

网络空间安全前沿技术丛书

智能互联时代，掐断便利与乐趣背后泄露隐私的黑手



[美]亨利·达尔齐尔 (Henry Dalziel)

[美]约书亚·施罗德 (Joshua Schroeder)

区文浩 (Man Ho Au)

著

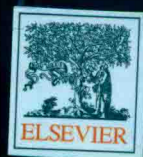
陈子越 李 巍 沈卢斌 译

[美]徐金光 (Kim-Kwang Raymond Choo)

悄无声息的战场

无线网络威胁和移动安全隐私

清华大学出版社



网络空间安全前沿技术丛书

悄无声息的战场

无线网络威胁和移动安全隐私

[美]亨利·达尔齐尔 (Henry Dalziel)

[美]约书亚·施罗德 (Joshua Schroeder) 著

区文浩 (Man Ho Au)

[美]徐金光 (Kim-Kwang Raymond Choo)

陈子越 李 巍 沈卢斌 译

清华大学出版社

北京

本书封底贴有 Elsevier 防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

悄无声息的战场:无线网络威胁和移动安全隐私/(美)亨利·达尔齐尔(Henry Dalziel)等著;陈子越,李巍,沈卢斌译. —北京:清华大学出版社,2019

(网络空间安全前沿技术丛书)

书名原文:Meeting People via WiFi and Bluetooth; Mobile Security and Privacy: Advances, Challenges and Future Research Directions

ISBN 978-7-302-51292-9

I. ①悄… II. ①亨… ②陈… ③李… ④沈… III. ①互联网络—网络安全—研究
IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 220267 号

责任编辑:梁颖 柴文强

封面设计:常雪影

责任校对:焦丽丽

责任印制:宋林

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课件下载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京嘉实印刷有限公司

经 销:全国新华书店

开 本:190mm×235mm 印 张:23.75 字 数:360 千字

版 次:2019 年 7 月第 1 版 印 次:2019 年 7 月第 1 次印刷

定 价:79.00 元

产品编号:073559-01

本书献给

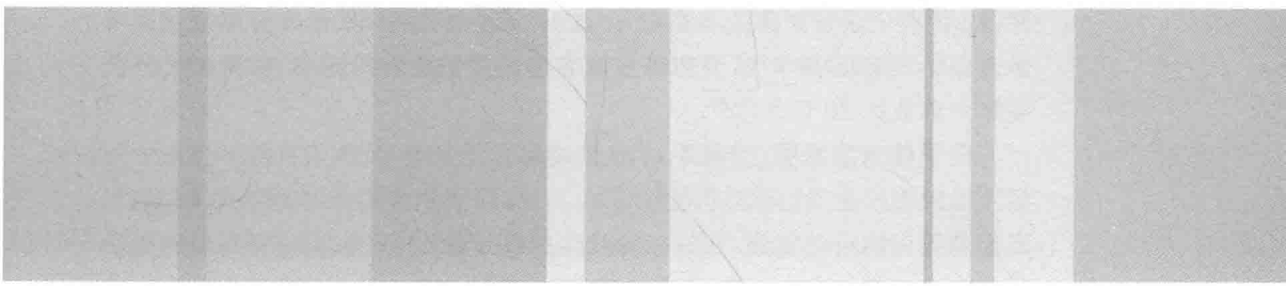


致力于

商用SD-WAN智能广域网平台应用开发的

华斧网络科技（AXESDN）公司

所有网络专家



译者序

物理学上,我们身处的时空有四个维度(3个空间轴和1个时间轴)。我们的宇宙由时间和空间构成,所以根据爱因斯坦的相对论称为四维时空。三维空间的物体可以用体积进行衡量,那又如何衡量四维时空呢?不妨把信息量的大小视为这个四维时空的衡量单位。单位时间内信息量越大,四维时空的精细程度就越高。比如用摄像机和录音笔记录同一场足球比赛,视频就要比纯音频多出非常多的信息,将它们在磁盘上保存下来所对应的文件大小也差别巨大,视频文件的大小就要比音频文件大出几个数量级。

信息无处不在,它是动态的,任意时刻它都在产生和湮灭。通过各种信息载体可以把信息记录下来,于是就出现了化石、纸张、胶卷、胶片、磁带、磁盘等,如何保护好这些信息载体就显得非常重要,同时信息安全应运而生。

