提出了多种反黑客方式和手段，希望广大读者通过学习和体会提高自身网络安全防范能力，同时也为各级信息安全主管提供一定的技术参考。

图书在版编目(CIP)数据

黑客与反黑客/张斌编著 .—北京：北京邮电大学出版社，2004
ISBN 7-5635-0886-4

Ⅰ.黑… Ⅱ.张… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2004)第 084597 号

书　　名：黑客与反黑客
主　　编：张　斌
责任编辑：张学静
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(100876)
电话传真：010-62282185(发行部) 010-62283578(FAX)
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×1 092 mm　1/16
印　　张：14.5
字　　数：371 千字
印　　数：1—4 000 册
版　　次：2004 年 9 月第 1 版　2004 年 9 月第 1 次印刷

ISBN 7-5635-0886-4/TP·125　　定　价：28.00 元

序 言

我们的世界正在日益演变成一个电子化的世界，所有的信息正在全面数字化，电子世界中四通八达的网络把人们联系在一起。在网络上，天涯变为咫尺，物理上的距离几乎都消弭于无形，人们可以运筹帷幄，决胜于千里之外。然而，网络方便的同时，也从来没有像今天这样担心网络黑客的威胁。人们不禁对人类有没有可能把握和控制互联网的安全使用提出了种种疑问？的确网络拥有的设备和协议以及网上的信息构成了一个极其复杂的系统，保证这样一个复杂的系统没有缺陷和漏洞是不可能的。环顾人类社会现象，我们认识到人体是一个复杂系统，但自然的演化给予人体相当的免疫力和自我控制能力；而同样作为高度复杂的航天飞机乃至航空母舰系统，都是由人刻意研制出来的，尽管在自动化程度上不尽人意，但如果设计没有出错它们应该是严格可控的。但是互联网，不管是今天还是未来，它与无穷浩瀚的信息资源发生联系，使得它既不同于人体也不同于一般的复杂机器。具有丰富内涵的网络空间至少目前是变成了一个不可控的复杂系统，钱学森几年前特地指出互联网可以说是一个“复杂巨系统”。

网络的黑客现象正是在这样的条件下诞生出来。从黑客的角度看，由于网络的复杂，协议众多，找到攻击入口和网络弱点的可能性很大，投入的尝试越多，攻击成功的机会也越大。如果攻击成功后的刺激很大，攻击者会变本加厉地投入力量。因此，与网络黑客的较量不仅仅是靠几件产品、几套工具，它是人与人的对阵，智力、经验之间的对策，乃至组织与组织之间较量。黑客的手法往往巧妙、技术高

明，通常是编程高手。在二十世纪六、七十年代，做一名计算机黑客是一件很荣耀的事情。“黑客”在当时用来形容独立思考然而却奉公守法的计算机迷。他们崇尚技术，骨子里渗透了英雄般的反权威思想。他们曾经云集在技术精英的堡垒麻省理工学院和斯坦福大学。作为一个群体，是一些地地道道的技术人员。然而，任何不负责任、失去方向和没有制约的权力都是令人恐怖的，包括计算机系统的控制权。随着部分黑客行为逐渐将注意力集中到涉及公司机密和国家安全的保密数据上，“黑客”的定义有了新的演绎。

如果黑客行为是一些涉世不深的青少年从一些“黑客俱乐部”、“黑客基地”等网站上了解到浅显的黑客手法和工具，由于法律意识的淡薄导致他们对入侵他人计算机系统的好奇和技术挑战心态，这只是要加强教育和引导的问题。然而，近些年国际间的事件纠纷往往引发网上的“爱国战争”，导致了各国都有一些自发或专门的“黑客组织”、“黑客纵队”等，这是一个不可小视的现实。

居心不良、恶意进行网络犯罪的分子利用黑客手法直接对计算机系统和信息网络构成了严重的安全危害。美国联邦调查局的报告表明，计算机安全犯罪，使美国每年有大约75%的公司蒙受损失。1995年统计，以白领犯罪为特征的计算机安全事件给全球造成的经济损失高达150亿美元。一名俄罗斯黑客通过安装在地下室的简单设备入侵层层设防的美国花旗银行，使其损失1600万美元现金。

随着冷战的结束和信息全球化步伐的加快，世界各国政府高度重视国家信息保障问题，并先后调整了国家安全战略，使信息保障在国家安全战略诸要素中的地位开始上升，成为国家安全战略中不可分割的重要组成部分。美国SGI公司于2003年一次就获得国防部2600万美元的订单，提供超级计算机、软件和技术服务，用于发展更先进的军事武器。而戴尔公司曾出售给海军陆战队6万台经过特别改进的个人电脑用于在作战前线的电子邮件等通信服务。在布什政府的2003年联邦预算中，用于电脑和网络安全的预算比2002年剧增了56%，达到42亿美元。布什总统还专门签署了一份用以确定“何时以何种方式”对敌人的计算机网络发动“黑客式毁灭性”的袭击，可导致敌国的雷达系统失灵、电力供应彻底中断、通信全部紊乱的“网上破袭战”。

