参考书目

[1] M Aamir Ali、B Arief、M Emms、A van Moorsel，“在线卡支付环境是否会在不知不觉中助长欺诈？” IEEE 安全与隐私杂志 (2017)

[2] M Abadi、RM Needham，“密码学的审慎工程实践
Protocols”，IEEE Transactions on Software Engineering v 22 no 1（96 年 1 月)第 6-15 页;也作为 DEC SRC 研究报告第 125 号（1994 年 6 月 1 日）

[3] A Abbasi，HC Chen，“可视化作者身份识别”，ISI
2006 年，LNCS 3975 第 60-71 页

[4] H Abelson、RJ Anderson、SM Bellovin、J Benaloh、M Blaze、W Die、J
Gilmore、PG Neumann、RL Rivest、JI Schiller、B Schneier，“风险
密钥恢复、密钥托管和可信第三方加密”，在 World
Wide Web Journal v 2 no 3（1997 年夏季)第 241–257 页

[5] H Abelson、RJ Anderson、SM Bellovin、J Benaloh、M Blaze、W Die、J
Gilmore、M Green、PG Neumann、RL Rivest、JI Schiller、B Schneier、M
Spectre，D Weizmann，“门垫下的钥匙：通过要求政府访问所有数据和通信来强制不安全”，麻省理工学院 CSAIL
技术报告 2015-026（2015 年 7 月 6 日）； ACM Communications v 58 no 10（2015 年 10 月)中的删节版

[6] M Abrahms，“恐怖分子真正想要什么”，国际安全 v 32 no
4 (2008) 第 78–105 页

[7] M Abrahms，J Weiss，“恶意控制系统网络安全攻击
案例研究 – Maroochy Water Services，澳大利亚”，ACSAC 2008

[8] A Abulafia、S Brown、S Abramovich-Bar，“一起涉及
新型墨水根除方法”，《法医学杂志》第 41 卷（1996 年)第 300-302 页

[9] DG Abraham、GM Dolan、GP Double、JV Stevens，“交易安全
System”，IBM Systems Journal v 30 no 2 (1991) pp 206–229

[10] Y Acar、M Backes、S Bugiel、S Fahl、PD McDaniel、M Smith，“SoK：课程
从应用软件平台的 Android 安全研究中学习”，
IEEE 标准普尔 2016 年第 433–451 页

[11] Y Acar、S Fahl、M Mazurek，“你也不是你的开发者：A
Beyond End 可用安全和隐私研究的研究议程
用户”，IEEE SecDev 2016

[12] N Achs，“VISA 对抗骗子”，Cards International（1992 年 10 月 20 日）
第 8-9 页

[13] O Ac i¸cmez, ¸CK Ko¸c, JP Seifert，“关于简单分支预测分析的力量”第二届 ACM 信息、计算机和通信安全研讨会 (2007) 第 312–320 页

[14] S Ackerman，J Ball“视神经：数百万雅虎网络摄像头图像被 GCHQ 拦截”，卫报，2014 年 2 月 28 日

[15] A Acquisti、A Friedman、R Telang，“侵犯隐私有代价吗？”，第五次信息安全经济学研讨会（2006 年）

[16] A Acquisti、G Loewenstein、L Brandimarte，“秘密和喜好：数字时代对隐私的需求和实现隐私的难度”，《Journal of
消费心理学 (2020)

[17] NR Adam，JC Wortmann，“统计的安全控制方法
数据库：一项比较研究”，ACM Computing Surveys v 21 no 4 (1989) pp 515–556

[18] EN Adams，“优化软件产品的预防性维护”，
IBM 研究与开发杂志，第 28 期第 1 期（1984 年）第 2-14 页

[19] J Adams，“风险”，伦敦大学学院出版社（1995 年）

[20] J Adams，“汽车、霍乱和奶牛：风险和不确定性的管理”，政策分析第 335 期，卡托研究所，华盛顿，1999 年

[21] E Addley《动物解放阵线轰炸机被判入狱 12 年》的
卫报 2006 年 12 月 6 日

[22] B Adida、M Bond、J Clulow、A Lin、RJ Anderson、RL Rivest，“关于 IBM 4758 CCA 中 EMV 安全消息传递的注释”，网址为 www.ross-anderson.com

[23] H Adkins, B Beyer, P Blankiship, P Lewandowski, A Oprea, A Stubblefield,
“构建安全可靠的系统”，Google 2020

[24] A Adler，“样本图像可以从人脸识别模板中独立恢复”，Proc。能。会议。电。比较。工程。 (2003) 第 1163–1166 页

[25] A Adler，“生物识别加密系统中的漏洞”，北约 RTA
研讨会：加强信息系统安全 生物识别技术 (IST
044-RWS-007)

[26] D Adrian、K Bhargavan、Z Durumeric、P Gaudry、M Green、JA Halder man、N Heninger、D Springall、E Thom e、L Valenta、B VanderSloot、E Wustrow、S Zanella-B guelin、P Zimmermann，“不完美的前向保密：Die-Hellman 如何在实践中失败”，ACM CCS 2015，weakdh.org

[27] Y Afina、C Inverarity、B Unal，“确保北约指挥、控制和通信系统的网络弹性”，查塔姆研究所，2020 年 7 月

[28] S Afroz、M Brennan、R Greenstadt，“检测在线写作风格中的恶作剧、欺诈和欺骗”，IEEE 安全与隐私研讨会 (2012) 第 461-475 页

[29] “支持服务器签名的可信系统第 2 部分：QCSD 的服务器签名保护配置文件”，419241-2，国家信息安全局，2018 年

[30] H Agnew，“Jim Chanos 从 Wirecard 空头中赚取 1 亿美元”，金融
时代 2020 年 7 月 24 日

[31] M Ahmed-Rengers、R Anderson、D Halatova、I Shumailov，“告密者得到缝合：关于举报的
困难”，安全协议工作室（2019 年）；在线为 arXiv:2006.14407 (2010)

[32] C Ajluni，“两种新的成像技术有望改善 IC 缺陷
Identification”，Electronic Design v 43 no 14（1995 年 7 月 10 日）第 37-38 页

[33] Y Akdeniz，“互联网儿童色情制品监管”（1999 年 12 月），http://www.cyber-rights.org/
reports/child.htm

[34] G Akerlof，“柠檬市场：质量不确定性和市场
机制”，经济学季刊 v 84 no 3 (1970) pp 488–500

[35] M Alagappan、JV Rajendran、M Doroslova ˇ cki、G Venkataramani，“DFS
多核平台上的隐蔽通道”，Visisoc 2017

[36] R Albert、HW Jeong、AL Barab´asi，“复杂的错误和攻击容限
网络”，在 Nature v 406 no 1 (2000) pp 387–482

[37] J Alfke，“Facebook 和去中心化标识符”，思想宫 12 月 2 日
2007年

[38] AM Algarni、YK Malaiya，“软件漏洞市场：发现者和购买者”，国际计算机、信息科学和

工程 v 8 no 3 (2014)

[39] M Ali、P Sapiezinski、M Bogen、A Korolova、A Mislove、A Rieke，“通过优化进行歧视：
Facebook 的广告投放如何导致
有偏见的结果”，ACM 人机交互会议录第 3 版（2019 年）

[40] M Ali、P Sapiezinski、A Korolova、A Mislove、A Rieke，“广告投放算法：政治信息的隐藏仲
裁者”，arXiv：1912.04255，Dev 17 2019

[41] E Allman，“管理技术债务”，ACM 通讯 v 55
第 5 期（2012 年 5 月）第 50-55 页

[42] M Allman、V Paxson，“关于使用共享测量数据的礼仪”，在互联网测量会议 (IMC 2007) 中，
网址为 http://www. imconf.net/imc-2007/papers/imc80.pdf

[43] F Almgren、G Andersson、T Granlund、L Ivansson、S Ulfberg，“我们如何破解密码本密
码”，http://codebook.org

[44] T Alves、D Felton，“TrustZone：集成硬件和软件安全”，Information Quarterly (2004)

[45] 美国工业安全协会，http://www.asisonline.org

[46] 国际特赦组织，“不断演变的针对中东和北非记者和人权维护者的网络钓鱼攻击”，2019 年 8
月 16 日

[47] E Amoroso，“计算机安全技术基础”，Prentice Hall
(1994)

[48] R Andersen，“圆形监狱已经在这里”，大西洋，2020 年 9 月

[49] C Anderson、K Sadjadpour，“伊朗的网络威胁：间谍、破坏和报复”，卡内基基金会，2018 年 1 月 4 日

[50] B Andersen、M Frenz，“音乐下载和 P2P 文件共享对音乐购买的影响：加拿大工业研究”，2007 年，http://strategis.ic.gc.ca/epic/site /ippd-dppi.nsf/en/h_ip01456e.html

[51] J Anderson，“计算机安全技术规划研究”，ESD-TR-73-51，美国空军电子系统部 (1973) http://csrc.nist。 gov/publications/history/index.html

[52] M Anderson、W Seltzer，《社会统计和统计机密：近期著作和基本文件》，网址为 http:// www.uwm.edu/%7Emargo/govstat/integrity.htm

[53] RJ Anderson，“解决一类流密码”，Cryptologia v XIV no 3（1990 年 7 月）第 285-288 页

[54] RJ Anderson，ACM 通信第 37 卷第 11 卷中的“为什么密码系统会失败”（1994 年 11 月）第 32-40 页；早期版本在 http://www.cl。 cam.ac.uk/users/rja14/wcf.html

[55] RJ Anderson，“责任与计算机安全：九项原则”，计算机安全 ESORICS 94，Springer LNCS v 875，第 231-245 页

[56] RJ Anderson，“欧洲的加密货币 市场、法律和政策”，密码学：政策和算法，Springer LNCS v 1029，第 75-89 页

[57] RJ Anderson，“临床系统安全 – 临时指南”，英国医学杂志 v 312 no 7023（1996 年 1 月 13 日）第 109-111 页； HTTP://www.cl.cam.ac.uk/ftp/users/rja14/guidelines.txt

[58] RJ Anderson，“临床信息系统的安全性”，英国医学协会 (1996)

[59] RJ Anderson，“临床信息系统的安全策略模型”，1996 年 IEEE 安全和隐私研讨会第 30-43 页 http://www. cl.cam.ac.uk/users/rja14/policy11/policy11.html

[60] RJ Anderson，“BMA 安全政策更新”，[63] 第 233-250 页

[61] RJ Anderson，“永恒服务”，载于 Pragocrypt 会议记录 96 页 242–252

[62] RJ Anderson（编辑），第一届信息隐藏国际研讨会论文集（1996），Springer LNCS v 1174

[63] RJ Anderson（编辑），“个人医疗信息 安全、工程和伦理”，Springer-Verlag（1997）

[64] RJ Anderson，“关于数字行驶记录仪的安全性”，ESORICS 98，施普林格 LNCS v 1485 第 111–125 页

[65] RJ Anderson，“临床信息系统中的安全和隐私”，载于“重新思考 IT 与健康”，J Lenaghan（编辑），IPPR（98 年 11 月）第 140-160 页

[66] RJ Anderson，“冰岛健康数据库的 DeCODE 提案”； Læknabladhidh（冰岛医学杂志）v 84 no 11（98 年 11 月)第 874-5 页,http://www.cl.cam.ac.uk/users/rja14/#Med

[67] RJ Anderson，“支付系统的形式验证”,Industrial Strength Formal Methods:A Practitioners Handbook 章节,MG Hinchey 和 JP Bowen（编辑）,Springer Verlag（1999 年 9 月)第 43-52 页

[68] RJ Anderson，“如何在彩票中作弊（或大规模并行需求工程）”,第 15 届年度计算机安全应用会议（1997 年）;第 xix-xxvii 页;在 http://www.cl.cam.ac.uk/~rja14/lottery/lottery.html

[69] RJ Anderson，“千年虫 不要惊慌的原因”,http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/y2k.html

[70] RJ Anderson，“关于冰岛健康数据库安全目标的评论”,网址为:http://www.cl.cam.ac.uk/ftp/users/rja14/iceland-admiral.pdf

[71] RJ Anderson，“加密交易集的正确性”,2000 年安全协议会议记录,Springer LNCS v 2133,第 125-141 页

[72] RJ Anderson，“为什么信息安全很难 从经济角度来看”,ACSAC 2001,第 358-365 页；也作为杰出的演讲在 安全战略计划,2001 年

[73] RJ Anderson，“密码学和竞争政策 ‘可信’问题 Computing ”,第二届经济与信息安全研讨会（2003 年）

[74] RJ Anderson，“开放系统和封闭系统是等价的（即在理想世界中）”,自由和开源软件的观点,麻省理工学院出版社 2005 年,第 127-142 页

[75] RJ Anderson，“关闭网络钓鱼漏洞 欺诈、风险和非银行”,载于支付系统中的非银行机构:创新、竞争和风险,美国美联储,圣达菲,2007 年 5 月 2-4 日

[76] RJ Anderson，“安全经济学资源页面”,网址为 http://www.cl.cam。 ac.uk/~rja14/econsec.html

[77] RJ Anderson，“祝所有银行家圣诞快乐”,https://www.lightbluetouchpaper.org，2010 年； https://www.lightbluetouchpaper.org/2010/12/25/merry-christmas-all-bankers/

[78] RJ Anderson，“安全经济学 个人观点”,ACSAC 2012

[79] RJ Anderson，“消费者支付创新的风险和隐私影响”,互联时代的消费者支付创新,堪萨斯城 美联储,2012 年 3 月

[80] RJ Anderson，“我们的医疗记录的隐私正在被出售 o ”,The 卫报 2012 年 8 月 28 日

[81] RJ Anderson，“信息专员会保持一致吗？”， https://www.lightbluetouchpaper.org 2012 年 11 月 20 日

[82] RJ Anderson，“隐私是如何丢失的”，网址为 https://lightbluetouchpaper.org
2013 年 4 月 28 日

[83] RJ Anderson，“O ender tagging”，https://lightbluetouchpaper.org
2013 年 9 月 2 日

[84] RJ Anderson，“隐私与政府监控：网络效应与公共选择的关系”，信息经济学研讨会
安全 (2014)

[85] RJ Anderson，“宵禁标签 血淋淋的细节”https://
lightbluetouchpaper.org 2014 年 12 月 13 日

[86] RJ Anderson，“在普林斯顿会见斯诺登”，https：
//lightbluetouchpaper.org 2015 年 5 月 2 日

[87] RJ Anderson，“支付 AI 费用的人做主”，The Edge 问题 2015：您如何看待会思考的机器？，https://
www.edge。组织/响应细节/26069

[88] RJ Anderson，“Future ID”，2019 年 3 月 19 日，网址为 https://www.
lightbluetouchpaper.org/2019/03/19/future-id/

[89] RJ Anderson，剑桥大学软件与安全工程，2020 年，https://www.cl.cam.ac.uk/teaching/1920/
SWSecEng/
材料.html

[90] RJ 安德森、C 巴顿、RB 欧姆、R 克莱顿、M 范埃滕、M 列维、T
Moore, S Savage，“衡量网络犯罪的成本”，WEIS 2012

[91] RJ Anderson, C Barton, RB¨ohme, R Clayton, C Ga n´an, T Grasso, M
Levi、T Moore、M Vasek，“衡量网络犯罪不断变化的成本”，
威斯 2019

[92] RJ Anderson，T Berger-Wolf，“老虎的隐私”，Usenix Security 2018

[93] RJ Anderson，SJ Bezuidenhoudt，“关于电子支付的可靠性
Systems”，IEEE Transactions on Software Engineering v 22 no 5（1996 年 5 月）第 294-301 页

[94] RJ Anderson、E Biham、LR Knudsen，“Serpent：高级加密标准的提案”，作为 AES 候选者提交给 NIST；
在[95]

[95] RJ Anderson、E Biham、L Knudsen，“The Serpent Home Page”，http://
www.cl.cam.ac.uk/~rja14/serpent.html

[96] RJ Anderson, N Bohm, T Dowty, F Fisher, D Kor , E Munro, M Thomas,
“关于数据共享审查的咨询回复”，FIPR 2008 年 2 月 15 日

[97] RJ Anderson、RB¨ohme、R Clayton、T Moore，“安全经济学和
内部市场”，ENISA，2008 年

[98] RJ Anderson，M Bond，“对嵌入式系统的 API 级攻击”，载于
IEEE Computer v 34 no 10（2001 年 10 月）第 67-75 页

[99] RJ Anderson，M Bond，计算机系统中的“协议分析、可组合性和计算”：理论、技术和应用，Springer 2003，
第 7-10 页

[100] RJ Anderson、M Bond、J Clulow、S Skorobogatov，“密码处理器 一项调查”，剑桥大学计算机实验室技术报告第 641 号（2005 年 7 月）； Proc 中的缩短版本。 IEEE v 94 no 2（2006 年 2 月)第 357–369 页

[101] RJ Anderson, I Brown, R Clayton, T Dowty, D Kor , E Munro, 儿童数据库 安全和隐私”，信息专员办公室，英国，2006 年 11 月

[102] RJ Anderson，I Brown，T Dowty，W Heath，P Inglesant，A Sasse，数据库州，约瑟夫·朗特里改革信托基金，2009 年

[103] RJ Anderson、B Crispo、JH Lee、C Manifavas、V Maty´as、FAP Petitcolas，“全球互联网信任登记册”，麻省理工学院出版社（1999 年)http://www.cl。 cam.ac.uk/Research/Security/Trust-Register/

[104] R Anderson, S Fuloria，“安全经济学和关键国家基础设施”，WEIS 2009；信息安全和隐私经济学 (2010) 第 55-66 页

[105] R Anderson, S Fuloria，“谁控制 o 开关？”在 IEEE SmartGrid Comm (2010)

[106] RJ Anderson，MG Kuhn，“防篡改 警告”，载于第二届 Usenix 电子商务研讨会论文集（96 年 11 月)第 1-11 页

[107] RJ Anderson，MG Kuhn，“对防篡改设备的低成本攻击”，安全协议 (1997) 第 125–136 页

[108] RJ Anderson，MG Kuhn，“软风暴 北约的机会”，载于保护 21 世纪的北约信息系统，华盛顿哥伦比亚特区，1999 年 10 月 25 日至 26 日

[109] RJ Anderson、JH Lee，“Jikzi：安全发布的新框架”，载于安全协议 99，Springer LNCS v 1976 第 21-36 页

[110] RJ Anderson，TW Moore，“信息安全经济学 - 及其他”，in Crypto 2007，Springer LNCS 4622，第 68-91 页

[111] RJ Anderson，TW Moore，“经济学和互联网安全：一项调查最近的分析、实证和行为研究”，牛津数字经济手册（2011 年）

[112] RJ Anderson，RM Needham，“公钥协议的稳健性原则”，Crypto 95 Springer LNCS v 963 第 236-247 页

[113] RJ Anderson，RM Needham，“今日计算机科学”中的“为撒旦的计算机编程”，施普林格计算机科学讲义 v 1000（1995)第 426-441 页

[114] RJ Anderson、RM Needham、A Shamir，“隐写文件系统”，第二届信息隐藏国际研讨会，Springer LNCS 第 1525 卷，第 74-84 页

[115] RJ Anderson，MR Roe，“GCHQ 协议及其问题”，Euro crypt 97，Springer LNCS v 1233，第 134-148 页

[116] RJ Anderson, I Shumailov, M Ahmed, A Rietmann, “Bitcoin Redux”,
信息安全经济学研讨会 (2018)

[117] T Anderson，“安全研究人员警告说,随着根证书开始大量过期,未来将出现麻烦网络”，
The Register,2020 年 6 月 10 日

[118] CM Andrew,V Mitrokhin， 剑与盾:Mitrokhin
克格勃档案和秘史》,基本书籍（1999 年）

[119] M Andrews,JA Whitaker，“如何破解 Web 软件”,Addison-Wesley
2006年

[120] http://www.anonymizer.com

[121] 匿名者，“我是谷歌的告密者。数百万美国人的医疗数据处于危险之中”,《卫报》,2019 年
11 月 14 日

[122] JC Anselmo，“美国更容易受到电磁攻击”,载于
Aviation Week and Space Technology v 146 no 4（1997 年 7 月 28 日)第 67 页

[123] D Antonioli、NO Tippenhauer 和 KB Rasmussen，“旋钮坏了：
在蓝牙加密密钥协商中利用低熵
BR/EDR”,Usenix 2019

[124] D Antonioli、NO Tippenhauer 和 KB Rasmussen，“偏见:蓝牙 Im
假冒攻击”,IEEE S&P 2020

[125] 匿名书目,2007 年,http://freehaven.net/anonbib/

[126] APACS，“国外欺诈加剧了信用卡欺诈损失”,2007 年 10 月 3 日;在 http://
www.apacs.org.uk/media_centre/press/03.10.07.html;另见 The Register,http://
www.theregister.co.uk/2007/10/03/card_fraud_trends/

[127] APACS，“支付建议 保护您的 PIN”,2007 年 8 月 16 日;在 http://www.apacs.org.uk/
media_centre/press/08_16_07.html

[128] Apple， iOS 安全性,2019 年 5 月

[129] T Appleby，“令人毛骨悚然的借记卡骗局被发现”,环球邮报 (10/12/1999) 第 1 页

[130] I Arghire，“基于硬件的密码管理器以纯文本形式存储凭证”,安全周,2019 年 12 月 9 日

[131] Arm Inc.，“Cache Speculation Side-channels”v 2.4,2018 年 10 月

[132] 美国陆军，“电磁脉冲 (EMP) 和设施的暴风雨保护”,工程兵团出版物仓库,Hyattsville
（1990 年）

[133] A Arora、R Krishnan、A Nandkumar、R Telang、YB Yang，“影响
漏洞披露和补丁可用性 实证分析”，
第三届信息安全经济学研讨会 (2004)

[134] A Arora、CM Forman、A Nandkumar、R Telang，“补丁发布时间的竞争和战略影响”,在
经济研讨会上
信息安全 (2006)

[135] SE Asch，“社会心理学”,牛津大学出版社 1952 年

[136] D Asonov,R Agrawal，“键盘发声”,IBM Almaden
研究中心, 2004

[137] “ASPECT – 个人通信技术的高级安全性”,位于 http://www.esat.kuleuven.ac.be/cosic/
aspect/index.html

[138] 美联社，“对惠普前董事长的指控被撤销 其他三人在董事会间谍案中被指控没有入狱”,2007 年
3 月 14 日,http://www.msnbc.msn.com/id/17611695/

[139] C Aspinwall、A Giorgi、D DiFurio，“美国的几名波音 737 Max 8 飞行员抱怨疑似安全缺陷”,达拉
斯晨报,2019 年 3 月 12 日

[140] R Atkinson，“对付我们已部署部队的最有效武器”和“简易爆炸装置问题正在失控。我们必须止
血”,华盛顿邮报,2007 年 9 月 30 日； “有两年的学习曲线。 . .在那两年里死了很多人”,2007
年 10 月 1 日； “你无法通过装甲来解决这个问题”,2007 年 10 月 2 日； “如果你不追查网
络,你就永远无法阻止这些东西”,2007 年 10 月 3 日,所有链接都来自 https://
blog/2007/09/print/weapon-of-choice/

[141] D Aucsmith，“防篡改软件:一种实现”,[62] 页
317–333

[142] D Aucsmith（编辑）,第二届国际研讨会论文集
信息隐藏（波特兰,98 年 4 月）,Springer LNCS 1525

[143] B Audone,F Bresciani，“主动屏蔽中的信号处理和
测向技术”,IEEE 电磁学汇刊
兼容性 v 38 no 3（1996 年 8 月)第 334-340 页

[144] B Auxier、L Rainie、M Anderson、A Perrin、M Kumar、E Turner，“美国人和隐私:关注、困惑和感
觉无法控制
他们的个人信息”,皮尤研究中心,2019 年 11 月 15 日

[145] A Aviv，“通过智能手机交互启用的侧信道”,博士论文，
宾夕法尼亚大学, 2012

[146] A Aviv、B Sapp、M Blaze、JM Smith，“加速度计侧的实用性
智能手机上的频道”ACSAC 2012

[147] R Axelrod,合作的演变,基础书籍（1984）

[148] I Ayres,SD Levitt，“从不可观察的受害者预防措施中衡量正外部性:Lojack 的实证分析”,《经济
学季刊》第 108 期第 1 期（1998 年 2 月）,http://www.nber.org/papers /w5928

[149] D Austin，“洪水警告”,银行技术（1999 年 7 月至 8 月)第 28- 页
31

[150]“计算机作战规则挫败五角大楼”,载于《航空周刊》和
空间技术 v 147 no 11 (15/9/97) pp 67–68

[151] J Bacon，“并发系统”,Addison-Wesley（1997）

[152] J 培根、K 穆迪、J 贝茨、R 海顿、CY Ma、A McNeil、O Seidel、M
Spiteri，“分布式应用程序的通用支持”,IEEE 计算机
（2000 年 3 月)第 68-76 页

[153] L Badger、DF Sterne、DL Sherman、KM Walker、SA Haghighat，“实用
UNIX 的域和类型执行，”在 1995 年 IEEE 会议记录中
安全和隐私研讨会第 66-77 页

[154] M Baggott，“打击欺诈的聪明方法”，苏格兰银行家（95 年 11 月)第
32–33

[155] M Baker、D Gates，“波音公司改变了 737 MAX 驾驶舱中的钥匙开关，限制了关闭 o MCAS 的能力”，西
雅图时报，2019 年 5 月 10 日

[156] P Baker，“约翰博尔顿的五点收获”aA Zs 回忆录，纽约
时代 2020 年 6 月 18 日

[157] G Baldini、E Leverett、R Clayton、R Anderson，“‘物联网’中安全、保障和隐私的标准化和认证”欧
盟委员会联合研究中心，2017

[158] D Balfanz，EW Felten，“手持电脑可以变得更智能
Cards”，第八届 USENIX 安全研讨会 (1999)，第 15-23 页

[159] T Balmforth，“俄罗斯推迟对冠状病毒的主权互联网测试”，
路透社 2020 年 3 月 20 日

[160] J Bamford， The Puzzle Palace：关于美国国家安全局的报告，美国最机密的
Agency ，Houghton, Mi in (1982)

[161] 国际清算银行，“电子产品的安全性和可靠性”
支付系统，英国计算机协会 (1982)

[162] 加强跨境支付：全球路线图的组成部分 –
向 G20 提交的第二阶段报告，国际清算银行，2020 年 7 月

[163]“银行卡欺诈：银行业的蓬勃发展”，《银行业自动化公告》
欧洲（92 年 3 月)第 1-5 页

[164] J Baniak、G Baker、AM Cunningham、L Martin，“Silent Sentry Passive
监视”，洛克希德·马丁公司任务系统 (1999)

[165] S Bano、A Sonnino、M Al-Bassam、S Azouvi、P McCorry、S Meiklejohn、G Danezis，“SoK：区块链时代的
共识”，arXiv:1711.03936 (2017)

[166] B Barak、O Goldreich、R Impagliazzo、S Rudich、A Sahai、S Vadhan、K Yang，“关于混淆程序的（不)可能
性”，Crypto 2001，http://www.wisdom.weizmann.ac .il/~oded/p_obfuscate.html

[167] M Barbaro, T Zeller, “AOL Searcher No. 4417749 的一张脸”，
纽约时报 2006 年 8 月 9 日

[168] R Barbulescu、P Gaudry、A Joux、E Thom`e，“启发式拟多项式
小特征有限域中的离散对数算法”，
Eurocrypt 2014 第 1-16 页

[169] A Barisani，B Bianco，“实用的 EMV PIN 拦截和欺诈检测
化”，https://github.com/abarisani/，2017

[170] JP Barlow，“思想经济”，连线，1994 年 3 月 1 日

[171] E Barkan、E Biham、N Keller，“仅即时密文密码分析
GSM 加密通信”Technion 技术报告 CS-2006-07

[172] R Barkan、S Ayal、D Ariely，“伦理失调、正当理由和道德行为”，《心理学当前观点》第 6 卷（2015 年）第 157-161 页

[173] RL Barnard，“入侵检测系统”，Butterworths（1988 年）

[174] T 巴恩斯，“NSA 告密者现实获胜者被隔离关押了一段时间一周，没有人解释为什么”，The Intercept 2018 年 9 月 26 日

[175] A Barnett，“英国的 UFO 秘密被揭露”，发表于 The Observer 2000 年 6 月 4 日

[176] S Baron-Cohen，本质区别 erence：男人、女人和极端男性大脑，企鹅，2003

[177] S Baron-Cohen、AM Leslie、U Frith，“自闭症儿童有‘心理理论’吗？”认知（1985 年 10 月）v 21 no 1 pp 37–46

[178] J Barr，“The Gates of Hades”，Linux World 2000 年 4 月；在 http://www. linuxworld.com/linuxworld/lw-2000-04/lw-04-vcontrol_3.html

[179] B Barrow, B Quinn，“数百万人处于芯片和密码欺诈者的危险之中”，载于每日邮报 2006 年 6 月 5 日

[180] B Bartholomew, JA Guerrero-Saade，“挥舞你的假旗！欺骗策略混淆了目标攻击的归因，卡巴斯基实验室，2016 年 10 月 6 日

[181] D Bartz, A Oreskovic，“更新 3-Facebook 与我们就隐私案达成和解 FTC” 路透社 2011 年 11 月 30 日

[182] D Basin、R Sasse、J Toro，“EMV 标准：破坏、修复、验证”，arXiv：2006.08249，2020 年 6 月 15 日

[183] R Baskerville，“信息系统安全设计方法：对信息系统开发的影响”，ACM Computing Surveys v 265 (1993) pp 375–414

[184] PJ Bass，“GPT 电话系统经历的电话卡和技术发展”，GEC Review v 10 no 1 (95) pp 14-19

[185] ‘Bates and others v Post Oce group litigation，2019 年，网址为 https://www.postofficetrial.com/

[186] W Bax，V Dekker，“在 de medische kaartenbak 遇见 zijn allen meekijken”，在 Trouw 2007 年 12 月 11 日

[187] S Baxter，“随着空军‘失去’核导弹，美国按下了恐慌按钮”，载于星期日泰晤士报 2007 年 10 月 21 日

[188] BBC 在线新闻，“‘待售’税务记录丑闻”，2003 年 1 月 16 日，网址：https://news.bbc.co.uk/1/hi/business/2662491.stm

[189] BBC 在线新闻，“对指纹判决的‘救济’”，2006 年 2 月 7 日，网址为 https://news.bbc.co.uk/1/hi/scotland/4689218.stm

[190] BBC 在线新闻，“学校制定生物识别规则”，2007 年 7 月 23 日，网址为 https://news.bbc.co.uk/1/hi/education/6912232.stm

[191] BBC 在线新闻，“PC 剥离器帮助垃圾邮件传播”，2007 年 10 月 30 日，网址为 https://news.bbc.co.uk/1/hi/technology/7067962.stm

[192] BBC 在线新闻，“爱尔兰最差司机之谜”，2009 年 2 月 19 日，http://news.bbc.co.uk/1/hi/northern_ireland/7899171.stm

[193] BBC 在线新闻，“G4S 和 Serco 失去标签合同”，2013 年 12 月 12 日，网址为 https://www.bbc.co.uk/news/uk-25348086

[194] BBC 在线新闻，“公民身份修正案：印度新的‘反穆斯林’法解释”，2019 年 12 月 11 日

[195] S Beattie、S Arnold、C Cowan、P Wagle、C Wright，“为最佳正常运行时间安排安全补丁的应用”，LISA XVI (2002) 第 101-110 页

[196] A Beautement，MA Sasse，M Wonham，“合规预算：管理组织中的安全行为”NSPW 2008

[197] F Beck，“集成电路故障分析 准备技术指南”
niques ，威利 (1998)

[198] J Beck，“法医笔迹检查中的错误来源”，期刊
法医学 v 40 (1995) pp 78–87

[199] G De Becker，“贝佐斯调查发现沙特人获得了他的私人财产
数据” The Daily Beast 2019 年 3 月 30 日

[200] GS Becker，“罪与罚：一种经济方法”，发表于期刊
政治经济学 v 76 no 2（1968 年 3 月/4 月）第 169–217 页

[201] I Becker、A Hutchings、R Abu-Salma、RJ Anderson、N Bohm、SJ Mur doch、MA Sasse、G Stringhini，“银行欺诈报销的国际比较：客户看法和合同条款”，Journal of

网络安全，第 3 卷第 2 期 (2017) 第 109–125 页

[202] L Beckwith、C Kissinger、M Burnett、S Weidenbeck、J Lowrance、A Black well、C Cook，“最终用户程序员调试中的修补和性别”，CHI 06，蒙特利尔，2006 年 4 月；在 http://eusesconsortium.org/gender/

[203] JB B´edrune G Campana，“大家冷静点，这是抢劫！”，Black Hat 2019；在 https://donjon.ledger.com/BlackHat2019-presentation/

[204] I Beer，“深入了解在野外发现的 iOS 漏洞利用链”，谷歌零项目博客，2019 年 8 月 29 日，网址为 https://googleprojectzero.blogspot。 com/2019/08/a-very-deep-dive-into-ios-exploit.html

[205] S Begley，“指纹匹配因可能存在错误而受到更多攻击”，《华尔街日报》，2005 年 10 月 7 日，第 B1 页；在 http://online.wsj.com/article_print/SB112864132376462238.html

[206] HA Beker，C Amery，“加密政策”，网址为 http://www.baltimore。 com/library/whitepapers/mn_cryptography.html

[207] HJ Beker、JMK Friend、PW Halliden，“简化电子资金转账销售点系统中的密钥管理”，载于 Electronics Letters v 19 (1983) pp 442–443

[208] H Beker，F Piper，“密码系统”，诺斯伍德（1982）

[209] H Beker，M Walker，“零售环境中安全电子资金转移的密钥管理”，密码学进展 – Crypto 84 Springer
LNCS v 196 第 401–410 页

[210] DE Bell, L LaPadula, 安全计算机系统 , ESD-TR-73-278, Mitre
公司; v I 和 II:1973 年 11 月,v III:1974 年 4 月

[211] M Bellare、J Kilian、P Rogaway,密码学进展中的“密码块链的安全性” Crypto 94 Springer LNCS v
839,第 341-358 页

