硅谷安全创业教父、Palo Alto Networks公司联合创始人 弓峰敏博士 作序并推荐

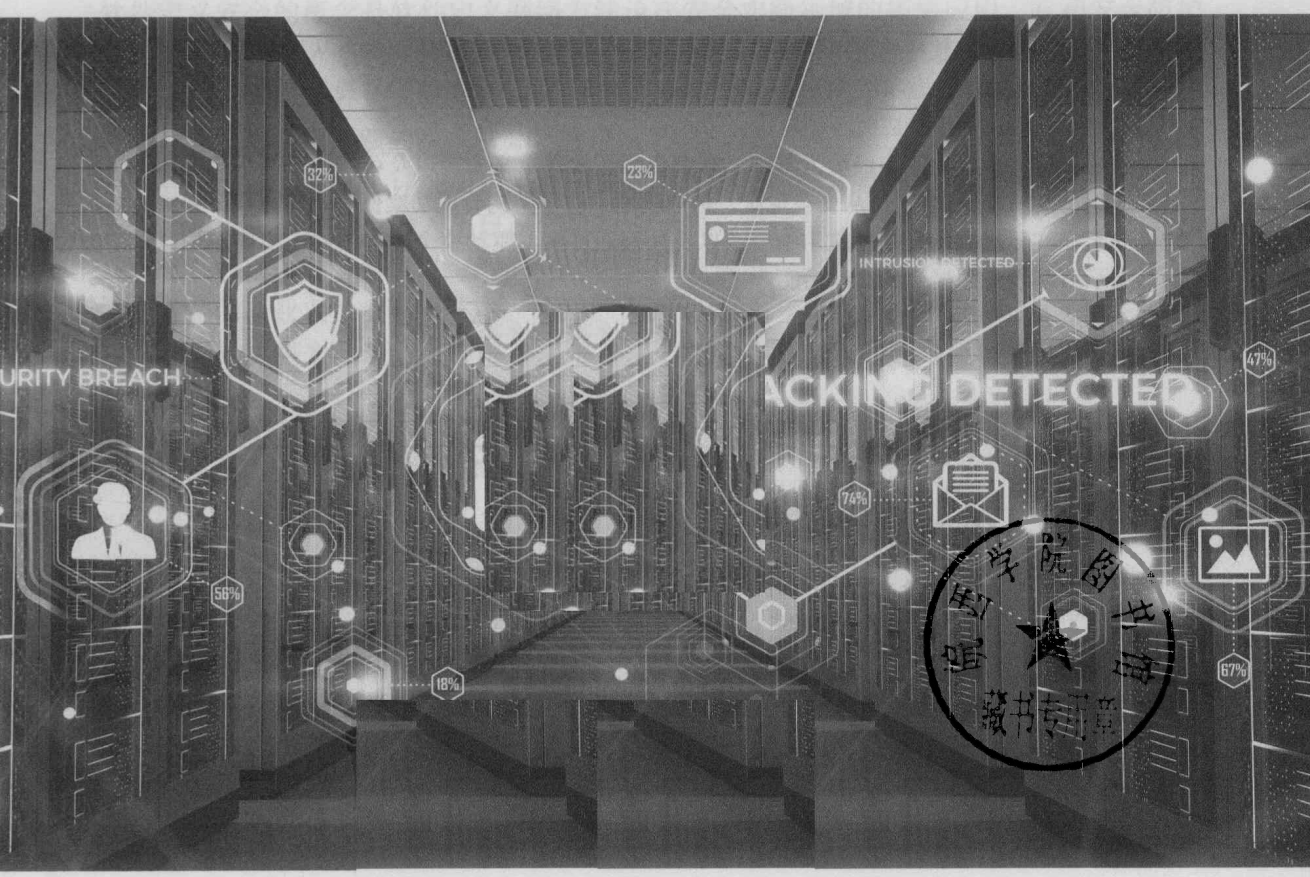
软件定义安全及可编程对抗系统实战

金飞 周辛酉 陈玉奇 著

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

软件定义安全及可编程对抗系统实战

金飞 周辛酉 陈玉奇 著



人民邮电出版社
北京

图书在版编目（CIP）数据

软件定义安全及可编程对抗系统实战 / 金飞，周辛酉，陈玉奇著. -- 北京 : 人民邮电出版社，2018.7(2018.7重印)
ISBN 978-7-115-48502-1

