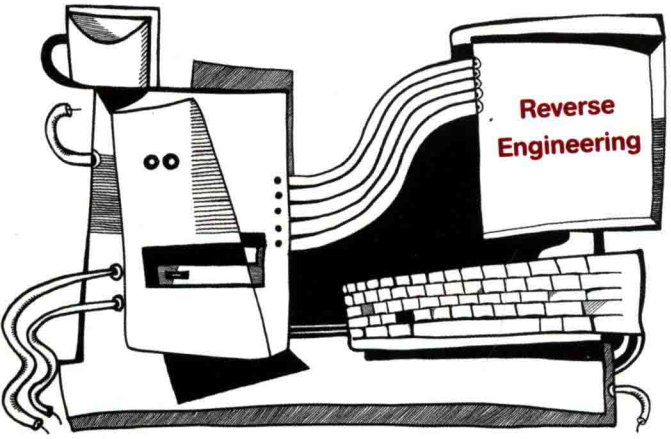
安天 ANTIY
异步图书 www.epubit.com.cn

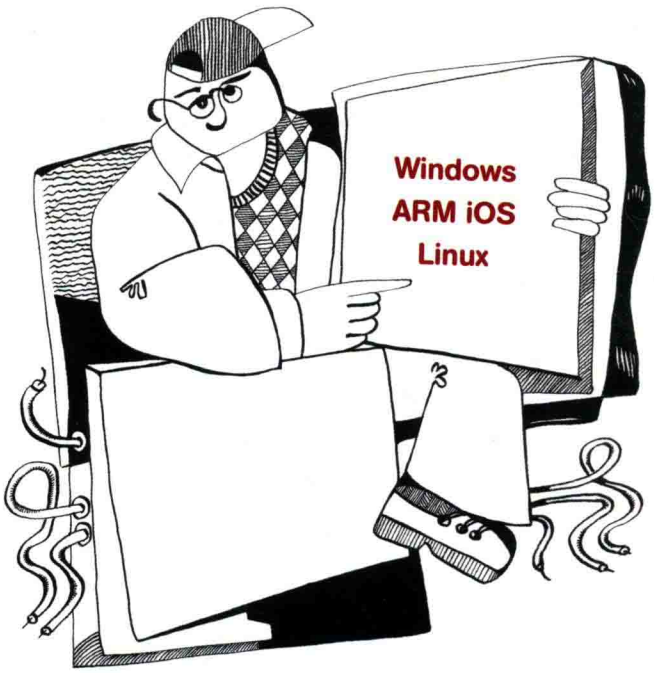


- 了解逆向工程的权威指南
- 初学者必备的大百科全书
- 安天网络安全工程师培训必读书目

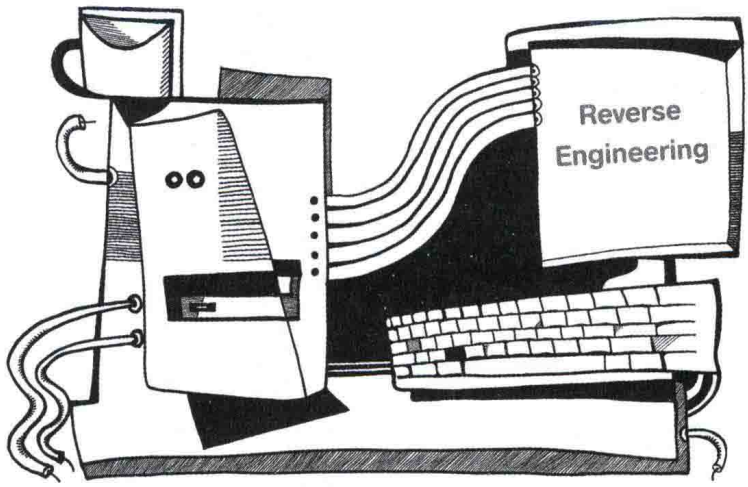
Reverse Engineering for Beginners

逆向工程权威指南 上册

[乌克兰] Dennis Yurichev◎著
Archer 安天安全研究与应急处理中心◎译



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



Reverse Engineering for Beginners

逆向工程权威指南 上册

[乌克兰] Dennis Yurichev◎著
Archer 安天安全研究与应急处理中心◎译

人民邮电出版社
北京

图书在版编目（CIP）数据

逆向工程权威指南 /（乌克兰）丹尼斯（Dennis Yurichev）著；Archer，安天安全研究与应急处理中心译. -- 北京：人民邮电出版社，2017.4
ISBN 978-7-115-43445-6