[212] M Bellare,P Rogaway，“最佳非对称加密”,在进展中
密码学 – Eurocrypt 94,Springer LNCS v 950 第 103-113 页;另见 RFC 2437

[213] SM Bellovin，“在互联网上找到的数据包”,在计算机通信中
Review v 23 no 3（1993 年 7 月)第 26-31 页

[214] SM Bellovin，“防御序列号攻击”,RFC 1948
（1996 年 5 月）

[215] SM Bellovin，“IP 安全协议的问题领域”,第六届 Usenix Unix 安全研讨会论文集（1996 年）;在
http://www.cs。 columbia.edu/~smb/papers/badesp.pdf

[216] SM Bellovin，“加拿大的借记卡欺诈”,comp.risks v 20.69;在 http:
//catless.ncl.ac.uk/Risks/20.69.html

[217] SM Bellovin，“许可行动链接”,网址为 http://www.research.att。
com/~smb/nsam-160/

[218] SM Bellovin，“ICMP 追溯消息”,2000 年 3 月,draft-bellovin- 互联网草案,http://
itrace-00.txt search.ietf.org/internet-drafts/

[219] SM Bellovin，“Comcast 阻止点对点 Trac 的更多信息”,2007 年 10 月 22 日,http://
www.cs.columbia.edu/~smb/blog/2007-10/2007-10-22 .网页;和“康卡斯特显然阻止了一些点对
点流量”,2007 年 10 月 19 日,同上。

[220] S Bellovin、M Blaze、E Brickell、C Brooks、V Cerf、W Die、S Landau、J Peterson、J Treichler，“将通信
援助执法法应用于 IP 语音的安全影响”http： //www.itaa.org/news/docs/CALEAVOIPreport.pdf

[221] SM Bellovin,WR Cheswick,A Rubin，“防火墙和互联网安全，
第二版:击退狡猾的黑客,Addison-Wesley (2003)

[222] SM Bellovin,M Merritt，“加密密钥交换:基于密码的协议可防止字典攻击”,IEEE 安全与隐私研讨会论
文集（1992 年)第 72-84 页

[223] J Benaloh，“ElectionGuard 初步规范 v0.85”,Microsoft Re
搜索,2020

[224] M Benantar、R Guski、KM Triodle，“访问控制系统:从以主机为中心到以网络为中心的计算”,IBM
Systems Journal v 35 no 1 (96) pp 94–112

[225] W Bender、D Gruhl、N Morimoto、A Lu，“数据隐藏技术”,载于
IBM Systems Journal v 35 第 3–4 (96) 页 313–336

[226] T Benkart、D Bitzer，“BFE 适用于 LAN 环境”,第十七届全国计算机安全会议（1994 年）； NIST 出
版的论文集,第 227–236 页

[227] Y Benkler，“网络宣传 操纵、虚假信息和
美国政治牛津的激进化 (2018)

[228] Y Berger、A Wool、A Yeredor，“使用键盘声学发射的字典攻击”，ACM CCS 2006

[229] R Bergman，DM Halbfinger，“以色列对伊朗港口的黑客攻击是伊朗的最新齐射
网络攻击交流”，纽约时报，2020 年 5 月 19 日

[230] M Bernhard、J Benaloh、JA Halderman、RL Rivest、PYA Ryan、PB Stark、V Teague、PL Vora、
DS Wallach，“无记名投票的公开证据”，arXiv:1707.08619，2017 年 8 月 4 日

[231] J Bennetto，“爱尔兰共和军如何密谋转移伦敦”，《独立报》，4 月
12 1997

[232] DJ Bernstein，“对 AES 的缓存定时攻击”，预印本，2005 年

[233] I Berres 2018，“Was Patienten jetzt wissen mussen”，¨ 明镜周刊 11 月 26 日
2018

[234] J Bessen，“产业集中度与信息技术”，SSRN 3044730，2019

[235] A Bessey、K Block、B Chelf、A Chou、B Fulton、S Hallem、C Henri-Gros、
A Kamsky、S McPeak、D Engler，“数十亿行代码之后：使用静态分析来查找现实世界中的错误”，
在 Communications of the
ACM v 53 第 2 期，2010 年 2 月

[236] B Beyer、C Jones、J Peto 、NR Murphy，“站点可靠性工程”，
谷歌图书 (2013)

[237] K Biba，“安全计算机系统的完整性考虑”，Mitre Corporation MTR-3153 (1975)

[238] S Biddle，“NSA 泄密是真实的，斯诺登文件证实”拦截，2016 年 8 月 19 日

[239] AD Biderman，H Zimmer，“人类行为的操纵”，Wiley 1961；在 http://www.archive.org/
details/ TheManipulationOfHumanBehavior

[240] J Bidzos，“詹姆斯·比佐斯的口述历史访谈”，查尔斯·巴贝奇
研究所 2004 年 12 月 11 日

[241] B Biggio，F Rolli，“野生模式：对抗性机器学习兴起十年后”，arXiv:1712.03141，2018 年 7 月 19
日

[242] E Biham，A Biryukov，A Shamir，“Skipjack 的密码分析减少到
31 轮使用不可能的差异”在密码学进展中 – Eurocrypt 97，Springer LNCS v 1592 第 12-23 页

[243] E Biham、O Dunkelman、S Indesteege、N Keller、B Preneel，“如何偷车 对 KeeLoq 的实际攻
击”，2007 年，http://www.cosic.esat。 kuleuven.be/keeloq/

[244] E Biham，L Neumann，“打破蓝牙配对：固定坐标
无效曲线攻击”，SAC 2019 第 250-273 页

[245] E Biham,A Shamir，“数据加密的差分密码分析”
标准”,施普林格 (1993)

[246] E Biham,A Shamir，“秘密密钥密码系统的差分故障分析”,密码学进展 – Crypto 97 Springer
LNCS v 1294 pp 513-525

[247] C Bing,J Schectman，“特别报道:阿联酋秘密黑客团队的美国雇佣兵”,路透社,2019 年 1 月
30 日

[248] A Biryukov、A Shamir、D Wagner，“A5/1 的实时密码分析
PC”,快速软件加密 (2000)

[249] R Bishop,R Bloomfield，“长期可靠性的保守理论
增长预测”,IEEE Transactions on Reliability v 45 no 4 (Dec 96) pp 550–560)

[250] DM Bishop，“将 COMPUSEC 应用于战场”,第 17 届年度
全国计算机安全会议 (1994) 第 318–326 页

[251] M Bishop,M Dilger，“检查文件访问中的竞争条件”,载于
计算系统 Usenix v 9 no 2（1996 年春季)第 131–152 页

[252] Wolfgang Bitzer, Joachim Opfer Schaltungsanordnung zum Messen der
Korrelationsfunktion zwischen zwei vorgegebenen Signalen [用于测量两个提供信号
之间的相关函数的电路布置]。
德国专利 DE 3911155 C2,Deutsches Patentamt,1993 年 11 月 11 日

[253] J Blackledge，“从分形和混沌中赚钱:微柱”,载于
今日数学 v 35 no 6（99 年 12 月)第 170-173 页

[254] RD Blackledge，“DNA 与指纹”,《法医学杂志》第 40 卷（1995 年)第 534 页

[255] B Blair，“让总统处于核黑暗中”,布鲁斯·布莱尔的核专栏,2004 年 2 月 11 日,网址为 https://
web.archive.org/web/20120511191600/ http://www.cdi.org/布莱尔/permissive-action-
links.cfm

[256] GR Blakley，“保护加密密钥”,在 NCC 会议记录中
AFIPS (1979),第 313–317 页

[257] B Blakley、R Blakley、RM Soley，“CORBA 安全性:介绍
使用对象的 Addison-Wesley 进行安全计算 (1999)

[258] MA Blaze，“托管加密标准中的协议失败”,载于
第二届 ACM 计算机和通信安全会议第 59-67 页

[259] Matt Blaze，“密码学和物理安全:权利扩大在
Master-Keyed Mechanical Locks”,IEEE 安全与隐私研讨会 2003

[260] MA Blaze，“对安全协议的更广泛的看法”,在安全
2004 年协议,Springer LNCS v 3957,第 106–132 页

[261] MA Blaze，“计算机科学家的安全破解”,宾夕法尼亚大学技术报告（2004 年）,网址为 http://
www.crypto.com/papers/

[262] MA Blaze,SM Bellovin，“窃听,窃听我的网络之门”,在
ACM 通讯（2000 年 10 月）,内部风险 124;在

[263] MA Blaze、J Feigenbaum、J Lacy，“去中心化信托管理”，载于
1996 年 IEEE 安全与隐私研讨会论文集第 164-173 页

[264] D Bleichenbacher，“针对基于 RSA 加密标准 PKCS #1 的协议的选择密文攻击”，密码学进展 –
Crypto 98 Springer LNCS v 1462 第 1-12 页

[265] G Bleumer，“电子邮资系统 技术、安全、生态
经济学，施普林格 2006

[266] B Blobel，“肿瘤学临床记录系统。德国东部癌症登记的经验和发展”，[63]，第 39-56 页

[267] JA Bloom、IJ Cox、T Kalker、JPMG Linnartz、ML Miller、CBS Traw，
“DVD 视频的复制保护”，在 IEEE 会议记录 v 87 no 7
（1999 年 7 月）第 1267–1276 页

[268] P Bloom，“笛卡尔”婴儿：儿童发展如何解释
我们人类 ，绿箭侠 (2005)

[269] S Blythe、B Fraboni、S Lall、H Ahmed、U de Riu，“复杂硅芯片的布局重构”，IEEE 固态电路杂志 v 28 no
2（93 年 2 月）第 138–145 页

[270] WE Boebert，“关于 NSA Linux 发布之际的一些想法”，Linux Journal，2001 年 1 月 24 日；在 http://www.linuxjournal.com/article/4963

[271] WE Boebert，RY Kain，“分层完整性的实用替代方案
策略”，第 8 届全国计算机安全会议 NIST (1985) p 18

[272] BW Boehm，“软件工程经济学”，Prentice Hall（1981 年）

[273] A Bogdanov、D Khovratovich、C Rechberger，“完整 AES 的 Biclique 密码分析”，
Asiacrypt 2011 和 IACR 预印本编号。 2011-449

[274] RB¨ohme、N Christin、B Edelman、T Moore，“比特币：经济学、技术和治理”，《经济展望杂志》第 29 期第 2 期（2015 年春季）第 213-238 页

[275] RB¨ohme, G Kataria，“网络中相关性的模型和度量
保险”，在 WEIS 2006

[276] RB¨ohme, T Moore，“迭代的最薄弱环节 自适应模型
安全投资”，在 WEIS 2009

[277] N Bohm、I Brown、B Gladman，“电子商务 谁承担欺诈风险？”，信息政策研究基金会（2000 年）

[278] K Bolan，“里士满 IT 专家因帮助暴力犯罪组织被判入狱 9 年”，温哥华太阳报，2019 年 5 月 29 日

[279] M Bond，“了解安全 API”，博士论文，剑桥，2004 年

[280] M 邦德，“砰！爆头！ （在在线战术第一人称射击游戏的网络级异常上构建新战术）”（2006 年），网址为 http://www.lightbluetouchpaper.org/2006/10/02/

[281] M Bond，“Action Replay Justice”，2007 年 11 月 22 日，http://www. lightbluetouchpaper.org/2007/11/22/action-replay-justice/

[282] M Bond、O Choudary、SJ Murdoch、S Skorobogatov、RJ Anderson，“芯片和脱脂：使用预播放攻击克隆 EMV 卡”IEEE 安全和隐私研讨会（2014 年）

[283] M Bond、D Cvr ˇ cek、S Murdoch，“打开蛹”，剑桥计算机实验室技术报告编号。 592, 2004

[284] M Bond、SJ Murdoch、J Clulow，“激光打印 PIN 邮件程序漏洞报告”，2005 年，网址为 https://murdoch.is/papers/cl05pinmailer-vuln.pdf

[285] D Boneh、RA Demillo、RJ Lipton，“关于检查密码协议故障的重要性”，密码学进展 – Eurocrypt 97，施普林格 LNCS v 1233 第 37-51 页

[286] D Boneh，M Franklin，“来自 Weil 配对的基于身份的加密”，密码学进展 2001 年 CRYPTO 会议记录，Springer LNCS 2139，第 213-29 页

[287] D Boneh，V Shoup，“应用密码学研究生课程”，https：//cryptobook.us, 2017

[288] L Boney、AH Tewfik、KN Hamdy，“音频信号的数字水印”，1996 年 IEEE 国际多媒体会议论文集计算与系统，第 473–480 页

[289] J Bonneau，“猜测人类选择的秘密”，博士论文，剑桥大学计算机实验室技术报告 819（2012 年）

[290] J Bonneau，“深入探讨：EFF 的随机密码短语新词表”EFF 2016 年 7 月 19 日

[291] J Bonneau、E Bursztein、I Caron、R Jackson、M Williamson，“秘密、谎言和帐户恢复：谷歌使用个人知识问题的教训”，WWW 2015

[292] J Bonneau、C Herley、PC van Oorschot、F Stajano，“寻求替代Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes”，IEEE Security & Privacy 2012，以及作为技术报告的完整版本

[293] J Bonneau、A Miller、J Clark、A Narayanan、JA Kroll、EW Felten，“SoK：比特币和加密货币的研究前景和挑战”IEEE 安全与隐私 (2015)

[294] J Bonneau、S Preibusch，“密码丛林：网络上人工身份验证的技术和市场失败”，WEIS 2010

[295] J Bonneau、S Preibusch、R Anderson，“每十一个钱包送一份生日礼物？客户选择的银行 PIN 的安全性”，金融密码学 2012 年

[296] J Bonneau，E Shutova，“多词密码短语的语言特性”，2012 年

[297] SC Bono、M Green、A Stubblefield、A Juels、AD Rubin、M Szydlo，“安全加密启用 RFID 设备的分析”，Usenix 2005

[298] V Bontchev，“可能的宏病毒攻击及其预防方法”，载于
计算机与安全 v 15 第 7 (96) 页 595–626

[299] N Borisov、I Goldberg、D Wagner，“拦截移动通信：
802.11 的不安全性”，在 Mobicom 2001

[300] NS Borenstein，“实用网络商务的风险和陷阱”，ACM 通讯 v 39 no 6（96 月 6 日)第 36-44 页

[301] F Boudot, P Gaudry, A Guillevic, N Heninger, E Thom´e, P Zimmermann,
“RSA-250 分解”，Cado-nfs-discuss 邮件列表，2020 年 2 月 28 日

[302] E Bovenlander，智能卡安全受邀演讲，Eurocrypt 97，报道
在[107]

[303] E Bovenlander，RL van Renesse，“智能卡和生物识别：一个
概述”，载于计算机欺诈和安全公告（12 月 95 日)第 8-12 页

[304] O Bowcott，“英美监视制度‘七年’是非法的”
卫报 2015 年 2 月 6 日

[305] C Bowden、Y Akdeniz，“密码学和民主：自由的困境”，在解放网络空间：公民自由、人权和
Internet Pluto Press (1999) 第 81-125 页

[306] D Bowen，“自上而下的审查”，2007 年 8 月，http://www.sos.ca.gov/
选举/elections_vsr.htm

[307] J Bowen，“驱逐外交官向以色列发出强烈信号”，BBC
新闻，2011 年 3 月 23 日

[308] M Brader，“车门锁遥控器激活另一辆车的警报”，comp.risks 21.56（2001 年 7 月）

[309] M Brader，“如何减掉 10,000,000 磅”，comp.risks v 24 no 25，4 月
2006年19日

[310] T Bradshaw，“Uber 失去了在伦敦运营的执照”，《金融时报》
2019 年 11 月 25 日

[311] RM Brady，RJ Anderson，“麦克斯韦的磁流体模型”，arXiv
1502.05926 2015 年 2 月 20 日

[312] RM Brady、RJ Anderson、RC Ball，“墨菲定律、进化物种的适应性和软件可靠性的限制”，剑桥大学计算机
实验室技术报告 no. 471 (1999)

[313] R Brandom，“你的手机最大的漏洞是你的指纹”，The
边缘 2016 年 5 月 2 日

[314] S Brands，“重新思考公钥基础设施和数字证书 –
建立隐私”，麻省理工学院出版社（2000 年）

[315] JT Brassil、S Low、NF Maxemchuk，“文本文档电子分发的版权保护”，载于 IEEE 会议记录 v 87 no 7
（1999 年 7 月)第 1181-1196 页

[316] 布雷， “发现 Logan 缺乏‘面部测试’”，波士顿环球报，2002 年 7 月 17 日

[317] M Brelis，“据称用于淫秽电话的患者档案”，波士顿环球报，1995 年 4 月 11 日；也在 comp.risks v 17 no 7

[318] M Brennan、S Afroz、R Greenstadt“对抗式文法：规避作者识别以保护隐私和匿名”ACM Transactions on Information System Secusity v 15 no 3（2012 年 11 月）

[319] DFC Brewer，MJ Nash，“中国墙模型”，载于 1989 年会议记录 IEEE 计算机协会安全和隐私研讨会第 215-228 页

[320] B Brewin，“CAC 使用近一半的 DOD 网络入侵，Croom 说”，fcw.com，2007 年 1 月 25 日，http://www.fcw.com/article97480-01-25-07

[321] T Brewster，“美国秘密研究中心内部：从 Facebook 收集指纹、入侵智能手表和抗击 COVID-19”，福布斯 2020 年 7 月 13 日

[322] D Brin，“透明社会：技术会迫使我们在隐私和自由之间做出选择吗？”，Perseus Press (1999) 杂志版，连线，1996 年 12 月，http://www.wired.com/wired /archive/4.12/fftransparent.html

[323] R Briol“Emanation：如何对数据保密”，信息保护电磁安全研讨会，SEPI 91，罗马，1991 年

[324] 英国标准 8220-1.2000，“建筑物防犯罪指南 第 1 部分：住宅”

[325] WJ Broad、J Marko 、DE Sanger，“以色列对蠕虫病毒的测试在伊朗核延迟”，纽约时报，2011 年 1 月 15 日

[326] J Brodkin，“在‘自愿’计划没有通过之后，FCC 需要反自动呼叫技术锻炼”，Ars Technica 2020 年 4 月 1 日

[327] M Broersma，“打印机制造商抨击再填充限制”，ZDnet，2002 年 12 月 20 日，http://news.zdnet.co.uk/story/0,,t269-s2127877,00.html

[328] F Brooks，“人月神话：软件工程论文集”，Addison-Wesley（1995 周年纪念版）

[329] I Brown、CT Marsden、J Lee、M Veale，“选举网络安全 一个英联邦最佳实践指南”，英联邦秘书处，2020 年

[330] D Brumley，D Boneh，“远程定时攻击是实用的”，在计算机中 Networks v 48 no 5（2005 年 8 月）第 701–716 页

[331] D Brown，“RSA-OAEP 在标准模型中无法证明的安全性”，IACR 电子版第 2006/223 号，网址为 http://eprint.iacr.org/2006/223

[332] JDR Buchanan、RP Cowburn、AV Jausovec、D Petit、P Seem、XO Gang、D Atkinson、K Fenton、DA Allwood、MT Bryan，“文档和包装指纹识别”，载于 Nature v 436 no 28（2005 年 7 月）第 475 页

[333] JM Buchanan，“经济政策的构成”，1986 年诺贝尔奖演讲，http://nobelprize.org/nobel_prizes/economics/laureates/1986/buchanan-lecture.html

[334] RT Buchanan，“雄鹿党成员声称他是 ^aA Ygrossly exploited^a
A Z´ 由膝上舞俱乐部 Spearmint Rhino 在一个晚上花光了三分之一的薪水之后”，《独立报》，2014 年 11 月 11 日

[335] H Buehler，瑞士国际广播电台采访，1994 年 4 月 7 日。在 http://www.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/rpub.cl.msu.edu/crypt/docs/hans-buehler-crypto-spy.txt

[336] http://archives.neohapsis.com/archives/bugtraq/

[337] R Buhren、C Werling、JP Seifert，“在证明更新之前不安全：分析 AMD SEV 的远程证明”，CCS 2019

[338] J Van Bulck，M Minkin，O Weisse，D Genkin，B Kasikci，F Piessens，M Silberstein、TF Wenisch、Y Yarom、R Strackx，“预示：提取具有瞬时乱序执行的英特尔 SGX 王国的钥匙”，Usenix 安全 2018

[339] J Van Bulck，D Moghimi，M Schwarz，M Lipp，M Minkin，D Genkin，Y Yarom、B Sunar、D Gruss、F Piessens，“Lvi：通过微架构负载值注入劫持瞬态执行”，IEEE 研讨会
安全和隐私 2020

[340] Bull、Dassault、Diebold、NCR、Siemens Nixdorf 和 Wang Global，“保护概况：自动提款机/柜员机”，1.0 版（1999 年），网址为 http://www.commoncriteriaportal.org/

[341] DB Bulloch，“追踪恐怖主义资金：SWIFT 计划和美国反恐金融制度”，阿姆斯特丹法律论坛 v 3 (2011), SSRN 1964531

[342] Bundesamt fur Sicherheit in der Informationstechnik（德国信息安全局），Schutzmaßnahmen gegen Lauschangri e [Protection against bug]，Faltbl¨atter des BSI v 5，波恩，1997 年； http://www.bsi. bund.de/literat/faltbl/laus005.htm

[343] Bundesamt fur Sicherheit in der Informationstechnik（德国信息 Security Agency），Elektromagnetische Schirmung von Geb¨auden, 2007, BSI TR-03209

[344] Bundesverfassungsgericht，“Beschluss des Ersten Senats”，2006 年 4 月 4 日，1 BvR 518/02 Absatz-Nr。(1–184)，位于 http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html

[345] J Bunnell、J Podd、R Henderson、R Napier、J Kennedy-Mo att，“认知、联想和传统密码：召回率和猜测率”，载于 Computers and Security v 16 no 7 (1997) 第 645-657 页

[346] M Burgess，“朝鲜的精英黑客正在用加密技术资助核武器突袭”，《连线》杂志，2019 年 4 月 3 日

[347] J Burke, P Warren，“手机如何让间谍看到我们的一举一动”，《观察家报》2002 年 10 月 13 日；在 http://observer.guardian.co.uk/uk_news/story/0,6903,811027,00.html

[348] N Burow、SA Carr、J Nash、P Larsen、M Franz、S Brunthaler、M Payer，“控制流完整性：精度、安全性和性能”，ACM 计算调查，2017 年

[349] T Burt，“破坏世界上最大的在线犯罪网络的新行动”，
微软在这些问题上,2020 年 3 月 10 日

[350] G Burton，“IT 安全专家需要以完全不同的方式看待建筑物中的物联网安全,Cundall 主管 Chris Grundy 说，”计算
2019 年 7 月 12 日

[351] G Burton，“今年到目前为止,已有 600 多个美国政府实体遭到勒索软件攻击 而且只会变得更糟”，
Computing,2019 年 10 月 1 日

[352] G Burton，“谷歌从 Chrome 网络中删除了 Avast 和 AVG 扩展程序
存储“不必要的”数据收集”,Computing,2019 年 12 月 18 日

[353] J Busch2020，“如何破解 GE 冰箱的 RWPFE 滤水器”，
Groovypost 2020 年 5 月 7 日

[354] L Butler，“Post Oce 老板因邮政局长减薪而获得 7% 的加薪”，
卫报 2018 年 10 月 19 日

[355] RW Butler,GB Finelli，“生命关键软件可靠性实验量化的不可行性”,ACM 关键系统软件研讨会 (1991) 第 66-76 页

[356] Buro Jansen & Janssen，“制定规则:拦截与隐私”,2000 年 8 月 8 日,http://www.statewatch.org/news/2002/nov/11jj.htm

[357] M Burrows、M Abadi、RM Needham，“认证的逻辑”,载于伦敦皇家学会会刊 A v 426（1989)第 233-271 页;作为 DEC SRC 研究报告 39 发布的早期版本

[358] G Burton“Equifax 使用默认的‘admin’用户名和密码来保护
hacked portal”,计算 2019 年 10 月 21 日

[359] D Byler，“北方‘再教育’技术的全球影响
中国西部”,全球政策中心 2020 年 6 月 8 日

[360] RW Byrne, A Whiten，“马基雅维利智能 猴子、类人猿和人类的社会专长和智力进化”,牛津,1988 年;另见 A Whiten,RW Byrne，“马基雅维利智能 II – 扩展和评估”,剑桥 1997 年

[361] 内阁办公室，“国家民事紧急情况风险登记册”2017 年版

[362] “4G 和 5G 认证的比较介绍”,有线电视实验室，
2019 年冬季

[363] C Cadwalladr，“Facebook 在英国脱欧中的作用 以及对民主的威胁”，
TED2019

[364] E Caesar，“成为暗网 Em 之家的冷战地堡
pire”,纽约客,2020 年 7 月 27 日

[365] L Cai,H Chen，“关于基于运动的击键推理攻击的实用性”,第五届国际可信和可信计算会议论文集，
TRUST 12 ppp 273-290

[366] A Cain，“在信封之前,人们通过字母锁定保护信息”,Atlas Obscura,2018 年 11 月 9 日,网址为 https://www.atlasobscura.com/articles/what-did-people-do-before-envelopes-letterlocking

[367] F Caldicott，“患者身份信息审查报告”，卫生部，1997 年

[368] RE Calem，“纽约的 Panix 服务因黑客攻击而瘫痪”新
纽约时报 1996 年 9 月 14 日

[369] A Caliskan、JJ Bryson、A Narayanan，“自动从语言语料库派生的语义包含类似人类的偏见”，
Science v 356 no 6334 pp 183–186

[370] A Caliskan-Islam，R Harang，A Liu，A Narayanan，C Voss，F Yamaguchi，R
Greenstadt，“通过代码风格对程序员进行去匿名化”，USENIX
安全性 (2015) 第 255-270 页

[371] J Camp，C Wolfram，“定价安全”，CERT 信息生存能力研讨会论文集（2000 年 10 月 24-26
日）第 31-39 页

[372] J Camp，S Lewis，“信息安全经济学”，Springer 2004

[373] D Campbell，“有人在倾听”，载于《新政治家》（1988 年 8 月 12 日）第 1 页，第 10-12 页；在
http://jya.com/echelon-dc.htm

[374] D Campbell，“创造历史：1988 年第一份 Ech elon 报告的原始来源向前迈进”（2000 年 2 月
25 日），http://cryptome.org/
梯队-mndc.htm

[375] D Campbell，“Operation Ore Exposed”，PC Pro，2005 年 7 月，存档于 https://
www.duncancampbell.org/content/operation-ore

[376] D Campbell，“性、谎言和丢失的录像带”，PC Pro，2007 年 4 月，存档于 https://
www.duncancampbell.org/content/operation-ore

[377] D Campbell、P Lashmar，“新冷战：美国如何为其最老朋友 美元监视我们”，载于《独立报》
（2000 年 7 月 2 日）

[378] K Campbell、L Gordon、M Loeb、L Zhou，“公开宣布的信息安全漏洞的经济成本：来自股票市场
的经验证据”，《计算机安全杂志》第 11 卷第 3 期（2003 年）第 431-448 页

[379] O Campion-Awwad、A Hayton、L Smith、M Vuaran，“NHS 中的 IT 国家计划”，剑桥，2014 年，
https://www.lightbluetouchpaper.org/2014/08/13/largest-ever -公民政府-灾难/
在

[380] C 卡内拉、J 范布克、M 施瓦茨、M 利普、B 冯伯格、P 奥特纳、F
Piessens、D Evtyushkin、D Gruss，“瞬态系统评估
执行攻击和防御”，USENIX 安全研讨会 2019

[381] C Canella、M Schwarz、M Haubenwallner、M Schwarzl、D Gruss，“KASLR：
打破它，修复它，重复”，ACM CCS (2020)

[382] C Cant、S Wiseman，“简单可靠的堡垒主机”，第 13 届年度计算机安全应用会议（1997 年）第
24-33 页

[383]“指纹身份证领跑黑马”，卡世界独立（5月
94）第 2 页

[384] “German A555 takes its toll”, in Card World International (12/94–1/95) p
6个

[385] BL Cardin，“普京对俄罗斯和欧洲民主的不对称攻击 对美国国家安全的影响”少数派报告,美国参议院外交关系委员会,2018 年 1 月 10 日

[386] Cards International 第 117 期（9 月 29 日)中的“高科技有助于减少信用卡欺诈”94)

[387] “Visa 加强其反欺诈技术”,Cards International no 189 (12/12/97) p 5

[388] JM Carlin，“UNIX 安全更新”,Usenix Security 93,第 119-130 页

[389] M Carr,SF Shahandashti，“重新审视商业密码管理器中的安全漏洞”,arXiv 2003.01985 2020 年 3 月 17 日

[390] J Carroll， Big Blues: The Unmaking of IBM ,Crown Publishers（1993）

[391] H Carter，“汽车钟表修理工被判入狱九个月”,《卫报》2 月 15 日 2000

[392] R Carter，“What You Are ... Not What You Have”,国际安全评论访问控制特刊（93/94 冬季）第 14-16 页

[393] 案例,M Meltzer,S Adair，“数字镇压:大规模监控和对维吾尔人的剥削”,Volexity 2019 年 9 月 2 日

[394] M Castro,B Liskov，“实用拜占庭容错”,关于操作系统设计与实现 (1999)

[395] L Cauley，“NSA 拥有庞大的美国人电话数据库”,《今日美国》,2005 年 11 月 11 日,http://www.usatoday.com/news/washington/ 2006-05-10-nsa_x.htm

[396] E Cebuc，“我们在 2020 年如何处理 Android 的覆盖攻击？” F 安全实验室 2020 年 3 月 27 日

[397] M Ceglowski，“我在尝试保护国会竞选活动中学到的东西”,Idlewords,2019 年 5 月 26 日,网址为 https://idlewords.com/2019/05/what_i_learned_trying_to_secure_congressional_campaigns.htm

[398] 民主与技术中心,http://www.cdt.org/

[399] L Cerulus，“欧盟委员会 to sta :切换到 Signal 消息传递应用程序”，Politico Pro 2020 年 2 月 20 日

[400] Chainalysis“加密货币犯罪报告”,2019 年 1 月

[401] Chainalysis“2020 年加密货币犯罪状况”,2020 年 1 月

[402] “政府电子监控活动的性质和范围”，民主与技术中心,2006 年 7 月

[403] D Cerdeira、N Santos、P Fonseca、S Pinto，“SoK:了解 TrustZone 辅助 TEE 系统中普遍存在的安全漏洞”,IEEE 2020 年安全与隐私研讨会

[404] P Chain,F Filloux，“车轮上的代码:重塑汽车,第 5 集”周一笔记,2020 年 8 月 9 日

[405] Chakraborty，“Boots 如何流氓”,卫报 2016 年 4 月 13 日

[406] Chaos Computer Club，“如何伪造指纹？”，https：
//web.archive.org/web/20090327044558/http://www.ccc.de/biometrie/
fingerabdruck_kopieren.xml?language=en (2004)

[407] L Chapman，“你不听话的仆人”，Penguin Books（1979）

[408] 英国特许屋宇装备工程师学会，“安全工程”，
应用手册 AM4 (1991)

[409] M Chase、T Perrin、G Zaverucha，“信号专用组系统和
支持高效可验证加密的匿名凭证”，Cryp tology ePrint 2019/1416 2019 年 12 月 10 日

[410] D Chaum，“无法追踪的电子邮件、回信地址和数字假名”，ACM 通讯 v 24 no 2（1981 年 2 月）

[411] D Chaum，“无法追踪支付的盲签名”，在 Crypto 82 中，
全会出版社 (1983) pp 199–203

[412] D Chaum，A Fiat，M Naor，“无法追踪的电子现金”，在 CRYPTO
88，施普林格 LNCS v 403 第 319–327 页

[413] S Checkoway，J Maskiewicz，C Garman，J Fried，S Cohney，M Green，N
Heninger、RP Weinmann、E Rescorla、H Shacham，“瞻博网络双 EC 事件的系统分析”CCS
2016

[414] A Chen，“将鸡巴照片和斩首从你的
Facebook Feed”，连线，2014 年 10 月 23 日

[415] YS Cheng，XY Ji，TY Lu，WY Xu，“DeWiCam：检测隐藏的无线
通过智能手机拍摄的相机” AsiaCCS 2018

[416] R Chesney，“电话元数据：联系人链接程序是联合国
有救吗？” Lawfare 博客 2019 年 3 月 6 日

[417] K Chiu，“世界上最大的网民待在家里，中国的互联网无法应对”，Abacus News 2020 年 2 月 17 日

[418] “‘互联网审判’聚焦韩国网络暴徒”朝鲜日报
2005 年 7 月 8 日

[419] MO Choudary，MG Kuhn，“高效、便携的模板攻击”，IEEE
信息取证与安全交易 v 13 no 2（2018 年 2 月）

[420] T Christakis，“欧盟/欧洲人权法院关于大规模监控的法律的碎片化：对老大哥观察判决的初步思考”，欧洲法律博客
2018 年 9 月 20 日

[421] N Christin，“丝绸之路之旅：大型匿名在线市场的测量分析”，WWW 2013

[422] KH Chuang、E Bury、R Degraeve、B Kaczer、G Groeseneken、I Ver bauwhede、D Linten，“使
用 CMOS 分解位置的物理不可克隆函数”，IEEE 国际可靠性物理研讨会 (IRPS)（2017 年）

[423] F Church（主席），“情报活动 参议院第 21 号决议”，美国参议院，第 94 届国会，第一届会议，
http://cryptome.org/nsa-4th.htm

[424] RB Cialdini，“影响力 科学与实践”，Pearson 2009

[425] WS Ciciora，“机顶盒内部”，IEEE Spectrum v 12 no 4（95 年 4 月）
第 70-75 页

[426] C Cimpanu，“较新的 Diameter 电话协议同样易受攻击
SS7”，哔哔电脑 2018 年 7 月 2 日

[427] C Cimpanu，“在 Ruby 库中发现用于检查强密码的后门”，ZDNet 2019 年 7 月 8 日

[428] C Cimpanu，“专家说，DNS-over-HTTPS 导致的问题多于它解决的问题”，ZDNet，2019
年 10 月 6 日

[429] C Cimpanu，“欧盟 eIDAS 身份验证系统中修补的主要漏洞”，ZDNet 2019 年 10 月 29 日

[430] C Cimpanu，“由于压力大和职业倦怠，CISO 的平均任期仅为 26 个月”，ZDNet，2020 年
2 月 12 日

[431] C Cimpanu，“Android 恶意软件可以窃取 Google Authenticator 2FA 代码”，
ZDNet 2020 年 2 月 27 日