Ⅰ. ①软… Ⅱ. ①金… ②周… ③陈… Ⅲ. ①软件开发－安全技术 Ⅳ. ①TP311.522

中国版本图书馆CIP数据核字(2018)第109245号

内 容 提 要

软件定义安全由软件定义网络引申而来，实现安全由业务和应用驱动，从而实现复杂网络的安全防护，提升安全防护能力和用户安全体验。可编程对抗防御系统是F5公司提出的一种基于云端的安全服务，可以灵活、便捷地应对各种攻击。

本书以作者多年的工作经验为基础，详细介绍了软件定义安全以及可编程对抗系统的相关概念和具体应用。本书共分10章，从安全现状、核心问题、防御架构、成功案例等几个方面，详细阐述软件定义安全在实际对抗场景中的应用细节，以及如何通过脚本驱动整个防御体系，实现高频、灵活的防御，展示可编程防御架构的实际功能。

本书适合架构师、IT管理人员、应用开发人员和安全相关人员阅读。

◆ 著　　金　飞　周辛酉　陈玉奇
责任编辑　傅道坤
责任印制　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：17.25
字数：372千字　　2018年7月第1版
印数：3 001－5 000册　　2018年7月河北第3次印刷

定价：69.00元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字20170147号

序

目前，全球企业安全防护技术与实践和用户对安全目标的准确认知、对市场中现有安全产品性能的准确定位，以及在生产环境中有效利用这些安全产品的安全运维体系息息相关。这种运营态势需要与业务无缝结合，需要高度的自动化。

软件定义安全的概念是软件定义网络方法论在安全实践领域的拓展应用。它和安全防护的新范式（持续监测、诊断和缓解，Continuous Monitoring，Diagnostics，and Mitigation）是相辅相成的。这本《软件定义安全及可编程对抗系统实战》总结了当前的安全现状和挑战，系统性地分享了对安全实践的深度认知，重点以 F5 公司的产品体系为技术参考，以多个客户实践中碰到的场景为案例，详细演示了怎样实现软件驱动，建设动态防御能力，做好安全的运营工作。作者还在讲解中融入了自己的思考和一些心得体会。尽管本书中的案例，尤其是安全系统配置的很多细节是以 F5 产品为基础的，但是从事企业安全架构设计、安全工具开发，以及安全运维的专业人员都可以从本书中获得有益的借鉴。

相信本书对提高安全从业人员的目标认知和工具评估能力，以及运维系统的搭建能力会有很大帮助。

——弓峰敏博士

硅谷安全创业教父、Palo Alto Networks 公司联合创始人

作者简介

金飞，F5 亚太区安全解决方案架构师，主要研究方向为信息安全技术及防御架构设计。担任中央电视台、环球时报、中国银监会、北京市银监局等单位的信息安全顾问。于 2008 年参与了北京奥运会、北京残奥会的信息安全保障工作，并在 2009 年协助破获首例网络电话诈骗案。

周辛酉，MBA，现任 F5 中国区技术经理；资深讲师，资深架构师，可编程控制专家。主要研究方向为云计算及开发运维下的可编程控制、云计算及传统数据中心的安全架构及对抗、弹性架构及应用的高可用性、智能运维及自动化、软件定义的应用服务、业务连续性部署等。

陈玉奇，F5 公司资深安全方案顾问，具有十多年的信息安全从业经验，熟悉各类信息安全技术和产品，自 2012 年起加入 F5 公司，负责应用交付和安全方案的设计和推广，专注于 DDoS 攻击防护和应用层攻击防护研究。在加入 F5 之前，曾先后供职于 Servgate 和 Radware 公司，从事应用交付、信息安全方案设计和支持等工作。