Ⅰ. ①逆… Ⅱ. ①丹… ②A… ③安… Ⅲ. ①工业产品－计算机辅助设计－指南 Ⅳ. ①TB472-39

中国版本图书馆CIP数据核字(2016)第243654号

版权声明

◆ 著　[乌克兰] Dennis Yurichev
译　Archer 安天安全研究与应急处理中心
责任编辑　陈冀康
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
北京天宇星印刷厂印刷

◆ 开本：787×1092　1/16
印张：61.5　彩插：1
字数：1 990 千字　2017 年 4 月第 1 版
印数：1 – 3 000 册　2017 年 4 月北京第 1 次印刷

著作权合同登记号　图字：01-2014-3227 号

定价：168.00 元（上、下册）

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：京东工商广字第 8052 号

内 容 提 要

逆向工程是一种分析目标系统的过程，旨在识别系统的各组件以及组件间关系，以便能够通过其他形式或在较高的抽象层次上，重建系统的表征。

本书专注于软件的逆向工程，是写给初学者的一本权威指南。全书共分为上、下两册，十二个部分，共 102 章，涉及 X86/X64、ARM/ARM-64、MIPS、Java/JVM 等重要内容，详细解析了 Oracle RDBMS、Itanium、软件狗、LD_PRELOAD、栈溢出、ELF、Win32 PE 文件格式、x86-64（critical sections、syscalls、线程本地存储 TLS、地址无关代码（PIC）、以配置文件为导向的优化、C++ STL、OpenMP、SHE 等众多技术问题，堪称是逆向工程技术百科全书。除了详细讲解，本书还给出了很多习题来帮助读者巩固所学的知识，附录部分给出了习题的解答。

本书适合对逆向工程技术、操作系统底层技术、程序分析技术感兴趣的读者阅读，也适合专业的程序开发人员参考。

序　从逆向视角透视代码大厦的那些砖石

相对于本书的中文名字《逆向工程权威指南》，我更喜欢它的英文原名《Reverse Engineering for Beginners》，可以直译为“逆向工程入门者必读”。在国外的程序员圈中，这本书被简称为《RE4B》，作者的 Blog 式连载已经引发了持续关注和好评。

本书的重要特色在于其清晰的章节结构，涵盖了函数、语句、结构体、数组等这些构成代码大厦的基本元素，如显微镜般逐一对比了这些元素在 X86、ARM 和 MIPS 体系架构下的“切片”影像。本书几乎每个章节都按照 X86、ARM、MIPS 三个体系架构分别展开，可以让读者深入对比理解在三种体系架构下，同样的指令、函数及数据结构呈现的异同和特点。无论对分析工程师，还是编码工程师来说，本书都是能更深入理解代码大厦原材料的工作指南。这是基础性、系统性的文献工作，也是令人耳目一新的结构安排。对于在中国传统高校计算机教育中，通过简单的 X86 ASM 来学习和了解体系结构的工程师来说，这也是尽快打通 ARM、MIPS 知识背景的“全栈”指南。对于那些从各种破解教程来切入逆向领域的安全爱好者来说，这更像是一份“正餐”。对于作者来说，我相信这个写作过程是充满激情的，但也充满了艰难和痛苦。对于 Dennis 这样的逆向工程专家来说，这本书的写作过程，更多的不是在探索未知的世界，也不是对高级技巧和经验的总结，而是要对看起来相对枯燥的单元式资料进行整理，将一些对其已经是常识的东西转化为系统而书面化（并易于读者理解）的语言。