近来发生在巴勒斯坦与以色列之间的“巴以黑客战争”已愈演愈烈，这场以互联网为载体的，由一些掌握网络黑客技术的政治活跃分子所发动的网络战被称作一场针对异教徒的“电子讨伐战”。这些活跃在网络战场上的“士兵”不断地进攻敌方的电脑服务器、散布病毒、入侵网站、发动电子邮件炸弹攻击，无论是规模还是激烈程度都在连续升级。一位21岁的以色列黑客声称：“计

算机安全本身就没有什么规则可言。”他和同伙攻击了一家黎巴嫩真主党和巴勒斯坦网站，从而导致阿拉伯和犹太人之间的网络战全面升级。而在巴勒斯坦一方认为与其称这是一场网络战，还不如说是一场信息战——一场超越传统媒体，让全世界了解自己的观点和主张的战斗。黎巴嫩真主党网站上声明：“我们的反击将只限于网络。我们将继续向全世界提供真实的信息，以此来反击对方的谎言。”

起于黑客行为、涉及信息对抗的网络现象，已经引起我国政府的密切关注。首先，国内许多网络在建网初期较少或者根本就没有考虑安全防范措施，不少网络工程本身没有认真处理网络系统的安全环节，是经不起严格验收的。大多的网络系统还缺乏配备有经验的安全管理员。根据国家权威部门的测试结果，国内相当大比例的单位计算机系统都多少存在安全漏洞，随时可让黑客入侵。无须多加说明，我国目前极其需要加固网络安全的措施，同时解决缺乏网络及电脑高级系统管理人才的问题。创造必要的条件保证这些技术人员在技术上的深造是极其有意义的，本书正是从黑客的基本手法介绍到反黑客的必要防范措施入手，汇集了详细丰富的技术资料，为读者提供了十分通俗易读且相当实用的一本读物。作者在从事黑客入侵防范工作中具有丰富的实践经验，以书会友，相信读者将从本书中获得各自的收益。

互联网的发展，包括网络安全的发展走过了一段曲折的弯路。不管是某些利益驱动的诱惑，还是部分领导盲目地跟近，今天我们应该引起反思。亡羊补牢，为时不晚，我希望全社会都能加强对网络的正确认识，加强安全防范意识，为我国未来网络经济的持续健康发展扫清道路。

许榕生

目 录

第 1 篇 黑客文化篇

第 1 章 罗马城的建成

1.1 网络奠基人:黑客 …… 3
1.2 贡献 …… 4

第 2 章 历史和发展

2.1 黑客文化的发展 …… 7
2.2 特点 …… 8

第 3 章 黑客精神的变迁

3.1 变迁 …… 10
3.2 老黑客与新黑客 …… 11

第 2 篇 黑客技术篇

第 4 章 黑客威胁

4.1 黑客入侵的步骤 …… 16
4.2 黑客技术的基本原理和方法 …… 16
4.2.1 口令入侵 …… 16
4.2.2 端口扫描 …… 17
4.2.3 网络监听 …… 17
4.2.4 放置特洛伊木马程序 …… 17
4.2.5 电子邮件攻击 …… 17
4.2.6 WWW 的欺骗技术 …… 18
4.2.7 其他攻击方法 …… 18
4.3 黑客技术基础 …… 18
4.3.1 TCP/IP 协议简介 …… 18
4.3.2 协议简介 …… 19

4.3.3 Ethernet …… 21
4.3.4 Internet 地址 …… 22
4.3.5 IP 协议和路由 …… 22
4.3.6 TCP 协议 …… 23
4.3.7 Linux 网络编程(Berkeley Sockets) …… 24
4.3.8 WinSock 网络编程 …… 25

第 5 章 信息收集型攻击

5.1 什么是信息收集 …… 27
5.2 信息搜集的步骤 …… 28
5.3 简单信息收集 …… 28
5.3.1 Finger …… 28
5.3.2 Whois …… 28
5.3.3 Nslookup …… 29
5.3.4 Tracertroute …… 29
5.4 端口扫描 …… 31
5.4.1 什么是端口扫描 …… 31
5.4.2 常用的端口扫描技术介绍 …… 32
5.5 堆栈指纹识别 …… 33
5.5.1 堆栈指纹识别技术 …… 33
5.5.2 利用 TCP/IP 堆栈进行远程操作系统判别 …… 38
5.5.3 探测远程主机操作系统指纹的全新技术 …… 39
5.6 数据侦听 …… 44
5.6.1 网络监听的原理 …… 44
5.6.2 检测网络监听的方法 …… 46
5.6.3 著名的 Sniffer 监听工具 …… 47