[432] C Cimpanu，“Microsoft 双密钥加密进入公共预览版”，ZD
净 2020 年 7 月 21 日

[433] C Cimpanu，“中国现在阻止所有使用加密的 HTTPS trac
TLS 1.3 和 ESNI”，ZDNet 2020 年 8 月 8 日

[434] J Cipriani，“iOS 13：iPhone 的 5 大新安全和隐私功能”，CNet，2019 年 9 月 22 日

[435] D Cire?san、U Meier、J Schmidhuber，“用于图像分类的多列深度神经网络”，arXiv：
1202.2745，2012 年 2 月 13 日

[436] D Clark，D Wilson，“商用和军用计算机的比较
安全策略”，载于 1987 年 IEEE 安全与隐私研讨会论文集，第 184-194 页

[437] P Clark、H Warrell、T Bradshaw、S Neville “汉考克本土追踪应用程序的兴衰”，《金融
时报》，2020 年 6 月 26 日

[438] R Clark，“打破紫色的人”，Little, Brown (1977)

[439] I Clarke，“免费网络项目主页”，网址为 http://freenet。 sourceforge.net/

[440] RW Clarke，“通过环境设计预防犯罪的理论”；另见“情境犯罪预防：成功案例研究”，
Har row 和 Heston (1997)

[441] R Clayton，“技术风险”，剑桥国际经济犯罪研讨会（2003 年），http://www.cl.cam.ac.uk/
~rnc1/talks/030910-TechnoRisk.pdf

[442] R Clayton，“网络空间中的匿名性和可追溯性”，博士论文，2005 年；
剑桥大学技术报告 UCAM-CL-TR-653

[443] R Clayton，“不安全的实词认证协议（或为什么网络钓鱼如此有利可图）”，剑桥安全协
议研讨会 2005

[444] R Clayton，私人谈话，2006 年

[445] R Clayton，“当固件攻击时！ （D-Link 的 DDoS）”，Light Blue Touch paper，2006 年 4 月 7 日

[446] R Clayton，“ClimateGate 电子邮件‘黑客’”，2009 年，网址为 https://www.cl.cam。ac.uk/~rnc1/climategate-20091215.pdf

[447] R Clayton，M Bond，“使用低成本 FPGA 设计破解的经验”DES 密钥”，CHES 研讨会 (2002)，Springer LNCS 2523，第 579-592 页

[448] R Clayton、SJ Murdoch、R Watson，“忽略中国的防火墙”，第 6 届隐私增强技术研讨会（2006 年）

[449] J Clulow，“安全加密 API 的设计和分析”Devices ，MSc Thesis, 纳塔尔大学 2003

[450] FB Cohen，“计算机病毒短期课程”，Wiley（1994 年）

[451] K Cohn-Gordon、C Cremers、L Garratt，“妥协后安全” IACR 预印本，v 1.4 2019 年 10 月

[452] B Collier，“构建的力量：在 Tor 项目中探索隐私、技术和权力的社会世界”，信息、通信和社会，(2020)，网址为 https://www.cl.cam.ac .uk/~bjc63/power_to_structure.pdf

[453] B Collier、R Clayton、A Hutchings、D Thomas，“网络犯罪（通常）很无聊：维护网络犯罪经济体的基础设施”，信息安全经济学研讨会（2020 年）

[454] B Collier、D Thomas、R Clayton、A Hutchings，“引导引导者：衡量执法干预对 DoS 市场的影响”，2019 年互联网衡量会议

[455] A Collins，“法院裁定软件时间锁定是非法的”，载于《计算机》每周（93 年 8 月 19 日）第 1 页

[456] D Cohen，J Hashkes，“控制广播传输访问的系统任务”，欧洲专利号 EP0428252

[457] D Coldewey，“优步在致命事故中检测到行人但紧急制动被禁用”，TechCrunch 2018 年 5 月 24 日

[458] B Collier，“构建的力量：在 Tor 项目中探索技术、隐私和权力的社会世界”，信息、通信和社会 (2020)，https://www.cl.cam.ac。英国/~bjc63/power_to_structure.pdf

[459] P Collier, A Hoe er，“内战中的贪婪与不满”，牛津经济学院经济论文 v 56 (2004) pp 563–595

[460] “蜂窝市场中的电信欺诈：有多少是炒作，有多少是真实的？”，载于计算机欺诈和安全公告（97 年 6 月）第 11-14 页

[461] Treadway 委员会发起组织委员会 (CSOTC)，“内部控制 综合框架”（COSO 报告，1992 年）；来自 http://www.coso.org/

[462] 共同标准，“协作保护配置文件 - 的好处演进的通用标准实施”，2014 年 9 月

[463] “传达英国的未来”,http://www.fipr.org/polarch/
劳动.html

[464] A Compagno、M Conti、D Lain、G Tsudik，“不要使用 Skype 和打字！ IP 语音中的声学窃听”，
arXiv:1609.09359 (2016);后来 ASIA CCS 2017 第 703–715 页

[465] 计算机应急响应小组协调中心,网址为 http://www.cert.org/

[466] “三星针对 Galaxy S10 指纹安全漏洞推出修复方案”,Comput
ing 新闻 2019 年 10 月 24 日

[467] JB Condat，“法国 PBX 系统的收费欺诈”,载于《计算机法》和
安全报告 v 10 no 2（94 年 3 月/4 月)第 89-91 页

[468] D Conner，“加密技术 保护您的无线设计”,载于
EDN (18/1/96) 第 57–68 页

[469] K Connolly，“价值‘高达十亿欧元’的宝藏从德累斯顿被盗
博物馆”,卫报,2019 年 11 月 25 日

[470] E Constable，“美国运通降低在线欺诈风险”

[471] L Constantin，“DigiNotar 违规一年后,Fox-IT 详细说明了
妥协”,PC World 2012 年 10 月 31 日

[472] 美国消费者报告，“2009 年雪佛兰 Malibu 与 1959 年 Bel Air 碰撞测试”,2009 年,网址
为 https://www.youtube.com/watch?v=fPF4fBGNK0U

[473] D Coppersmith，“数据加密标准 (DES) 及其强度”
对抗攻击”,IBM 报告 RC 18613 (81421)

[474] M Coppins，“耗资数十亿美元的虚假宣传运动重新选举
总裁”,大西洋 2020 年 2 月 10 日

[475] 欧洲委员会，“关于自动处理个人数据的个人保护公约”,欧洲条约系列第 108 号（1981 年 1 月
28 日）

[476] FJ Corbat´o，“关于构建会失败的系统”,Communications of the
ACM 第 4 卷第 9 期,(1991) 第 72-81 页

[477] R Cordery,L Pintsov，“信息安全在邮资中的历史和作用
证据和支付”,Cryptologia v XXIX no 3（2005 年 7 月)第 257-271 页

[478] S Cordier，“Bracelet ´electronique, ordonnance de protection, TGD...Ce que
contient la loi sur les violences conjugales”,《世界报》,2019 年 12 月 18 日

[479] V Costan,S Devadas，“英特尔 SGX 解释”,IACR Cryptology ePrint
2016/086 (2016)

[480] F Courbon、SP Skorobogatov、C Woods，“逆向工程 Flash EEP
使用扫描电子显微镜的 ROM 存储器”,国际智能卡研究和高级应用会议 (2016) 第 57-72 页

[481] J Cox，“数百名赏金猎人可以使用 AT&T、T-Mobile 和
多年来的 Sprint 客户位置数据”主板 2019 年 2 月 6 日

[482] G Corfield，“我帮助抓住了丝绸之路老板 Ross Ulbricht:卧底特工告诉了所有人” The Register 2019 年 1 月 29 日

[483] L Cosmides,J Tooby，“社会交换的认知适应”,在 适应思维:进化心理学和文化的产生（1992）

[484] J Cox，“犯罪分子正在利用电话网络骨干网清空 银行账户”,Vice 2019 年 1 月 31 日

[485] J Cox，“黑客正在直接闯入电信公司以采取 关于客户电话号码”,Vice 2020 年 1 月 10 日

[486] J Cox，“从 ATM 机吐出现金的恶意软件已在整个 世界”,Vice 2019 年 10 月 15 日

[487] C Cowan、C Pu、D Maier、H Hinton、J Walpole、P Bakke、S Beattie、A Grier、P Wagle、Q Zhang，“StackGuard:缓冲区溢出攻击的自动自适应检测和预防”,第 7 届 Usenix 安全会议 (1998) 第 63-77 页

[488] J Cox，“将跟踪地球上任何电话的公司”,The 每日野兽 2017 年 8 月 28 日

[489] J Cox，“数百名赏金猎人可以使用 AT&T、T-Mobile 和 Sprint 多年的客户位置数据”,Vice,2019 年 2 月 6 日

[490] LH Cox、JP Kelly、R Patil，“平衡多变量表格数据的质量和机密性”,统计数据库中的隐私 (2004) Springer LNCS v 3050 第 87-98 页

[491] J Cradden，“打印机制造商受到新欧盟法律的打击”,Electricnews.net,2002 年 12 月 19 日,http://www.electricnews.net/news.html?code=8859027

[492] L Cranor，“是时候重新考虑强制更改密码了”,Tech@FTC 博客 2016 年 3 月 2 日

[493] L Cranor,S Garfinkel，“安全可用性”,O Reilly 2005

[494] S Craver，“关于活跃战争巢穴中的公钥隐写术”,在第二届国际信息隐藏研讨会（1998 年)中，施普林格 LNCS v 1525 第 355–368 页

[495] SA Craver,M Wu,BD Liu,A Stubblefield,B Swartzlander,DS Wallach，D Dean,EW Felten，“字里行间的解读:来自 SDMI 的教训 挑战”,在 Usenix 安全研讨会上 (2000)

[496] RJ Creasy，“VM/370 分时系统的起源”,IBM Journal of Research & Development v 25 no 5（1981 年 9 月)第 483-490 页

[497] J Cr´emer、YA de Montjoye、H Schweizter，“数字时代的竞争政策”,欧盟委员会竞争总司,2019 年

[498] C Criado Perez，“隐形女性”,Chatto & Windus 2019

[499] “El Gobierno dice que le hackearon el Bolet´ n Ocial resoluciones sobre coronavirus”,EL 造假 Cronista,2020,https://www.cronista.com/informaciongral/El-Gobierno-3月15日 informo-que-le-hackearon-el -Boletin-Oficial-con falsas-resoluciones-sobre-coronavirus-20200314-0005.html

[500] H Crouch，“两家 NHS 信托与 Sensyne Health 签署协议”，Digi talHealth 2019 年 2 月 4 日

[501] Cryptome.org，Deepwater 文档，2007 年 5 月；在 http://cryptome。组织/深水/deepwater.htm

[502] C Culnane、BIP Rubinstein、V Teague，“停止开放数据总线，我们想要获得 O ”，arXiv:1908.05004 2019 年 8 月 15 日

[503] J Cumberledge，“首先不要伤害 独立报的报告药品和医疗器械评论”，英国卫生部社会关怀，2020 年 7 月

[504] W Curtis、H Krasner、N Iscoe，“软件设计的实地研究大型系统的流程”，ACM 通讯 v 31 no 11（88 年 11 月）第 1268–87 页

[505] F D Addario，“测试安全性的有效性”，安全管理2001 年 10 月在线

[506] T Dafoe，“一名黑客冒充一位受人尊敬的英国艺术品经销商诈骗了荷兰博物馆出资 310 万美元”，Artnet 新闻，2020 年 1 月 30 日

[507] J Daemen、V Rijmen，“Rijndael 的设计：AES – 高级加密标准”，Springer（2002 年）

[508] P Daian、S Goldfeder、T Kell、YQ Li、XY Zhao、I Bentov、L Breidenbach、A Juels，“Flash Boys 2.0：去中心化交易所的领先交易、交易重新排序和共识不稳定性”，arXiv：1904.05234 Apr 10 2019

[509] G Danezis，“分布式账本：它们有什么有趣之处？”显眼的喋喋不休 2018 年 9 月 27 日

[510] G Danezis，B Wittneben，“大规模监视的经济学”，第五信息安全经济学研讨会 (2006)

[511] G Danezis，RJ Anderson，“抵制审查的经济学”，载于IEEE 安全和隐私 v 3 no 1 (2005) 第 45-50 页

[512] G Danezis、C Diaz，“隐私技术调查”，2007 年，http://homes.esat.kuleuven.be/~gdanezis/anonSurvey.pdf

[513] JM Darley，B Latan´e，“紧急情况下的旁观者干预：责任的分散”，人格与社会心理学杂志 v 8 no 4 第 1 部分第 377–383 页

[514] M Darman，E le Roux，“用于军事网络的新一代地面和卫星微波通信产品”，载于电气通信（Q4 94）第 359-364 页

[515] 欧盟数据保护专员和EES 国家和瑞士，第 20 届国际数据保护会议，圣地亚哥德孔波斯特拉，1998 年 9 月 16-18 日

[516] Daubert 诉 Merrell Dow Pharmaceuticals，113 S. Ct. 2786 (1993)

[517] J Daugman，“通过测试对人进行高置信度视觉识别Statistical Independence”，在 IEEE Transactions on Pattern Analysis and机器智能 v 15 第 11 期（93 年 11 月）第 1148–1161 页

[518] J Daugman，“生物识别决策景观”，技术报告编号 TR482，剑桥大学计算机实验室。

[519] J Daugman、C Downing“寻找二重身：评估 IrisCode 冒名顶替者分布的普遍性”，IET Biometrics（2015 年）

[520] G Davidson，“苏格兰政府废除具名人士计划，John Swinney 确认”，《苏格兰人报》，2019 年 9 月 19 日

[521] DW Davies，WL Price，“计算机网络安全”Wiley（1984 年）

[522] G Davies，“从古至今的货币史”，威尔士大学出版社 (1996)

[523] W Davies，“WhatsApp 出了什么问题”，《卫报》，2020 年 7 月 2 日

[524] D Davis，“公钥密码学中的合规性缺陷”，第六届 Usenix 安全研讨会论文集（1996 年 7 月）第 171–178 页

[525] J Davis，“黑客摧毁了欧洲网络最发达的国家”，载于连线，2007 年 8 月 21 日

[526] D Deahl，“这个 10 岁的孩子能够使用 Face 解锁他妈妈的 iPhone ID”，The Verge 2017 年 11 月 14 日

[527] D Dean、EW Felten、DS Wallach，“Java 安全：从 HotJava 到 Netscape and Beyond”，载于 1996 年 IEEE 研讨会论文集安全和隐私第 190-200 页

[528] J Dean，“谷歌研究：回顾 2019 年，展望 2020 年和 Beyond”，Google AI 博客，2020 年 1 月 9 日

[529] C Deavours、D Kahn、L Kruh、G Mellen、B Winkel，“密码学 昨天，《今天和明天》，Artech House (1987)

[530] C Deavours、D Kahn、L Kruh、G Mellen、B Winkel，“Cryp 选集”tologia – History, People and Technology , Artech House (1997)

[531] C Deavours，L Kruh，“机器密码学和现代密码分析”，雅泰之家 (1985)

[532] JF de Beer，“对版权法的宪法管辖”，载于“The 公共利益：加拿大版权法的未来”，Irwin Law (2005)

[533] CC Demchak，Y Shavitt，“中国的格言 不留任何未被利用的接入点：中国电信 BGP 劫持的隐藏故事”，军事网络航空 v 3 no 1 https://scholarcommons.usf.edu/mca /vol3/iss1/ 7

[534] B Demoulin、L Kone、C Poudroux、P Degauque，“屏蔽数据传输线的电磁辐射”，[701] 第 163-173 页

[535] I Denley, S Weston-Smith，“实施访问控制以保护急性医院临床信息系统中患者信息的机密性”，《健康信息学杂志》第 4 期第 3-4 期（1998 年 12 月）第 174-178 页

[536] I Denley, S Weston-Smith，“二级医疗临床信息系统中的隐私”，载于《英国医学杂志》第 318 卷（1999 年 5 月 15 日）第 1328-1331 页

[537] DE Denning，“安全信息流的格子模型”，ACM 通讯 v 19 no 5 pp 236-248

[538] DE Denning，“密码学和数据安全”，Addison-Wesley（1982 年）

[539] DE Denning，“信息战与安全”，Addison-Wesley（1999）

[540] DE Denning，“行动主义、黑客行动主义和网络恐怖主义：互联网作为影响外交政策的工具”，InfowarCon 2000

[541] DE Denning、PJ Denning、M Schwartz，“跟踪器：对统计数据库安全的威胁”，载于 ACM Transactions on Database Systems v 4 no 1 (1979) pp 76–96

[542] DE Denning，PH MacDoran，“基于位置的身份验证：接地 Cyberspace for Better Security”，在计算机欺诈和安全公告中（96 年 2 月）第 12-16 页

[543] DE Denning, J Schlorer，“统计数据库的推理控制”，载于 IEEE Computer v 16 no 7（1983 年 7 月）第 69-82 页

[544] 国防部，“国防部可信计算机系统评估标准”，DoD 5200.28-STD，1985 年 12 月

[545] 国防部，“理解可信系统的隐蔽通道分析指南”，NCSC-TG-030（1993 年 11 月）

[546] 国防部，“密码管理指南”，CSC-STD-002-85 (1985)

[547] 国防部，“理解数据残留的指南”自动化信息系统，NCSC-TG-025 (1991)

[548] 国防部，“CSC-STD-003-85 背后的技术原理：计算机安全要求”，CSC-STD-004-85 (1985)

[549] 国防部，新闻抄本，2007 年 10 月 20 日，http://cryptome.org/af-squirm/af-squirm.htm

[550] 司法部，“搜查和扣押计算机指南”，1994 年；在 http://www.epic.org/security/computer_search_guidelines。文本

[551] 司法部，“韩国国民和其他数百人在全球范围内关闭由比特币资助的最大的暗网儿童色情网站”，2019 年 10 月 16 日

[552] 司法部，“中国军人因侵入信贷而被控计算机欺诈、经济间谍和电汇欺诈报告机构 Equifax”，2020 年 2 月 10 日

[553] 司法部，“俄亥俄州居民被控经营暗网基于比特币的“混合器”，洗钱超过 3 亿美元”，2020 年 2 月 13 日

[554] Y Desmedt、Y Frankel，“阈值密码系统”，密码学进展 密码学报 89，Springer LNCS v 435，第 307-315 页

[555] B De Sutter、C Collberg、M Dalla Preda、B Wyseur，“软件保护决策支持和评估方法”，来自 Dagstuhl 的报告研讨会19331（2019）

[556] W Die,ME Hellman，“密码学新方向”,IEEE Trans actions on information theory v 22 no 6（11 月 76 日)第 644-654 页

[557] W Die,ME Hellman，“NBS 数据加密标准的详尽密码分析”,Computer v 10 no 6（6 月 77 日)第 74-84 页

[558] W Die、S Landau，“在线隐私 窃听和加密的政治”,麻省理工学院出版社（1998 年）

[559] M van Dijk、A Juels、A Oprea、RL Rivest，“FLIPIT：‘秘密接管’的游戏”,《密码学杂志》第 26 期第 4 期（2013 年 10 月)第 655-713 页;作为 Ron Rivest 的 Crypto 2011 杰出演讲

[560] E Dijkstra，“并发编程控制中的一个问题的解决方案”,载于 ACM 通讯 v 8 no 9 (1965) p 569

[561] R Dingledine，“Tor 安全咨询：“早期中继”trac 确认攻击”,Tor 博客,2014 年 7 月 30 日

[562] I Dinur、K Nissim，“在保护隐私的同时披露信息”,数据库系统原理 (2003),第 202-210 页

[563] Profil de Protection – Machine a Voter , Direction centrale de la s ecurit e de system emes d information (2007)

[564] R Diresta、C Miller、V Molter、J Pomfret、G Tiert，“讲述中国的故事：中国共产党塑造全球叙事的运动，斯坦福互联网观察站,2020 年 7 月

[565] “2018 年年度欺凌调查”,丢掉标签

[566] AK Dixit，“无法无天与经济学”,普林斯顿大学出版社,2003 年

[567] RC Dixon，“具有商业应用的扩频系统”,Wiley (1994)

[568] H Dobbertin，“MD4 密码分析”,密码学杂志 v 11 no 4 (1998) pp 253–270

[569] T Docan-Morgan，“欺骗性沟通的帕尔格雷夫手册” (2019)

[570] C Doctorow，“SAMBA 与 SMB:对抗性互操作性是柔道网络效应”,Boing Boing,2019 年 7 月 17 日

[571] C Doctorow，“W3C 批准 DRM 标准三年后,不再可能制作功能独立的浏览器”，BoingBoing 2020 年 6 月 29 日

[572] V Dodd，“数百人因英国有组织犯罪网络被破解而被捕”，卫报,2020 年 7 月 2 日

[573] M Dodson,M Vingaard,AR Beresford。“使用全球蜜罐网络检测有针对性的 ICS 攻击”,2020 年国际网络冲突会议 (CyCon)

[574] P Doerfler,M Marincenko,J Ranieri,J Yu,A Moscicki,D McCoy,K Thomas，“评估登录挑战和对帐户的防御收购”,IW3C2 2019

[575] Z Do man，“新的 SIM 卡间谍软件攻击使 10 亿部手机瘫痪
处于风险之中”，福布斯，2019 年 9 月 12 日

[576] B Dole、S Lodin、E Spa ord，“放错位置的信任：Kerberos 4 会话密钥”，在互联网协会网络和分布式系统安全研讨会上，
IEEE，第 60-70 页

[577] L Donnelly，“超过 2600 万 NHS 患者担心安全漏洞”，每日
电讯报 2017 年 3 月 17 日

[578] Z Dorfman，J McLaughlin，“中央情报局的通信遭受了灾难
营养妥协。它始于伊朗”，雅虎新闻，2018 年 11 月 2 日

[579] Z Dorfman、J McLaughlin、SD Naylor，“独家：俄罗斯对 FBI 通信系统进行了‘惊人的’破坏，升级了美国领土上的间谍游戏”，雅虎新闻，2019 年 9 月 16 日

[580] JR Douceur，“女巫攻击”，IPTPS 2002，http://www.divms.uiowa。
edu/~ghosh/sybil.pdf

[581] P Drahos、J Braithwaite，“信息封建主义 谁拥有知识经济？”，Earthscan 2002

[582] S Drimer，“银行不帮助打击网络钓鱼”，Light Blue Touchpaper，3 月
10 2006

[583] S Drimer，“不稳定的 FPGA 设计安全性 一项调查”，2007 年

[584] S Drimer，SJ Murdoch，“让你的敌人靠近：距离限制智能卡中继攻击”，第 16 届 USENIX 安全研讨会（2007 年）

[585] S Drimer、SJ Murdoch、RJ Anderson，“优化失败：读卡器
用于网上银行”，金融密码学 2009

[586] IE Dror、D Charlton、AE P´eron，“上下文信息使专家容易做出错误的鉴定”，国际法医学 156 (2006) 74-78

[587] IE Dror, D Charlton，“专家为何会犯错”，载于《法医学杂志》
鉴定 v 56 no 4 (2006) pp 600–616

[588] I Drury，“指指点点”，载于 Security Surveyor v 27 no 5（97 年 1 月）页
15–17

[589] C Duckett，“谷歌零项目转变为完整的 90 天披露以提高补丁的采用”，ZDNet 2020 年 1 月 8 日

[590] P Ducklin，“为什么今天有 300 万个 Let s Encrypt 证书被取消”，Sophos 的 Naked security，2020 年 3 月 4 日

[591] C Duhigg，“亚马逊势不可挡吗？”纽约客（2019 年 10 月 21 日）

[592] I Duncan, L Aratani，“美国联邦航空局初步批准了设计修正
737 Max”，华盛顿邮报，2020 年 8 月 3 日

[593] JM Dutertre，V Beroulle，P Candelier，S De Castro，LB Faber，ML Flottes，
P Gendrier、DH´ely、R Leveugle、P Maistri、G Di Natale、A Papadimitriou、
B Rouzeyre，“CMOS 28 nm 技术节点的激光故障注入：故障模型分析”，密码学故障诊断和容错研讨会（2018 年）

[594] C Dwork,A Roth，“差异隐私的算法基础”，
理论计算机科学的基础和趋势第 9 期第 3-4 期（2014 年)第 211-407 页

[595] C Dwork、F McSherry、K Nissim、A Smith，“将噪声校准为私人数据分析中的灵敏度”，第三届密码学理论会议（2006 年）

[596] A Dyck、A Morse、L Zingales，“谁吹响了公司欺诈的哨子？”，金融杂志，2010 年 11 月 9 日；首次发表为 NBER 工作论文 12882，2007 年 2 月

[597] C Dyer，“欧洲对英国数据保护‘缺陷’的担忧”，载于
卫报 2007 年 10 月 1 日

[598] N Eagle、A Pentland、D Lazer，“使用手机数据推断社交网络结构”，2007 年，http://
reality.media.mit.edu/pdfs/network_structure.pdf

[599] D Easley，J Kleinberg，“网络、人群和市场：推理
高度互联的世界”，剑桥大学出版社（2010 年）

[600] D Easter，“ 暴风雨 对英美通信安全和情报的影响，1945-1970”，情报与国家安全（2020 年）

[601] W van Eck，“视频显示单元的电磁辐射：窃听风险？”载于 Computers & Security v 4 (1985) pp 269–286，网址为 https://cryptome.org/emr.pdf

[602] 经济学家，“生活在全球金鱼缸”，1999 年 12 月 18-24 日，
圣诞特辑

[603] 经济学家，“值得付出的代价？”，2005 年 5 月 19 日

[604] 经济学家，“终于得到信息”，2007 年 12 月 13 日

[605] 经济学人，“俄罗斯人正在回避国家控制的 YouTube 电视”，
2019 年 3 月 7 日

[606] 经济学家，“在遗传疾病中，谁有权知道或不知道什么？”（印刷版中的“不太快乐的舞蹈”），2019 年 9 月 28 日

[607] 经济学人，“为什么各州急于封存数以千万计的旧犯罪记录”，2019 年 11 月 14 日

[608] 经济学家，“金融世界的神经系统正在重新布线”，
2020 年 5 月 7 日

[609] 经济学人，“美国不希望中国主导 5G 移动
网络”，2020 年 4 月 8 日

[610] 经济学人，“Wirecard 如何一直愚弄大多数人”，
2020 年 6 月 25 日

[611] 经济学家，“在操纵选举后，白俄罗斯
抗议者” 2020 年 8 月 16 日

[612] B Edelman，“在线‘信任’证书中的逆向选择”，第五次信息安全经济学研讨会（2006 年）；在 http://weis2006.econinfosec.org/

[613] A Edwards，“BOLERO，航运业的 TTP 项目”，信息安全技术报告 v 1 no 1 (1996) pp 40-45

[614] C Edwards，“电动汽车生命周期难题”，工程与技术 (E&T) v 18 第 8 期（2020 年 8 月/9 月）第 26-29 页

[615] S Edwards、D Guido、JP Smith、E Sultanik，“Voatz 安全评估 II 卷 I：技术发现”，Trail of Bits，2020 年 3 月 12 日

[616] V Edwards，“有争议的艺术家 Spencer Tunick 抗议 Facebook 和 Instagram 禁止女性乳头在新的裸体模特聚会 约克市”，每日邮报，2019 年 6 月 2 日

[617] M Eichin，J Rochlis，“使用显微镜和镊子：分析 1988 年 11 月的互联网病毒”，载于 1989 年 IEEE 安全与隐私研讨会论文集，第 326-343 页

[618] 电子前沿基金会，http://www.eff.org

[619] 电子前沿基金会，“破解 DES：加密研究、窃听政治和芯片设计的秘密”，EFF（1998）；http://cryptome。 org/破解-des.htm

[620] Electronic Frontier Foundation, Felten, et al., v. RIAA, et al.在 http://www.eff.org/IP/DMCA/Felten_v_RIAA/

[621] 电子前沿基金会，“DocuColor 跟踪点解码 指南”，位于 http://w2.eff.org/Privacy/printers/docucolor/

[622] G Elich，“朝鲜与超音符之谜”，韩国政策研究所 2008 年 4 月 14 日

[623] P Elkington、A Dickinson、M Mavrogordato、D Spencer、R Gillams、A De Grazia、S Rosini、D Garay Baquero、L Diment、N Maho bia、H Morgan“治疗 COVID 的医护人员个人呼吸器规格-19 (PeRSo)” https://engrxiv.org/rvcs3/，规格和视频位于 https://www.southampton.ac.uk/publicpolicy/support-for-policymakers/policy-projects/perso.page

[624] M Ellims，“安全需要安全吗？”，2006 年 ESCAR，http://www.pi-shurlok.com/uploads/documents/security_and_safety.pdf

[625] JH Ellis，非秘密加密的历史，1987 年，http://www.jya。 com/ellisdoc.htm

[626] M Elliott、E MacKey、K O Hara、C Tudor，“匿名化决策框架”，曼彻斯特大学，2016 年；在 https://ukanon。 net/ukan-resources/ukan-decision-making-framework/

[627] C Ellison、B Schneier，“PKI 的十大风险：关于公钥基础设施你没有被告知的内容”，计算机安全期刊 v XIII no 1（2000 年）；也在 http://www.counterpane.com/pki-risks.html

[628] M Emms、B Arief、N Little、A van Moorsel，“O ine 的风险验证 PIN 非接触式卡”，金融密码学 (2013) 第 313–321 页

[629] 可从 EMVCo LLP 获取 EMV 文件,网址为 http://www.emvco.com/

[630] P Enge、T Walter、S Pullen、CD Kee、YC Chao、YJ Tsai，“全球定位系统的广域增强”,载于 IEEE 会议记录 v 84 no 8（8 月 96 日)第 1063-1088 页

[631] 电子隐私信息中心,http://www.epic.org

[632] M Ellims,J Botham，“自动驾驶汽车安全规则问题”，安全关键系统俱乐部研讨会,2020 年

[633] EPIC，“1987-1998 年联邦笔式登记器和陷阱与跟踪设备的批准”,网址为 http://www.epic.org/privacy/wiretap/stats/penreg。网页格式

[634] EPIC，“美国法院行政办公室主任的报告”,http://www.epic.org/privacy/wiretap/stats/1999-report/wiretap99.pdf

[635] J 爱泼斯坦,H Orman,J McHugh,R Pascale,M Branstad,A Marmor Squires，“高保证窗口系统原型”,在 Journal of 计算机安全 v 2 no 2–3 (1993) 第 159–190 页

[636] J Epstein、R Pascale，“高保证窗口系统的用户界面”,第九届年度计算机安全应用会议（1993 年）,第 256-264 页

[637] RG Epstein、S Ember、T Gabriel、M Baker，“爱荷华州党团会议如何成为民主党史诗般的惨败”,纽约时报,2020 年 2 月 11 日

[638] T Escamilla，“入侵检测 防火墙之外的网络安全”，威利 (1998)

[639] J Essinger，“ATM 网络 他们的组织、安全和未来”，爱思唯尔 1987

[640] 网络;消费者物联网的网络安全,ETSI EN 303 645 v 2.0.0,2019 年 11 月 26 日

[641] A Etzioni，“隐私的限制”,基本书籍（1999 年）

[642] 欧盟委员会，“影响评估 修改关于打击恐怖主义的框架决定 2002/475/JHA”,布鲁塞尔,2007 年 11 月 6 日，证监会(2007)1424

[643] 欧洲数字版权,网址为 https://www.edri.org

[644] 欧洲议会，“监视技术的发展和滥用经济信息的风险”,卢森堡（1999 年 4 月)PE 166.184 / 第 3/4 部分,位于 http://www.gn.apc.org/duncan/stoa.htm

[645] 欧洲议会和理事会,关于电力内部市场通用规则的指令 2009/72/EC 和废除指令 2003/54/EC

[646] 欧洲电信标准协会， CYBER;消费者物联网的网络安全:基本要求”,ETSI EN 303 645 V2.1.0 (2020–04)

[647] 欧盟，“关于在处理个人数据和此类数据的自由流动方面保护个人的指令”，

指令 95/46/EC

[648] 欧盟，“关于保留与提供公共电子通信服务或公共通信网络相关的数据而生成或处理的指令”，2006/24/EC

[649] 欧盟，“通过隐私增强技术促进数据保护
nologies (PETs)”，COM(2007) 228 决赛，布鲁塞尔，2007 年 5 月 2 日

[650] Eurosmart，“保护配置文件 – 带嵌入式软件的智能卡集成电路”，1999 年，网址为 http://www.commoncriteriaportal.org/

[651] 欧盟，“2000 年 6 月 22 日第 1334/2000 号理事会条例（EC)建立共同体制度以控制两用物品和技术的出口”

[652] 欧盟，“委员会指令 2009/4/EC – 防止和检测对行驶记录仪记录的操纵的反措施”，2009 年 1 月 23 日

[653] 欧盟，欧洲议会第 2017/745 号条例 (EU)
和理事会的 2017

[654] 欧盟，RAPEX A12/0157/19，安全门快速警报系统
危险的非食品产品，2019 年 2 月

[655] 欧盟，“ENISA（欧盟网络安全局)和关于信息和通信技术网络安全认证和废除条例 (EU) No 526/2013（网络安全法）”，2019 年 4 月 17 日

[656] 欧盟，欧洲议会和理事会关于货物销售合同某些方面的指令 (EU) 2019/771，修订了法规 (EU) 2017/2394 和指令 2009/22/EC，以及废除指令 1999/44/EC ，2019 年 5 月 20 日

[657] R Evans、D Leigh，“通用汽车子公司为‘被吹嘘的’私人数据支付骗子，
法院告诉”，《卫报》，2007 年 4 月 24 日

[658] R Evans，“在警方向黑名单提供详细信息后，工会会员被拒绝工作”，卫报，2019 年 3 月 7 日

[659] I Evtimov、WD Cui、E Kamar、E Kiciman、Ti Kohno、J Li，“现实世界中的安全和机器学习”，arXiv:2007.07205，2020 年 7 月 3 日