逆向工程一直被宣传为一种充满乐趣和带有神秘主义的技能，而逆向分析者的工作看起来更有乐趣的原因，似乎就是在指令奔涌中逆流而上，绕开种种限制和保护，找到代码中的“宝藏”——错误、漏洞或者是被加密算法层层掩盖的数据结构。这个由媒体所打造的形象，也为部分逆向爱好者所自矜。而这也导致逆向领域的书籍和教程，更多地围绕着一些高阶的技巧展开，更多地讲解如何绕过加密和保护，却忘记了逆向工程的初衷是要洞察系统及软件的整体结构和机理。由于之前的逆向领域相关出版物中缺少“代码大全”式的基础读本，本书的完成填补了这一空白，然而，这不仅需要作者有高超的逆向研究能力，也要有正向系统的思维和视野。

本书的译者之一 Archer 提出想邀请安天的工程师们一同完成本书的翻译时，我曾经觉得他是不是“疯了”。本书当时并无定稿的英文版本，只是 Dennis 持续发布的 Blog 式的连载。尽管网络连载已经引发了好评如潮，但其精彩篇章彼时还如散落在海底的珍珠，尚未串成珠链。以 Dennis 天马行空的写作风格和追求完美主义的性格，他必然会在未完成全部章节的期间，不断地增加体系结构的新热点（如 ARM64）和修补既有章节的内容，甚至会改动原有的样例代码，导致本书原版定稿遥遥无期。我觉得，与其说正在养病的 Archer 接手翻译这本书是一份艰难的任务，倒不如说，Dennis 写完本书根本就是一份不可完成的任务。

因此当接近千页的样书摆在我面前时，我被深深震撼了，那种感觉和我之前依靠自己极为蹩脚的英语扫过的英文电子稿不同，我能想象 Archer 是如何一边咳嗽着、一边码字或者校对代码；以及安天 CERT 的同事们是如何在样本分析任务饱和的情况下挤出时间来一点点推动翻译进展的。当我在视频例会上向安天各地的部门负责人展示样书时，我能看到每个人的赞叹和兴奋，那种兴奋不啻于我们自己发布了一份最新的长篇分析报告。

二进制分析，是安全分析工程师，包括有志于投身安全领域的编码工程师的基本功底之一。硅谷一些安全人士都曾提及一个有趣的说法——华人的系统安全天赋。中国安全厂商和安全工作者，在系统安全领域和分析工作中，正在不断取得新的进步。在国际网络安全企业中，华人承担关键系统安全研究和分析工作的占比也很高，国际高校的一些华人研究者在新兴领域展开系统安全研究，同样取得了很大的

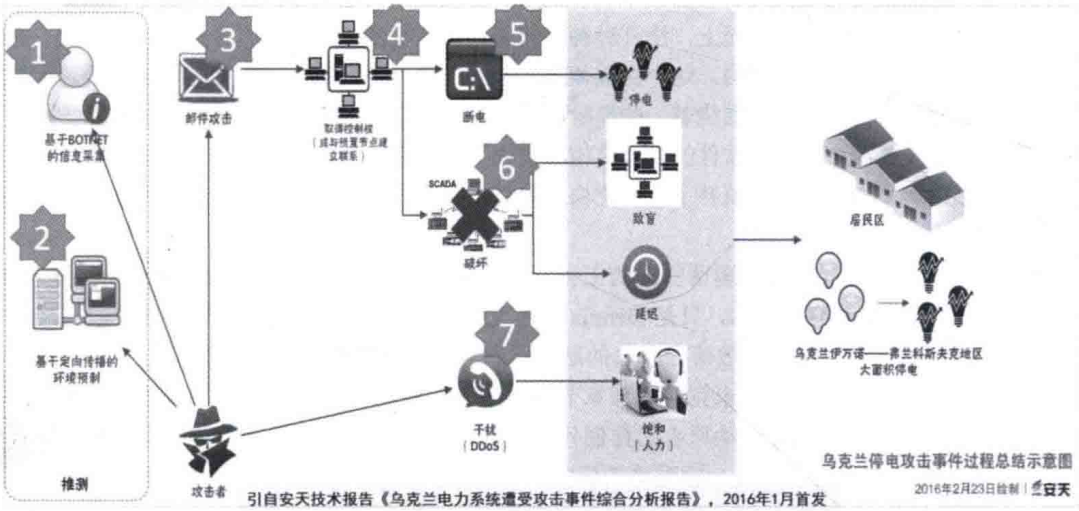
国际影响。遗憾的是，Web 和应用开发的兴起，一定程度上让更多年轻安全从业人员的目光转向 Web 和应用安全，当前新的安全从业者整体的二进制分析能力正在下降，存在着基本功缺失的问题，非常需要系统性的补课。