第 6 章 欺骗型攻击

6.1 欺骗攻击类型 …… 49
6.1.1 IP 欺骗 …… 49
6.1.2 电子邮件欺骗 …… 52
6.1.3 Web 欺骗 …… 53
6.1.4 非技术类欺骗 …… 54
6.2 身份隐藏:代理、肉鸡跳 …… 54
6.2.1 对“肉鸡”的利用 …… 54
6.2.2 利用“肉鸡”进行攻击 …… 56
6.2.3 几个常见攻击 …… 61
6.3 IP 欺骗 …… 62

6.3.1　基本概念…… 62
6.3.2　IP 欺骗 …… 63
6.3.3　IP 欺骗原理 …… 64
6.3.4　IP 欺骗过程 …… 66
6.4　域名劫持…… 68
6.5　会话劫持攻击…… 69
6.5.1　攻击原理…… 69
6.5.2　会话劫持攻击程序…… 70
6.6　man in middle …… 71
6.6.1　SSL 中间人攻击…… 71
6.6.2　利用 DNS 的转向进行 Man-in-the-Middle 攻击 …… 73
6.7　cookie 诱入 …… 74
6.7.1　cookie 欺骗原理 …… 74
6.7.2　cookie 欺骗 …… 74
6.8　社会工程学…… 76
6.8.1　社会工程学…… 76
6.8.2　社会工程学攻击实例…… 76

第 7 章　服务拒绝攻击

7.1　拒绝服务攻击…… 78
7.1.1　产生原因…… 78
7.2　常见 DoS 简介 …… 80
7.2.1　死亡之 PING(ping of death) …… 80
7.2.2　泪滴(teardrop) …… 80
7.2.3　SYN 洪水 (synflood)…… 81
7.3　碎片攻击…… 84
7.3.1　为什么存在 IP 碎片 …… 84
7.3.2　IP 碎片攻击 …… 85
7.3.3　ping of death …… 85
7.3.4　jolt2 …… 85
7.4　DDOS …… 86
7.5　反弹式 DDOS …… 91

第 8 章　利用型攻击

8.1　利用型攻击概述…… 94
8.2　口令猜测…… 94
8.2.1　口令攻击的一般方法…… 94
8.2.2　口令攻击的常用工具…… 95

8.3 特洛伊木马…… 96
8.3.1 木马概述…… 96
8.3.2 木马原理…… 97
8.4 缓冲区溢出…… 99
8.4.1 缓冲区溢出原理…… 99
8.4.2 制造缓冲区溢出 …… 100

第 9 章 其他攻击新手段,攻击的发展趋势。

9.1 IDS 躲避攻击新技术 …… 103
9.2 攻击技术发展趋势 …… 104

第 3 篇 反黑客篇

第 10 章 信息安全官方组织

10.1 概述…… 109
10.2 国内主要的紧急响应小组…… 109
10.3 国外主要的官方信息安全组织…… 110
10.4 国际间的信息安全合作组织…… 113

第 11 章 信息安全保障简介

第 12 章 信息安全保护技术

12.1 概述…… 117
12.2 防火墙…… 117
12.2.1 防火墙能做什么…… 118
12.2.2 防火墙的种类…… 118
12.2.3 防火墙的技术…… 120
12.2.4 防火墙的局限性…… 120
12.2.5 防火墙技术展望…… 120
12.3 安全协议…… 121
12.3.1 安全协议概述…… 121
12.3.2 IPSec …… 121
12.3.3 SSH 介绍 …… 124
12.3.4 SSL 介绍(Secure socket Layer & Security Socket Layer) …… 125
12.3.5 PKI 介绍…… 126
12.3.6 SET 协议介绍 …… 127
12.4 密码技术…… 127
12.4.1 信息加密概述…… 128

12.4.2　密码的分类…… 128
12.4.3　近代加密技术…… 129
12.4.4　加密应用方式…… 132
12.4.5　加密体制及比较…… 133
12.4.6　密钥管理技术…… 135
12.4.7　密码协议…… 136
12.5　虚拟专用网(VPN) …… 139
12.5.1　原理及特点…… 140
12.5.2　VPN 实现技术 …… 141
12.5.3　VPN 的应用 …… 145