致　谢

本书部分内容来自于F5工程师徐世豪、范恂毅、王英楠，技术经理刘旭峰，在此表示感谢！

前　言

信息安全是非常特殊的行业，在其他行业领域，多数情况下是领导型厂商代表行业的技术制高点，引领行业的发展方向，但信息安全行业的顶尖技术很多时候掌握在黑客手上，他们握有新的攻击技法，不断用独特的视角反复审视信息安全的基础架构，寻找新的攻击机会。而安全厂商正在竭尽全力地跟随和追赶新的攻击手段，为被攻击目标提供补救或加固的方案、产品及服务。这就是信息安全行业中攻防博弈的真实写照，永远都是先有矛后有盾。所以，信息安全厂商能在多大程度上跟上黑客的节奏，是衡量其技术能力的重要标准。

信息安全行业的另外一个重要趋势是企业小型化，掌握最先进防御技术的公司，从传统视角来看规模都非常小，比如美国的 Shape Security 公司。这些公司在一些细分的安全防御场景中颇有技术建树，能够解决非常具体和有针对性的安全问题。这种类型的公司如雨后春笋般地冒出来，它们要么是在短期之内获得巨大的风险投资，要么就是被较大的安全公司以高价收购，其活跃程度远远超过传统的安全厂商。

再者，安全行业正在走进场景防御的阶段，任何不落地到场景中的安全技术都是纸上谈兵。以网络为重心的安全防御已经成为明日黄花，攻击应用场景和商业模式已经越来越普遍。未来的信息安全将进入以用户行为分析为基础，以软件定义安全和可编程防御架构为实现技术，通过运营商和实体数据中心防御体系的联动，抵御机器和人混合攻击的 SecurityaaS 的时代。

威胁就在当下，攻击从未如此犀利！信息安全行业现在如火如荼，国家对信息安全的发展非常关切，媒体上关于信息安全案件的介绍也屡见不鲜，IT 从业人员往往也能随口说出多家安全公司的名字。但是，即使这样，就可以说了解信息安全行业了吗？其实还远远不够，俗语云“一花一世界，一树一菩提”，让我们看看信息安全世界的全貌吧！

这就是信息安全在世界范围内的全景图，其中的每一个图标都代表一家公司，而且这里面有非常多的创新公司，它们绝大多数拿到了非常丰厚的风险投资，而且在各自的信息安全细分领域内经营得风生水起。这才是信息安全的魅力所在。

软件定义安全是未来的行业趋势和发展方向，在对抗场景中会有非常多的表现形式和支持技术。本书依托 F5 公司的安全理念和技术路线，重新定义了可编程防御系统，并使用大量详实的案例和多场景安全架构，进一步证明软件定义安全理论的优势和现实意义：可以使得防御架构更加灵活，能够应对越来越高频变化的攻击脚本。

本书内容

第 1 章，“攻击技术的发展现状及趋势”，讲述了新的攻击技法和发展方向，以帮助大家重新认知信息安全。

第 2 章，“软件定义安全与安全生态和正确认知”，介绍了软件定义安全的概念、发展历程及相关的安全生态。

第 3 章，“F5 的安全属性”，讲述了 F5 公司在安全领域内的积累和底层架构。

第 4 章，“F5 的安全产品体系及应用场景”，逐一讲解 F5 的安全产品体系及每一种产品的具体应用场景。

第 5 章，“F5 可编程生态”，详细介绍了 F5 可编程知识体系和 F5 可编程生态环境。

第 6 章，“F5 可编程的安全应用场景”，介绍了 F5 可编程技术在不同对抗场景中的实际应用。

第 7 章，“F5 安全架构”，全面细致地剖析了 F5 公司诸多的安全架构。

第 8 章，“应用案例分享”，分享了作者在金融和通信等行业的一些成功应用案例，希望可以起到抛砖引玉的作用。

第 9 章，“信息安全的销售之道”，介绍了信息安全领域的销售人员会用到的一些方法，以及作者从业多年以来的一些体会。

第 10 章，“技术文档：6 天跟我学 iRules”，介绍了 iRules 的相关知识和使用技巧。

阅读前提

为了能更好地理解本书，读者需要具有网络、编程、安全方面的基础知识；如果具有一定的实际 IT 运维和信息安全对抗经验，则会对本书讲述的安全架构有更深刻的感悟。

本书读者

如果你是一位架构师，一位网络工程师，一位应用开发人员，一位传统安全产品的运维人员，你会越来越深刻地体会到，单一的技能已经无法应对现在面向场景的信息安全对抗，比如 BDDoS（行为 DDoS，Behavior DDoS）、薅羊毛攻击等。如果你想知道如何应对这些威胁，那么本书非常适合你——SecDevOps 是本书的主旨。