[660] M Fairhurst，“重新审视签名验证:促进生物识别技术的实际利用”，电子和通信工程杂志第 9 卷第 6 期（97 年 12 月)第 273-280 页

[661] C Farivar，“俄罗斯男子认罪，承认他运行了臭名昭著的 Kelihos 僵尸网络”，Ars Technica，2018 年 9 月 13 日

[662] K Faulkner、P Bentley、L Osborne，“你的秘密待售:现在 NHS 在披露在线购买处方的患者的详细信息后被出售 o ”，《每日邮报》

[663] B Feder，“人脸识别技术改进”，《纽约时报》3 月
14 2003

[664] 联邦航空管理局，“需要采取进一步行动来改进美国联邦航空局对自愿披露报告计划的监督”，监
察长办公室审计报告第 1 号。 AV-2014-036,2014 年 4 月 10 日

[665] 美国联邦航空管理局，“适航指令;波音公司
公司飞机”,Federal Register v 83 no 237（2018 年 12 月 11 日)第 63561-5 页

[666] 美国联邦航空管理局，“美国联邦航空局简史”,https：//www.faa.gov/about/history/
brief_history/,2020 年 6 月

[667] 联邦统计方法委员会， 统计政策工作文件 22（2005 年修订）– 统计披露限制报告

方法

[668] 联邦贸易委员会诉 Audiotex Connection, Inc. 和其他公司,http://www.ftc.gov/os/1997/9711/
Adtxamdfcmp.htm

[669] 联邦贸易委员会和商务部，《全球和国家商业法中的电子签名性质 消费者同意书》

第 101(c)(1)(C)(ii) 节中的规定,2001 年 6 月

[670] 联邦贸易委员会，“身份盗窃:当坏事发生在你的好名声上”,http://www.consumer.gov/idtheft/

[671] 联邦贸易委员会， ChoicePoint 解决了数据安全违规指控;支付 1000 万美元的民事罚款,500
万美元用于消费者赔偿”,2006 年 1 月 26 日 http://www.ftc.gov/opa/2006/01/
choicepoint.shtm

[672] 美国科学家联合会,http://www.fas.org

[673] H Federrath,J Thees，“Schutz der Vertraulichkeit des Aufenthaltsorts von
Mobilfunkteilnehmern”,载于 Datenschutz und Datensicherheit（1995 年 6 月）,第
338-348 页

[674] P Fellwock（使用化名“Winslow Peck”），“美国电子间谍:回忆录”,Ramparts v 11 no 2
（1972 年 8 月)第 35-50 页;在 http://jya.com/nsa-elint.htm

[675] AP 毛毡,A Ainslie,RW Reeder,S Consolvo,S Thyagaraja,A Bettes,H
Harris, J Grimes，“改进 SSL 警告:理解和遵守”,CHI 2015

[676] AP Felt、E Ha、S Egelman、A Haney、E Chin、D Wagner，“Android 权限:用户注意力、理解和行
为”,SOUPS 2012

大学, 1973

[677] AG Ferguson，“警务预测警务”,华盛顿大学法
评论 v 94 no 5 (2017)

[678] D Ferraiolo,R Kuhn，“基于角色的访问控制”,第 15 届全国计算机安全会议,NIST（1992)第
554-563 页

[679] D Ferraiolo、R Kuhn、R Chandramouli，“基于角色的访问控制”,Artech
房子, 2007

[680] H Ferradi、RG´eraud、D Naccache、A Tria，“当有组织犯罪适用时
学术成果 对卡内监听设备的取证分析”，
IACR 密码学 ePrint 存档报告 2015/963，2015 年 10 月 5 日

[681] J Ferrigno, M Hlav´a v c，“当 AES 闪烁时：引入光学侧信道”，
IET 信息安全 v 2 no 3 (2008) pp 94–98

[682] D Fewer、P Gauvin、A Cameron，“数字版权管理技术和消费者隐私 根据加拿大隐私法评
估 DRM 应用”，加拿大互联网政策和公共利益

诊所，2007 年 9 月

[683] A Fiat，M Naor，“广播加密”，载于 Crypto 93，Springer LNCS v 773，第 480-491 页

[684] S Figueroa-Lorenzo、JA norga、S Arrizabalaga，“IIoT 协议调查：基于 CVSS 的漏洞风险
分析度量”，ACM
计算调查 v 55 no 2（2020 年 4 月）

[685] PFJ Fillery，AN Chandler，“缺乏优质软件是否是信息安全问题的密码？”，IFIP SEC 94 论
文 C8

[686] “FCA 因 IT 故障对 RBS、NatWest 和 Ulster Bank Ltd 罚款 4200 万英镑”，
金融行为监管局，2014 年 11 月 20 日

[687]“最终通知，Tesco Personal Finance plc，参考编号 186022”，Fi
金融行为监管局，2018 年 10 月 1 日

[688]“将 FinCEN 的规定应用于某些涉及
可兑换虚拟货币”，美国金融犯罪执法网络，2019 年 5 月 9 日

[689]“心理学家和银行就卡片上照片的优点发生冲突”，载于
Financial Technology International Bulletin v 13 no 5（96 年 1 月）第 2-3 页

[690] D Fine，“为什么 Kevin Lee Poulsen 真的在监狱里？”，http://www.well。
com/user/fine/journalism/jail.html

[691] A Finkelstein, M Shattuck，“CAPSA 及其实施：向剑桥大学审计委员会和审查委员会报告”，

剑桥大学记者编号 5861，2001 年 11 月 2 日

[692] P Finn，“对爱沙尼亚的网络攻击代表了一种新的战斗策略”洗涤
吨邮政 2007 年 5 月 19 日

[693] ML Finucane、P Slovic、CK Mertz、J Flynn、TA Satterfield，“性别、种族和感知风险： ‘白人
男性’效应”，Health、risk & society v 2 no 2 (2000) pp 159–172

[694] G Fiorentini、S Pelzman，“有组织犯罪的经济学”，剑桥
大学出版社1995

[695] RA Fisher，“自然选择的遗传学理论”，克拉伦登出版社，牛津（1930 年）；第二版。多佛出版
社，纽约 (1958)

[696] J Flanagan，“监狱电话欺诈（或西班牙语的风险）”，华盛顿大学 sta 报报道，comp.risks
v 12.47；在 http://catless.ncl.ac.uk/Risks/20.69.html

[697] M Fleet，“通过紫外线测试的纸币上的五个表情句子”，载于每日电讯报（1999 年 12 月 23 日），可在 http://www.telegraph.co.uk 获得:80/

[698] N Fletcher，“巴克莱银行老板 Jes Staley 因举报人被罚款 A ˇ c642,000 丑闻”，《卫报》，2018 年 5 月 11 日

[699] E Flitter，“富国银行虚假账户丑闻的价格上涨了 3 美元 亿”，纽约时报 2020 年 2 月 21 日

[700] SN Foley，“聚合和分离作为非干扰特性”，载于 计算机安全杂志 v 1 no 2 (1992) pp 158–188

[701] Fondazione Ugo Bordoni，“信息保护电磁安全研讨会”，意大利罗马，1991 年 11 月 21-22 日

[702] “Target 的首席执行官在大规模数据泄露和加拿大崩溃后辞职”，福布斯，2014 年 5 月 8 日

[703] J Ford、T Kinder，“Wirecard 之后:是时候审计审计师了吗？”，《金融时报》，2020 年 7 月 3 日

[704] “新的中国恐慌 为什么美国不应该对其最新的恐慌 Challenger”，Foreign Aairs 2019 年 12 月 6 日

[705] S Forrest, SA Hofmeyr, A Somayaji，“计算机免疫学”，ACM 通信 v 40 no 10（97 年 10 月)第 88-96 页

[706] DS Fortney，JJ Lim，“确定信息在计算机化报警系统中重要性的技术方法”，第十七届全国 Computer Security Conference (1994)，NIST 出版的论文集；第 348-357 页

[707] K Foster、C Greene、J Stavins，“2018 年消费者支付调查 选择:总结结果”，亚特兰大联邦储备银行（2019 年）

[708] 信息政策研究基金会，http://www.fipr.org

[709] B Fox，“不要调整你的设置。 . .我们已经承担了无线电控制”，在新 科学家 2000 年 1 月 8 日

[710] LJ Fraim，“SCOMP:多级安全问题的解决方案”，载于 IEEE Computer v 16 no 7（83 年 7 月)第 26-34 页

[711] L Franceschi-Bicchierai，“AT&T 承包商和 Verizon 员工 被控帮助 SIM 交换犯罪团伙” Vice 2019 年 5 月 31 日

[712] L Franceschi-Bicchierai，“Verizon 使 SIM 交换变得困难。为什么不 AT&T、Sprint 和 T-Mobile？”，Vice 2019 年 9 月 19 日

[713] T Frank，“更严格的 TSA 炸弹测试提高了安检人员的风险”，美国 今天 2007 年 10 月 18 日

[714] J Franklin、V Paxson、A Perrig、S Savage，“对自然和 互联网不法分子财富的成因”，ACM CCS (2007)

[715] J Franks、P Hallam-Baker、J Hostetler、S Lawrence、P Leach、A Luotonen、L Stewart，“HTTP 身份验证:基本和摘要访问身份验证”， RFC 2617

[716] “Banks fingerprint customers to cut check fraud”,Fraud Watch (1997)
没有 1 第 9

[717] “芯片卡减少了法国的欺诈行为”,Fraud Watch (1996) no 1 p 8

[718] “关于增加警告的假冒和跨境欺诈”,Fraud Watch (1996) no 1 pp 6–7

[719] “手指细节系统跨越 1:100,000 错误拒绝障碍”,在欺诈
观看 (1996) 第 2 期第 6-9 页

[720] “广泛的信用卡窃取引起欧洲的关注”,Fraud Watch (1997) v 3 pp 1-2

[721] SJ Freedberg,“陆军授予洛克希德 7500 万美元用于 AI 网络/干扰吊舱”,
突破防御 2020 年 4 月 29 日

[722] P Freiberger,M Swaine,“山谷之火 个人的形成
计算机”,麦格劳-希尔 (1999)

[723] 一位法国人,“冷战策划者的秘史”连线 3 月 11 日
2020

[724] J Fridrich,“数字媒体中的隐写术:原理、算法和
Applications ,剑桥大学出版社 2009

[725] P Frigo、E Vannacci、H Hassan、V van der Veen、O Mutlu、C Giu rida、H Bos、K Razavi “TRRespass:
利用目标行刷新的多方面”,arXiv:2004.01807 2020 年 4 月 3 日

[726] A Frik、N Malkin、M Harbach、E Peer、S Egelman,“承诺就是承诺
– 承诺设备对计算机安全意图的影响”,
气2019

[727] J Frizell、T Phillips、T Groover,“对国家安全和应急准备电信的电子入侵威胁:一份意识文件”,NCSC
（NIST,1994 年)第 378-399 页

[728] M Frost,“间谍世界:加拿大和美国情报局内部
lishments ,Diane Publishing Co (1994)

[729] N Frost,“麦克唐纳道格拉斯-波音合并如何导致 737 Max 危机”,Quartz,2020 年 1 月 3 日

[730] DA Fulghum,“通信拦截 Pace EP-3”,航空周刊和空间技术 v 146 no 19 (5/5/97) pp 53-54

[731] S Fuloria、R Anderson、F Alvarez、K McGrath,“子站的密钥管理:对称密钥、公钥还是无密钥?”在
IEEE 电力系统会议暨展览会 (PSCE 2010)

[732] P Fussey,D Murphy,“关于伦敦大都会警察局对现场面部识别技术试验的独立报告”,人权中心,

埃塞克斯大学 (2019)

[733] M Galecotti,“俄罗斯的窃听者走出阴影”,简氏
情报评论 v 9 no 12（97 年 12 月)第 531-535 页

[734] R Gallagher,“英国间谍如何侵入比利时的内幕”
最大的电信公司”,The Intercept,2014 年 12 月 13 日

[735] R Gallagher，“英国间谍如何入侵欧洲盟友并逍遥法外”拦截，2018 年 2 月 17 日

[736] LA Galloway、T Yunusov，“首次接触：非接触式支付中的新漏洞”，https://leigh-annegalloway.com/presentation-materials/ 2019 年 12 月 4 日

[737] E Galperin，M Marquis-Boire，J Scott-Railton，“监视的量子：叙利亚恶意软件活动中熟悉的参与者和可能的假旗”，EFF 和公民实验室

[738] F Galton 爵士，“个人身份和描述”，发表于《自然》(21/6/1888) 第 173-177 页

[739] F Galton 爵士，“指纹”，麦克米伦出版社，1892 年

[740] HF Gaines，“密码分析 密码及其解决方案的研究”，多佛(1939, 1956)

[741] J Gamba、M Rashed、A Razaghpanah、J Tapiador、N Vallina-Rodriguez、“预装 Android 软件分析”，IEEE S&P 2020

[742] D Gambetta，“黑社会法典：罪犯如何沟通”，普林斯顿大学 (2009)

[743] J Gamblin，“近 20% 的 1000 个最流行的 Docker 容器有没有 Root 密码”，Kenna 安全博客，2019 年 5 月 20 日

[744] T Gandy，“打击欺诈的脑电波”，银行技术（95 年 12 月/96 年 1 月）第 20-24 页

[745] F Ganji、S Tajik、JP Seifert，“攻击者为何获胜：关于网络的可学习性XOR Arbiter PUF 的信任和可信计算 2015 第 22–39 页

[746] HC Gao, JX Yan, F Cao, ZY Zhang, L Lei, MY Tang, P Zhang, X Zhou, XQ Wang、JW Li，“对文本验证码的简单通用攻击”，NDSS 2016

[747] FD Garcia，G de Koning Gans，R Muijrers，P van Rossum，R Verdult，R Wickers Schreur、B Jacobs，“拆解 MIFARE Classic”，ESORICS 2008 年，施普林格 LNCS v 5283 第 97-114 页

[748] FD Garcia、D Oswald、T Kasper、P Pavlid´es，“锁定它并仍然丢失它 – 关于汽车远程无钥匙进入系统的（在）安全性”，Usenix 2016

[749] R 加德纳，A Yasinsac，M Bishop，T Kohno，Z Hartley，J Kerski，D Gainey，R Walega、E Hollander、M Gerke，“Diebold 投票机软件的软件审查和安全分析”，佛罗里达州立大学，2007 年 7 月 27 日

[750] S Garfinkel，“数据库国家”，O Reilly and Associates (2000)

[751] S Garfinkel，“同时安全和可用的计算机系统的设计原则和模式”，博士论文，麻省理工学院 2005 年，http://www.simson.net/thesis/

[752] S Garfinkel、JM Abowd、C Martindale，“了解对公共数据的数据库重建攻击”，ACM Queue v 16 no 5，2018 年 11 月 28 日

[753] S Garfinkel,G Spa ord，“实用 Unix 和互联网安全”,O Reilly
和同事 (1996)

[754] B Gassend、D Clarke、M van Dijk、S Devadas，“硅物理随机
函数”ACM CCS 2002 第

[755] W Gates、W Buett，“比尔和沃伦秀”，《财富》杂志,20/7/1998

[756] B Gellman，“爱德华·斯诺登 (Edward Snowden) 在美国国家安全局 (NSA) 揭露数月后表
示,他的使命已经完成”,华盛顿邮报,2013 年 12 月 23 日

[757] B Gellman、D Linzer、CD Leonnig，“监控网络几乎没有嫌疑人”，
华盛顿邮报 2006 年 2 月 5 日,p A01

[758] RM Gerecht，“反恐神话”,大西洋月刊,7 月至 8 月
2001年

[759] J Germain，“我们回到慕尼黑向 Windows 的迁移 现在要花多少钱？！ e100 米!登记册
2018 年 1 月 4 日

[760] E German，“问题识别”,http://onin.com/fp/problemidents。
网页格式

[761] E German，“对指纹的法律挑战”,http://www.onin.com/
fp/daubert_links.html

[762] JJ Gibson，“视觉感知的生态方法”,Houghton Mif
弗林 1979

[763] D Gi ord,A Spector，“The CIRRUS Banking Netowrk”,ACM 通讯 v 28 no 8（1985 年
8 月)第 797-807 页

[764] D Gilbert，“如果只有同性恋导致全球变暖”,洛杉矶时报,2006 年 7 月 2 日

[765] N Gilens，“新的司法部文件显示
无保证电子监控”,ACLU 博客,2012 年 9 月 27 日

[766] M Gill, A Spriggs，“评估闭路电视的影响”,英国家庭 Oce 研究 292

[767] J Gillum、J Kao、J Larson，“互联网上提供了数百万美国人的医学图像和数据。任何人都可以偷
看。” ProPublica 2019 年 9 月 17 日

[768] J Gilmore，“Nacchio 影响间谍探测”,丹佛邮报,2007 年 10 月 20 日;引用于
“美国国家安全局在布什就职后立即征集非法的 Qwest 大规模窃听”，
密码学列表 2007 年 10 月 20 日

[769] T Gilovich、D Grin、D Kahneman，“启发式和偏见 直觉判断的心理学”,剑桥大学出版社
2002 年

[770] AA 佐丹奴, HA Sunkenberg, HE de Pdero, P Stynes, DW Brown, SC Lee,
“扩频联播 MF 无线电网络”,载于 IEEE Transactions on Communications v TC-30 no 5
（1982 年 5 月)第 1057-1070 页

[771] V Goel，“Verizon 将为雅虎少支付 3.5 亿美元”,纽约时报 2 月
21 2017

[772] WN Goetzmann，“金融文明”,http://viking.som.yale.edu/will/finciv/chapter1.htm

[773] J Goguen、J Meseguer，“安全策略和安全模型”，载于 1982 年 IEEE 计算机协会研究研讨会论文集
安全和隐私第 11-20 页

[774] B Goldacre，“Care.data 一片混乱。这让我心碎”，《卫报》2 月 28 2014

[775] I Goldberg, D Wagner，“随机性和 Netscape 浏览器”，载于 Dr Dobbs Journal 第 243 期（96 年 1 月)第 66-70 页

[776] L Goldberg，“回收的冷战电子产品战斗蜂窝电话 Thieves”，Electronic Design v 44 no 18（1996 年 9 月 3 日)第 41-42 页

[777] S Goldwasser、S Micali，“概率加密”，J Comp Sys Sci v 28 (1984) pp 270–299

[778] G Goller、G Sigl，“使用标准无线电设备对智能手机和嵌入式设备进行侧信道攻击”，COSADE 2015，第 255-270 页

[779] D Gollmann，“计算机安全”，第三版，Wiley（2010 年）

[780] D Gollmann，“什么是身份验证？”，载于安全协议 (2000)，Springer LNCS 1796，第 65-72 页

[781] R Golman、D Hagman、G Loewenstein，“信息回避”，期刊 经济文献诉 LV（2017 年 3 月）

[782] S Golovnev，P Gaudry，“破解莫斯科互联网投票系统的加密方案”，金融密码学 2020

[783] L Gong，“深入了解 Java 2 平台安全性：体系结构、API 设计和实施”，Addison-Wesley (1999)

[784] L Gong，DJ Wheeler，“矩阵密钥分配方案”，在 Journal of 密码学 v 2 no 1 (1990) pp 51–59

[785] R Gonggrijp、WJ Hengeveld、A Bogk、D Engling、H Mehnert、F Rieger、P Sche ers、B Wels，“Nedap/Groenendaal ES3B 投票计算机 安全分析”，2006 年 10 月，http://www.wijvertrouwenstemcomputersniet。 nl/Nedap-en

[786] D Goodin，“eBay 诈骗剖析”，载于 The Register，2007 年 3 月 21 日；在 http://www.theregister.co.uk/2007/03/21/ebay_fraud_anatomy/

[787] D Goodin，“Firefox 泄漏可能泄露敏感信息”，载于 The Register，8 月 13 2007

[788] D Goodin，“TJX 同意向银行支付 4100 万美元以弥补 Visa 损失”，载于 The 频道注册，2007 年 12 月 3 日

[789] D Goodin，“乌克兰 eBay 骗局将唐氏综合症患者变成现金机器”，于 The Register 2007 年 11 月 8 日

[790] D Goodin，“苏联人如何使用 IBM Selectric 键盘记录器监视美国外交官”，The Register，2015 年 10 月 13 日

[791] D Goodin，“3ve 的 BGP 劫持者如何躲避互联网 并使 2900 万美元”，Ars Technica，2018 年 12 月 21 日

[792] D Goodin，“警方在破解昂贵的 IronChat 后解密了 258,000 条消息
加密应用”，Ars Technica，2018 年 7 月 11 日

[793] D Goodin，“Checkm8 的开发者解释了为什么 iDevice 越狱利用会改变游戏规则”，Ars Technica，
2019 年 9 月 28 日

[794] D Goodin，“归还租车五个月后，男人仍然有遥控器，Ars Technica，2019 年 10 月 28 日

[795] D Goodin，“论坛破解了 Ken Thompson 和
其他 Unix 先驱”，Ars Technica，2019 年 10 月 10 日

[796] D Goodin，“秘密执行了具有 1 亿次下载量的 Google Play 应用程序
有效载荷”，Ars Technica，2019 年 8 月 27 日

[797] D Goodin，“Evil Corp 的头目住得很大。现在悬赏 500 万美元”，Ars Technica，2019 年 12 月 5 日

[798] D Goodin，“新发布的 Checkra1n 越狱对 iDevice 意味着什么
安全”，Ars Technica，2019 年 11 月 15 日

[799] D Goodin，“数十亿 Wi-Fi 芯片中的一个缺陷让攻击者解密数据”，
有线 2020 年 2 月 27 日

[800] “因版权而被删除的内容”，谷歌透明度报告（2018 年），网址为 https://
transparencyreport.google.com/copyright/overview

[801] KE Gordon，RJ Wong，“编程金属的导电丝
电极非晶硅反熔丝”，国际会议记录
电子设备会议，12 月 93 日；转载为第 6-3 至 6-10 页，QuickLogic
数据手册 (1994)

[802] 英国政府，“收藏 政府安全”，网址为 https://www.gov。英国/政府/收藏/政府安全 (2019)

[803] MF Grady, F Parisi，“网络安全的法律和经济学”，剑桥
大学出版社, 2006

[804] RM Graham，“信息处理实用程序中的保护”，ACM 通讯 v 11 no 5（1968 年 5 月）第 365-369 页

[805] FT Grampp，RH Morris，“UNIX 操作系统安全”，AT&T Bell
实验室技术杂志第 63 卷第 8 期（84 年 10 月）第 1649–1672 页

[806] S Granneman，“电子投票崩溃”，载于 The Register 2003 年 11 月 18 日

[807] RD Graubart、JL Berger、JPL Woodward，“分区模式，工作站评估标准，版本 1”，Mitre MTR
10953，1991（也由国防情报局作为文档 DDS-2600-6243-91 发布）

[808] J Gray、P Syverson，“概率系统多级安全的逻辑方法”，分布式计算 v 11 no 2 (1988)

[809] A Greenberg，“ 区块链强盗 正在猜测私钥和评分
百万》，《连线》杂志，2019 年 4 月 23 日

[810] A Greenberg，“一个神秘的黑客组织正在进行供应链劫持
Spree”，《连线》杂志，2019 年 3 月 3 日

[811] A Greenberg，“拯救互联网的黑客 Marcus Hutchins 的自白”，《连线》杂志，2020 年 5 月 12 日

[812] T Greening，“Ask and Ye Shall Receive: A Study in Social Engineering”，载于
SIGSAC 评论 v 14 no 2（96 年 4 月）第 9-14 页

[813] A Greenberg，“NotPetya 的不为人知的故事，最具破坏性的 Cy
历史上的反击”，连线，2018 年 8 月 22 日

[814] G Greenwald，“美国国家安全局收集数百万 Verizon 客户的电话记录
tomers daily”，卫报，2013 年 6 月 7 日

[815] G Greenwald，“XKeyscore：NSA 工具收集‘用户在互联网上所做的几乎所有事情’”，卫报，2013 年 7
月 13 日

[816] G 格林沃尔德，“无处可藏”，企鹅 (2015)

[817] G Greenwald、E MacAskill，“NSA Prism 程序利用了用户数据
苹果、谷歌等”，卫报，2013 年 6 月 9 日

[818] G Greenwald、E MacAskill、L Poitras，“爱德华·斯诺登：国家安全局监控揭露背后的告密者”，卫报，2013
年 6 月 11 日

[819] M Gregory、P Losocco，“使用 Flask 安全架构促进风险适应性访问控制”，2007 年安全增强 Linux 研讨
会，http://selinux-symposium.org/2007/agenda.php

[820] J Grierson，“负责 1.13 亿英镑欺诈的团伙头目被判入狱 11 年”，卫报，2016 年 9 月 21 日

[821] A Griew, R Currell，“电子病人安全策略”
Record ，威尔士大学阿伯里斯特威斯分校健康信息学研究所，
1995 年 3 月

[822] JM Grin，A Shams，“比特币真的不受束缚吗？” SSRN 3195066
2018

[823] H Griths，“汽车犯罪再次上升，去年有 113,000 辆汽车被盗”，
汽车快递 2019年4月25日

[824] H Griths、N Willis，“Klein Heidleberg – 一种领先时代数十年的二战双基地雷达系统”（2010 年），网址
为 https://www.cdvandt.org/kh.htm

[825] V Groebner、J Peck、M Kyburz，“你是谁？：早期现代欧洲的身份识别、欺骗和监视”，Zone Books，2007
年

[826] E Groll，“‘奥巴马的将军’认罪泄露 Stuxnet 操作，”
外交政策 2016 年 10 月 16 日

[827] J Gross，“让患者的详细信息保密，即使是来自亲属”，纽约
泰晤士报 2007 年 7 月 3 日

[828] P Grother、M Ngan、K Hanaoka，“人脸识别供应商测试 (FRVT)”
NIST IR 2871，2019 年 9 月 11 日

[829] D Grover，“计算机软件的保护 其技术和应用”，英国计算机学会/剑桥大学出版社（1992）

[830] D Gruhl、W Bender，“信息隐藏以挫败偶然的造假者”，在第二届信息隐藏国际研讨会论文集中
（波特兰，98 年 4 月），Springer LNCS v 1525 第 1-15 页

[831] L Gudgeon、P Moreno-Sanchez、S Roos、P McCorry、A Gervais，“SoK：
第二层区块链协议”，金融密码学 2020

[832] LC Guillou、M Ugon、JJ Quisquater，“智能卡 标准化
专用于公共密码学的安全设备”，[1748] 第 561–613 页

[833] U Guin，K Huang，D DiMase，JM Carulli，M Tehranipoor，Y Makris，
“假冒集成电路：全球半导体供应链中日益严重的威胁”，Proc IEEE v 102 no 8（2014
年 8 月）

[834] GD Guo，N Zhang，“基于深度学习的人脸识别调查”，
计算机视觉与图像理解 189（2019)102805

[835] R Gupta、SA Smolka、S Bhaskar，“论顺序和随机化
分布式算法”，ACM Computing Surveys v 26 no 1（94 年 3 月)第 7-86 页

[836] M Gurman，“苹果允许一些视频应用程序在不收取 30% 费用的情况下销售节目
切”，彭博社，2020 年 4 月 1 日

[837] P Gutmann，“从磁性和固态存储器中安全删除数据”，第六届 USENIX 安全研讨会论文集
（1996 年 7 月)第 77-89 页

[838] P Gutmann，“实用强随机数的软件生成”，第七届 Usenix 安全研讨会论文集（1998 年
1 月)第 243-257 页

[839] P Gutmann，“奥克兰的停电，或奥克兰 你的 Y2K Beta 测试站点”，https://
www.cs.auckland.ac.nz/~pgut001/misc/mercury。 txt 1998 年 5 月 24 日

[840] P Gutmann，“半导体器件中的数据残留”，载于 Usenix Se
安全研讨会 (2001)

[841] P Gutmann，“无效的银行证书只会吓到 300 个用户中的一个”，Cryptog
raphy 列表 2005 年 5 月 16 日

[842] P Gutmann，“Windows Vista 内容保护的成本分析”，2007 年 4 月，http://
www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html

[843] P Gutmann，“出售的商业验证码破解器”，密码列表
2007 年 10 月 22 日

[844] S Haber，WS Stornetta，“如何为数字文档添加时间戳”，发表于期刊
密码学 v 3 no 2 (1991) pp 99–111

[845] S Haber，WS Stornetta，“位串的安全名称”，第 4 届 ACM 计算机和通信安全会议（1997
年)第 28-35 页

[846] W Hackmann，“Asdics at war”，在 IEE Review v 46 no 3（2000 年 5 月)页
15–19

[847] “Chris Carey 在新西兰被捕”，Hack Watch News（9/1/1999）

[848] C Hagen、C Weinert、S Sendner、A Dimitrienko、T Schneider，“所有数字都是美国:移动信使中大规模滥用联系人发现”，
维尔茨堡大学, 2020

[849] N Hager，“秘密力量 新西兰在国际间谍网络中的作用”，Craig Potton Publishing (1996)，
http://www.nickyhager.info/Secret_Power.pdf

[850] N Hager、R Gallagher，“斯诺登的启示/五眼俱乐部的代价:对友好国家的大规模间谍”，新西兰先驱报和西莫尔摇滚，2015 年 3 月 5 日

[851] D Hakim、RJ Epstein、S Saul，“选举剖析 ^aA YMeltdown^a ¨ A Z´
在佐治亚州”，纽约时报 2020 年 7 月 25 日

[852] JA Halderman，“亚马逊的 MP3 商店明智地放弃水印”，2007 年 10 月 2 日，http://
www.freedom-to-tinker.com/?p=1207

[853] JA Halderman，N Heninger，“国家安全局如何破解这么多密码？” 2015 年 10 月 14 日，自由修补

[854] JA Halderman、SD Schoen、N Heninger、W Clarkson、W Paul、JA Calan drino、AJ Feldman、J Appelbaum、EW Felten，“以免我们记住:对加密密钥的冷启动攻击”，ACM 通信 v 52第 5 期（2009 年)第 91–98 页

[855] PS Hall, TK Garland-Collins, RS Picton, RG Lee, Radar , Brassey s New
战场武器系统和技术系列 (v 9)，ISBN 0-08-037711-4

[856] M Hamburg，“了解英特尔的 Ivy Bridge 随机数生成器”，电子设计，2012 年 12 月 11 日

[857] C Hamby，C Moses，“波音拒绝配合新调查
Deadly Crash”，纽约时报，2020 年 2 月 6 日

[858] J Hammer，“十亿美元的银行工作”，纽约时报，2018 年 5 月 13 日

[859] C Han，I Reyes，A Feal，J Reardon，P Wijesekera，N Vallina-Rodriguez，A Elazari、KA Bamberger、S Egelman，“价格（不)合适:比较
免费和付费应用程序中的隐私”，PoPETS (2020)

[860] H Handschuh、P Paillier、J Stern，“探测对防篡改设备的攻击”，加密硬件和嵌入式系统 – CHES 99，第 303-315 页

[861] R Hanley，“数以百万计的盗窃案困扰着新泽西地区”，纽约时报，
1981 年 2 月 9 日，立法会 A；1页

[862] R Hanson，“窃听能否保持成本效益？”，在 Communications of the
ACM v 37 第 12 期（94 年 12 月)第 13-15 页

[863] D Hardt，“OAuth 2.0 授权框架”，IETF RFC 6749 Oct
2012

[864] C Harper，“PlusToken 骗局如何利用超过 1% 的比特币供应量潜逃”，Botcoin 杂志，2019 年 8 月 19 日

[865] V Harrington、P Mayhew，“手机盗窃”，英国家庭 Oce 研究
研究 235，2002 年 1 月

[866] K Harris，“加利福尼亚州的人类追踪状况”，加利福尼亚州司法部，2012 年

[867] T 哈里斯，“技术如何劫持你的思想 来自魔术师和
Google 设计伦理学家”，Medium，2016 年 5 月 18 日

[868] MA Harrison、ML Ruzzo、JD Ullman，“操作系统保护”，ACM 通信 v 19 no 8（1976 年 8 月）第
461-471 页

[869] D Harz，“窃取制造商的所有抵押品”，Medium 2020 年 2 月 20 日

[870] A Hassey，M Wells，“临床系统安全 实施 BMA
政策和指南”，[63] 第 79-94 页

[871] AJ Hawkins，“Waymo 的无人驾驶汽车：幽灵骑在机器人出租车的后座”，The Verge，2019 年
12 月 9 日

[872] S Haykin，“认知雷达：未来之路”IEEE 信号杂志
2006 年 2 月处理

[873] 健康与人类服务，“个人身份健康信息隐私标准”，HHS 45 CFR parts 160 aA¸S164, 65
联邦
在 82461^aA¸S82,510 注册；另见 82,777–82,779

[874] HSE 团队检查运营的控制和监督
BNFL s Sellafield Site ，健康与安全主管，2000

[875] “2018-9 年年度回顾”，NHS 医疗安全调查处

[876] LJ Heath，“1967-1974 年美国海军舰队广播系统的系统性安全弱点分析，被 CWO John Walker
利用”，佐治亚理工学院理学硕士论文，网址为 http://www.fas.org/ irp/eprint/heath.pdf

[877] B Heath，“美国几十年来秘密跟踪了数十亿次通话”，《今日美国》
2015 年 4 月 8 日

[878] T Heim，“对 500,000 个 DNA 数据库错误的愤怒”，每日电讯报，
2007 年 8 月 28 日

[879] N Heintze，“可缩放文档指纹识别”，在第二个 USENIX 作品中
电子商务商店 (1996) 第 191–200 页

[880] P Helland，“任何其他名称的身份”，ACM 通讯
2019 年 4 月，第 80-87 页

[881] S Helmers，“anon.penet.fi 的简史 传奇的匿名转发器”，CMC 杂志，1997 年 9 月；在 http://
www.december.com/cmc/mag/1997/sep/helmers.html

[882] JL Hennessy，DA Patterson，“计算机体系结构：定量应用程序
proach” Morgan Kaufmann 2017 年 12 月

[883] A Henney，R Anderson，“智能计量 – Ed Milliband 的中毒 Chal
冰”，Lightbluetouchpaper 2012 年 2 月 8 日

[884] E Henning，“无能的印记”，c t 杂志，2007 年 9 月 3 日；在 http://www.heise-security.co.uk/
articles/95341