第 13 章　入侵检测

13.1　概述…… 146
13.2　入侵检测 IDS …… 146
13.3　IDS 发展历程…… 147
13.4　基本分类…… 148
13.4.1　网络 IDS …… 149
13.4.2　网络节点 IDS …… 150
13.4.3　主机 IDS …… 150
13.5　主要检测技术…… 151
13.5.1　异常检测技术…… 151
13.5.2　模式匹配技术…… 152
13.5.3　协议分析技术…… 152
13.5.4　会话检测技术…… 153
13.6　当前的难点…… 153
13.6.1　攻击形式复杂化…… 154
13.6.2　误报率高…… 154
13.6.3　环境适应能力差…… 154
13.6.4　缺乏标准…… 154
13.6.5　其他问题…… 155
13.7　当前热点…… 155
13.7.1　数据挖掘技术…… 155
13.7.2　主动响应技术…… 155
13.7.3　自动反击技术…… 155
13.7.4　基于特定应用的 IDS …… 155
13.7.5　Correlation 技术 …… 156
13.8　发展方向…… 156

第 14 章　应急响应

14.1　概述…… 158
14.1.1　应急响应的定义…… 158
14.1.2　应急响应的对象…… 158
14.1.3　应急响应做什么…… 159
14.1.4　谁来负责应急响应…… 159
14.2　应急响应与安全生命周期…… 159
14.2.1　为什么需要应急响应…… 160
14.2.2　安全事件影响的严重性…… 160
14.2.3　安全漏洞的普遍性…… 160
14.2.4　攻击和恶意代码的流行性…… 160
14.2.5　入侵检测能力的局限性…… 160
14.2.6　网络和系统管理的复杂性…… 160
14.2.7　法律方面…… 161
14.3　应急响应组…… 161
14.3.1　应急响应组起源…… 161
14.3.2　什么是应急响应组…… 161
14.3.3　公益性应急响应组…… 162
14.3.4　内部应急响应组…… 162
14.3.5　商业的应急响应组…… 162
14.3.6　厂商的应急响应组…… 162
14.3.7　应急响应涉及的关键技术…… 163
14.4　应急响应的发展方向…… 163
14.4.1　技术的进展…… 163
14.4.2　社会方面的进展…… 164

第 15 章　系统备份和恢复

15.1　概述…… 166
15.2　系统备份…… 166
15.2.1　对数据的潜在威胁…… 167
15.2.2　数据丢失的各种逻辑现象…… 168
15.3　数据备份技术…… 168
15.4　数据恢复技术…… 170

第 16 章　陷阱技术

16.1　研究现状…… 173
16.2　Honeypot 简介 …… 174

16.3　包含的等级…… 174
16.3.1　低级别包含的 Honeypot …… 174
16.3.2　中等级别包含的 honeypot …… 175
16.3.3　高等级别包含的 honeypot …… 176
16.4　Honeypot 在网络中的拓扑和 Honeynet …… 178
16.4.1　Honeypot 的部署 …… 178
16.4.2　Honeynets …… 179
16.5　Honeypot 的信息收集 …… 180
16.5.1　基于主机的信息收集…… 180
16.5.2　基于网络的信息收集…… 181
16.5.3　主动方式的信息收集…… 181
16.6　陷阱网络安全欺骗系统…… 182
16.6.1　功能上具有主动防御的特点…… 182
16.6.2　结构上具有分布式防御，集中式控制管理的特点 …… 182
16.6.3　应用上适用范围广泛、使用灵活，可以伪装任何服务和系统…… 182
16.6.4　系统稳定，具有很强的自保护功能 …… 183

第 17 章　计算机取证

17.1　概述…… 184
17.2　计算机取证的主要原则…… 187
17.3　计算机取证的基本步骤…… 188
17.4　研究发展方向…… 188
17.4.1　相关技术…… 188
17.4.2　相关工具…… 189

第 4 篇　案例篇

第 18 章　黑客 VS 微软

18.1　案情…… 193
18.2　入侵…… 193
18.3　反思…… 194

第 19 章　电子政务安全解决方案

19.1　电子政务概述…… 195
19.2　网络结构与应用系统…… 195
19.3　风险分析…… 195
19.3.1　物理层安全风险分析…… 196
19.3.2　网络层安全风险分析…… 196

19.3.3 系统层安全风险分析…… 197
19.3.4 应用层安全风险分析…… 197
19.3.5 管理层安全风险分析…… 197
19.4 安全解决方案…… 198

第5篇 反思篇

第20章 对黑客技术的思考

第21 章黑客精神对现代教育的启示

第22章 网上没有绝对自由

第23章 网络战:另一场世界大战

23.1 闪电战:偷袭大网站 …… 211
23.2 黑客究竟有多黑…… 212
23.3 反击战:敌人在哪里 …… 214

参考文献…… 215

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