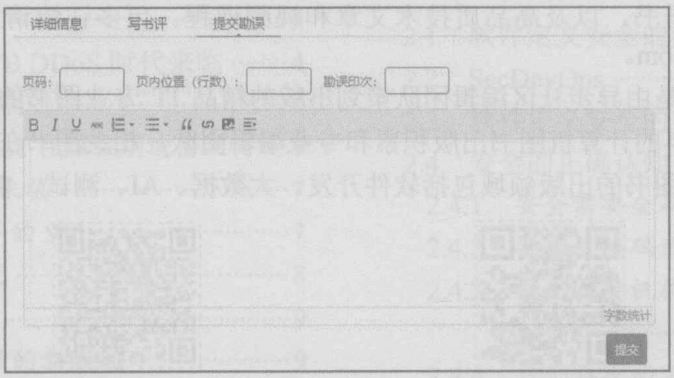
资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，点击“提交勘误”，输入勘误信息，点击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。



扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，

以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线提交投稿（直接访问 www.epubit.com/selfpublish/submission 即可）。

如果您是学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号

目　录

第 1 章　攻击技术的发展现状及趋势 ……1

1.1　真实还是幻象：暗网 ……1
1.1.1　何为“暗网” ……1
1.1.2　洋葱浏览器 ……3
1.1.3　“丝绸之路” ……3
1.1.4　暗网体系 ……4
1.2　IoT 安全？TB DDoS 时代来临 ……4
1.2.1　IoT 的脆弱性 ……4
1.2.2　Botnet＋IoT 核爆级别攻击架构 ……6
1.2.3　TB 时代来临 ……7
1.2.4　虚拟世界的 911 ……7
1.2.5　威胁将至 ……8
1.3　浏览器攻击 ……9
1.3.1　横空出世的新威胁 ……9
1.3.2　坏人在哪里 ……10
1.3.3　Dyer 木马剖析 ……11
1.3.4　验证弱点 ……12
1.4　撞库攻击 ……17
1.4.1　金融诈骗第一环 ……17
1.4.2　撞库工具以及如何发现低频撞库 ……18
1.5　API 攻击 ……19
1.5.1　API 攻击的威胁性 ……21
1.5.2　API 攻击的种类 ……22
1.5.3　API 攻击的缓解方法 ……24
1.5.4　API 开发和管理 ……24
1.6　薅羊毛攻击 ……25
1.7　从 WannaCry 到 Armada Collective ……26
1.8　安全威胁总结与归纳 ……27

第 2 章　软件定义安全与安全生态和正确认知 ……28

2.1　软件定义安全的概念 ……28
2.2　SecDevOps ……29
2.3　软件定义安全的行业准备 ……30
2.4　安全的正确认知 ……31
2.4.1　安全需要全局观 ……32
2.4.2　安全从编码开始 ……33
2.4.3　安全需要机构分离、业务融合 ……35
2.4.4　我们再也回不去了 ……37
2.4.5　云对安全的影响 ……39

第 3 章　F5 的安全属性 ……40

3.1　F5 安全的历程 ……40
3.2　全代理架构 ……41
3.3　底层核心 TMOS ……43
3.4　行业评价 ……45

第 4 章　F5 的安全产品体系及应用场景 ……48

4.1　ASM——行业领导者 ……49
4.1.1　产品概述 ……49
4.1.2　功能特点及应用场景 ……50
4.2　FPS——颠覆性安全产品 ……73

4.2.1 产品概述 ……73
4.2.2 功能特点及应用场景 ……73
4.3 APM——可视化逻辑流程图……82
4.3.1 产品概述 ……83
4.3.2 功能特点及应用场景 ……84
4.4 AFM——性能霸主……85
4.4.1 产品概述 ……86
4.4.2 功能特点及应用场景 ……86
4.5 DHD——为对抗而生……89
4.5.1 产品概述 ……89
4.5.2 功能特点及应用场景 ……89