[885] ER Henry，“指纹的分类和使用”George Rutledge &
儿子们,伦敦,1900 年

[886] I Herbert，“没有证据表明在儿童色情调查中有人‘杀了他’
self ”,载于《独立报》,2005 年 10 月 1 日

[887] C Herley，“规模世界中目标攻击者的困境”,WEIS
2010

[888] A Hern，“微软总裁对应用商店的批评给苹果带来压力”,卫报,2020 年 6 月 21 日

[889] 希罗多德,《历史》;第 1 册 123.4,第 5 册 35.3 和第 7 册 239.3

[890] T Herr、J Lee、W Loomis、S Scott，“打破信任:危机的阴影
和不安全的软件供应链”,大西洋理事会,2020 年 7 月

[891] J Van den Herrewegen,FD Garcia，“引擎盖下:故障
诊断安全”,ESORICS 2018

[892] A Herzberg、M Jakobsson、S Jarecki、H Krawczyk、M Yung，“主动
公钥和签名系统”,第 4 届 ACM CCS (1997) pp 100–110

[893] 惠普公司，“IA-64 指令集架构指南”（2000 年）

[894] TS Heydt-Benjamin、DV Bailey、K Fu、A Juels、T OHare，“第一代支持 RFID 的信用卡中的漏洞”,第 11 届国际
2007年金融密码学和数据安全会议

[895] HM Heys，“线性和差分密码分析教程”,在 Cryp
tologia v XXVI no 3（2002 年 7 月)第 189-221 页

[896] HJ 高地“电磁辐射重访”,在计算机与 Se
curity v5 (1986) 85–93 和 181–184

[897] K Hill，“我们所知道的可能终结隐私的秘密公司”，
纽约时报 2020 年 1 月 18 日

[898] K Hill,A Krolik，“您孩子的照片如何为监控提供动力
技术”,纽约时报,2019 年 10 月 11 日

[899] K Hill, H Murphy，“你的 DNA 档案是私人的?一位佛罗里达州的法官只是说否则”,纽约时报,2019 年 11 月 5 日

[900] K Hill,S Mattu，“监视我的房子”,Gizmodo 2018 年 2 月 7 日

[901] R Hill，“欧盟委员会下令大规模召回令人毛骨悚然、漏水的儿童追踪智能手表”,The Register,2019 年 2 月 4 日

[902] TF Himdi,RS Sandhu，“用于受控共享的基于格的模型
沙特朝觐系统中的机密信息”,第 13 届年度计算机安全应用会议第 164-174 页

[903] E von Hippel，“作为用户创新网络的开源软件项目”,开源软件经济学 2002（图卢兹）

[904] W von Hippel,R Trivers，“自欺欺人的演变和心理学”，
TBehavioral and Brain Sciences v 34 (2011) 第 1-16 页

[905] J Hirshleifer，“隐私:其起源、功能和未来”，载于《法律杂志》
研究 v 9（1980 年 12 月)第 649–664 页

[906] Jack Hirshleifer，“从最薄弱的环节到最好的机会:公共物品的自愿提供”，《公共选择》第 41
卷，(1983 年)第 371-386 页

[907] Jack Hirshleifer，“逆境中的经济行为”，芝加哥大学
出版社, 1987

[908] T 霍布斯，“利维坦,或共同体的物质、形式和力量”
Wealth Ecclesiasticalall 和 Civil,通常称为 Leviathan （1651 年）

[909] H Hodson，“DeepMind 和谷歌:控制人工智能的战斗”，经济学人 1848,2019 年 4 月/5 月

[910] J Ho man，“在类型强制系统上实施 RBAC”，第 13 期
年度计算机安全应用大会 (1997) 第 158–163 页

[911] G Hoglund,G McGraw，“利用软件 – 如何破解代码”，Addi
儿子韦斯利 2004

[912] G Hoglund,G McGraw，“利用在线游戏 – 大量作弊
分布式系统,Addison-Wesley 2007

[913] R Holiday，“相信我,我在说谎 媒体操纵者的自白”，简介书籍（2018 年）

[914] P Hollinger，“Barcode Babel 的单一语言”，《金融时报》7 月
25 2000

[915] C Holloway，“控制加密密钥的使用”，在计算机中
和安全 v 14 第 7 (95) 页 587–598

[916] G t Hooft，“量子力学的元胞自动机解释”，
arXiv 1405.1548, 2014

[917] N Homeier、R Horne、M Maran、D Wade，“北方有太阳风暴风险
美国电网”伦敦劳合社 (2013)

[918] BD Hong、SW Bae、YD Kim，“GUTI 重新分配揭秘:蜂窝
使用更改临时标识符进行位置跟踪”NDSS 2018

[919] N Hopkins，“Ofgem 利用国家安全法让我们沉默,吹口哨
鼓风机声称”，卫报 2018 年 9 月 17 日

[920] AL Hopkins、TB Smith、JH Lala，“FTMP – 高度可靠的故障
飞机的容错多处理器”，IEEE 会议记录 v 66 np
10（1978 年 10 月)第 1221–1240 页

[921] DI Hopper，“当局起诉成人网站”，华盛顿邮报 8 月 23 日
2000

[922] G Horn、B Preneel，“未来移动系统中的身份验证和支付”，ESORICS 98,Springer LNCS v
1485,第 277-293 页； Journal of Computer Security v 8 no 2–3 (2000) pp 183–207 期刊
版本

[923] JD 霍顿、R 哈兰、E 阿什比、RH 库珀、WF 希斯洛普、DG 尼克森，
WM Stewart,OK Ward，“级联漏洞问题”，载于计算机安全杂志 v 2 no 4 (93) pp 279-290

[924] M Horton，“历史上的司机违规时间:1 年”，Moving On Mar
20 2019

[925] 下议院卫生委员会，“电子病历”，2006-7 年会议第 6 次报告，网址为 http://www.publications.parliament。
英国/pa/cm200607/cmselect/cmhealth/422/422.pdf

[926] JD Howard，“1989-1995 年互联网安全事件分析”，博士论文（1997 年），卡内基梅隆大学，http://
www.cert. org/research/JHThesis/Start.html

[927] M Howard、D LeBlanc，“编写安全代码”，（第二版），Microsoft
出版社 2002

[928] J Hsu、M Gaboardi、A Haeberlen、S Khanna、A Narayan、BC 皮尔斯、A
Roth，“差分隐私:选择 Epsilon 的经济方法”，
中国科学基金 (2014)

[929] Q Hu、JY Yang、Q Zhang、K Liu、XJ Shen，“一种自动印章印记验证方法”，模式识别 v 28 no 8（95 年 8
月）第 251-266 页

[930] A Huang，“破解 Xbox 逆向工程简介”，
无淀粉出版社 (2003)

[931] 华为网络安全评估中心监督委员会，年度报告
(2019)

[932] G Huber，“CMW 介绍”，ACM SIGSAC v 12 no 4（94 年 10 月）pp
6–10

[933] M Hughes，“智能冰箱很酷，但在短短几年后，你可能会被厨房里一块结霜的大砖困住”，The Register
2020 年 6 月 8 日

[934] N Humphrey，“智力的社会功能”，载于乙醇的增长点
学 (1976) 第 303–317 页

[935] D Hurst 2020，“澳大利亚网络攻击:来自‘国家’的复杂攻击
基于演员 ，PM 说“卫报 2020 年 6 月 19 日

[936] A Hutchings，“在网络空间飞行:监管全球旅行欺诈”，Policing:A Journal of Policy and Practice
2018 年 9 月 10 日

[937] A Hutchings，“乘坐喷气式飞机离开:以欺诈方式获得机票的交易”，Crime, law, and social change v
70 no 4, pp 461–487

[938] A Hutchings、R Clayton、R Anderson，“关闭网站以防止
犯罪。多伦多:eCrime”eCrime 2016

[939] A Hutchings、S Pastrana、R Clayton，“取代大数据”，载于《网络犯罪的人为因素》，Rutger Leukfeldt
和 Thomas J Holt（编）
劳特利奇，2020 年

[940] N Htoo-Mosher、R Nasser、N Zunic、J Straw，“E4 ITSEC 评估
PRISM on ES/9000 Processors”，第 19 届全国信息系统安全会议（1996 年），NIST 出版的论文集，
第 1-11 页

[941] M Hypponen，“恶意软件走向移动”，《科学美国人》，2006 年 11 月，第
70–77

[942] “通信在沙漠风暴行动中的作用”,IEEE 通信杂志（特刊)第 30 期第 1 期（92 年 1 月）

[943]“在英国复制的新英格兰购物中心 ATM 骗局”,载于《信息》
Security Monitor v 9 第 7 期（94 年 6 月)第 1-2 页

[944] 信息安全监视器中的“粉红色死亡袭击美国西部蜂窝”
第 9 卷第 2 期（94 年 1 月)第 1-2 页

[945] Independent Security Evaluators Inc.，“光学媒体的内容保护”,2005 年 5 月

[946] 信息系统审计与控制协会，“信息和相关技术的控制目标”,http://www.isaca.org/cobit.htm

[947] 信息系统审计与控制协会，“ISACA 提供的考试准备材料”,网址为 http://www.isaca.org/cert1.htm

[948] “美联储称赞开放数据健康云的发布”,《信息周刊》,11 月 12 日
2013

[949] 国际原子能机构 (IAEA)，“核材料和核设施的实物保护”,INFCIRC/225/Rev.4 (1999)

[950] 《国际审计标准 315（2019 年修订版）》,International Au
审计和鉴证标准委员会,2019 年 12 月

[951] IBM， IBM 4758 PCI 密码协处理器 – CCA 基本服务参考和指南,IBM 4758-001 的 1.31 版

[952] IEEE 卡纳汉会议,http://www.carnahanconference.com/

[953] IEEE Spectrum,核安全特刊,v 37 no 3（2000 年 3 月）

[954] CC Ife、Y Shen、SJ Murdoch、G Stringhini，“恶意浪潮:网络上恶意文件传送生态系统的纵向测量”，

亚洲CCS 2019

[955] I Ilves，“为什么谷歌和苹果决定欧洲民主国家如何对抗冠状病毒？”卫报 2020 年 6 月 16 日

[956] “前电台主管‘策划’电视卡骗局”,《独立报》1998 年 2 月 17 日;另见“海盗的沉没”,周日独立
报,1998 年 3 月 1 日

[957] 信息专员办公室，“对数据使用的调查和
政治运动中的分析”,2018 年 7 月 11 日

[958] 信息专员办公室，“警方提取手机数据
英格兰和威尔士的军队”,2020 年 6 月

[959] 英特尔公司，“英特尔架构软件开发人员手册 – 第 1 卷:基本架构”,订单号 243190（1997）

[960] 英特尔公司等，“高级访问内容系统 (AACS) –
技术概述（资料性）”,2004 年 7 月 21 日

[961] 国际电工委员会，“数字音频接口”,IEC
60958,日内瓦,1989 年 2 月

[962] 国际标准化组织，“道路车辆 网络安全工程”，ISO/SAE DIS 21434，2020

[963] M Isaac、K Conger，“谷歌、Facebook 和其他公司扩大集团以确保美国大选”，纽约时报，2020 年 8 月 12 日

[964] KK Ispoglu、B AlBassam、T Jaeger、M Payer，“面向块的编程：自动化面向数据的攻击”，CCS 2018

[965] T Iwata，K Kurosawa，“OMAC：一键 CBC MAC”，Fast Software 加密 (2003) Springer LNCS v 2887 第 129–153 页

[966] R Iyengar，“Apple 将支付高达 5 亿美元的费用以了结关于放缓的诉讼 down older iPhones”，CNN，2020 年 3 月 2 日

[967] C Jackson、DR Simon、DS Tan、A Barth，“对扩展的评估 验证和画中画网络钓鱼攻击”，USEC 2007

[968] 我是杰克逊，个人通讯

[969] L Jackson，“BT 在免费电话欺诈后被迫支付退款”，载于 The 星期日电讯报 1997 年 2 月 9 日

[970] B Jacobs，“Maximator：欧洲信号情报合作，来自 荷兰视角”，情报与国家安全杂志 2020 年 4 月 7 日

[971] TN Jagatic、NA Johnson、M Jakobsson、F Menczer，“社交网络钓鱼”，在 ACM 通讯 v 50 第 10 期（2007 年 10 月)第 94–100 页

[972] G Jagpal，“数字图像中的隐写术”，本科论文，Cam 桥梁大学，1995

[973] AK Jain、L Hong、S Pankanti、R Bolle，“身份认证系统 使用指纹”，在 IEEE 会议记录 v 85 no 9（9 月 97 日)第 1365-1388 页

[974] S Jajodia、W List、G McGregor、L Strous（编辑），“诚信和内部 信息系统控制 - 第 1 卷：增加对信息系统的信心，Chapman & Hall (1997)

[975] M Jakobsson，“建模和预防网络钓鱼攻击”，金融 密码学 2005

[976] M Jakobsson、S Myers，“网络钓鱼和对策”，Wiley 2007

[977] A Jamieson，“保护数字支付 支付行业的转型”，保险商实验室（2019 年）

[978] 横向整合：实现信息的更广泛的访问模型 Dominance ，JASON Program Oce 报告 JSR-04-132，2004 年

[979] M Jay，“ACPO 的入侵者政策 承保？”，载于 Security Surveyor v 26 no 3（95 年 9 月)第 10-15 页

[980] N Je eries、C Mitchell、M Walker，“一种拟议的可信架构 第三方服务”，在密码学：策略和算法中，施普林格 LNCS v 1029 第 98–104 页

[981] F Jejdling，“爱立信移动报告”，2019 年 11 月

[982] R Jenkins，“穿墙小偷使用 MP3 播放器”，《泰晤士报》，2006 年 11 月 15 日

[983] S Jha，“网络安全知识领域”，网络安全知识体系 v 1.0 2019 年 10 月

[984] KX Jin，“让人们安全并了解冠状病毒”，Facebook，2020 年 3 月 26 日，网址为 https://about.fb.com/news/2020/03/coronavirus/

[985] D Joel、Z Berman、I Tavor、N Wexler、O Gaber、Y Stein、N Shefi、J Pool、S Urchs、DS Margulies、F Liem、JH¨anggi、LJ¨ancke、Y Assaf，“生殖器以外的性：人脑马赛克”，PNAS，2015 年 12 月，第 112 卷，第 50 页，第 15468-15473 页；首次发布于 2015 年 11 月 30 日

[986] 约翰·杨建筑师，http://www.jya.com

[987] LK John, A Acquisti, G Loewenstein，“飞机上的陌生人：泄露敏感信息的情境依赖意愿”，消费者研究杂志 v 37 no 5 (2011) pp 858-873

[988] K Johnson，“少一件值得相信的事情：假取款机的欺诈”，纽约时报 1993 年 5 月 13 日，第 1 页

[989] RG Johnston，ARE Garcia，“安全封条的漏洞评估”，《安全管理杂志》第 20 期第 1 期（97 年 6 月）第 15-27 页；备份于 http://www.cl.cam.ac.uk/~rja14/preprints/Johnston/

[990] RV Jones，“最秘密的战争”，华兹华斯出版社（1978，1998）

[991] DW Jones，B Simons，“破碎的选票 在电子时代你的选票会算数吗？”斯坦福大学 (2012)

[992] RV Jones，“对情报的思考”，章鱼（1989）

[993] J Jonsson、B Kaliski，“公钥加密标准 (PKCS) #1：RSA 加密规范版本 2.1”，RFC 3447

[994] A Jøsang, K Johannesen，“模拟电话接入中的认证网络”，载于 Pragocrypt 96，CTU 出版社，第 324-336 页

[995] Dorothy Judd v Citibank, 435 NYS, 2d series, pp 210–212, 107 Misc.2d 526

[996] A Juels，RL Rivest，“Honeywords：使密码破解可检测”，IEEE SIGSAC 2013

[997] MY Jung，“生物识别市场和行业概览”，IBG，2005 年 12 月 8 日

[998] M Kaczorowski、B Baker，“BeyondProd：谷歌如何从基于边界的安全转向云原生安全”，谷歌云博客，2019 年 12 月 17 日

[999] P Kafka，“专家解释 Facebook 的政治广告问题”Vox，2019 年 12 月 10 日

[1000] B Kahle，“图书馆一直在将旧书带给数字学习者：四出版商起诉阻止它”，互联网档案博客，2020 年 7 月 22 日

[1001] D Kahn，“密码破译者”，麦克米伦 (1967)

[1002] D Kahn，“抓住谜团”，Houghton Mi in（1991）；国际标准书号 0-395-42739-8个

[1003] D Kahn，“冷战中的苏联 Comint”，Cryptologia v XXII no 1（98 年 1 月）第 1-24 页

[1004] D Kahneman，“有限理性地图：直觉视角
判断与选择”，诺贝尔奖演讲，2002

[1005] D Kahneman， Thinking, Fast and Slow Penguin 2012

[1006] L Kahney，“联邦调查局想要 iPhone 的后门。蒂姆库克说不”，连线 2019 年 4 月 16 日

[1007] AM Kakhki、S Jero、D Cho nes、C Nita-Rotaru，《失恋》，“花了很长时间
看看 QUIC”，IMC 2017

[1008] B Kaliski，“PKCS #7：加密消息语法版本 1.5”，RFC
2315

[1009] JB Kam，GI Davida，“替代排列的结构化设计
加密网络”，在安全计算基础，学术
按 (1978)

[1010] M Kam、G Fielding、R Conn，“专业文件审查员的作家鉴定”，《法医学杂志》第 42 卷（1997
年）第 778-786 页

[1011] M Kam、G Fielding、R Conn，“货币激励对非专业人员在文件检查能力测试中的表现的影响”，
载于
法医学杂志 v 43 (1998) pp 1000–1004

[1012] MH Kang，IS Moskowitz，“用于快速、可靠、安全通信的泵”，第一届 ACM CCS，1993 年，第
118-129 页

通过数据复制实现安全：SINTRA 原型”，第 17 届全国计算机安全会议（1994 年），第 77-87
页

[1013] MH Kang，IS Moskowitz，DC Lee，“网络泵”，在 IEEE Transac
软件工程 v 22 第 5 期（96 年 5 月）第 329–338 页

[1014] MH Kang，IS Moskowitz，B Montrose，J Parsonese，“两个案例研究
NRL 泵原型”，第 12 届 ACSAC，1996 年，第 32-43 页

[1015] MH Kang，IS Moskowitz，S Chincheck，“泵：十年的秘密
乐趣”，第 21 届 ACSAC（2005 年）

[1016] CS Kaplan，“隐私计划可能引发 O 辩论”，纽约时报
（2000 年 7 月 28 日）

[1017] ED Kaplan，C hegarty，“了解 GPS – 原理和应用”，
Artech House（第二版，2006 年）

[1018] PA Karger、VA Austell、DC Toll，“结合保密性和完整性的新强制性安全策略”，IBM 研究报
告 RC 21717 (97406) 2000 年 3 月 15 日

[1019] PA Karger，RR Schell，“三十年后”：Multics 的教训
安全评估”，ACSAC 2002 第 119-126 页

[1020] F Kasiski, Die Geheimschriften und die Dechi rier-Kunst , Mittler &
孙,柏林 (1863)

[1021] “KASUMI 规范”,ETSI/SAGE v 1 (23/12/1999),位于 http://www.
etsi.org/dvbandca/

[1022] J Katz、Y Lindell，“现代密码学导论”,CRC 出版社（第二版,2015 年）

[1023] S Katzenbeisser,FAP Petitcolas，“信息隐藏 – 技术
隐写术和数字水印”,Artech House (2000)

[1024] A Katwala，“创造完美测谎仪的竞赛 以及
成功”卫报 2019 年 9 月 5 日

[1025] C Kaufman、R Perlman、M Speciner，“网络安全 – 私人通信”
公共世界中的信息化”,Prentice Hall 1995

[1026] EM Kearns、AE Betus、AF Lemieux，“为什么有些恐怖袭击比其他袭击更受媒体关注？”正义季刊，
2018

[1027] DT Keitkemper、SF Platek、KA Wolnik，“DNA 与指纹,在 Jour
法医学年鉴 v 40 (1995) p 534

[1028] MB Kelley，“奥巴马政府承认针对伊朗的网络攻击是
美以联合进攻的一部分”,商业内幕,2012 年 6 月 1 日

[1029] GC Kelling、C Coles，“修复破损的窗户：恢复我们社区的秩序并减少犯罪”,Martin Kessler Books
（1996 年）

[1030] H Kelly，“Facebook、Twitter 因发布包含冠状病毒错误信息的帖子而对特朗普进行处罚”,华盛顿
邮报,2020 年 8 月 7 日

[1031] L Kelly, T Young, in Computing 2007 年 1 月 25 日;在 http://www.vnunet.com/
computing/news/2173365/uk-firms-naive-usb-stick

[1032] J Kelsey、B Schneier、D Wagner，“协议交互和选择协议攻击”,载于《安全协议》 第五届国际会
议论文集
研讨会 (1997) Springer LNCS v 1361 第 91–104 页

[1033] J Kelsey、B Schneier、D Wagner、C Hall，“对伪随机数生成器的密码分析攻击”,第五届国际快速
研讨会
软件加密 (1998),Springer LNCS v 1372 第 168–188 页

[1034] J Kelsey、B Schneier、D Wagner、C Hall，“侧信道密码分析
产品密码”,ESORICS 98,Springer LNCS v 1485,第 97-110 页

[1035] R Kemp、N Towell、G Pike，“眼见为实：照片、信用卡和欺诈”,Applied Cognitive Psychology v
11 no 3 (1997) pp 211–222

[1036] R Kemmerer，“共享资源矩阵方法论：一种方法
识别存储和定时通道”,IEEE Transactions on Computer Systems v 1 no 3 (1983) pp 256–
277

[1037] MG Kendall,B Babington-Smith，“随机性和随机抽样
Numbers”,第 1 部分,皇家统计学会杂志 v 101,第 147-166 页； 《皇家统计学会期刊增刊》第 2
部分,第 6 卷第 1 期,第 51-61 页

[1038] T Kendall，“色情、强奸和互联网”，软件和互联网行业经济学（Softint 2007），http://people.clemson.edu/~tkendal/internetcrime.pdf

[1039] ST Kent，MI Millett， 谁去那里？通过隐私的角度进行身份验证”，国家研究委员会 2003 年；在 http://www.nap. edu/catalog.php?record_id=10656

[1040] JO Kephardt，SR White，“计算机病毒流行率的测量和建模”，载于 1993 年 IEEE 安全和隐私研讨会论文集第 2-15 页

[1041] JO Kephardt，SR White，DM Chess，“计算机病毒流行病学”，IEEE Spectrum v 30 no 5（93 年 5 月）第 27-29 页

[1042] A Kerckhos，“La Cryptographie Militaire”，载于 Journal des Sciences Mil itaires，1883 年 1 月 9 日，第 5-38 页； http://www.cl.cam.ac.uk/users/fapp2/kerckhoffs/

[1043] D Kesdogan、H Federrath、A Jerichow，“位置管理策略增加移动通信中的隐私”，第 12 届国际信息安全会议（1996 年）第 39-48 页

[1044] LM Khan，“亚马逊的反垄断悖论”，耶鲁法律杂志 v 126，第 710 页–805 (2017)

[1045] J Kieselbach, JP Ziegler, “Mit der Axt”, Der Spiegel 2019 年 11 月 25 日

[1046] JD Kilgallin 2020，“保护物联网设备的 RSA 密钥证书”，https://info.keyfactor.com/factoring-rsa-keys-in-the-iot-era，2020 年 12 月 18 日

[1047] J Kilian、P Rogaway，“如何保护 DES 免受穷举密钥搜索”，密码学进展 – Crypto 96 Springer LNCS v 1109 pp 252–267

[1048] YG Kim, R Daly, Jeremie Kim, C Fallin, JH Lee, DH Lee, C 威尔克森，K Lai O Mutlu，“在不访问内存的情况下翻转内存中的位：一个 DRAM 干扰错误的实验研究”，ISCA 2014

[1049] T Kinder，“监管机构概述了拆分四大会计师事务所的计划”，金融时报 2020 年 2 月 27 日

[1050] T Kinder，“四大被告知要在 10 月之前概述审计拆分计划”，金融时报，2020 年 7 月 6 日

[1051] T Kinder、D McCrum，“安永对威胁其全球声誉的三起审计案件进行灭火”，《金融时报》，2020 年 6 月 8 日

[1052] J King，“Bolero 可信第三方服务的实际应用”，in Computer Fraud and Security Bulletin（95 年 7 月）第 12-15 页

[1053] S Kirchgaessner，“Je Bezos hack：亚马逊老板的手机‘被沙特王储黑了’”，卫报，2020 年 1 月 22 日

[1054] S Kirchgaessner，“揭露：沙特人涉嫌在美国”，卫报 2020 年 3 月 29 日

[1055] N Kitroe ，“波音低估了 737 Max 上的驾驶舱混乱，NTSB 说”，纽约时报，2019 年 9 月 26 日

[1056] DV Klein，“挫败饼干； Unix 的调查和改进
密码安全”，USENIX 安全研讨会论文集（1990 年）

[1057] P Klemperer，“拍卖：理论与实践 图卢兹经济学讲座”，普林斯顿 2004 年；在 http://
www.nuffield.ox.ac.uk/users/klemperer/VirtualBook/VBCrevisedv2.asp

[1058] RL Klevans、RD Rodman，“语音识别”，Artech House（1997 年）

[1059] HM Kluepfel，“保护地球村及其资源：互连信令系统#7 电信网络的基线安全”，First ACM CCS
(1993) pp 195–212； IEEE Communications Magazine v 32 no 9（9 月 94 日）第 82-89 页
的更高版本

[1060] N Koblitz，“数论和密码学课程”，Springer Grad
uate 数学课本 no 114 (1987)

[1061] N Koblitz，A Menezes，“对‘可证明的安全性’的另一种看法”，在期刊中
密码学 v 20 no 1 (2007) pp 3–37

[1062] ER Koch, J Sperber, Die Datenmafia , Rohwolt Verlag (1995)

[1063] M Kochanski，“数据不安全设备调查”，Cryptologia v IX no 1 pp 1-15

[1064] P Kocher，“对 Die-Hellman 实施的定时攻击，RSA，
DSS 和其他系统”，密码学进展 – Crypto 96 Springer
LNCS v 1109 第 104–113 页

[1065] P Kocher，“差分功率分析”，密码学进展 – 密码学
99 Springer LNCS v 1666 第 388–397 页

[1066] P Kocher，“获得功率分析和相关攻击对策保证的设计和验证策略”，夏威夷 FIPS 物理安全研讨
会，2005 年；在 http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/
papers/physecpaper09.pdf

[1067] P Kocher、J Ja e、B Jun、P Rohatgi，“差分功率分析简介”，密码工程杂志 (2011) v 1 pp 5–27

[1068] P Kocher、D Genkin、D Gruss、W Haas、M Hamburg、M Lipp、S Mangard、T Prescher、M
Schwarz、Y Yarom，“幽灵攻击：利用投机执行”，arXiv:1801.01203 2018 年 1 月 3 日

[1069] P Kocher，J Horn，A Fogh，D Genkin，D Gruss，W Haas，M Hamburg，
M Lipp、S Mangard、T Prescher、M Schwarz、Yuval Yarom，“幽灵攻击：利用推测执行”，IEEE
安全与隐私研讨会 2019

[1070] J Koebler，“为什么美国农民用
乌克兰固件”，Vice，2017 年 3 月 21 日

[1071] J Koebler，“黑客绕过 GE 荒谬的冰箱 DRM”，Vice Jul
12 2020

[1072] BI Koerner，“震惊美国政府的网络攻击内幕”，
连线 2016 年 10 月 23 日

[1073] J Koetsier，“Apple 刚刚削弱了 IDFA，给一个价值 800 亿美元的行业带来了损失
进入剧变”，福布斯 2020 年 6 月 24 日

[1074] A Kofman，“数字监狱:电子监控如何驱动被告
Into Debt”,纽约时报杂志,2019 年 7 月 3 日

[1075] T Kohno、A Stubblefield、AD Rubin、DS Wallach，“电子投票系统分析”,约翰霍普金斯 TR
2003-19;也发表在 IEEE
安全和隐私研讨会 (2004)

[1076] S Kokolakis，“隐私态度和隐私行为”,计算机和
安全 v 64 (2017)

[1077] S Kokolakis、D Gritzalis、S Katsikas，“健康的通用安全策略
信息系统”,《健康信息学杂志》第 4 卷第 3-4 期（1998 年 12 月)第 184-195 页

[1078] OK¨ommerling,MG Kuhn，“防篡改智能卡处理器的设计原则”,Usenix 智能卡技术研讨会，
（1999)第 9-20 页

[1079] OK¨ommerling, FK¨ommerling，“集成电路的防篡改封装”,美国专利 7,005,733,2000 年 12
月 26 日

[1080] A Kondi,R Davis，“国防部的软件加密”,第 20 届国家
信息系统安全会议 NIST (1997) pp 543–554

[1081] 库特先生，“在 Ennetcom 之后,荷兰警方逮捕了另一家荷兰公司 PGP Safe,原因是其涉嫌向（主
要是？)黑社会提供加密电话”,Mattijs R. Koot 的笔记本,2017 年 5 月 14 日

[1082] C Kopp，“电磁炸弹 电子大规模杀伤性武器”,网址为 https://web.archive.org/web/
20120218213215/http://www.abovetopsecret.com/forum/thread59555/pg1

[1083] DP Kormann,AD Rubin，“护照单点登录协议的风险”,计算机网络（2000 年 7 月）;在 http://
avirubin.com/vita.html

[1084] K Korosec，“大众解雇入狱的奥迪 CEO 鲁珀特施泰德”,Techcrunch 10 月 2 日
2018

[1085] K Koscher、A Czeskis、F Roesner、S Patel、T Kohno、S Checkoway、D Mc
Coy、B Kantor、D Anderson、H Shacham、S Savage，“现代汽车的实验安全分析”2010 年 IEEE
安全和安全研讨会
隐私第 447-462 页

[1086] M Kosinski、D Stillwell、T Graepel，“私人特征和属性可以从人类行为的数字记录中预测”，
PNAS,2013 年 4 月 9 日,第 110 卷第 15 期,第 5802-5805 页

[1087] M Kotadia，“花旗银行电子邮件看起来很可疑:顾问”,Zdnet,2006 年 11 月 9 日

[1088] KPHO，“被鸡奸的前麦当劳员工赢得 610 万美元”,KPHO,10 月 6 日
2007年;在 http://www.kpho.com/news/14277937/detail.html

[1089] H Krawczyk、M Bellare、R Canetti， HMAC:消息的键控散列
身份验证”,RFC 2104（1997 年 2 月）

[1090] B Krebs，“风暴蠕虫到底有多严重？”,载于《华盛顿邮报》
2007 年 10 月 1 日

[1091] B Krebs，“Salesforce.com 承认数据丢失”,在华盛顿
2007 年 11 月 6 日后

[1092] B Krebs，“打破 SIM 卡交换器和 SIM 卡交换神话” Krebs on Security
2018 年 11 月 7 日

[1093] B Krebs，“专家:IT 外包巨头 Wipro 的违规行为” Krebs on Security 2019 年 4 月 15 日

[1094] B Krebs，“墨西哥的罗马尼亚 Skimmer Gang 被 KrebsOnSecurity 盗走 12 亿美元” Krebs on Security 2020 年 6 月 3 日

[1095] S Krempl，“Lauschangri am Geldautomaten”，载于 Der Spiegel，1999 年 1 月 8 日;在 http://web.archive.org/web/20001031024042/http://www.spiegel。 de/netzwelt/technologie/0,1518,13731,00.html

[1096] S Krishna，“让我们通过密码地狱的人后悔一切”，
Engadget 2017 年 8 月 8 日

[1097] HM Kriz，“Phreaking 被法国电信总局认可”，在 Chaos Digest 1.03（93 年 1 月）

[1098] A Krizhevsky、I Sutskever、GE Hinton，“使用深度卷积神经网络的 ImageNet 分类”NIPS 2012 第 1097-1105 页

[1099] I Krsul，EH Spa ord，“作者身份分析:识别程序的作者”，载于 Computers and Security v 16 no 3 (1996) pp 233–257

[1100] H Kuchler，“我们能否相信谷歌拥有我们的健康数据？”，《金融时报》，2020 年 1 月 20 日

[1101] D Kugler，“‘中间人’对蓝牙的攻击”，载于 金融密码学 2004，
Springer LNCS v 2742 第 149-161 页

[1102] MG Kuhn，“对总线加密安全微控制器 DS5002FP 的密码指令搜索攻击”，IEEE Transactions on Computers v 47 no 10（1998 年 10 月)第 1153-1157 页

[1103] MG Kuhn，IEEE 安全与隐私研讨会（2002 年)中的“CRT 显示器的光学时域窃听风险”

[1104] MG Kuhn，“平板显示器的电磁窃听风险”，PET 2004，网址为 http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf

[1105] MG Kuhn，RJ Anderson，“软风暴:使用电磁辐射的隐藏数据传输”，In Information Hiding (1998)，Springer
LNCS v 1525 第 126–143 页

[1106] R Kuhn、P Edfors、V Howard、C Caputo、TS Philips，“改善公共
开放环境中的交换网络安全”，计算机，1993 年 8 月，第 32-35 页

[1107] M Kumar，“新的 SIM 卡缺陷让黑客劫持任何电话
发送短信”，黑客新闻，2019 年 9 月 12 日

[1108] S Kumar、C Paar、J Pelzl、G Pfei er、M Schimmler，“用
COPACOBANA – 成本优化的并行密码破解器”，CHES 2006

[1109] D Kundaliya，“Android 设备正越来越多地成为联合国的目标
可删除的广告软件，研究人员警告 ，计算 2020 年 7 月 7 日

[1110] L Kuo，“中国监控公司追踪 250 万新疆居民”，
在卫报 2019 年 2 月 18 日

[1111] J Kuo，“Storm Drain”，反恶意软件工程团队博客，2007 年 9 月 20 日，网址为 http://blogs.technet.com/
antimalware/default.aspx

[1112] GD Kutz、G Aloise、JW Cooney，“核安全 NRC 为加强密封放射源许可程序而采取的行动
无效”，GAO 报告 GAO-07-1038T，2007 年 7 月 12 日