二进制分析能力，是对安全工程师的基础能力要求。但要对抗 APT 等新兴威胁，仅仅有基本功是不够的，还需要在更开阔的架构视野上，具备从攻击链、体系化等角度逆向分析研判攻击行为的全程、攻击对手的全貌的能力。

当年受到一些破解教程的误导，一些接触逆向工程的年轻人把破解序列号等当成逆向工程的目的，从而导致浅尝辄止，没有真正理解逆向工程的博大精深。即使是安天部分资深的分析工程师，也往往更乐于寻找解析攻击者的个性技巧和那些有“难度”的分析细节，并常以此感到自豪，而不能站到对攻击作业过程完整复盘和对攻击者画像的角度来看待问题，而后者才是一类高阶的逆向工程。

我们是从分析“震网”所遇到的系列挫折中，从对 Flame 蠕虫马拉松式的、收效甚微的模块分析中，认识到了传统分析工程师所面临的这种困境的。在“震网”分析中，由国际知名厂商的架构师和分析工程师所组成的混编分析团队，就能比安天完全由软硬件安全分析工程师组成的分析小组，取得更多的分析成果和进展。因为安全厂商和 APT 攻击之间，不是简单的查杀反制和单点的分析对抗，而是体系化对抗。从认识到这个问题开始，安天的分析团队一方面继续强化二进制分析的基本功底；另一方面自我批判那种“视野从入口点开始”的狭隘分析视角，避免我们自己从透析攻击者载荷的高级技巧中找到太多“快感”，而忘记那些更重要的全局性因素。