第 5 章 F5 可编程生态……93

5.1 DevCentral——F5 全球技术社区 ……93
5.2 TMSH ……94
5.3 iControl ……94
5.4 iApp ……95
5.5 iCall……96
5.6 iRules ……96
5.6.1 iRules 概念 ……96
5.6.2 iRules 的特点 ……97
5.6.3 iRules 开发工具 iRule Editor ……97
5.6.4 iRules 事件及事件驱动 ……98
5.6.5 iRules 事件触发顺序 ……100
5.6.6 iRules 案例解析 ……101
5.6.7 如何编写运行快速的 iRules ……106

第 6 章 F5 可编程的安全应用场景……107

6.1 iRules 缓解 Apache Range 攻击 ……107
6.1.1 功能概述 ……107
6.1.2 F5 配置 ……107
6.1.3 JMeter 伪造 Range 攻击 ……108
6.1.4 Range 攻击分析 ……109
6.1.5 iRules 防护 SlowPost……110
6.1.6 开启防护 ……110
6.2 iRules 通过 cookie 实现黑名单阻断限制……112
6.2.1 功能介绍 ……112
6.2.2 iRules 基于 cookie 识别用户 ……112
6.2.3 开启防护情况 ……113
6.3 iRules 缓解 DNS DoS 攻击……115
6.3.1 功能概述 ……115
6.3.2 实验环境相关配置 ……115
6.3.3 iRules 基于 DNS 频率进行防护 ……117
6.3.4 开启防护情况 ……118
6.4 iRules 基于源地址 HTTP 链接的频率实现限制 ……119
6.4.1 功能概述 ……119
6.4.2 F5 配置 ……120
6.4.3 JMeter 配置 ……121
6.4.4 未开启防护的情况 ……122
6.4.5 iRules 限制 HTTP 连接频率……123
6.4.6 开启防护情况 ……124
6.5 iRules 缓解 SlowHeader 类型攻击……125
6.5.1 功能概述 ……125
6.5.2 HTTP Attack 过程……125
6.5.3 Slow Header 攻击分析 ……127
6.5.4 iRules 防护 Slow Header……128
6.5.5 开启防护情况 ……128
6.5.6 非 iRules 方式防护 ……129
6.6 iRules 缓解 Slow Post 攻击……130
6.6.1 功能概述 ……130
6.6.2 HTTP Attack 攻击……130
6.6.3 Slow Post 攻击分析 ……131
6.6.4 iRules 防护 Slow Post……133
6.6.5 开启防护情况 ……133
6.7 iRules 实现 TCP 连接频率的限制……135

6.7.1 功能概述 ……135
6.7.2 JMeter 配置 ……135
6.7.3 未开启防护情况 ……137
6.7.4 iRules 基于 TCP 连接频率防护 ……138
6.7.5 开启防护情况 ……139
6.8 iRules 实现 TCP 总连接数限制 ……140
6.8.1 功能概述 ……140
6.8.2 未开启防护情况 ……140
6.8.3 iRules 基于 TCP 总数防护 ……141
6.8.4 开启防护情况 ……142
6.9 iRules 实现统计单 IP 历史最大访问频率 ……143
6.9.1 功能概述 ……143
6.9.2 iRules 查看连接频率 ……143
6.9.3 学习模式效果 ……144
6.10 iRules 实现多个 IP 中历史最大频率统计 ……145
6.10.1 功能概述 ……145
6.10.2 iRules 查看连接频率 ……146
6.10.3 学习模式效果 ……147
6.11 iRules 实现反插脚本进行防护 ……149
6.11.1 功能概述 ……149
6.11.2 iRules 基于反插脚本进行防护 ……149
6.11.3 开启防护情况 ……150
6.12 iRules 实现黑名单阻断限制 ……152
6.12.1 功能概述 ……152
6.12.2 iRules 限制 HTTP 连接频率与黑名单防护 ……152
6.12.3 开启防护情况 ……153
6.13 iRules 利用白名单缓解 DNS DoS 攻击 ……155
6.13.1 功能概述 ……155
6.13.2 F5 配置 ……155
6.13.3 iRules 基于白名单进行防护 ……156
6.13.4 请求域名未在 DNS 白名单中的防护情况 ……158
6.13.5 请求域名在 DNS 白名单中的防护情况 ……159
6.13.6 IP 白名单放过功能 ……160
6.14 iRules 缓解国外银行 DDoS 攻击 ……162