[1113] K Kwiatkowski，“五角大楼的新文件 高级军方
Ocer 揭露国防部极端分子如何压制信息并歪曲真相以驱使国家走向战争”，沙龙，2004 年 3 月 10 日

[1114] A Kwong, D Genkin, D Gruss, Y Yarom, “RAMBleed: Reading Bits in
无需访问的内存”，IEEE 安全与隐私研讨会（2020 年）

[1115] “用于 Win95/NT 的 L0phtCrack 2.52”，位于 http://www.l0pht.com/l0phtcrack/

[1116] J Lacy、SR Quackenbush、A Reibman、JH Snyder，“知识产权保护系统和数字水印”，信息隐藏
(1998), Springer LNCS v 1525 第 158-168 页

[1117] RJ Lackey，DW Upmal，“Speakeasy：军事软件无线电”，IEEE
Communications Magazine v 33 no 5（95 年 5 月）第 56-61 页

[1118] F Lambert，“自动驾驶仪上的特斯拉司机承认在撞上警车时看了一部电影”Elektrek，2020 年 8 月 26 日

[1119] F Lambert，“The Big Tesla Hack：一名黑客获得了对整个车队的控制权，但幸运的是他是个好人”
Elektrek，2020 年 8 月 27 日

[1120] G Lambourne，“指纹故事”，哈拉普 (1984)

[1121] L Lamont，“真正的乐透赢家是……收银台的那个人”，
悉尼先驱晨报，2007 年 5 月 3 日

[1122] L Lamport，“分布式系统中的时间、时钟和事件排序
系统”，ACM 通讯 v 21 no 7（1978 年 7 月）第 558-565 页

[1123] L Lamport，电子邮件消息于 12:23:29 发送至 DEC SRC 公告板
PDT，1987 年 5 月 28 日。链接号 75，

[1124] L Lamport、R Shostak、M Pease，“拜占庭将军问题”，载于
ACM 编程语言和系统事务 v 4 no 3 (1982) pp 382–401

[1125] B Lampson，“关于限制问题的注释”，ACM 通讯 v 16 no 10（1973 年 10 月）第 613-615 页

[1126] S Landau, A Lubin，“检查异常，解释价值：美国自由法案的元数据计划是否应该扩展？”，《哈佛国家安
全杂志》第 11 卷，第 308-358 页（2020 年）

[1127] R Landley，“DIVX 之子：DVD 复制控制”，Motley Fool，http://www.
fool.com/portfolios/rulemaker/2000/rulemaker000127.htm

[1128] P Landrock，“BOLERO 中的角色和责任”，TEDIS EDI
可信第三方研讨会（1995 年）

[1129] CE Landwehr, AR Bull, JP McDermott, WS Choi, A Taxonomy of
计算机程序安全缺陷，并举例，美国海军报告
NRL/FR/5542–93-9591 1993 年 11 月 19 日

[1130] T Lavin，“‘学习编码”的恶臭，右翼起源”新
共和国 2019 年 2 月 1 日

[1131] J Leake，“塞拉菲尔德的工人使用伪造的通行证”，《星期日泰晤士报》4 月
2 2000

[1132] S LeBlanc, KE Register, Constant Battles: Why We Fight , 圣马丁
(2003)

[1133] D Lee，“黑莓修改为‘帮助贩毒集团’”，BBC 新闻，3 月 16 日
2018

[1134] DY Lee、DH Jung、IT Fang、CCTsai、RA Popa，“对 O 芯片的攻击
Hardware Memory Enclaves Using the Memory Bus” IEEE 研讨会
安全和隐私 (2000)

[1135] HC Lee，RE Guesslen（编辑），“指纹技术的进步”，Elsevier
(1991)

[1136] K Lee、B Kaiser、J Meyer、A Nayaranan，“无线网络的实证研究
SIM 交换的运营商身份验证”，CITP，普林斯顿，2020 年 1 月 10 日

[1137] W Lee，“恶意软件和攻击技术知识领域”，网络安全
知识体系，v 1.0 2019 年 10 月

[1138] D Leigh，“打击窃取个人数据的公司”，载于《卫报》
2006 年 11 月 15 日

[1139] D Leloup，M Untersinger，“评论 les services de renseignement font la chasse aux
employ´es des t´el´ecoms”，Le Monde 2016 年 12 月 8 日

[1140] AK Lenstra、JP Hughes、M Augier、JW Bos、T Kleinjung、C Wachter，“Ron 错了，Whit 是对的”
IACR ePrint 2012/064

[1141] AK Lenstra，HW Lenstra，“数场筛的发展”，
施普林格数学讲义 v 1554 (1993)

[1142] D Leppard, P Nuki, “BA sta sell fake duty-free goods”, in Sunday Times
1999 年 9 月 12 日

[1143] J Lerner，J Tirole，“论坛购物模型”，美国经济
评论 v 96 no 4 pp 1091–1113 (2006)

[1144] L Lessig，“网络空间的代码和其他法律”，基础书籍（2000）； 代码：
2.0 版，基础书籍（2006 年）；在 https://www.lessig.org/

[1145] L Lessig，“自由文化：创造力的本质和未来”，Penguin
(2005)；在 https://www.lessig.org/

[1146] G Leurant、T Peyrin，“SHA-1 是一个混乱：第一次选择前缀冲突和对 PGP 信任网络的应用”，IACR
预印本 2020-014，2020 年 1 月 7 日

[1147] E莱弗里特, 定量评估和可视化控制系统
tack Surfaces ,剑桥大学哲学硕士论文,2011 年

[1148] E Leverett、R Clayton、R Anderson“标准化和认证
物联网中的安全、保障和隐私”,欧盟委员会 (2017)

[1149] NG Leveson,“Safeware – 系统安全和计算机”,Addison-Wesley (1995),特别是附录“医
疗设备 – Therac-25”

[1150] NG Leveson,“复杂的、基于控制的改进设计过程
使用 STPA 和概念架构的系统”,麻省理工学院,2020 年 1 月 11 日

[1151] S Levitt,SJ Dubner,“恶魔经济学:流氓经济学家探索隐藏
万物的一面”,威廉·莫罗 (William Morrow),2005 年

[1152] HM Levy,“基于能力的计算机系统”,数字出版社,1984 年

[1153] I Levy, C Robinson,“更知情的特殊访问原则
辩论”,Lawfare 博客,2018 年 11 月 29 日

[1154] K Levy, B Schneier,“亲密关系中的隐私威胁”,Journal of
网络安全 v 6 no 1 (2020)

[1155] A Lewcock,“体力”,《计算机商业评论》第 6 期第 2 期(98 年 2 月)第 24-27 页

[1156] O Lewis,“Re: News: London nailbomber used the Net”,发布到 ukcrypto 邮件列表,
2000 年 6 月 5 日,存档于 http://www.chiark.greenend.org。英国/邮递员/listinfo/
ukcrypto

[1157] Lexmark International, Inc. 诉 Static Control Components, Inc.,美国上诉法院(第六巡
回法院),2004 年 10 月 26 日,网址为 www.eff.org/legal/cases/Lexmark_v_Static_Control/
20041026_Ruling.pdf

[1158] J Leyden,“泰国警方破获信用卡窃听骗局”,The Reg ister 2006 年 8 月 4 日,http://
www.theregister.co.uk/2006/08/04/thai_wiretap_scam/

[1159] J Leyden,“黑客入侵 TK Maxx”,载于 The Register 2007 年 1 月 19 日;在
http://www.theregister.co.uk/2007/01/19/tjx_hack_alert/

[1160] J Leyden,“意大利在全球窃听联盟中名列前茅”,载于 The Register,2007 年 3 月 7 日;
在 http://www.theregister.co.uk/2007/03/07/wiretap_trends_ss8/

[1161] J Leyden,“联邦调查局告诉他们需要网络邮件授权”,2007 年 6 月 19 日在 The Register
中;在 http://www.theregister.co.uk/2007/06/19/webmail_wiretaps_appeal/

[1162] MY Li, Y Meng, JY Liu, HJ Zhu, XH Liang, Y Liu, N Ruan,“当csi遇到公共wifi:通过wifi信号
推断你的手机密码”,
CCS 2016 第 1068–1079 页

[1163] LS Liebst、R Philpot、P Poder、MR Lindegaard,“乐于助人的旁观者:
来自闭路电视捕捉到的公共冲突的当前证据”,发现社会
2019 年 6 月 5 日

[1164] H Lin,“五角大楼的理论混乱和文化障碍
关于信息和网络操作”,Lawfare 博客,2020 年 3 月 27 日

[1165] R Linde，“操作系统渗透”，全国计算机会议，
AFIPS (1975) 第 361–368 页

[1166] David Lindenmayer，Ben Scheele“不要发表”，科学杂志 v
356 号 6340（2017 年 5 月 26 日)第 800-801 页

[1167] JPMG Linnartz，“基于嵌入的复制控制的‘票’概念
ded Signalling”，ESORICS 98，Springer LNCS 1485，第 257-274 页

[1168] JPMG Linnartz，M van Dijk，“针对敏感度攻击的分析
图像中的电子水印”，[142] 第 258–272 页

[1169] J Linsky 等人，“蓝牙 简单配对白皮书”，来自 www.
蓝牙网站

[1170] S Liao “间谍软件应用程序滥用 iOS 企业证书来跟踪目标” The
边缘，2019 年 4 月 8 日

[1171] SB Lipner，“橙皮书的生与死”，《美国年鉴》
计算史 (2015)

[1172] M Lipp、M Schwarz、D Gruss、T Prescher、W Haas、S Mangard、P Kocher、D Genkin、Y
Yarom、M Hamburg，“Meltdown”，arXiv:1801.01207 2018 年 1 月 3 日

[1173] A Liptak，“据报道，黑客使用 NSA 开发的工具来攻击
巴尔的摩的计算机系统”，The Verge，2019 年 5 月 25 日

[1174] D Litchfield，C Anley，J Heasman，B Grindlay，“数据库黑客”
手册：捍卫数据库服务器，Wiley 2005

[1175] B Littlewood，“预测软件可靠性”，在 Philosophical Transac
伦敦皇家学会的 tions A327 (1989), pp 513–527

[1176] FF Liu，Y Yarom，Q Ge，G Heiser，RB Lee，“末级缓存侧通道
Attacks are Practical” IEEE 安全与隐私研讨会 2015

[1177] XY Liu, Z Zhou, WR Diao, Z Li, KH Zhang，“当善变恶时：
智能手表的击键推理，ACM CCS 2015 第 1273–1285 页

[1178] WF Lloyd，“关于人口支票的两个讲座”，牛津大学
按 (1833)

[1179] C Loch, A DeMeyer, MT Pich, 管理未知 , Wiley (2006)

[1180] L Loeb，“安全电子交易 – 介绍和技术参考”，Artech House（1998 年）

[1181] N Lomas，“有针对性的广告为在线出版商提供很少的额外价值，研究
建议”，Techcrunch 2019 年 5 月 31 日

[1182] 伦敦政治经济学院，“身份项目 对英国身份证法案及其影响的评估”，2005 年，http://
eprints.lse.ac.uk/id/eprint/29117

[1183] J Long，Google 黑客数据库，网址为 http://johnny.ihackstuff.com/
ghdb.php

[1184] D Longley，S Rigby，“自动搜索关键人物的安全漏洞
agement”，Computers & Security v 11（1992 年 3 月)第 75-89 页

[1185] HC Longuet-Higgins、K Prazdny，“移动视网膜图像的解释”，Proc Roy Soc B v 208 (1980) pp 385–397

[1186] PA Loscocco、SD Smalley、PA Muckelbauer、RC Taylor、SJ Turner、JF Farrell，“失败的必然性：安全性的错误假设现代计算环境”，在第20届国家信息系统安全会议，NIST 出版的论文集（1998 年第 303-314 页）

[1187] PA Loscocco、SD Smalley，“将对安全策略的灵活支持集成到 Linux 操作系统中”，在 FREENIX Track 会议记录中：2001 年 USENIX 年度技术会议 (FREENIX 01)（2001 年 6 月）。另请参阅 NSA SELinux 站点：http://www.nsa.gov/selinux

[1188] JR Lott，“更多的枪支，更少的犯罪：了解犯罪和枪支管制”法律，芝加哥大学出版社 2000

[1189] J Loughry, DA Umphress，“光学发射的信息泄漏”，ACM 信息和系统安全交易 v 5 no 3（2002 年 8 月）第 262-289 页

[1190] B Lovejoy，“Apple 因拒绝帮助 iTunes 礼品卡诈骗受害者而被起诉”，9to5Mac，2020 年 7 月 20 日

[1191] WW Lowrance，“隐私与健康研究”，向美国国务卿报告卫生与公共服务部（1997 年 5 月）

[1192] J Luk`a ∨ s、J Fridrich、M Goljan，“图像的数字‘子弹划痕’”，ICIP 05；在 http://www.ws.binghamton.edu/fridrich/Research/ICIP05.pdf

[1193] I Lunden，“Apple 在法国因反竞争销售被罚款 1.2B 美元实践” TechCrunch 2020 年 3 月 16 日

[1194] JM Luo、Y Cao、R Barzilay，“通过最小成本流进行神经解密：从乌加里特到线性 B”，arXiv 1906.06718（2019 年 6 月 16 日）

[1195] HT Luong、HD Phan、DV Chu、VQ Nguyen、KT Le、Luc、LT Hoang，“了解越南的网络犯罪：从前导点规定到Legislative System and Law Enforcement，国际网络杂志犯罪学 (2019) 第 290–308 页

[1196] J Lynch，“HART：国土安全部庞大的新数据库将包括人脸识别、DNA 和人们的“非显而易见的关系”” 远征军2018 年 6 月 7 日

[1197] B Lysyk，“安大略省审计长年度报告”，2014 年

[1198] M Lyu，“软件可靠性工程”，IEEE 计算机学会出版社 (1995)

[1199] E MacAskill、J Borger、N Hopkins、N Davies、J Ball，“GCHQ 利用光纤电缆秘密访问世界通信”，2013 年 6 月 21 日

[1200] R Maclean，“马里总统在军中被捕后辞职政变”，纽约时报，2020 年 8 月 18 日

[1201] D Mackenzie，“机械化证明 计算、风险和信任”，麻省理工学院出版社 2001年

[1202] D Mackett，“航空公司安全飞行员”，Hot Air，2007 年 7 月 16 日，http://hotair.com/archives/2007/07/16/a-pilot-on-airline-security/

[1203] B Macq，“特刊 多媒体信息的识别和保护”，IEEE 会议记录 v 87 no 7（1999 年 7 月）

[1204] M Madden、L Rainie，“美国人对隐私、安全和隐私的态度监视”，皮尤研究中心，2015 年 5 月 20 日

[1205] W Madsen，“Crypto AG：美国国家安全局的特洛伊木马妓女？”，载于《秘密行动季刊》（1998 年冬季），网址为 http://www.mediafilter.org/caq/cryptogate/

[1206] W Madsen，“政府支持的计算机战和破坏”，载于计算机与安全 v 11 (1991) 第 233–236 页

[1207] M Magee，“HP 喷墨墨盒具有内置的有效期 – Carly 狡猾的消耗品计划”，The Inquirer，2003 年 4 月 29 日，网址为 http://www. theinquirer.net/?article=9220

[1208] K Maguire，《卫报》中的“为名人提供 o 垃圾箱的揭发者”2000 年 7 月 27 日

[1209] S Maguire，“调试开发过程”，微软出版社（1994 年）

[1210] F Main，“您的电话记录正在出售”，芝加哥太阳时报，2006 年 1 月 5 日

[1211] D Maio、D Maltoni，“指纹中的直接灰度细节检测”，IEEE 模式分析和机器智能交易 v 19 no 1（97 年 1 月）第 27-40 页

[1212] S Makkaveev，“Pwn2Own Qualcomm compute DSP for fun and profit”，De fCon 2020；同样在 CheckPoint 博客上，“Qual comm^aA Zs Snapdragon 芯片上的 400 多个漏洞威胁手机^a A Z 全球可用性”，2020 年 8 月 7 日

[1213] D Maltoni、D Maio、AK Jain、S Prabhakar，“指纹识别手册”nition , Springer-Verlag New York, 2003

[1214] S Mangard、E Oswald、T Popp，“功率分析攻击 揭示智能卡的秘密，Springer 2007

[1215] G Manaugh，“全明星珠宝大盗的兴衰”，The大西洋 2019 年 12 月 17 日

[1216] F Manjoo，“计算机病毒 25 岁”，沙龙，2007 年 7 月 12 日

[1217] T Mansfield、G Kelly、D Chandler、J Kane，“生物识别产品测试最终报告”，第 1.0 期，2001 年 3 月 19 日，国家物理实验室；在 www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf

[1218] W Marczak、J Dalek、S McKune、A Senft、J Scott-Railton、R Deibert，“BAD TRAFFIC Sandvine 的 PacketLogic 设备用于在土耳其部署政府间谍软件并将埃及用户重定向到 Aliate Ads？”，Munk 学校，多伦多2018 年 3 月 9 日

[1219] W Marczak、J Scott-Railton，“价值百万美元的持不同政见者 NSO Group 的 iPhone 零日漏洞用于对付阿联酋人权捍卫者”，多伦多大学 https://citizenlab.ca/2016/08/million-dollar-持不同政见者-iphone-零日-nso-group-uae/ 2016 年 8 月 24 日

[1220] D Margolis、M Risher、B Ramakrishnan、A Brotman、J Jones，“SMTP MTA 严格的传输安全 (MTA-STS)”RFC 8461（2018 年 9 月）

[1221] 马里诺，“Vergecast：Facebook 准备好迎接 2020 年了吗？”，The Verge 8 月 27 日 2019

[1222] J Marko ，“睡鼠说的话：60 年代反主流文化如何塑造个人电脑”，Viking Adult（2005 年）

[1223] J Marko ，“大型间谍系统在 103 个国家掠夺计算机”，纽约时代 2009 年 3 月 28 日

[1224] L Marks，在丝绸和氰化物之间 1941-1945 年的密码制造者战争，哈珀柯林斯 (1998)

[1225] P Marks，“用音频技术开锁”，通讯 ACM，2020 年 8 月 13 日

[1226] M Marlinspike，“技术预览：Signal 的私人联系人发现”，Signal 博客，2017 年 9 月 26 日

[1227] M Marlinspike、T Perrin，“X3DH 密钥协议协议”，https://signal.org/docs/specifications/ 2016 年 11 月 4 日

[1228] V Marotta、V Abhishek、A Acquisti，“在线跟踪和出版商收入：实证分析”，WEIS 2019

[1229] P Marquardt、A Verma、H Carter、P Traynor，“(sp)iphone：使用手机加速度计解码附近键盘的振动”，CCS 2011，第 551-562 页

[1230] M Marquis-Boire、G Greenwald、M Lee，“XKEYSCORE – NSA 的全球私人通信谷歌”The Intercept，2015 年 7 月 1 日

[1231] M Marquis-Boire、B Marczak、C Guarnieri、J Scott-Railton，“只有你点击两次 FinFisher 的全球扩散”，蒙克学校，多伦多，2013 年 3 月 13 日

[1232] S Marsh，“美国与英国一起指责俄罗斯发动 NotPetya 网络攻击”，The 卫报 2018 年 2 月 15 日

[1233] L Martin，“使用半导体故障分析工具进行安全分析”，FIPS 物理安全研讨会，夏威夷，2005 年

[1234] AG Mart´ nez，“特朗普如何在没有俄罗斯广告的情况下征服 Facebook”，连线 2018 年 2 月 23 日

[1235] JL Mashaw，DL Harfst，哈佛大学“汽车安全斗争”（1990 年）

[1236] S Mason，“电子证据 披露、发现和可采性”，LexisNexis 北海 (2007)

[1237] S Masondo，“员工窃取‘万能钥匙’后，邮政银行被迫更换 1200 万张银行卡”，星期日泰晤士报，2020 年 6 月 14 日，https://www.timeslive.co.za/sunday-times/news/ 2020-06-14-postbank-强制更换-1200万张银行卡-after-employees-steal-master-

[1238] M Mastanduno，“治国方略和奖学金中的经济与安全”，国际组织诉 52 号 4（1998 年秋季）

[1239] S Matala、T Nyman、N Asokan，“对发展的历史洞察力移动 TEE”，阿尔托大学安全系统组博客，2019 年 6 月 20 日

[1240] JM Matey，O Naroditsky，K Hanna，R Kolczynski，DJ LoIacono，S Mangru，M Tinker、TM Zappia、WY Zhao，“移动中的虹膜：在受限较少的环境中采集用于虹膜识别的图像”，Proc IEEE v 94 no 11（2006 年 11 月）第 1936-1947 页

[1241] SA 马蒂森。 “在哈利法克斯发生网络钓鱼 英国银行发送营销电子邮件，其自己的员工将其识别为假冒”，信息安全新闻，2005 年 10 月 7 日，网址为 http://www.infosecurity-magazine.com/news/051007_halifax_email。 htm

[1242] A Mathur、G Acar、M Friedman、E Lucherini、J Mayer、M Chetty、A Narayanan，“大规模黑暗模式：从 11K Shop ping 网站抓取中发现”，arxiv：1907.07032 2019 年 7 月 16 日

[1243] M Matsubara，“日本汽车行业正在采取下一步措施进行网络安全协作”，Lawfare 2020 年 7 月 7 日

[1244] M Matsui，“DES 密码的线性密码分析方法”，在 Eurocrypt 93，施普林格 LNCS v 765 第 386-397 页

[1245] M Matsui，“新块加密算法 MISTY”，第四届国际快速软件加密研讨会（1997 年），Springer LNCS v 1267，第 54-68 页

[1246] T Matsumoto、H Matsumoto、K Yamada、S Hoshino，“人工影响指纹系统上的‘胶粘’手指”SPIE 会议记录 v 4677，光学安全与防伪技术 IV, 2002

[1247] R Matthews，“一个人的力量”，载于《新科学家》（10/7/1999）第 26-30 页

[1248] T Matthews、K O Leary、A Turner、M Sleeper、J Palzkill Woelfer、M Shelton、C Manthorne、EF Churchill、S Consolvo，“幸存者的故事：应对亲密伴侣虐待时的隐私和安全实践” 气 2017

[1249] V Maty´as，“在药物处方分析中保护医生的身份”，《健康信息学杂志》第 4 卷第 3-4 期（1998 年 12 月）第 205-209 页

[1250] V Mavroudis、P Svenda，“JavaCard：您不知道自己在使用的执行环境”，软件可持续发展研究所，2018 年 7 月 13 日

[1251] J Maynard Smith, G Price, “动物冲突的逻辑”, in Nature v 146 (1973) 第 15-18 页

[1252] R Mayrhofer、J Vander Stoep、C Brubaker、N Kralevich，“Android 平台安全模型”，arXiv：1904.05572，2019 年 4 月 11 日

[1253] K McCarthy，“这是你们都喜欢的嬉皮士、支持隐私、支持自由的 Apple：香港抗议安全应用程序被 iOS 商店禁止”，The Register，2019 年 10 月 2 日

[1254] K McCarthy，“物联网是一场安全噩梦，揭示了最新的现实世界分析：未加密的流量、网络交叉、易受攻击操作系统”，The Register，2020 年 3 月 11 日

[1255] J 麦科马克。 “欧洲加扰系统 – 黑皮书”，第 5 版（1996 年），沃特福德大学出版社

[1256] D McCrum，“Wirecard：时间线”，金融时报，2020 年 6 月 25 日

[1257] D McCullagh，“美国追踪加密踪迹”，连线，2000 年 5 月 4 日；统计学 http://www.uscourts.gov/wiretap99/contents.html 上的抽动

[1258] D McCullagh，R Zarate，“扫描技术模糊图片”，《连线》，2002 年 2 月 16 日；在 http://www.wired.com/politics/law/news/2002/02/50470

[1259] K McCurley，在 IACR 大会上的讲话。加密货币 98，圣诞老人酒吧加利福尼亚州巴拉市，1998 年 8 月

[1260] D McCullough，IEEE 中的“多级安全连接定理”软件工程交易 v 16 no 6（1990 年 6 月）第 563–568 页

[1261] P McDaniel，K Butler，W Enck，H Hursti，S McLaughlin，P Traynor，MA Blaze，A Aviv，P Cern´y，S Clark，E Cronin，G Shah，M Sherr，A Vigna，R Kemmerer， D Balzarotti、G Banks、M Cova、V Felmetsger、W Robertson、F Valeur、JL Hall、L Quilter，“EVEREST：选举相关设备、标准和测试的评估和验证”，最终报告，2007 年 12 月 7 日；在 http://www.sos.state.oh.us/sos/info/EVEREST/ 14-AcademicFinalEVERESTReport.pdf

[1262] AD McDonald，MG Kuhn，“StegFS：一种隐写文件系统，用于 Linux”，[1520] 第 463–477 页

[1263] D MacEoin，“英国伊斯兰教的劫持 极端主义文学如何颠覆英国的清真寺”，政策交流（2007 年）

[1264] M McFarland，“联邦调查局将优步自动驾驶汽车死亡归咎于分心的测试司机”，CNN，2019 年 11 月 20 日

[1265] E McGaughey，“俄罗斯支持的欺诈程度意味着公投无效”，伦敦政治经济学院，2018 年 11 月 14 日

[1266] G McGraw，“软件安全 构建安全”，Addison-Wesley，2006年

[1267] G McGraw、H Figueroa、V Shepardson、R Bonett，“机器学习系统的架构风险分析：走向更安全的机器学习”，BIML，2020

[1268] D McGrew，J Viega，“伽罗瓦/计数器操作模式（GCM）”，2004 年 1 月提交给 NIST 操作流程模式；更新 2005 年 5 月

[1269] J McGroddy，HS Lin，“FBI 三部曲信息技术回顾”学现代化计划》，国家科学院出版社，2004

[1270] J McHugh，“基于 EMACS 的 SAT 降级器”在计算机和
网络安全,IEEE Computer Society Press (1986) pp 228–237

[1271] N McInnes、G Wills、E Zaluska，“基于 VoIP 的 PBX 蜜罐的威胁分析”,Infonomics Society (2019) 第
113-118 页

[1272] I McKie，“为 Shirley McKie 辩护！” 2000 年 6 月 23 日,网址:http:
//onin.com/fp/mckievindication.html

[1273] I McKie, M Russell, Shirley McKie – 无罪的代价 , Birlinn,
2007年

[1274] J McLaughlin,Z Dorfman，“ 破碎 :在秘密战斗中进行拯救
美国数字时代的卧底间谍”,雅虎新闻,2019 年 12 月 30 日

[1275] J McLean，“计算机安全的规范和建模”,在 Com
puter v 23 no 1（1990 年 1 月)第 9–16 页

[1276] J McLean，“安全模型”,在软件工程百科全书中，
约翰威利父子公司 (1994)

[1277] J McLean，“一类‘可能性’的一般组合理论
Properties”,IEEE Transactions on Software Engineering v 22 no 1（1996 年 1 月）
第 53-67 页

[1278] D McLeod，“FNB 在强烈反对后放弃密码决定”,Tech
中环 2019 年 8 月 20 日

[1279] J McMillan，“手机帮助确保网上银行安全”,PC World，
2007 年 9 月 11 日

[1280] R McMillan，“Mt. Gox 的内幕,比特币 4.6 亿美元的灾难”,2014 年 3 月 3 日连线

[1281] 医学机密， “健康 数据、AI 和 Google Deep https://medconfidential.org/
Mind”， 在 whats-the-story/
health-data-ai-and-google-deepmind/

[1282] J Meek，“机器人警察”,《卫报》,2002 年 6 月 13 日,http://www.
guardian.co.uk/Archive/Article/0,4273,4432506,00.html

[1283] N Megaw，“英国消费者被拖入 Wirecard 的崩溃”,金融
时代 Jun 29 2020

[1284] C Meijer,R Verdult，“强化 Mifare 的纯密文密码分析
经典卡片”ACM CCS (2015)

[1285] C Meijer,B van Gastel，“自加密欺骗:en 中的弱点
固态硬盘的加密”,IEEE 安全与隐私 (2019)

[1286] J Meikle，“G4S 和 Serco 因欺诈移交违法者标记合同
索赔”,卫报,2013 年 12 月 12 日

[1287] M Mehrnezhad、M Aamir Ali、F Hao、A van Moorsel，“NFC 支付间谍:对非接触式支付的隐私攻击”,国际会
议
安全标准化研究 (2016) pp 92-111

[1288] J Mendez，“Steam 如何使用 DRM 及其对您的意义
游戏”,Black Shell Media,2017 年 6 月 28 日

[1289] AJ Menezes、PC van Oorschot、SA Vanstone，“应用密码术手册”，CRC 出版社（1997 年）；可在 http://www.cacr.math 在线获取。 uwaterloo.ca/hac/

[1290] J Menn，“独家：秘密合同与美国国家安全局和安全行业先驱有关”，路透社，2013 年 12 月 20 日

[1291] J Menn，“独家：政府和银行的高安全性锁被研究人员入侵”，路透社，2019 年 8 月 6 日

[1292] J Menn、K Paul、R Satter，“独家新闻：Twitter 的 1,000 多人有能力帮助破解账户”，路透社，2020 年 7 月 23 日

[1293] J Mercer，“文件欺诈威慑策略：四个案例研究”，载于
光学安全和防伪技术 II (1998)，IS&T 和 SPIE v 3314，第 39–51 页

[1294] H Mercier，D Sperber，“人类为什么推理？ Arguments for an Argumentative Theory”，Behavioral and Brain Sciences v 34 no 2 pp 57–74, 2011, and at SSRN 1698090

[1295] R Mercuri，“计算机系统的物理可验证性”，第五届国际计算机病毒与安全会议（1992 年 3 月）；另请参见 R Mercuri，“电子投票制表检查与平衡”，博士论文，宾夕法尼亚大学，2000 年，网址为 http://www.notablesoftware.com/evote.html

[1296] R Merkle，“公钥密码系统协议”，IEEE 研讨会
安全和隐私 1980

[1297] M Mesa，“网络钓鱼规模：恶意行为者结合个性化电子邮件，
以高管为目标的各种恶意软件”，ProofPoint，2016 年 4 月 5 日

[1298] TS Messergues、EA Dabish、RH Sloan，“智能卡功率分析攻击调查”，Usenix 智能卡技术研讨会 (1999) 第 151-161 页

[1299] E Messmer，“国防部希望在 PKI 中重新发挥活力”，网络世界 8 月 15 2005

[1300] C Metz，“人工智能正在改变谷歌搜索。网络的其余部分是下一个”，《连线》杂志，2016 年 2 月 4 日

[1301] CH Meyer，SM Matyas，“密码学：计算机的新维度”
数据安全”，Wiley，1982 年

[1302] C Meyer，Joerg Schwenk，“SoK：从 SSL/TLS 攻击中吸取的教训”
WISA 2013 第 189–209 页

[1303] R Meyer-Sommer，“巧妙地分析智能卡上简单功率分析的简单性和强大功能”，加密硬件和嵌入式系统研讨会（2000 年）； Springer LNCS v 1965 第 78-92 页

[1304] A Michael，“网络探测：虚拟攻击的政治化”，防御
英国科学院 2012 年 10 月

[1305] J Micklethwait，A Wooldridge，“巫医 管理大师在说什么，为什么重要以及如何理解它”，随机
房子 (1997)

[1306] 微软公司，“Windows Media Rights Manager 的架构”，2004 年 5 月

[1307] 微软公司，“索尼 DRM Rootkit”，2005 年 11 月 12 日

[1308] 微软公司，“安全开发生命周期 微软 SDL 的简化实施”，2010 年 11 月 4 日

[1309] Microsoft Azure，“什么是 Azure Key Vault？”，2019 年 1 月 7 日

[1310] A Midgley，“RIP 和 NHSNet”，ukcrypto 邮件列表，2000 年 7 月 1 日

[1311] S Mihm，“造假者的国度”，哈佛大学 2007 年

[1312] S Milgram，“服从权威：实验观点”，哈珀
柯林斯，（1974 年，2004 年重印）

[1313] J Millen，“拒绝服务保护的资源分配模型”，
in 计算机安全杂志 v 2 no 2-3 (1993) pp 89-106

[1314] A Miller，“SourMint：iOS 中的恶意代码、广告欺诈和数据泄漏”，Synk，
2020 年 8 月 26 日

[1315] B Miller，“Vital Signs of Security”，IEEE Spectrum（2 月 94 日）第 22-30 页

[1316] C Miller、C Valasek，“远程利用未改装的乘用车”，https://www.illmatics.com 2015 年 8 月
10 日

[1317] GA Miller，“神奇的数字七，正负二：我们处理信息的能力的一些限制”，在 Psychological Review
v 63 (1956) pp 81-97

[1318] ML Miller、IJ Cox、JA Bloom，“现实世界中的水印：一个
Application to DVD”第六届ACM国际多媒体会议（1998）； GMD 报告第 41 卷，第 71-76 页

[1319] JR Minkel，“确认：美国人口普查局放弃了二战中日裔美国人的名字”，《科学美国人》，2007 年 3
月 30 日

[1320] SF Mires，“邮政安全设备和基于信息的标记的生产、分发和使用”，联邦纪事 v 65 no 191 2000
年 10 月 2 日，第 58682-58698 页

[1321] A Mirian、Z Ma、D Adrian、M Tischer、T Chuenchujit、T Yardley、R
Berthier、J Mason、Z Durumeric、JA Halderman、M Bailey，“互联网
Wide View of ICS Devices”2016 年隐私、安全和信任大会

[1322] A Mirian、J DeBlasio、S Savage、GM Voelker、K Thomas，“Hack for Hire：
探索新兴市场的账户劫持”，全球
网络会议 2019 第 1279–1289 页

[1323] “BBC 因假比赛被 Ofcom 罚款 400,000 英镑”，《每日镜报》7 月
30 2008

[1324] 米切尔和韦伯，“身份盗窃”，YouTube（2007 年）

[1325] KD Mitnick，“欺骗的艺术：控制人为因素
安全”，威利 (2002)

[1326] V Mladenov、C Mainka、K Mayer zu Selhausen、M Grothe、J Schwenk “1 万亿美元退款 如
何欺骗 PDF 签名”，CCS 2019