电子技术与数字化时代的飞速发展使得信息产生的速度和容量呈倍数地增长,而此前附着于信息载体上的安全的重要性被信息自身安全的重要性取而代之。信息的安全性就像达摩克利斯之剑一样悬在每个人的头顶,在感叹信息技术伟大的同时却处处受到它的掣肘,稍有不慎,便可能遭遇其带来的意想不到的麻烦。2016年,全球已约有3000起公开的数据泄露事

件,22亿条记录被泄露或者盗取^①;2017年全年超过50亿条信息被泄露或者盗取^②。自2015年10月以来在黑客的暗网里贩售的网易、腾讯、新浪、搜狐账户总数达18亿之多^③。

电子技术的发展,使得手机日益成为人类社会必不可少的用具。手机极大地便利了生活,尤其是智能手机,它帮助我们全天候地保持在线状态,它记录我们的行动轨迹,它保存着我们的影音图像,它忠实地把我们的生活记录在小小的设备中。利用合法或非法的手段,就可以通过它了解手机主人的社交网络、行动轨迹、情感历史,甚至可以推测其性格特点。用一句话来概括,智能手机可以保存其使用者的几乎全部信息特征。

据媒体报道,2016年美国联邦调查局(FBI)针对两起刑事犯罪案件向美国苹果公司提出解锁嫌犯iPhone手机的请求,苹果公司就iPhone加密问题与FBI争执得不可开交,苹果公司公开回应不会对任何破解iPhone手机的请求提供帮助。但事与愿违,联邦调查局在最后时刻还是在第三方的帮助下成功访问了手机。虽然美国政府并未指明是谁助其破解了iPhone手机,但之后有报道称,是一家名为Cellebrite的以色列安全公司帮助了FBI。螳螂捕蝉黄雀在后,2017年早些时候,Cellebrite遭到了黑客的攻击,可以破解iPhone的安全公司被黑客窃取了超过900GB的用户数据。像这样矛与盾的故事随时随地都在上演。在信息技术迅猛发展的趋势下,机构甚至个人都可以依托强大的计算能力破解任何密码和密钥。机器学习的发展、算法的应用、计算机算力的快速提升已经严重威胁了曾坚不可摧的密码学。无论多么复杂的密钥算法,在强大和智能的机器学习威胁下,都将不再安全。这对执法者和躲在黑暗角落里的黑客来说都是福音。

每个人都应学会如何保护个人信息的安全,就如同人人都需要保护自己的人身安全一样重要。保护自己人身安全需要强化安全意识和身体体魄,个人信息的安全也需要知识的积累和必要的投入。

本书详尽分析了大量用户的典型行为,以及与之相伴的安全和隐私风险,并提供了一系列安全建议供用户参考。本书通过系统化地讲解手机安

① <https://www.zybuluo.com/codeep/note/612396>

② <http://www.aqniu.com/industry/30413.html>

③ <http://t.cj.sina.com.cn/articles/view/5095232218/12fb312da0010018fb>

全和隐私保护的概念,对比阐述传统的防护方法与基于机器学习的防护软件的优缺点,向用户介绍了如何保护个人的信息以减少隐私泄露和财产损失的风险。

这是一场涉及所有人的、旷日持久的战役,知己知彼方能百战不殆。为了保护个人隐私和数据安全,我们应将信息安全列为基础教育的必修课;同时政府机构须完善其信息安全法律法规,加强对个人数据的保护;个体尤其要养成良好的隐私保护习惯;当然还需要企业制作更加精良强大的工具以保护个人信息安全。