第 7 章 F5 安全架构 ……166

7.1 F5 API 防御架构 ……167
7.2 F5 DDoS 防御架构 ……169
7.3 F5 SSL 安全架构 ……176
7.4 F5 浏览器安全架构 ……179
7.5 F5 IoT 安全架构 ……180
7.6 F5 DNS 安全架构 ……183

第 8 章 应用案例分享 ……186

8.1 力挽狂澜：运营商清洗中心 ……186
8.1.1 案例背景 ……186
8.1.2 行业分析 ……187
8.1.3 功能设计 ……188
8.1.4 测试拓扑 ……189
8.1.5 服务内容 ……190
8.1.6 防御功能验证 ……191
8.1.7 客户反馈及演示解读 ……217
8.1.8 架构优化 ……220
8.2 贴身护卫：公有云安全 ……222
8.3 场景安全：企业级清洗中心 ……223
8.4 高频之战：航空公司黄牛软件 ……225
8.4.1 案例背景 ……225
8.4.2 对抗思路及措施 ……225
8.5 最陌生的熟人：商业银行秒杀案例 ……232
8.5.1 秒杀背景介绍 ……232

8.5.2 防御架构概述 ……232
8.5.3 业务场景及用户需求 ……233
8.5.4 iRules 防护原理 ……234
8.5.5 ASM 防护方案及原理 ……236
8.6 汇聚之地：企业统一认证案例 ……237
第 9 章 信息安全的销售之道 ……240
9.1 预习作业 ……240
9.2 信息安全的交流 ……244
9.2.1 建立信任 ……244
9.2.2 明确需求类型 ……244
9.2.3 替客户多想一步 ……244
9.2.4 引入更多资源 ……245
9.3 上兵伐谋：F5 Security Combine ……245
第 10 章 技术文档：6 天跟我学 iRules ……247
10.1 第一天：基本概念 ……247
10.1.1 变量 ……247
10.1.2 事件 ……248
10.1.3 函数 ……248
10.1.4 条件语句 ……248
10.2 第二天：Hello World！ ……249
10.3 第三天：几个常用的 iRules ……251
10.4 第四天：switch 模型和强大的 class ……254
10.5 第五条：理一理头绪 ……256
10.6 第六天：分析 iRules ……259
用互联网思维认知世界 ……262

第 1 章　攻击技术的发展现状及趋势

中国古语，知己知彼，百战不殆。但是真实的世界真的是你认为的样子吗？我们是否生活在一个经过修饰或伪装的世界里？也许可以这样阐述，这个世界里有一小部分人可以看到完全不一样的世界，如同黑客帝国里生活在锡安（Zion）而非母体（Matrix）中的人类（见图 1-1）。

图 1-1　真实的世界

1.1　真实还是幻象：暗网

1.1.1　何为“暗网”

网络是层级划的，分为表层网络（Surface Web）和深网（Deep Web），如图 1-2 所示。

图 1-2　网络层级

表层网络主要由我们日常接触的一些应用构成，例如 Google、Facebook、Twitter、Hotmail、WeChat 之类的应用。再往下就是暗网（Dark Web）、幻影网络（Shadow Web）、马里亚纳网络（Marianas Web）。

表层网络最大的特点是信息查重率很高，相同的信息会在很多网站主机中同时存在。相比之下深网里的情况会非常不同，暗网的规模是表层网络的 400～500 倍，大约有 100 亿条不查重的数据。常规的搜索引擎和浏览器无法访问到这些信息，必须通过特殊的软件或网关才能做到，其中最具代表性的是洋葱浏览器（Tor Browser）。表层网络和深网的对比关系如图 1-3 所示。