[1327] D Modic,RJ Anderson，“阅读本文可能会损害您的计算机：
恶意软件警告心理学”,Computers in Human Behavior v 41 pp 71–79 and SSRN 2374379

[1328] A Moghimi、G Irazoqui、T Eisenbarth，“CacheZoom:SGX 如何放大
缓存攻击的力量”CHES 2017 第 69-90 页

[1329] D Moghimi、B Sunar、T Eisenbarth、N Heninger TPM-失败:TPM 满足
时序和格攻击”,arXiv:1911.05673 2019 年 11 月 13 日

[1330] “信用卡欺诈净赚 60 亿欧元”,F Mollet,Cards International (22/9/95) 第 3 页

[1331] JV Monaco，“SoK:键盘记录侧通道”,IEEE 安全研讨会
权利和隐私 (2018)

[1332] “D´emant`element d un r´eseau de t´el´ephonie crypt´ee, utilis´e par des organi
sations criminelles”,世界报,2020 年 7 月 2 日

[1333] YA de Montjoye、CA Hidalgo、M Verleysen、VD Blondel，“在
人群:人类流动性的隐私界限”,科学报告 v 3 no 1376 (2013)

[1334] YA de Montjoye、J Quoidbach、F Robic、A Pentland，“使用基于手机的新型指标预测人格”,2013 年
社会计算、行为文化建模和预测国际会议
(SBP 2013) 第 48-55 页

[1335] B Moore，“基督城的教训:媒体最终如何承认
极右翼恐怖主义”,Signal,2019 年 4 月 3 日

[1336] SW Moore、RJ Anderson、R Mullins、G Taylor、J Fournier，“平衡的自我
检查智能卡应用程序的异步逻辑”,微处理器和微系统杂志 v 27 no 9（2003 年 10 月)第 421-430 页

[1337] T Moore、R Anderson，“大脑类型如何影响在线安全”,安全与人类行为（2008 年）

[1338] T Moore, A Friedman, A Procaccia，“‘网络战士’会保护我们吗？
探索信息系统攻击与防御之间的权衡”,新安全范式研讨会 (2010) 第 85-94 页。

[1339] T Moore, N Christin，“当心中间人:实证分析
比特币交易风险”,金融密码学 2013 年第 25-33 页

[1340] L Moran，“高音喇叭对 Jack Dorsey 的帐户提出冷点
被妥协”,亨顿邮报,2019 年 8 月 31 日

[1341] B Morgan，“给客户 50,000 英镑账单的脱衣舞俱乐部失去了执照”晚间
标准 2020 年 1 月 31 日

[1342] R Morris，“4.2BSD Unix TCP/IP 软件的弱点”,贝尔实验室计算机科学技术报告第 1 号。 117,
1985.2.25;在 http://www.cs.berkeley.edu/~daw/security/seq-attack.html

[1343] R Morris,受邀演讲,Crypto 95

[1344] R Morris、K Thompson，“密码安全:案例历史”,Communi
ACM 阳离子 v 22 no 11（1979 年 11 月)第 594-597 页

[1345] M Motoyama、D McCoy、K Levchenko、S Savage、GM Voelker，“分析
地下论坛”，IMC (2011)

[1346] DP Moynihan，“保密 美国经验”，耶鲁大学出版社
(1999)

[1347] P Mozur，“Skype 从包括苹果在内的中国应用商店中消失”，
纽约时报，2017 年 11 月 21 日

[1348] P Mozur，“借助黑客和摄像头，北京的电子天罗地网在香港关闭”，纽约时报，2020 年 8 月 25 日

[1349] C Mueller、S Spray、J Grear，“引爆的独特信号概念
核武器安全”，Sand91-1269，UC-706

[1350] J Mueller，夸大其词 政治家和恐怖主义行业如何膨胀
国家安全威胁，以及我们为何相信它们，Simon 和 Schuster 2006

[1351] S Mukherjee，“冠状病毒危机对美国人的启示
医学”，纽约客 2020 年 4 月 27 日

[1352] T Mulhall，“所有黑客都去哪儿了？动机、威慑和犯罪转移研究”，载于计算机和安全 v 16 no 4 (1997) pp 277–
315

[1353] S Mullender（编辑），“分布式系统”，Addison-Wesley（1993 年）

[1354] E Munro，“Munro 儿童保护审查：最终报告 以儿童为中心的系统”，教育部，2011 年 5 月 10 日

[1355] SJ Murdoch，“浏览器存储密码：风险还是机会？”，2006 年 4 月 18 日，淡蓝色触控纸；在 http://
www.lightbluetouchpaper.org/ 2006/04/18/browser-storage-of-passwords-a-risk-or-opportunity/

[1356] SJ Murdoch，“热门与否：通过时钟偏差揭示隐藏服务”，第 13 届 ACM 计算机和通信安全会议。 2006年

[1357] SJ Murdoch，“软件工程在电子选举中的作用”，Light Blue Touchpaper，2007 年 7 月 13 日，网址为 https://
www.lightbluetouchpaper.org/2007/07/13/the-role-of-software-工程电子选举/

[1358] SJ Murdoch，“匿名系统中的隐蔽通道漏洞”，博士
论文，剑桥 2007

[1359] SJ Murdoch，“大使馆电子邮件帐户被未加密的密码破坏”，2007 年 9 月 10 日；在 http://
www.lightbluetouchpaper.org/2007/09/10/

[1360] SJ Murdoch，“Tor 数据报设计的比较”，Tor 技术报告
2011-11-001，2011 年 11 月 7 日

[1361] 小杰 默多克，来自 “英国议会关于 保护 骗子
苏美尔 经济的 罪”， 边沁的 凝视十一月
5个 2019； https://www.benthamsgaze.org/2019/11/05/uk-parliament-
on-protecting-consumers-from-economic-crime/

[1362] SJ Murdoch、RJ Anderson，“Visa 和 MasterCard SecureCode 验证，或如何不设计身份验证”金融密码学
（2010 年）

[1363] SJ Murdoch,G Danezis，“Tor 的低成本 Trac 分析”,IEEE Sym
关于安全和隐私的声明 (2005)

[1364] SJ Murdoch、S Drimer、RJ Anderson、M Bond，“芯片和密码损坏”，
IEEE 安全与隐私研讨会 (2010)

[1365] SJ Murdoch、Piotr Zieli´nski，“通过互联网进行的采样流量分析
交易级对手”,PETS 2007

[1366] K Murdock、D Oswald、FD Garcia、J Van Bulck、D Gruss、F Piessens，“Plundervolt：
针对英特尔 SGX 的基于软件的故障注入攻击”,网址为 https://www.plundervolt.com
（2019 年）

[1367] JC Murphy、D Dubbel、R Benson，“货币的技术方法
安全”,光学安全和防伪技术 II
(1998),IS&T 和 SPIE v 3314 第 21-28 页

[1368] K Murray，“爱尔兰计算机程序的保护”,《计算机法与安全报告》第 12 期第 3 期（96 年 5 月/6
月)第 57-59 页

[1369] O Mutlu,JS Kim，“RowHammer:回顾”,arXiv:1904.09724 Apr
22 2019

[1370] R Nader，“任何速度都不安全:美国人的设计危险”
汽车 (1965)

[1371] A Nadler、A Aminov、A Shabtai，“通过 DNS 协议检测恶意和低吞吐量数据泄露”,arXiv
1709.08395

[1372] A Nadkarni、B Andow、W Enck、S Jha，“DIFC 的实际执法
Android”,Usenix 安全 (2016)

[1373] S Nagaraja,RJ Anderson，“隐蔽冲突的拓扑结构”,第五届信息安全经济学研讨会（2006 年）

[1374] S Nagaraja,RJ Anderson，“窥探龙:西藏运动的社交恶意软件监视”,剑桥大学计算机实验室技
术报告 746（2009 年）

[1375] S Nakamoto，“比特币:一种点对点电子现金系统”,http://bitcoin.org/bitcoin.pdf (2008)

[1376] E Nakashima，“Verizon 称它在没有法院命令的情况下移交数据”,华盛顿邮报,2007 年 10 月
16 日,第 A01 页;在 http://www.washingtonpost.com/wp-dyn/content/article/2007/10/15/
AR2007101501857.html

[1377] E Nakashima，“监控的故事 前技术员‘上交’
AT&T Over NSA Program”,华盛顿邮报,2007 年 11 月 7 日

[1378] E Nakashima，“FBI 准备了庞大的生物识别数据库 10 亿美元
包括虹膜和面部图像的项目”,华盛顿邮报
2007 年 12 月 22 日

[1379] E Nakashima，“机密报告列出了中国网络间谍承诺的美国武器系统设计”,华盛顿邮报,2013 年
5 月 27 日

[1380] RFH Nalder 少将，“皇家信号兵团的历史”,由皇家信号学会出版（1958 年）

[1381] 维基百科,Napster,http://en.wikipedia.org/wiki/Napster

[1382] A Narayanan，“如何识别 AI 蛇油”,Arthur Miller 科学与伦理讲座,麻省理工学院,2019 年 11 月 18 日

[1383] A Narayanan、J Bonneau、E Felten、A Miller、S Goldfeder，“比特币和加密货币技术》,普林斯顿大学出版社,2016 年

[1384] A Narayanan,V Shmatikov，“如何打破 Netflix 奖项的匿名性数据集”（2007 年 11 月)http://arxiv.org/abs/cs/0610105

[1385] M Nash，“MS 安全副总裁 Mike Nash 回复”,Slashdot,2006 年 1 月 26 日,http://interviews.slashdot.org/interviews/06/01/26/131246.shtml

[1386] M Nash、R Kennett，“在大型防御系统中实施安全策略采购”,第 12 届 ACSAC,第 15-23 页

[1387] B Nassi、Y Pirutin、A Shamir Y Elovici、B Zadov，“Lamphone – 实时从灯泡振动中恢复被动声音”BlackHat USA (2020)

[1388] 美国国家科学院、工程院和医学院，“确保投票:保护美国民主,国家科学院出版社（2018 年）

[1389] 国家审计署，“国防部长:战斗识别”,2002 年

[1390] 国家审计署，“NHS 中的 IT 国家计划:详细护理记录系统交付的更新”,2011 年 5 月 18 日

[1391] 国家审计署，“推出智能电表”,2018 年 11 月 23 日

[1392] 国家审计署，“调查验证”,2019 年 3 月 5 日

[1393]国家网络安全中心，《2019年度回顾》2019

[1394] 国家公路交通安全管理局，“特殊碰撞调查:2015 年特斯拉 Model S 70D 现场自动驾驶辅助系统碰撞调查”,报告编号 DOT HS 812 481,2018 年

[1395] 美国国家标准技术研究院,计算机安全出版物档案,http://csrc.nist.gov/publications/history/index.html

[1396] 美国国家标准技术研究院，“信息技术安全评估通用标准”,版本 2.0 / ISO IS 15408（1998 年 5 月）； 3.1 版（2006 年 9 月 - 2007 年 9 月）,网址为 http://www.commoncriteriaportal.org网站

[1397] 美国国家标准技术研究院,《数据加密标准》(DES) FIPS 46-3,1999 年 11 月,包含升级到三重 DES

[1398] 美国国家标准技术研究院，“托管加密”标准”,FIPS 185,1994 年 2 月

[1399] 美国国家标准技术研究院，“安全要求密码模块 (11/1/1994)

[1400] 美国国家标准技术研究院，“SKIPJACK 和 KEA 算法”,1998 年 6 月 23 日,http://csrc.nist.gov/encryption/skipjack-kea.htm

[1401] 美国国家标准技术研究院，“高级加密
标准”，FIPS 197，2001 年 11 月 26 日

[1402] 美国国家标准技术研究院， 数字签名标准
(DSS) ，FIPS 186-2，2000 年 1 月，带有 2001 年 10 月变更通知

[1403] 美国国家标准技术研究院， 数字签名标准
(DSS) ，FIPS 186-3，草案，2006 年 3 月

[1404] 美国国家标准技术研究院，“关于
分组密码操作模式”，特别出版物 800-38A 2001 年版

[1405] 美国国家标准技术研究院，“关于
分组密码操作模式：用于身份验证的 CMAC 模式 ，
特别出版物 800-38B，2005 年 5 月

[1406] 美国国家标准技术研究院，“关于
分组密码操作模式：用于身份验证和验证的 CCM 模式
保密性”，特刊 800-38C，2004 年 5 月

[1407] 美国国家标准技术研究院，“关于
分组密码操作模式：伽罗瓦/计数器模式 (GCM) 和
GMAC 的 NIST 特别出版物 800-38D，2007 年 11 月

[1408] 美国国家标准技术研究院，“重点推荐”
管理 – 第 1 部分：总则（修订版），特刊 800-57，2006 年 5 月

[1409] 美国国家标准技术研究院， 宣布要求
新密码哈希算法的候选算法提名
(SHA-3) Family”，Federal Register v 72 no 212，2007 年 11 月 2 日，第 62212–20 页

[1410] 美国国家标准技术研究院，“收到的评论意见
NIST 关于“政府使用密码算法和密码模块测试和验证程序的安全性和一致性要求标准”的
信息请求“联邦公报

公告2015-19743 (2018)

[1411] 国家研究委员会，“密码学在保护信息社会中的作用”，国家科学院出版社（1996 年）

[1412] 国家研究委员会， 备案：保护电子健康
《信息》，国家科学院出版社（1997）

[1413] 国家研究委员会，“加强美国的法医学”
州：前进的道路”（2009 年）

[1414] 国家安全局，“国家安全局安全手册”，网址为 http://www.cl。 cam.ac.uk/ftp/users/
rja14/nsaman.tex.gz

[1415]国家人工智能安全委员会《临时报告》，
2019 年 11 月

[1416] 国家统计局，“数据访问和保密协议”，网址为：//www.statistics.gov.uk

[1417] J Naughton，“忘掉无人驾驶技术吧 白色面包车的人会继续卡车运输”，
卫报 2017 年 4 月 16 日

[1418] J Naughton，“Facebook 的附庸国”，Memex 1.1，2019 年 3 月 5 日

[1419] J Naughton，“帮助互联网蓬勃发展的法律现在破坏了
民主”，卫报，2019 年 12 月 21 日

[1420] P Naur，B Randell，“软件工程 会议报告”，
北约科学航空司，Garmisch 1968

[1421] Y Nawaz，“摩根大通的区块链和密码学”，2018 年金融密码学，网址为 https://
www.lightbluetouchpaper.org/2018/02/26/financial-cryptography-2018/

[1422] R Neame，“管理健康数据隐私和安全”，[63] 第 225-232 页

[1423] RM Needham，“拒绝服务：一个例子”，在 Communications of the
ACM v 37 第 11 期（94 年 11 月）第 42-46 页

[1424] RM Needham，“命名”，[1353]，第 318-127 页

[1425] RM Needham，“硬件环境”，载于 1999 年的会议记录
IEEE 安全与隐私研讨会 p 236

[1426] RM Needham，MD Schroeder，“使用加密进行身份验证
大型计算机网络”，ACM 通讯 v 21 no 12
（12 月 78 日）第 993–999 页

[1427] U Neisser，“认知与现实：认知心理学的原理和影响”，弗里曼，1976 年

[1428] M Nesbitt，“在 Ethereum Classic 上检测到深度链重组
(ETC)”，Coinbase 博客，2019 年 1 月 7 日

[1429] P Neumann，“计算机相关风险”，Addison-Wesley（1995 年）

[1430] P Neumann，Principled Assuredly Trustworthy Composable Architectures，CHATS 项目最终报告
（2004 年），位于 http://www.csl.sri.com/users/neumann/

[1431] J Neumann，“护城河分类法”，反应轮，2019 年 9 月 19 日

[1432] 新南威尔士州最高法院，RTA 诉 Michell（新南威尔士州最高法院，2006 年 3 月 24 日，报道于“澳大利亚：新
南威尔士州最高法院放弃秘密决定”，http://www.thenewspaper.com/news /10/1037.asp

[1433] MEJ Newman，“复杂网络的结构和功能”，SIAM
评论 v 45 no 2 (2003) pp 167–256

[1434] MEJ Newman，“网络中的模块化和社区结构”，Proc。
国家队。学院。科学。美国诉 103，第 8577–8582 页（2006 年）；在 http://arxiv.org/abs/
physics/0602124

[1435] O Newman，“防御空间：暴力城市中的人与设计”，
麦克米伦 1972

[1436] R Newman、S Gavette、L Yonge、RJ Anderson，“保护国内
电力线通信”，SOUPS 2006 第 122-132 页

[1437] R Newman、S Gavette、L Yonge、RJ Anderson，“HomePlug AV 安全
机制”，2007 年 IEEE 电力线通信及其应用国际研讨会

[1438] C Newton，“The Trauma Floor”，The Verge，2019 年 2 月 25 日

[1439] C 牛顿，“马克扎克伯格说 Facebook 将转向强调加密的短暂消息”，The Verge，2019 年 3 月 6
日

[1440] J Newton，“打击造假者”，Cards International (21/12/94) 第 12 页

[1441] J Newton，“有组织的塑料假冒”，女王陛下的文具
办公室 (1996)

[1442] “消失的色拉油：一个价值 1 亿美元的谜团”，纽约时报，1 月
6 1964年

[1443] Nex，“拦截的新旧边界”，时事通讯博客 2020 年 7 月 28 日

[1444] Andrew Ng，“Equifax 黑客攻击是如何发生的，以及还需要做什么
完成”，Cnet 2018 年 9 月 7 日

[1445] S Nichols “WAN 的沉默：FBI DDoS-for-hire greaseball 删除
将网络洪水攻击“减少 11%”” The Register 2019 年 3 月 19 日

[1446] S Nichols“Apple 在长寿命 HTTPS 证书上投下炸弹：Safari 拒绝使用有效期超过 13 个月的新安
全证书”，The Register 2019 年 2 月 20 日

[1447] SJ Nightingale，H Farid，“评估基于服装的法庭的可靠性
sic identification”，PNAS 2020 年 1 月 15 日

[1448] N Nisan, T Roughgarden, E Tardos, VV Vazirani， 算法机制
设计 , CUP 2007

[1449] 尼克松，“欺诈者告诉我们身份已被破坏”，金融密码学 2020 年 2 月 2 日，网址为 https://
www.lightbluetouchpaper.org/2020/02/10/fc-2020/

[1450] K Nohl、D Evans、H Pl¨otz，“对加密 RFID 进行逆向工程
标签”，Usenix 安全 2008 年； 2007 年 Chaor 计算机大会上的早期版本

[1451] DA Norman，“谨慎的汽车和脾气暴躁的厨房：机器如何控制”，http://www.jnd.org/； 《未来
事物的设计》第 1 章（2008 年到期）

[1452] A Noroozian、J Koenders、E Van Veldhuizen、CH Ganan、S Alrwais、D Mc
Coy, M Van Eeten，“平台无处不在：分析关于防弹托管的解剖学和经济学的真实数据”，USENIX
Security 2019，第 1341-1356 页

[1453] R v Ipswich Crown Court ex parte NTL Ltd, [2002] EWHC 1585（管理员），
在 http://www.cyber-rights.org/documents/ntl_case.htm

[1454] “白皮书 – 5g 演进和 6g”，NTT Docomo，2020 年 1 月

[1455] 核管理委员会，www.nrc.gov

[1456] H Nugent，“通奸者拨打 118 118 求婚”，载于《泰晤士报》，5 月
2006年27日

[1457] F Oberholzer、K Strumpf，“文件共享对唱片销售的影响
– 实证分析”，2004 年 6 月；日志版本 F Oberholzer-Gee，
K Strumpf，“文件共享对唱片销售的影响：实证分析
分析，政治经济学杂志 v 115 (2007) pp 1–42

[1458] Victimation et Perceptions de la Suret e ，国家天文台 de la D elin
quance et de Responses P´enales (2017)

[1459] AM Odlyzko，“悲惨的损失还是幸运的摆脱？传统学术期刊即将消亡”，Notices Amer。数学。 Soc.，1995 年
1 月，在 http://www.dtc.umn.edu/~odlyzko/doc/tragic.loss.txt

[1460] AM Odlyzko，“通信的历史及其对互联网的影响”，位于 http://www.dtc.umn.edu/~odlyzko/doc/
networks.html

[1461] AM Odlyzko，“聪明和愚蠢的网络：为什么互联网像微软”，ACM netWorker，1998 年 12 月，第 38-46 页

[1462] AM Odlyzko，“互联网上的隐私、经济学和价格歧视”，ICEC 03：第五届电子商务国际会议论文集，第
355-366 页；在 http://www.dtc.umn.edu/~odlyzko/doc/

网络.html

[1463] AM Odlyzko，“互联网的定价和架构：电信和交通的历史观点”，TPRC 2004，网址为 http://www.dtc.umn.edu/
~odlyzko/doc/networks.html

[1464] 国家情报总监办公室，“关于使用国家安全机构的统计透明度报告 2017 日历年”

[1465] P Ohm，“违反隐私承诺：应对匿名化的意外失败”，UCLA Law Review v 57 (2010) p 1701

[1466] S O Kane，“戴姆勒因销售作弊汽车被罚款近 10 亿美元
排放测试”，The Verge，2019 年 9 月 24 日

[1467] N Okuntsev，“Windows NT 安全”，研发书籍（1999 年）

[1468] “Nicht nachmachen：Dieser Vignetten-Trick kostet Sie 300 欧元”，在线
焦点，2015 年 6 月 12 日

[1469] Open Net Initiative，“2004-2005 年中国的互联网过滤：国家研究”，2005 年 4 月 14 日，网址为 https://
opennet.net/

[1470] Open Net Initiative，“中国（包括香港）”，2006 年国家报告，网址为 https://opennet.net/

[1471] Open Net Initiative，“拔掉插头”，2007 年 10 月，网址为 https://opennet。
网/研究/公告/013

[1472] 开放权利组织，“2007 年 5 月选举报告 开放权利组织在苏格兰和英格兰的选举观察团的调查结果”，网址为：
http://www.openrightsgroup.org/e-voting-main

[1473] A Orben、T Dienlin、AK Przybylski，“社交媒体对青少年生活满意度的持久影响”，PNAS，2019 年 4 月 16 日

[1474] A Orlowski，“Schrems 打破了隐私护盾”，The Register，10 月 3 2017

[1475] A Orlowski，“英国间谍机构警告英国电信公司远离中兴设备”，The 注册 2018 年 4 月 16 日

[1476] 经济合作与发展组织，“隐私保护和个人数据跨境流动指南”，经合组织 文件编号 C(80)58 (1981)

[1477] 经济合作与发展组织，“CO4.4：青少年自杀（15-19 岁）”经合组织家庭数据库（2017 年）

[1478] M Orozco、Y Asfaw、A Adler、S Shirmohammadi、A El Saddik，“自动触觉系统参与者的识别”，IEEE 仪器与测量技术会议 (2005)，第 888–892 页

[1479] B Osborn、J McWilliams、B Beyer、M Saltonstall，“BeyondCorp 设计到谷歌的部署”，；登录：（2016 年春季）v 41 no 1

[1480] C Osborne，“加州大学旧金山分校向勒索软件黑客支付 114 万美元以挽救研究”，ZDNet，2020 年 6 月 30 日

[1481] C Osborne，“单击一下：Amazon Alexa 可能被用来窃取语音历史记录、PII、技能篡改”，ZDNet，2020 年 8 月 13 日

[1482] J Osen，“其他人的智慧之精华：网络空间中的剽窃和盗用”，载于计算机欺诈和安全公告 (11/97) 第 13-19 页

[1483] DA Osvik、A Shamir、E Tromer，“缓存攻击和对策：AES 案例”，RSA 会议密码学家轨道 2006，LNCS 3860，第 1-20 页

[1484] D Oswald、C Paar，“打破 Mifare DESFire MF3ICD40：现实世界中的功率分析和模板”，CHes 2011 第 207-222 页

[1485] Out-law 新闻，“工作组称 SWIFT 违反了数据保护法”，2006 年 11 月 27 日，http://www.out-law.com/page-7518

[1486] Out-law News，“SWIFT 将在 2009 年停止一些美国处理”，2007 年 10 月 15 日，在 http://www.out-law.com/page-8548

[1487] A Ozment，S Schechter，“引导互联网安全的采用协议”，在信息安全经济学第五次研讨会上安全，2006

[1488] A Ozment，S Schechter，“牛奶还是葡萄酒：软件安全性会随着时间的推移而提高吗？”在第 15 届 Usenix 安全研讨会上（2006 年）

[1489] D Page，“缓存存储器作为密码分析方的理论使用”Channel”，技术报告 CSTR-02-003，布里斯托大学，2002 年 6 月

[1490] G Pahl, W Beitz, Konstruktionslehre ；翻译为 工程设计：一种系统的方法”，Springer 1999

[1491] S Pancho，“协议分析中的范式转变”，载于 1999 年会议记录新安全范式研讨会，ACM (2000)，第 70-79 页

[1492] A Papadimoulis，“Wish-It-Was Two-Factor”，2007 年 9 月 20 日，http://worterthanfailure.com/Articles/WishItWas-TwoFactor-.aspx

[1493] N Papernot，“掠夺者的机器学习安全和隐私地图”，arXiv 1811.01134 2018 年 11 月 3 日

[1494] DJ Parker，“DVD 复制保护：终于达成协议？ – 在技术时代保护知识产权”，载于磁带/光盘杂志（96 年 10 月）

[1495] C Parsons, A Molnar, J Dalek, J Knockel, M Kenyon, B Haselton, C Khoo, R Deibert，“口袋里的捕食者对跟踪软件应用行业的多学科评估”，蒙克学校，2019 年 6 月 12 日

[1496] N Partridge，“数据发布审查”，卫生部，2014 年 6 月

[1497] J Pastor，“CRYPTOPOST – 邮件进程的加密应用程序 ing”，Journal of Cryptology v 3 no 2（1991 年 1 月）第 137-146 页

[1498] S Pastrana，G Suarez-Tangil，“初探加密货币挖矿恶意软件生态系统：十年的无限财富”，arXiv：1901.00846 2019 年 1 月 3 日

[1499] S Pastrana、DR Thomas、A Hutchings、R Clayton，“CrimeBB：启用大规模地下论坛网络犯罪研究”，万维网会议 (2018) 第 1845–1854 页

[1500] K Paul，“推特员工被控为沙特阿拉伯从事间谍活动”，The 卫报 2019 年 11 月 6 日

[1501] R Paul，“泄露的 Media Defender 电子邮件揭示秘密政府项目”，Ars Technica 2007 年 9 月 16 日

[1502] LC Paulson，“互联网协议 TLS 的归纳分析”，在安全 Protocols 1998 和 ACM Transactions on Computer and System Security v 2 no 3 (1999) pp 332–351

[1503] V Paxson，“使用反射器进行分布式拒绝分析服务攻击”，载于计算机通信评论 v 31 no 3，2001 年 7 月

[1504] M Payer， 软件安全 – 原则、政策和保护 2019

[1505] S 皮尔曼，J 托马斯，P Emani Naeini，H 哈比卜，L 鲍尔，N 克里斯汀，L Faith Cranor、S Egelman、A Forget，“让我们深入了解一下：在自然栖息地观察密码”，CCS 2017

[1506] J Pearson 2020，“独家：Facebook 同意在越南放慢 trac 后审查帖子 消息来源”，Thnomson Reuters 2020 年 4 月 21 日

[1507] PeckShield，“bZx Hack 全面披露（详细的利润分析）”，中 2020 年 2 月 17 日

[1508] C Percival，“缓存丢失的乐趣和利润”，BSDCan 2005

[1509] J Pereira，“破解密码：信用卡数据如何无线传输门”，《华尔街日报》，2007 年 5 月 4 日，第 A1 页

[1510] N Perlroth、S Shane，“在巴尔的摩及其他地区，被盗的 NSA 工具造成严重破坏”，纽约时报，2019 年 5 月 25 日

[1511] A Perrig，“数字图像的版权保护环境”，毕业论文，洛桑联邦理工学院 (1997)

[1512] T Perrin、M Marlinspike，“双棘轮算法”，https://signal.org/docs/specifications/ 2016 年 11 月 20 日

[1513] P Pesic，“迷宫的线索：弗朗西斯培根和解密 Nature”，载于 Cryptologia v XXIV no 3（2000 年 7 月）第 193-211 页

[1514] M Peters，“MTN 采取措施防止 SIM 卡交换欺诈”，IOL，2007 年 12 月 30 日

[1515] I Peterson，“从计数到写作”，MathLand 档案馆，http://www.maa.org/mathland/mathland_2_24.html

[1516] FAP Petitcolas、RJ Anderson、MG Kuhn，“对版权标记的攻击系统”，Information Hiding (1998) Springer LNCS v 1525 pp 219–239

[1517] FAP Petitcolas、RJ Anderson、MG Kuhn，“信息隐藏 一项调查”，in the Proceedings of the IEEE v 87 no 7（1999 年 7 月）第 1062–1078 页

[1518] H Petroski， To Engineer is Human ，Barnes and Noble Books（1994 年）

[1519] A Peyton，“以太坊经典遭受另一次 51% 黑客攻击”，Fintech Direct，2020 年 8 月 6 日

[1520] A Pfitzmann，第三届信息隐藏国际研讨会论文集（1999），Springer LNCS v 1768

[1521] B Pfitzmann，“信息隐藏术语”，信息隐藏 (1996) Springer LNCS v 1174 第 347–350 页

[1522] PJ Phillips、AN Yates、Y Hu、CA Hahn、E Noyes、K Jackson、JG Cava zos、G Jeckeln、R Ranjan、S Sankaranarayanan、JC Chen、CD Castillo、R Chellappa、D White、AJ O Toole，“法医、超级识别器和人脸识别算法的人脸识别准确性”，PNAS 2018 年 6 月 12 日 v 115 no 24 pp 6171–6176

[1523] Z Phillips，“Security Theater”，载于 Government Executive，2007 年 8 月 1 日，载于 http://www.govexec.com/features/0807-01/0807-01s3.htm

[1524] GE Pickett，“如何为公司产品选择‘正确’的安全功能？”，光学安全和防伪技术 II（1998 年），IS&T（影像科学与技术协会）) 和 SPIE（国际光学工程学会）v 3314

[1525] RL Pickholtz、DL Schilling、LB Milstein，“扩频通信理论 教程”，在 IEEE Transactions on Communications v TC-30 第 5 期（1982 年 5 月）第 855–884 页

[1526] RL Pickholtz、DB Newman、YQ Zhang、M Tatebayashi，“INTELSAT VI 和 VII 指挥网络的安全分析”，载于 IEEE 通讯选定领域论文集 v 11 no 5（1993 年 6 月）第 663-672 页

[1527] L 皮诺，“咨询恶魔”，柯林斯 2000

[1528] S Pinto、N Santos，“揭秘 Arm TrustZone：一项综合调查”，ACM Computing Surveys v 51 no 6（2019 年 2 月）

[1529] JC Plantin、G de Seta，“作为基础设施的微信：中国数字平台的技术民族主义塑造”，《中国传播学报》第 12 期第 3 期（2019 年）第 257-273 页

[1530] RA Poisel，“现代通信干扰原理和技术”，
雅泰之家 2003

[1531] Politech 邮件列表位于 http://www.politechbot.com/

[1532] GJ Popek,RP Goldberg，“可虚拟化第三方的正式要求
Generation Architectures”,ACM 通信 v 17 no 7（1974 年 7 月)第 412-421 页

[1533] E Porter，“Facebook 谬论:隐私由你决定”,纽约时报
2018 年 4 月 24 日

[1534] R Porter，“谷歌因在法国违反 GDPR 被罚款 5000 万欧元” The
边缘 2019 年 1 月 21 日

[1535] B Poser，“The Provenzano Code”,语言日志,2006 年 4 月 21 日;在 http://itre.cis.upenn.edu/
~myl/languagelog/archives/003049.html

[1536] Richard Posner，“隐私的经济理论”,法规（1978 年)第
19–26

[1537] Richard Posner，“隐私、保密和声誉”,载于 Bu alo Law Review v 28 no 1 (1979)

[1538] F Postma，“军事和情报人员可以通过
Untappd Beer App”,Bellingcat,2020 年 5 月 18 日

[1539] K Poulsen，“ATM Reprogramming Caper Hits Pennsylvania”,《连线》杂志，
2007 年 7 月 12 日

[1540] S Poulter，“电话公司的告密者说他的生活一直很痛苦”，
在每日邮报 2007 年 6 月 21 日

[1541] J Powles，“DeepMind 最新的 AI 健康突破存在一些问题”,Medium,2019 年 8 月 8 日

[1542] J Powles、H Hodson，“算法时代的 Google DeepMind 和医疗保健”,Health and Technology v 7
no 4（2017 年 12 月)第 351-367 页

[1543] S Prasad、E Bouma-Sims、AK Mylappan、B Reaves，“谁在召唤?通过音频和元数据分析来表征
Robocalls” Usenix Security 2020

[1544] J Preece、H Sharp、Y Rogers，“交互设计:超越人机交互”,Wiley（2002 年）

[1545] B Preneel,PC van Oorschot，“MDx-MAC 和构建快速 MAC,来自
哈希函数”,密码学进展 – Crypto 95,Springer LNCS v 963 第 1-14 页

[1546] 总统科学技术顾问委员会，“大数据和
隐私:技术视角”,2014 年 5 月 1 日

[1547] 新闻协会，“哈顿花园头目‘巴兹尔’被判有罪
1400 万英镑的抢劫案”,《卫报》,2019 年 3 月 15 日

[1548] L Presser、M Hruskova、H Rowbottom、J Kancir，“Care.data 和访问英国健康记录:患者隐私和公众
信任”,技术科学杂志,2015 年 8 月 8 日

[1549] RS Pressman，“软件工程:从业者的方法”，
McGraw-Hill（第 5 版,2000 年）

[1550] V Prevelakis,D Spinellis，“雅典空气”,IEEE Spectrum,2007 年 7 月

[1551] H Pringle，“现金的摇篮”,载于 Discover v 19 no 10（1998 年 10 月）

[1552] C Prins，“生物识别技术法”,载于《计算机法与安全》
报告 v 14 no 3（98 年 5 月/6 月)第 159–165 页

[1553] W Pritchard，“封锁对 Spotify 来说是一个福音。现在音乐家正在反击”,《连线》杂志，
2020 年 7 月 19 日

[1554] Privacy International，“谁在敲我的门？ Understanding Surveillance in Thailand 2017，
https://privacyinternational.org/sites/default/files/2017-10/thailand_2017_0.pdf