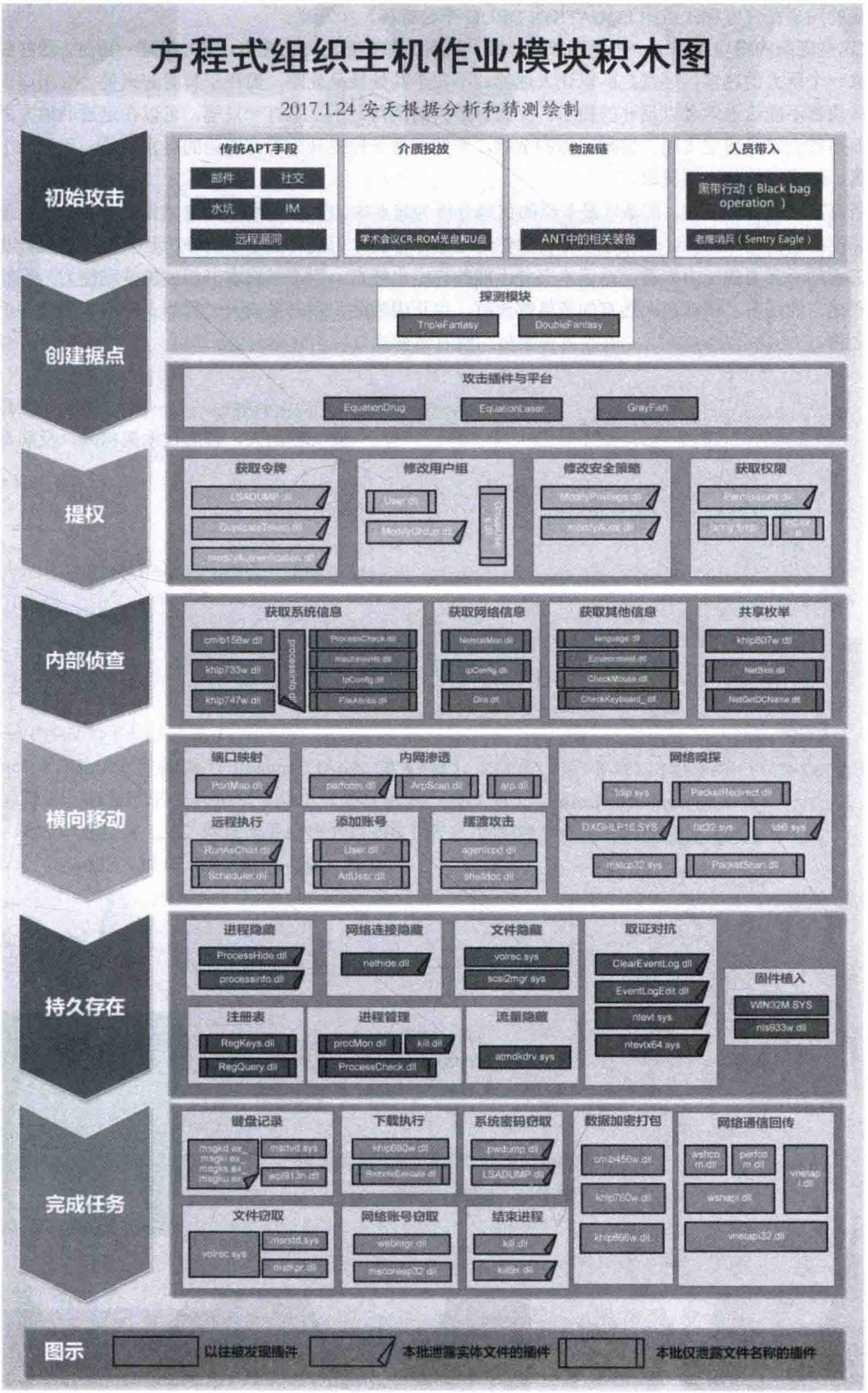
过去三年间，安天发布了针对 APT-TOCS、白象、方程式等组织相关的多篇分析报告，也分析了类似乌克兰国家电网遭遇攻击停电等与关键基础设施有关的安全事件。在乌克兰停电事件的分析中，我们已经初步走出了入口点视野，而尝试在更大的时空视角上还原事件。



引自安天技术报告《乌克兰电力系统遭受攻击事件综合分析报告》，2016年1月首发

而即使从微观的分析来看，高阶恶意代码也已经从一个附着在宿主上的代码片段或单体文件的木马，进化为一个庞大的工程体系。对于高级恶意代码来说，不仅有前端的持久化载荷和大量按需投放的“原子化”模块，其后更有一个庞大的支撑工程体系。对于前端，我们还能够依靠代码逆向来分析，而对于后面这个大到无形的“魅影”，我们更多的只能依靠分析恶意代码的指令体系、有限的网络感知捕获、少得可怜的可公开检索信息，以及作为信息安全动物的逻辑和本能来进行猜测。我们所要完成的工作，不仅仅是要逐一进行载荷模块分析，而是要对整个攻击面和攻击链的深入复盘。

2017 年 1 月 25 日，安天分析小组更新了针对方程式攻击组织的第四篇分析报告《方程式组织 EQUATION DRUG 平台解析》，基于对方程式组织大量恶意代码模块的分析，我们初步完成了一份有价值的工作，那就是方程式组织的主机作业模块积木拼图。