本书面向广泛的读者群体,包括手机用户、手机软件设计人员和手机安全从业人员。

为了帮助读者理解本书内容,全书大概可以分为以下五部分。

第一部分为第1~4章,解释了手机安全的概念、用户的典型行为和与之相伴随的安全风险。

第二部分包含第5章,解释了执法机构如何利用手机办公。

第三部分为第6~8章,解释了手机安全工作原理,引入机器学习技术,并详细列举各种技术和软件的差异性。

第四部分包含第9章,解释了执法机构如何对特定手机进行司法取证。

第五部分为第10~12章,解释了大数据和人工智能(AI)技术革命时代软件设计应该遵循的技术规范和设计理念。

本书在酝酿、准备、翻译过程中,受到了清华大学出版社电子信息事业部梁颖主任的悉心指导和鼎力支持,在此特别感谢。

由于译者水平有限,书中难免存在遗漏或有失准确之处,欢迎广大读者不吝指正。

译者

2018年10月

于瑞典斯德哥尔摩

目 录

第 1 章 通过 WiFi 追踪他人	1
摘要	1
关键词	1
1.1 设备关联扫描概述	2
1.2 需要的硬件和软件	8
1.3 结论	34
参考文献	35
第 2 章 移动安全及隐私	36
摘要	36
关键词	37
2.1 概要	37
2.2 移动安全面临的威胁	38
2.2.1 应用层威胁	38
2.2.2 Web 层威胁	39
2.2.3 网络层威胁	39

2.2.4 物理层威胁	39
本书的内容结构	40
参考文献	40
第3章 移动安全——从业者的观点	43
摘要	43
关键词	43
致谢	44
3.1 移动安全	44
手机使用的全球增长	46
3.2 原则	47
3.3 应用商店	49
3.4 合法应用程序	50
3.4.1 应用程序容器化	51
3.4.2 软件水印	52
3.5 身份管理问题	53
3.6 隐私	55
3.6.1 对隐私的需求	55
3.6.2 隐私的含义	57
3.7 漏洞	59
3.8 威胁	60
3.8.1 基于应用程序的威胁	61
3.8.2 基于互联网的威胁	62
3.8.3 网络威胁	65
3.8.4 物理威胁	67
3.8.5 旅行威胁	68
3.8.6 无意的数据泄露	68
3.9 风险	69
3.10 移动应用程序开发机构的移动安全策略	71

3.10.1	体系结构	71
3.10.2	基本设备管理	71
3.10.3	安全软件开发生命周期	71
3.10.4	数据验证	71
3.11	缓解措施	75
3.11.1	渗透缓解措施	79
3.11.2	旅行缓解措施	79
3.12	移动安全技术控件	80
3.12.1	密码、口令和生物识别	80
3.12.2	加密	81
3.12.3	虚拟专用网	87
3.12.4	用户培训	88
3.12.5	越狱和破解	88
3.12.6	补丁	89
3.12.7	资产管理	89
3.12.8	移动设备管理	90
3.12.9	移动应用管理	93
3.12.10	远程跟踪与擦除	93
3.12.11	防病毒或反恶意软件	93
3.12.12	传输安全	94
3.12.13	移动设备使用控制	94
3.12.14	内存	95
3.12.15	跨境数据窃取	95
3.12.16	监管保留	96
3.13	取证	96
3.14	总结	98
3.15	移动设备安全资源	101
	参考文献	102
	术语	103

关于作者	107
第4章 移动安全——终端用户是系统中最薄弱的环节	109
摘要	109
关键词	110
4.1 定义：“互联网络”的安全	110
4.2 智能手机漏洞的增长	111
4.3 企业网络安全	116
4.4 个人网络安全	117
4.5 结论	120
参考文献	121
第5章 老年移动设备用户的网络悟性	122
摘要	122
关键词	123
致谢	123
5.1 概要	123
5.1.1 贡献	124
5.1.2 章节概要	125
5.2 调查设计	125
5.3 结果和讨论	127
5.4 情景犯罪预防方法	136
5.5 结论	139
参考文献	140
第6章 移动设备在提高警务系统效率和效益方面所发挥的作用 ——从业者的观点	142
摘要	142
关键词	143

6.1 概要	143
6.2 交互式巡警系统	145
6.3 能力	147
6.3.1 信息管理与知识交流权限模型的局限性	147
6.3.2 智能个人助理	149
6.3.3 通信	149
6.3.4 拘留管理	150
6.3.5 情景意识	152
6.3.6 生物特征	153
6.4 结论	155
参考文献	156
补充阅读材料	156
第7章 基于监督学习检测安卓上的恶意软件	158
摘要	158
关键字	159
致谢	159
7.1 权限的背景介绍	161
7.2 恶意软件概述	165
7.2.1 恶意软件技术	165
7.2.2 恶意软件检测工具	166
7.3 机器学习	168
7.3.1 概念	169
7.3.2 相关研究：机器学习与权限	173
7.4 基于用户安全规范的表征和检测	179
7.4.1 采集样本	179
7.4.2 第一层	180
7.4.3 第二层	183
7.4.4 第三层	188