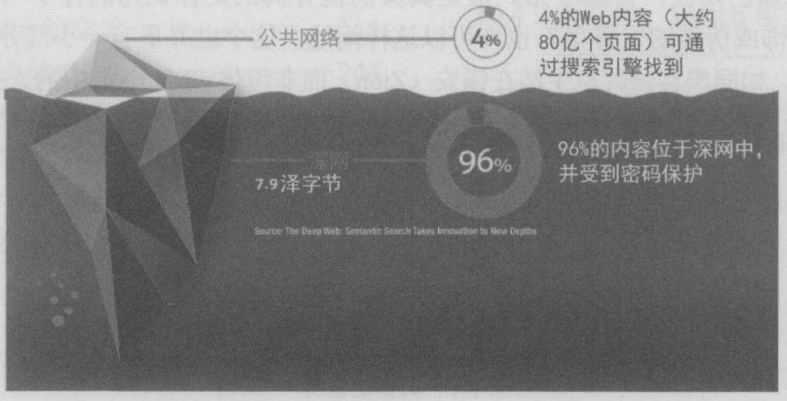


图 1-3　表层网络和深网的对比

为什么会有这么多的网站不能被搜索引擎找到并收录呢？这就要讲一下搜索引擎的工作原理。搜索引擎是靠网站根目录的 robots.txt 文件引导爬虫程序进行信息检索的。例如，www.bing.com 的 robots.txt 文件就是下面的内容。

```
User-agent: msnbot-media
Disallow: /
Allow: /shopping/$
Allow: /shopping$
Allow: /th?
User-agent: Twitterbot
Disallow:
User-agent: *
Disallow: /account/
Disallow: /bfp/search
Disallow: /bing-site-safety
Disallow: /blogs/search/
Disallow: /entities/search
Disallow: /fd/
Disallow: /history
```

```
Disallow: /hotels/search
Disallow: /images?
Disallow: /images/search?
Disallow: /images/search/?
……
```

robots.txt 文件主要告诉搜索引擎可以访问或不能访问哪些目录，如果某些网站不设置 robots.xt 文件，则意味着搜索引擎用常规方式不能收录该网站的信息并对外提供检索服务。这样一来，能找到这些网站并访问的人就会非常有限，甚至只有预先知道的人才能访问。而暗网里的绝大多数网站都属于这种类型。

需要强调的一点是，搜索引擎公司的浏览器工具栏（Tool Bar）或浏览器产品也会具有地址和信息收录的功能，这两个信息来源对于搜索引擎公司来说，与爬虫一样重要。这就能解释为什么在某些搜索引擎受限的地区，搜索引擎公司仍可以获得大量信息。基于浏览器获取信息是行业潜规则，区别在于做的程度和实现手段的高低。

1.1.2 洋葱浏览器

要访问底层网络资源，需要使用特殊的浏览器软件，其中最具代表性的是洋葱浏览器（Tor Browser）。洋葱浏览器是本着访问者不可能被追溯的宗旨而设计的，目的在于充分保护访问者的个人隐私。

在最初版本的洋葱浏览器中，提供了三个中间路由跳转节点，即从用户通过洋葱浏览器访问暗网服务器时，会在途中建立三个节点的动态路由，以确保路径的不可追溯性。洋葱浏览器后来发展到提供 5000 个中间路由跳转节点。至此，如果想获取最终用户的相关信息将变得异常困难。所以洋葱网络也叫匿名者网络。

而且随着 Tor 用户数量的增加，洋葱网络的路由复杂度呈几何级数增大，而且在一个 Timeout 时间节拍后，所有的路由都会重新设定，这也使得完全不可能通过路径复原实现终端追溯，这也是洋葱路由的真正可怕之处。

洋葱网络也具有两面性，匿名者有可能是用户，也有可能是攻击者。洋葱网络在保护终端隐私不被获取的同时，也为攻击者提供了更多的有利条件。事实也是如此，现在很多网络犯罪的真实控制者也大量使用洋葱浏览器进行伪装和逃避打击。从本质上来讲，技术本身没有好坏之分，关键在于用技术实现的目的是什么，以及是否违背了人类社会的共识。

1.1.3 “丝绸之路”

洋葱浏览器的设计者罗斯·乌布利希后来还创建了“丝绸之路”网站并将其上线运营。同时，基于比特币的支付体系也初步完成。

匿名者网络加虚拟货币最终也没让乌布利希逃脱法律的制裁，2013 年 10 月，他在毫无察觉的情况下被捕。尽管乌布利希锒铛入狱，但“丝绸之路”似乎并没有终结，到目前为止“丝绸之路”3.1 版本依然可以正常运转，不知道背后到底隐藏着多少不为人知的故事。