方程式组织主机作业模块积木图
2017.1.24 安天根据分析和猜测绘制
初始攻击
传统APT手段
邮件
社交
水坑
IM
远程漏洞
介质投放
学术会议CR-ROM光盘和U盘
物流链
ANT中的相关装备
人员带入
黑带行动（Black bag operation）
老鹰哨兵（Sentry Eagle）
创建据点
探测模块
TripleFantasy
DoubleFantasy
攻击插件与平台
EquationDrug
EquationLaser
GrayFish
提权
获取令牌
LSADUMP.dll
DuplicateToken.dll
修改用户组
User.dll
ModifyGroup.dll
Groups.dll
修改安全策略
ModifyPrivilege.dll
modifyAuser.dll
获取权限
内部侦查
获取系统信息
cmib158w.dll
khlp733w.dll
khlp747w.dll
ProcessInfo.dll
ProcessCheck.dll
mauiments.dll
IpConfig.dll
FileAttribs.dll
获取网络信息
NetstatMon.dll
IpConfig.dll
Dns.dll
获取其他信息
language.dll
Environment.dll
CheckMouse.dll
CheckKeyboard_dll
共享枚举
khlp807w.dll
NetBios.dll
NetGetDCName.dll
横向移动
端口映射
PortMap.dll
内网渗透
perfcom.dll
ArpScan.dll
arp.dll
网络嗅探
tdip.sys
PacketRedirect.dll
DXGHLP16.SYS
fat32.sys
ldd6.sys
mslcp32.sys
PacketScan.dll
远程执行
RunAsChild.dll
Scheduler.dll
添加账号
User.dll
AdUser.dll
摆渡攻击
agentcpd.dll
shelldoc.dll
持久存在
进程隐藏
ProcessHide.dll
processinfo.dll
网络连接隐藏
nethide.dll
文件隐藏
volrec.sys
scsi2mgr.sys
取证对抗
ClearEventLog.dll
EventLogEdit.dll
ntevt.sys
ntevtx64.sys
固件植入
WIN32M.SYS
nls933w.dll
注册表
RegKeys.dll
RegQuery.dll
进程管理
procMon.dll
kill.dll
ProcessCheck.dll
流量隐藏
atmdkdrv.sys
完成任务
键盘记录
msgkd.ex_
msgki.ex_
msgks.ex_
msgku.ex_
msfyd.sys
wpl913n.dll
下载执行
khlp880w.dll
RemoteExecute.dll
系统密码窃取
pwdump.dll
LSADUMP.dll
数据加密打包
cmlz456w.dll
khlp760w.dll
khlp868w.dll
网络通信回传
wsltcp
m.dll
perfcp
m.dll
vnetap
i.dll
wshapi.dll
vnetapi32.dll
文件窃取
volrec.sys
mrsfd.sys
mstkpr.dll
网络账号窃取
webmgr.dll
mscorexp32.dll
结束进程
kill.dll
kill2r.dll
图示
以往被发现插件
本批泄露实体文件的插件
本批仅泄露文件名称的插件

我的同事在《方程式组织 EQUATION DRUG 平台解析》中写道：

“这些庞杂的模块展开了一组拼图碎片，每一张图上都有有意义的图案，但如果逐一跟进，这些图案就会组成一个巨大的迷宫。迷宫之所以让人迷惑，不在于其处处是死路，而在于其看起来处处有出口，但所有的砖块都不能给进入者以足够的提示。此时，最大的期待，不只是有一只笔，可以在走过的地方做出标记，而是插上双翼凌空飞起，俯瞰迷宫的全貌，当然这是一种提升分析方法论的自我期待。我辈当下虽身无双翼，但或可练就一点灵犀。”

所有高阶的分析工作，都是以最基础的代码分析为起点的。无论是面对 APT 攻击的深度分析，还是对高级黑产行为的系统挖掘，仅有基本分析固然是远远不够的，但没有最基本的分析是万万不能的。从未来安全工程师所需要的能力来看，熟读本书并不能使你走出迷宫。但不掌握本书相关的基础能力，不能去透视代码迷宫的砖石，就连走入迷宫的资格都没有。也正因为此，本书是安天工程师人手一本的必备手册和必读之物。

肖新光

安天创始人，首席技术架构师，反病毒老兵

前　言

“逆向工程”一词用在软件工程领域的具体含义历来模糊不清。逆向工程是一种分析目标系统的过程，旨在识别系统的各组件以及组件之间的关系，以便通过其他形式或在较高的抽象层次上，重建系统的表征。按照目标系统的分类划分，人们常说的“逆向工程”大体可分为：