7.4.5	初步学习	189
7.4.6	提取规则	190
7.4.7	分类器	192
7.4.8	用户参与	196
7.5	系统实现	197
	接口	198
7.6	评价和讨论	201
7.6.1	检测性能	201
7.6.2	各层模型之间的比较	203
7.6.3	检测恶意软件家族	204
7.6.4	防病毒扫描程序	208
7.6.5	相关研究	209
7.6.6	局限性	215
7.7	总结和展望	216
附录 A	不同的权限组合和风险系数	217
附录 B	用于测试的正常应用程序	217
	参考文献	217
第 8 章	如何发现安卓应用程序的漏洞	224
	摘要	224
	关键词	224
8.1	介绍	225
8.2	背景	226
8.2.1	安卓安全机制	226
8.2.2	安卓应用程序漏洞分类	227
8.2.3	VulHunter	228
8.3	常见安全隐患	228
8.3.1	不安全的数据存储	228
8.3.2	传输层保护不足	229

8.3.3 意外的数据泄露	229
8.3.4 不严谨的授权和认证	229
8.3.5 破损的加密	230
8.3.6 WebView 漏洞	230
8.3.7 应用程序通信漏洞	231
8.3.8 配置错误漏洞	231
8.4 发现漏洞	231
8.4.1 静态分析方法	231
8.4.2 基于动态分析的方法	233
8.4.3 混合方法	234
8.5 讨论	235
8.5.1 基于静态分析方法的局限性	235
8.5.2 基于动态分析方法的局限性	235
8.5.3 未来方向	236
8.6 本章小结	236
参考文献	237
关于作者	239
第 9 章 安卓免费安全防护软件的有效性和可靠性的研究	240
摘要	240
关键词	241
9.1 介绍	241
9.2 安卓操作系统概述	243
9.2.1 安卓操作系统	243
9.2.2 安卓应用安全	249
9.2.3 安卓恶意软件威胁和对策	252
9.3 实验设置	266
9.3.1 实验过程	273
9.3.2 指标	275

9.4 实验结果	276
9.5 结论和未来工作	285
利益冲突声明	286
参考文献	286
第 10 章 基于 MTK 的山寨手机数字证据时间轴分析	292
摘要	292
关键词	292
致谢	293
10.1 介绍	293
10.2 相关工作	294
10.3 山寨手机的数字证据	295
10.3.1 物理数据存储和逻辑文件系统	296
10.3.2 从山寨手机闪存转储提取基线内容	297
10.4 数字证据的时间轴分析	300
10.4.1 在 Flash 转储器中被删除的内容和“快照”	300
10.4.2 电话簿上的时间轴分析	301
10.5 结论	304
参考文献	304
第 11 章 RESTful IoT 认证协议	306
摘要	306
关键词	307
11.1 介绍	307
11.2 REST 基础	308
11.3 RESTful IoT 协议	310
11.3.1 RESTful CoAP	310
11.3.2 RESTful RACS	312
11.4 RESTful IoT 协议的安全性	315

11.5 REST 消息认证	318
11.5.1 REST 消息签名	319
11.5.2 REST 消息验证	320
11.6 RESTful IoT 消息认证	321
11.6.1 RESTful CoAP 协议的消息验证	322
11.6.2 RESTful RACS 消息认证	324
11.7 结论和展望	326
参考文献	327
第 12 章 各种隐私模型的介绍	330
摘要	330
关键词	330
12.1 概要	331
组织结构	332
12.2 k -Anonymity 的定义	332
12.3 支持 k -Anonymity 的机制	334
12.4 差分隐私	337
12.4.1 概述	338
12.4.2 差分隐私的定义	338
12.5 拉普拉斯机制实现差分隐私	339
12.6 本章小结	340
参考文献	340
关于作者	342
第 13 章 数字签名方案在移动设备上的性能	344
摘要	344
关键词	345
致谢	345
13.1 概要	345

我们的贡献	346
13.2 相关工作	347
13.3 实验	347
13.3.1 加密设置	348
13.3.2 测试环境	348
13.3.3 实验结果和观察发现	351
13.4 本章小结	353
参考文献	353
关于作者	355