（1）软件逆向工程。研究编译后的可执行程序。

（2）建模逆向工程。扫描 3D 结构并进行后续数据处理，以便重现原物。

（3）重建 DBMS 结构。

本书仅涉及上述第一项，即软件逆向工程的知识范畴。

重点议题

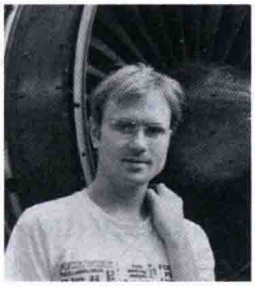
x86/x64、ARM/ARM64、MIPS、Java/JVM。

涉及话题

本书中涉及如下一些话题：

Oracle RDBMS（第 81 章）、Itanium（IA64，第 93 章）、加密狗（第 78 章）、LD_PRELOAD（67.2 节）、栈溢出、ELF、Win32 PE 文件格式（68.2 节）、x86-64（26.1 节）、critical sections（68.4 节）、syscalls（第 66 章），线程本地存储 TLS，地址无关代码 PIC（67.1 节）、以配置文件为导向的优化（95.1 节）、C++ STL（51.4 节）、OpenMP（第 92 章），SEH（68.3 节）。

作者简介



姓名：Dennis Yurichev
特长：逆向工程及计算机编程

联系方式：E-mail dennis(a)yurichev.com
Skype dennis.yurichev

译者简介

安天安全研究与应急处理中心（安天 CERT），是承担安天安全威胁应急处理、恶意代码分析、APT 攻

击分析取证等方面工作的综合研究和服务的部门，由资深安全工程师团队组成。安天 CERT 以“第一时间启动，同时应对两线严重威胁”为自身能力建设目标，在红色代码 II、口令蠕虫、震荡波、冲击波等重大安全疫情的响应中，提供了先发预警、深度分析和解决方案；并在 2010 年后针对震网、毒曲、白象、方程式等 APT 攻击组织和行动，进行了深入的跟踪分析。分析成果有效推动了安天核心引擎和产品能力的成长，获得了主管部门和用户的好评。

致谢

感谢耐心回答我提问的 Andrey “herm1t” Baranovich 和 Slava “Avid” Kazakov。

感谢帮助我勘误的 Stanislav “Beaver” Bobrytskyy、Alexander Lysenko、Shell Rocket、Zhu Ruijin 和 Changmin Heo。

感谢 Andrew Zubinski、Arnaud Patard (rtp on #debian-arm IRC)和 Aliaksandr Autayeu 的鼎力支持。

感谢本书的中文版翻译 Archer 和安天安全研究与应急处理中心。

感谢本书的韩语版翻译 Byungho Min。

感谢校对人员 Alexander “Lstar” Chernenkiy、Vladimir Botov、Andrei Brazhuk、Mark “Logxen” Cooper、Yuan Jochen Kang、Mal Malakov、Lewis Porter 和 Jarle Thorsen。

特别感谢承担最多校对工作的，同时也是补救最多纰漏的朋友 Vasil Kolev。

感谢封面设计 Andy Nechaevsky。

感谢 github.com 的朋友，谢谢他们所发的各种资料以及勘误。

本书使用了 LATEX 的多种工具。在此，我向它们的作者表示敬意。

捐赠

希望鼓励作者继续创作的读者，通过下述网站进行捐赠：

Dennis Yurichevdonate.html

为了表示感谢，每位捐赠者都会获得题名。此外，捐赠者感兴趣的内容将会被优先更新或补充。

捐赠人名录

25 * anonymous, 2 * Oleg Vygovsky (50+100 UAH), Daniel Bilar ($50), James Truscott ($4.5), Luis Rocha ($63), Joris van de Vis ($127), Richard S Shultz ($20), Jang Minchang ($20), Shade Atlas (5 AUD), Yao Xiao ($10), PawelSzczur (40 CHF), Justin Simms ($20), Shawn the R0ck ($27), Ki Chan Ahn ($50), Triop AB (100 SEK), AngeAlbertini (10+50 EUR), Sergey Lukianov (300 RUR), LudvigGislason (200 SEK), Gérard Labadie (40 EUR), Sergey Volchkov (10 AUD), VankayalaVigneswararao ($50), Philippe Teuwen ($4), Martin Haeberli ($10), Victor Cazacov (5 EUR), Tobias Sturzenegger (10 CHF), Sonny Thai ($15), BaynaAlZaabi ($75), Redfive B.V. (25 EUR), JoonaOskariHeikkilä (5 EUR), Marshall Bishop ($50), Nicolas Werner (12 EUR), Jeremy Brown ($100), Alexandre Borges ($25), Vladimir Dikovski (50 EUR), Jiarui Hong (100.00 SEK), Jim_Di (500 RUR), Tan Vincent ($30), Sri HarshaKandrakota (10 AUD), Pillay Harish (10 SGD), TimurValiev (230 RUR), Carlos Garcia Prado (10 EUR), Salikov Alexander (500 RUR), Oliver Whitehouse (30 GBP), Katy Moe ($14), Maxim Dyakonov ($3), Sebastian Aguilera (20 EUR), Hans-Martin Münch (15 EUR), JarleThorsen (100 NOK), VitalyOsipov ($100)。

FAQ

Q：学习汇编语言有何用武之地？

A：除去开发操作系统的研发人员之外，现在几乎没有什么人还要用汇编语言编写程序了。目前，编译程序优化汇编指令的水平已经超越编程人员的脑算水平[①]，而且 CPU 越来越复杂——即使一个人具备丰富的汇编语言的知识，也不代表他有多么了解计算机硬件。但是不可否认的是，汇编语言的知识至少有两大用处：首先，它有助于安全人员进行安全研究、分析恶意软件；其次，它还有助于帮助编程人员调试程序。本书旨在帮助人们理解汇编语言，而不是要指导读者用汇编语言进行编程。所以，作者组织了大量的源代码和对应的汇编指令，供读者研究。

Q：这本书太厚了，有没有精简版？

A：精简版可从网上下载：http://beginners.re/#lite。

Q：逆向工程方面的就业情况如何？

A：在 reddit 等著名网站里，很多著名公司一直在招聘熟悉汇编语言和逆向工程的 IT 专家，甚至专门招聘逆向工程领域的安全专家。有兴趣的读者可以访问以下网址：

http://www.reddit.com/r/ReverseEngineering/

http://www.reddit.com/r/netsec/comments/221xxu/rnetsecs_q2_2014_information_security_hiring

Q：我想要提些问题……

A：作者的邮件地址是：dennis(a)yurichev.com。

读者还可以在我们的网站 forum.yurichev.com 参与互动。

读者点评

- “构思精巧……而且免费……确实不错”——Daniel Bilar, Siege Technologies, LLC。
- “……了不起的免费读物！”——Pete Finnigan, Oracle RDBMS security guru。
- “……引人入胜，值得一读！”——Michael Sikorski,《Practical Malware Analysis: The Hands-On Guide to DissectingMalicious Software》的作者。
- “……谨向这本出色的教材致以个人的敬意！”——Herbert Bos，阿姆斯特丹自由大学教授，《Modern Operating Systems（4th Edition）》作者之一。
- “……令人惊讶、难以置信”。——Luis Rocha, CISSP / ISSAP，技术经理，Verizon 业务部网络及信息安全中心。
- “感谢如此辛劳的作者、感谢如此精彩的书。”——Joris van de Vis, SAP 集成平台及安全专员。
- “……部分内容可圈可点。”——Mike Stay，教员，联邦执法训练中心，Georgia, US。
- “这本书超赞！我的数名学生都在学习这本书，我计划把它当作研究生教材。”——Sergey Bratus，计算机科学系研究助理教授，（美）达特茅斯学院。
- “Dennis Yurichev 发表了一本逆向工程方面的宝典（还免费）！”TanelPoder, Oracle RDBMS 性能调控专家。
- “这本书可谓初学者的百科全书……”——Archer，中文译者，IT 安全研究员。

[①] 可查阅参考文献[Fog13b]。

目　录

第一部分　指令讲解