[1555] Privacy International，“电话提取的技术观察”,2019 年,https://privacyinternational.org/
long-read/3256/technical-look-phone-extraction

[1556] S Proctor、EY Wassermann、J Hatcli ，“安全可靠:在新的危害分析中深度集成安全性”,SAW
2017

[1557] S Proti`ere、A Boudaoud、Y Couder，“流体界面上的粒子波关联”,流体力学杂志 v 554 no 10
(2006) pp 85-108

[1558] A Pruneda，“Windows Media Technologies:使用 Windows Media Rights Manager 保护和分
发数字媒体”,MSDN 杂志,2001 年 12 月,网址为 http://msdn.microsoft.com/msdnmag/
issues/01/12/DRM /

[1559] 公共账户委员会，“公共账户委员会 第十九次报告:NHS 中被废除的 IT 国家计划”,2013 年 7 月

[1560] 公共账户委员会，“国防部核计划”,9 月
2018

[1561] 公共借阅权 (PLR),位于 http://www.writers.org.uk/guild/Crafts/Books/PLRBody.html

[1562] 公共记录办公室，“电子记录管理系统的功能要求”,1999 年 11 月

[1563] RD Putnam，“独自打保龄球:美国社区的崩溃和复兴”,Simon & Schuster,2000

[1564] T Pyszczynski、S Solomon、J Greenberg，“9/11 之后 Psy
恐怖心理学”,美国心理学会 2003

[1565] Quality Control Systems Corporation，“NHTSA 难以置信的安全声明”
用于特斯拉的 Autosteer 驾驶员辅助系统”,2019 年 2 月 8 日

[1566] B Quinn、J Ball、Rushe，“GCHQ 负责人指责美国科技巨头成为恐怖分子的‘首选网络’”,《卫
报》,2014 年 11 月 3 日

[1567] Z Quinn， Crash Override ,阿歇特 2017

[1568] JJ Quisquater,D Samyde，“电磁分析（EMA）:智能卡的措施和对策”国际会议

智能卡研究,Springer LNCS v 2140,第 200 - 210 页

[1569] R v Paul Matthew Stubbs,[2006] EWCA Crim 2312（2006 年 10 月 12 日）,http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWCA/Crim /2006/2312.html

[1570] H Ragab、A Milburn、K Razavi、H Bos、C Giu rida，“串扰：跨内核的推测性数据泄漏是真实的”，IEEE 安全和安全研讨会
隐私 (2021)

[1571] M Raghavan、S Barocas、J Kleinberg、K Levy，“减轻算法招聘中的偏见：评估索赔和实践”，arXiv：1906.09208 2019 年 6 月 21 日

[1572] Rain Forest Puppy，“问题披露政策 v1.1”，网址为 http://www.wiretrip。网/rfp/policy.html

[1573] R Ramesh，“NHS England 患者数据‘上传到谷歌服务器’，保守党国会议员说 ” 卫报 2014 年 3 月 3 日

[1574] R Ramesh，“评论家说，在线工具可用于识别公众人物的医疗服务”，卫报，2014 年 3 月 17 日

[1575] A Randal，“理想与现实：重温虚拟机和容器的历史”，arXiv:1904.12226，2019 年 4 月 27 日

[1576] M Randolph、W Diehl，“电源侧信道攻击分析：回顾外行学习 20 年”，Cryptography v 4 no 15 (2020)

[1577] J Rankin，“欧盟称中国是 Covid-19 虚假信息‘巨浪’的幕后黑手”，卫报 2020 年 6 月 10 日

[1578] W Rankl, W Eng, 智能卡手册 , Wiley (1997)；翻译自 Handbuch der Chpkarten ，Carl Hanser Verlag (1995)

[1579] S Ransbotham，“基于开源软件中的漏洞”，WEIS 2010

[1580] S Rashid，“打破分类帐安全模型”，https://saleemrashid.com/ 2018 年 3 月 20 日

[1581] FY Rashid，“使 https 证书每年过期的提案重新回到桌面”，Decipher 2019 年 8 月 15 日

[1582] B Ray，“我如何用一条短信破解 SIM 卡 以及网络不关心”，The Register 2013 年 9 月 23 日

[1583] ES Raymond，“地震作弊案例”，27/12/1999，位于 http://www.catb.org/~esr/writings/quake-cheats.html

[1584] ES Raymond，“大教堂和集市”，网址为 http://www.catb.org/~esr/writings/大教堂集市/

[1585] ES Raymond，“魔法大锅”，1999 年 6 月，http://www.catb.org/~esr/writings/magic-cauldron/magic-cauldron.html

[1586] A Razaghpanah，R Nithyanand，N Vallina-Rodriguez，S Sundaresan，M Allman、C Kreibich、P Gill，“应用程序、追踪器、隐私和监管机构：A 移动跟踪生态系统的全球研究”NDSS 2018

[1587] K Razavi, B Gras, E Bosman, B Preneel, C Giu rida, H Bos, “Flip Feng Shui：在软件堆栈中敲打针，”USENIX Security 2016

[1588] J Reardon,A Feal,AE Bar On,N Valina-Rodriguez,S Egelman，“泄露数据的 50 种方法:应用程序规避 Android 的探索
权限系统”,Usenix Security 2019

[1589] J Reason，“人为错误”,剑桥大学出版社 1990 年

[1590] MG Reed、PF Syverson、DM Goldschlag，“匿名连接和
洋葱路由”,IEEE 通讯特殊领域杂志 v 16 no 4（98 年 5 月)第 482-494 页

[1591] EM Redmiles，“数字安全教育中的质量和不公平”,博士
论文,马里兰大学,2019

[1592] J Rees，“南威尔士警方裁定面部识别使用非法”,BBC
新闻,2020 年 8 月 11 日

[1593] P Reidy，“MH17:五个最离奇的阴谋论”,The
卫报 2014 年 7 月 22 日

[1594] 无国界记者，“博主和网络持不同政见者手册”,2005 年,http://www.rsf.org/rubrique.php3?id_rubrique=542

[1595] E Rescorla，“SSL 和 TLS – 设计和构建安全系统”，
艾迪生卫斯理 2000

[1596] E Rescorla，“寻找安全漏洞是个好主意吗？”,第三次信息安全经济学研讨会（2004 年）

[1597] 路透社，“坦帕没有监控技术”,2003 年 8 月 21 日连线,http://www.wired.com/politics/law/news/2003/08/60140

[1598] M Reynolds，“第 230 条的奇怪故事,创造我们有缺陷的、破碎的互联网的晦涩法律”,《连线》杂志,2019 年 3 月 24 日

[1599] I Reyes、P Wijesekera、J Reardon、A Elazari Bar On、A Razaghpanah、N Vallina-Rodriguez、S Egelman，“‘有人不会想到孩子吗？’大规模检查 COPPA 合规性”,隐私增强技术会议记录(2018) 第 63-83 页

[1600] M 理查兹、R 安德森、S 欣德、J 凯、A 卢卡森、P 马修斯、M
Parker, M Shotter, G Watts, S Wallace, J Wise，“生物医学研究和医疗保健中数据的收集、链接和使用:伦理问题”,Nueld
生物伦理委员会,2015 年 2 月

[1601] D Richardson，“电子战技术和设备”,Sala
曼德图书 (1985)

[1602] T Richter、S Escher、D SchA unfeld、T Strufe，“法医分析和
印刷文件的匿名化” IH&MMSec 18 pp 127–138

[1603] LW Ricketts、JE Bridges、J Miletta，“EMP 辐射和防护技术”,Wiley 1975

[1604] M Ridley，“红皇后:性与人性的进化”，
维京图书 (1993)

[1605] G Rippon，“性别大脑”,Bodley Head,2019

[1606] J Risen、E Lichtblau，“布什让美国在没有法庭的情况下监视来电者”,纽约时报,2005 年 12 月 16 日

[1607] RL Rivest、A Shamir、L Adleman，“一种获取数字签名和公钥密码系统的方法”，ACM 通信 v 21 no 2（1978 年 2 月)第 120-126 页

[1608] RL Rivest、J Wack，“关于投票系统中‘软件独立性’的概念”，皇家学会哲学汇刊 A v 366 no 1881 pp 3759–67（2008 年 11 月）

[1609] MB Robinson，“‘CPTED’的理论发展:25 年对 C. Ray Jeery 的回应”，犯罪学理论进展第 8 期;在 http://www.acs.appstate.edu/dept/ps-cj/vitacpted2.html

[1610] AR Roddy，JD Stosz，“指纹特征 统计分析和
System Performance Estimates”，载于 IEEE 会议记录 v 85 no 9（9 月 97 日)第 1390-1421 页

[1611] J Rogers，“FAKE FIVER:购物者收到这张 5 英镑假钞后的警告 但它是假钞吗？”，《太阳报》，2018 年 5 月 13 日

[1612] WP Rogers，NA Armstrong，DC Acheson，EE Covert，RP Feynman，RB Hotz、DJ Kutyna、SK Ride、RW Rummel、JF Sutter、ABC Walker、AD Wheelon、CB Yeager、AG Keel，“总统向总统报告
挑战者号航天飞机事故调查委员会，1986 年 6 月 6 日

[1613] R Rohozinski、M Mambetalieva，“吉尔吉斯斯坦的选举监督”，2005 年，开放网络倡议，网址为 http://opennet.net/special/kg/

[1614] E Ronen、C O Flynn、A Shamir、AO Weingarten，“IoT Goes Nuclear:Cre ating a ZigBee Chain Reaction”，IACR Eprint 1047 (2016)

[1615] K Rooney，“新研究发现，大多数比特币交易都是骗局” CNBC
2019 年 3 月 22 日

[1616] SJ Root，“超越 COSO 加强公司治理的内部控制”，Wiley 1998

[1617] N Rosasco、D Larochelle，“更多安全技术如何以及为何在传统市场取得成功:SSH 成功的教训”，载于 WEIS 2003

[1618] S Rose、O Borchert、S Mitchell、S Connelly，“零信任架构（第二届
草案）”，SP 800-207（草案），2020 年 2 月

[1619] M Rosenberg，JE Barnes，“燃烧的圣经，一家俄罗斯通讯社和一个好到无法检查的故事”，纽约时报，2020 年 8 月 11 日

[1620] B Ross、C Jackson、N Miyake、D Boneh、JC Mitchell，“使用浏览器扩展进行更强大的密码验证”，载于 Usenix Security 2005;在 http://crypto.stanford.edu/PwdHash/

[1621] DE Ross，“两个签名”，comp.risks v 20.81:http://catless.ncl。 ac.uk/Risks/20.81.html

[1622] A Roth，“美国以 1 亿美元的银行计划向俄罗斯‘邪恶公司’黑客收费”，《卫报》，2019 年 12 月 5 日

[1623] “法国的信用卡欺诈急剧下降”，M Rowe，银行技术（94 年 5 月）
第 10 页

[1624] T Rowland，“拨错号码”，《卫报》，2006 年 5 月 18 日；在 http://www.guardian.co.uk/media/2006/may/18/newmedia。技术

[1625] A Roy, N Memon, A Ross “MasterPrint: Exploring the Vulnerability of 部分基于指纹的身份验证系统”，IEEE Transactions on 信息取证与安全 v 12 no 9（2017 年 9 月）2013–25

[1626] 英国皇家学会，“英国分离钚的战略选择”，9 月 2007年27日

[1627] 英国皇家学会，“作为开放企业的科学”，2012 年 6 月 21 日

[1628] WW Royce，“管理大型软件系统的开发：概念和技术”，在 Proceedings IEEE WESCON (1970) pp 1-9

[1629] HH Rubinovitz，“与将应用程序移植到分区模式工作站相关的问题”，ACM SIGSAC v 12 no 4（94 年 10 月）第 2-5 页

[1630] RA Rueppel，“流密码的分析与设计”，施普林格出版社 (1986)

[1631] RA Rueppel，“对 ISO CD 11166 银行业的批评：密钥管理 非对称算法的方法”，在第 3 届研讨会论文集中 密码学研究现状与进展，Fondazione Ugo Bordoni，罗马 1993，第 191-198 页

[1632] J Rushby、B Randell，“分布式安全系统”，IEEE Computer v 16 no 7（83 年 7 月）第 55-67 页

[1633] B Russell，对议会问题的回答，Hansard 2003 年 6 月 10 日专栏 762W

[1634] J Rutkowska，“每天运行 Vista！”，Invisible Things 博客，2007 年 2 月

[1635] M Ryan，“NSA Playset：蓝牙智能攻击工具”，在蓝牙 智能安全，http://lacklustre.net/bluetooth/，2015 年

[1636] DR Sa ord、DL Schales、DK Hess，“TAMU 安全包：一个 在学术环境中对互联网入侵者的持续反应”，在 Usenix 安全 (1993) 第 91–118 页

[1637] M Safi，“印度执政党下令在网上辱骂对手，索赔书”，卫报，2016 年 12 月 27 日

[1638] MJ Salganik、I Lundberg、AT Kindel 等人，“通过科学大规模合作测量生活结果的可预测性”，美国国家科学院院刊 v 117 no 15 pp 8398–8403，2020 年 3 月 30 日

[1639] JH Saltzer, MD Schroeder，“计算机信息保护 系统”，在 IEEE 会议记录 v 63 no 9（1975 年 3 月）第 1278-1308 页

[1640] JH Saltzer，MF Kaashoek，计算机系统设计原理，Morgan 考夫曼 2009

[1641] RG Saltman，“计算机化投票的准确性、完整性和安全性” Tallying ，国家统计局特刊 500-158 (1988)

[1642] J Saltzman、M Daniel，“男子在 1997 年枪杀警察时获释 法官在揭露指纹后作出裁决”，波士顿环球报，2004 年 1 月 24 日

[1643] P Samarati、L Sweeney，“在披露信息时保护隐私：k-匿名及其通过泛化和抑制的实施”，SRI 技术报告 SRI-CSL-98-04 (1998)

[1644] T Sammes，B Jenkinson，“法医计算 从业者指南”，施普林格 (2007)

[1645] I Sample，“NHS 患者记录彻底改变英国的医学研究”卫报 2012 年 8 月 28 日

[1646] P 萨缪尔森，“知识产权和全球信息经济”，ACM 通讯 v 39 no 1（96 年 1 月）第 23-28 页

[1647] P Samuelson、S Scotchmer，“逆向工程的法律和经济学”，耶鲁法律杂志（2002 年）

[1648] D Samyde、SP Skorobogatov、RJ Anderson、JJ Quisquater，“关于一个新的从内存中读取数据的方法”，IEEE 存储安全研讨会 (2002) 第 65-69 页

[1649] RS Sandhu，S Jajodia，“封面故事的多实例化”，在计算机中安全 ESORICS 92，LNCS v 648，第 307–328 页

[1650] P Sankar、S Mora、JF Merz、NL Jones，“患者对医疗的看法保密性 文献综述”，J Gen Intern Med 2003 8 月第 18 卷第 8 期 659–669 页

[1651] SANS 研究所，“十大互联网安全威胁的共识列表”，网址为 http://www.sans.org/，版本 1.22，2000 年 6 月 19 日

[1652] G Sandoval，“Glitches let Net shoppers get free goods”，CNET News.com，2000 年 7 月 5 日；在 http://news.cnet.com/news/0-1007-200-2208733.html

[1653] DE Sanger、K Benner，“美国指责朝鲜密谋损害经济作为间谍在 Sony Hack 中被指控”，纽约时报，2018 年 9 月 6 日

[1654] PF Sass，L Gorr，“21 世纪数字化战场的通信世纪”，IEEE Communications v 33 no 10（95 年 10 月）第 86-95 页

[1655] E Van der Sar，“BitTorrent ‘Copyright Troll’ Lawsuits Skyrocket in Swe书房”，Torrentfreak 2020 年 2 月 14 日

[1656] C Savage，“美国国家安全局电话项目耗资 1 亿美元，但只产生了两条独特的线索”，纽约时报，2020 年 2 月 25 日

[1657] S Saulny，“9/11 后 118 人因 ATM 盗窃案被起诉”，纽约时报，2003 年 6 月 19 日

[1658] J Scahill，J Begley，“间谍如何窃取加密城堡的钥匙”，The拦截 2015 年 2 月 15 日

[1659] W Schachtman，“技术如何差点输掉战争：在伊拉克，关键网络是社交网络而非电子网络”，《连线》杂志，2007 年 12 月 15 日，http://www.wired.com/politics/security/magazine /15-12/ff_futurewar?currentPage=all

[1660] M Schaefer，“符号安全条件被认为是有害的”，载于 1989 年 IEEE 安全和隐私研讨会论文集，第 20-46 页

[1661] DL Schilling，“流星爆发通信：理论与实践”，Wiley (1993)

[1662] DC Schleher，“信息时代的电子战”，Artech House (1999)

[1663] D Schmandt-Besserat，“写作的起源”，德克萨斯大学出版社（1996 年），http://www.dla.utexas.edu/depts/lrc/numerals/dsb1。网页格式

[1664] MN Schmitt，“适用于网络战的国际法塔林手册”，剑桥大学出版社 2013 年，第一版；2017 年，第二版

[1665] ZE Schnabel，“湖中鱼类总数的估计”，载于美国数学月刊 v 45 (1938) pp 348–352

[1666] PM Schneider，“Datenbanken mit genetischen Merkmalen von Straft¨atern”，在 Datenschutz und Datensicherheit v 22 (6/1998) pp 330–333

[1667] B Schneier，“应用密码学”，Wiley（1996 年）

[1668] B Schneier，“为什么计算机不安全”，comp.risks v 20.67

[1669] B Schneier，“秘密与谎言：网络世界中的数字安全”，威利 (2000)

[1670] B Schneier，“语义攻击：第三波网络攻击”，Crypto-Gram 通讯，2000 年 10 月 15 日，网址为 http://www.schneier.com/crypto-gram-0010.html

[1671] B Schneier，“超越恐惧：在不确定的情况下明智地思考安全”世界”，哥白尼书籍 (2003)

[1672] B Schneier，“真实世界的密码”，在 Crypto-Gram Newsletter 12 月 14 日，2006年

[1673] B Schneier，“选择安全密码”，2007 年 8 月 7 日；在 http://www. schneier.com/blog/archives/2007/08/asking_for_pass.html

[1674] B Schneier，“安全密码让您更安全，在 Crypto-Gram 时事通讯中 2007 年 1 月 11 日

[1675] B Schneier，“安全心理学”，RSA 会议（2007 年），网址为 http://www.schneier.com/essay-155.html

[1676] B Schneier，“Debian Linux 中的随机数错误”，2020 年 5 月 19 日

[1677] B Schneier，“9/11 导致汽车死亡人数过多”，2013 年 9 月 9 日

[1678] B Schneier，“评估 GCHQ 例外访问提案”，Lawfare 博客 2019 年 1 月 17 日

[1679] B Schneier，“原创引擎 黑客如何改变世界，无论好坏”，将于 2021 年出版；Bruce 在 2020 年安全与人类行为研讨会上宣布了这本书，他的演讲在 https://www.lightbluetouchpaper.org/2020/06/18/security-and-human-behaviour-2020/ 上进行了直播

[1680] B Schneier,A Shostack，“分手很难:为智能卡建模安全威胁”,USENIX 智能卡技术研讨会 1999，第 175-185 页,网址为 http://www.schneier.com / paper-smart-card-threats.html

[1681] M Schnyder，“Datenfluesse im Gesundheitswesen”,in in in Symposium fur ¨ Datenschutz und Informationssicherheit,苏黎世,10 月 98 日

[1682] RA Scholtz，“扩频通信的起源”,IEEE Transactions on Communications v TC-30 no 5（1982 年 5 月)第 822-854 页

[1683] M Schrems，“CJEU 判决 第一声明”,https://noyb.eu 16 2020

[1684] MD Schroeder，“计算机实用程序中相互可疑子系统的合作”,麻省理工学院博士论文,1972 年 9 月,MAC 项目技术报告 MAC TR-104 http://hdl.handle.net/ncstrl.mit_lcs/MIT/濒海战斗舰/ TR-104

[1685] 熊彼特，“现场直播将使摇滚乐变得更好”,The 经济学家,2020 年 6 月 17 日

[1686] 熊彼特，“公司为何与顽固的 IT 作斗争”,The 经济学家,2020 年 7 月 18 日

[1687] K Schwab，“googly eyes 如何解决当今最棘手的 UX 问题之一” 快公司 2019 年 8 月 27 日

[1688] M Schwarz、S Weiser、D Gruss，“Intel 实用飞地恶意软件 SGX”,arXiv:1902.03256 2019 年 2 月 8 日

[1689] M Schwarz、S Weiser、D Gruss、C Maurice、S Mangard，“恶意软件卫士扩展:滥用英特尔 SGX 来隐藏缓存攻击”,Cybersecurity v 3 (2020)

[1690] N斯科拉。 “卡玛拉·哈里斯 (Kamala Harris) 反对‘复仇色情’”,Politico Feb 1 2019

[1691] M Scorgie,Genizah Fragments（剑桥大学 Taylor-Schechter Genizah 研究单位通讯)第 29 期（1995 年 4 月)中的“会计师未开发资源”,网址为:http://www.lib.cam.ac.uk/ Taylor-Schechter/GF/GF29.html

[1692] J Scott-Railton,A Hulcoop,B Abdul Razzak,B Marczak,S Anstis,R Deibert，“黑暗盆地 揭露大规模的黑客雇佣行动”， 公民实验室 2020 年 6 月 9 日

[1693] Beale Screamer，“Microsoft DRM - 技术说明”和支持文档,Cryptome.org,2001 年 10 月 23 日;在 http://cryptome.org/beale-sci-crypt.htm

[1694] M Seaborn、T Dullien，“利用 DRAM rowhammer 漏洞获取内核权限”,Google 项目零博客，2015 年 3 月 9 日

[1695] T Seals 2020，“70% 的移动、桌面应用程序包含开源错误”,Threatpost 2020 年 5 月 25 日

[1696] “新的 RCS 技术使大多数 mbile 用户面临黑客攻击”,安全研究实验室,2019 年 11 月 29 日，https://www.srlanbs.de/bites/rcs-hacking/

[1697] E Selleck，“Apple 的 App Store 充斥着赌博和其他应用程序
That Abuse Enterprise Certificates”，iPhone 黑客，2019 年 2 月 12 日

[1698] L Seltzer，“英特尔新技术保护销售点数据”，ZDNet 2014 年 10 月 15 日

[1699] W Seltzer, M Anderson，“第二次战争权力法案下的人口普查保密性（1942-1947）”，美国人口协会年会，2007 年 3 月 30 日，纽约；在 Ocial Statistics and Statistical Confidentiality: Recent Writings and Essential Documents，http://www. uwm.edu/~margo/govstat/integrity.htm

[1700] R Senderek，“密钥实验 PGP 如何处理被操纵的密钥”，2000 年，位于 http://senderek.de/security/key-experiments.html

[1701] Chandak Sengoopta，“拉吉的印记”，Pan Macmillan 2004

[1702] R Severo，“Hedy Lamarr，统治 30 和 40 年代好莱坞的性感明星，享年 86 岁”，《纽约时报》2000 年 1 月 20 日；美国专利号 2,292,387（HK Markey 等人，1942 年 8 月 11 日）

[1703] A Shamir，“如何分享秘密”，ACM 通讯 v 22 no 11（1979 年 11 月）第 612-613 页

[1704] A Shamir，“基于身份的密码系统和签名方案”，载于 1984 年密码学报，Springer LNCS v 196，第 47-53 页

[1705] A Shamir，“研究公告：微处理器漏洞可能成为安全灾难”，2007 年 11 月，http://cryptome.org/bug-attack.htm

[1706] A Shamir、I Safran、E Ronen、O Dunkelman，“对小汉明距离对抗样本存在的简单解释”，arXiv 1901.10861，2019 年 1 月 30 日

[1707] M Sherr、E Cronin、S Clark、M Blaze，“窃听系统中的信号漏洞”，IEEE 安全和隐私 v 3 no 6（2005 年 11 月/12 月）第 13-25 页

[1708] H Shacham，“骨骼上无辜肉体的几何形状：无需函数调用（在 x86 上）返回到 libc”，ACM CCS 2007 第 552-561 页。

[1709] Y Shachmurove、G Fishman、S Hakim，“作为理性经济主体的窃贼”，技术报告 CARESS 工作论文 97-07，宾夕法尼亚大学经济与社会分析研究中心

科学，1997 年 6 月

[1710] J Shafer，“特朗普的每日分心剂量”，Politico 2020 年 5 月 19 日

[1711] G Shah、A Molina、M Blaze，“键盘和隐蔽通道”，2006 年第 15 届 USENIX 安全研讨会，网址为 http://www.crypto.com/papers/

[1712] A Shaik、R Borgaonkar、SJ Park、JP Seifert，“4G 和
5G 蜂窝接入网络协议：公开设备功能”，WiSec 2019 第 221-231 页

[1713] Y Shaked, A Wool，“破解蓝牙 PIN”，2005 年，http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html

[1714] CE Shannon，“通信的数学理论”，贝尔系统
技术期刊 v 27 (1948) 第 379–423、623–656 页

[1715] CE Shannon，“保密系统的通信理论”，贝尔系统
技术杂志 v 28 (1949) pp 656–715

[1716] C Shapiro，“民粹主义时代的反垄断”，SSRN 3058345，2017

[1717] C Shapiro，“保护美国经济中的竞争：合并
控制、科技巨头、劳动力市场”，经济展望杂志 v 33 no 3 (2019) pp 69–93

[1718] C Shapiro，H Varian，“信息规则”，哈佛商学院出版社
(1998)

[1719] K Sharad、G Danezis，“一种自动化的社交图去匿名化
技术”，WPES 14 – 电子社会隐私研讨会 (2014) 第 47-58 页

[1720] M Sharif、S Bhagavatula、L Bauer、M Reiter，“附属于犯罪：对最先进的人脸识别的真实和
隐秘攻击”，ACM CCS (2016)

[1721] D Sherwin，“欺诈 无法管理的风险”，金融犯罪评论 v 1 no 1（2000 年秋季）第 67-69
页

[1722] S Sheye，“SSL 客户端证书 不保护网络”，在 Cryptomathic
NewsOnInk 季刊（2006 年 11 月）

[1723] B Shneiderman，“以人为本的人工智能：可靠、安全和
值得信赖”，国际人机交互杂志 v 36 no 6 (2020) pp 495–504

[1724] JF Shoch、JA Hupp，“ 蠕虫 程序 – 早期经验
分布式计算”，Comm ACM v 25 no 3 (1982) pp 172–180

[1725] PW Shor，“量子计算机算法”，第 35 届 FOCS（1994 年），
IEEE，第 124-134 页

[1726] 2020 年 1 月 13 日对驾驶员和车辆标准局的 FOI 请求的简短回应，网址为 https://
www.whatdotheyknow.com/request/tachograph_offence_statistics

[1727] A Shostack，P Syverson，“隐私的价格是多少？ （以及为什么身份盗窃既不是身份也不
是盗窃）”，信息安全经济学，Kluwer Academic Publishers，2004 年，第 11 章

[1728] V Shoup，“重新考虑 OAEP”，IBM 苏黎世，瑞士，2001 年 9 月 18 日；在 http://
www.shoup.net/papers/oaep.pdf

[1729] JL Shreeve，“芯片与痛苦：金融惨败”，《独立报》四月刊
22 2009

[1730] I Shumailov、YR Zhao、D Bates、N Papernot、R Mullins、R Anderson，“海绵示例：对神
经网络的能量延迟攻击”，arXiv 2006.03463 2020 年 6 月 5 日

伊利亚·舒迈洛夫，

[1731] I Shumailov、L Simon、J Yan、R Anderson，“Hearing your touch: A new acoustic
side channel on smartphones”，arXiv:1903.11137 (2019)，基于第一作者 2017 年的
哲学硕士论文

[1732] I Shumailov、YR Zhao、R Mullins、R Anderson，“禁忌陷阱:对抗样本的行为检测”，arXiv：1811.07375，2018 年 11 月 18 日

[1733] I Shumailov、YR Zhao、R Mullins、R Anderson，“走向可验证的对抗样本检测”，arXiv：2002.08740，2020 年 2 月 20 日

[1734] D Shumow，N Ferguson，“关于 NIST 后门的可能性 SP800-90 Dual Ec Prng”，Crypto rump session (2007)

[1735] O Sibert、D Bernstein、D Van Wie，“DigiBox:信息商务的自我保护容器”，Usenix Security（1995）

[1736] O Sibert、PA Porras、R Lindell，“英特尔 80x86 安全性分析 IEEE Transactions on Software Engineering v 22 no 5（96 月 5 月)第 283-293 页中的“体系结构和实现”

[1737] D Silver、A Huang、CJ Maddison、A Guez、L Sifre、G van den Driessche、J Schrittwieser，我 Antonoglou，V Panneershelvam，M Lanctot，S Dieleman，D Grewe、J Nham、N Kalchbrenner、I Sutskever、T Lillicrap、M Leach、K Kavukcuoglu、T Graepel、D Hassabis，“通过深度神经网络和树搜索掌握围棋游戏”Nature v 529 (2016) 第 484-489 页

[1738] C Silverman，“安装在数百万 Android 手机上的应用程序跟踪用户执行数百万美元广告欺诈计划的行为”，BuzzFeed 新闻，2018 年 10 月 23 日

[1739] C Silverman，“流行的 VPN 和广告拦截应用正在秘密收集用户数据”，BuzzFeed 新闻，2020 年 3 月 9 日

[1740] C Silverman，R Mac，“Facebook 解雇了一名收集右翼页面获得优惠待遇证据的员工”，BuzzFeed 新闻，2020 年 8 月 6 日

[1741] N Silvester，“侵入总理健康记录的医生逃脱了起诉”，每日记录 2012 年 1 月 10 日

[1742] C Simoiu、C Gates、J Bonneau、S Goel，“‘我被告知要购买软件，否则我的电脑就丢了。我忽略了它:勒索软件研究”，SOUPS 2019

[1743] Luther Simjian – 本周发明家，网址为 https://lemelson.mit.edu/资源/luther-george-simjian

[1744] D Simmons，“BBC 愚弄汇丰银行语音识别安全系统”，BBC 2017 年 5 月 19 日

[1745] GJ Simmons，“囚徒问题和潜意识通道”，载于 CRYPTO 83 会议记录，Plenum Press (1984) pp 51–67

[1746] GJ Simmons，“用于验证用户身份和授权的系统销售点或访问点”，Cryptologia v 8 no 1 (1984) pp 1–21

[1747] GJ Simmons，“如何确保为验证条约合规性而获得的数据是值得信赖的”，GJ Simmons，IEEE 会议记录 v 76 no 5（1988 年;转载为 [1748] 中的一章）

[1748] GJ Simmons（编）“当代密码学 信息科学”完整性”，IEEE 出版社（1992 年）

[1749] GJ Simmons，“信息认证调查”，[1748] pp 379–439

[1750] GJ Simmons，“共享秘密和/或共享控制简介
方案及其应用”，[1748] 第 441–497 页

[1751] GJ Simmons,在 1993 年 ACM 计算机和计算机会议上的受邀演讲
通信安全,弗吉尼亚州费尔法克斯,1993 年 11 月 3 日至 5 日

[1752] GJ Simmons，“潜意识通道;过去和现在”，欧洲电信交易 v 5 no 4（94 年 7 月/8 月)第
459–473 页

[1753] GJ Simmons，“潜意识通道的历史”，在 IEEE 期刊上
Selected Areas in Communications v 16 no 4（1998 年 4 月)第 452–462 页

[1754] H Simon，“行政行为”，第 4 版,自由出版社,1997 年

[1755] H Simon，“人工科学”，第 3 版,麻省理工学院出版社,1996 年

[1756] L Simon、RJ Anderson，“PIN Skimmer:通过摄像头时代和麦克风推断 PIN”第三次 ACM
安全和隐私研讨会
智能手机和移动设备 (SPSM 2013) 第 67–78 页

[1757] L Simon,RJ Anderson，“Android 出厂重置的安全分析”，
移动安全技术 (MoST) 2015

[1758] L Simon、D Chisnall、RJ Anderson，“What you get is what you C:控制主流 C 编译器中
的副作用”,IEEE 欧洲安全与隐私研讨会 (EURo S&P) 2018,https://sites .google.com/
view/laurent-simon

[1759] L Simon、WD Xu、RJ Anderson，“我打字时不要打扰我:通过在安卓键盘上的手势打字推断
输入的文本”PoPETs 2016 v 3 pp 136–154

[1760] R Singel，“雅虎揭发中国持不同政见者知道调查是 Po
litical, Documents Show – UPDATED”, 连线 2007 年 7 月 31 日

[1761] R Singel，“点击……窃听:FBI 窃听网络如何运作”，
在连线 2007 年 8 月 29 日

[1762] N Singer,A Krolik，“Grindr 和 OkCupid 传播个人详细信息,研究
说”,EarthInfo 现在 2019 年 1 月 14 日

[1763] N Singer、N Perlroth、A Krolik，“Zoom Rushes to Improve Privacy for
消费者涌入其服务”,纽约时报,2020 年 4 月 8 日

[1764] M Singh、P Leu、S Capkun，“带脉冲重排序的 UWB:确保测距
对抗中继和物理层攻击” NDSS 2019

[1765] A Sipress，“通过手机跟踪 Trac； Md., VA. to Use Transmission to pinpoint
Congestion”,华盛顿邮报 (22/12/1999) p A01

[1766] KS Siyan、J Casad、J Millecan、D Yarashus、P Tso、J Shoults、 Windows
NT Server 4 – Professional Reference ,New Riders Publishing (1996)

[1767] SP Skorobogatov，“现代微控制器中的复制保护”,位于 http://www.cl.cam.ac.uk/
~sps32/mcu_lock.html

[1768] SP Skorobogatov，“静态 RAM 中的低温数据剩磁”,剑桥大学技术报告 UCAM-CL-TR-536
（2002 年 6 月）,位于 http://www.cl.cam.ac.uk/techreports/ UCAM-CL-TR-536.html

[1769] SP Skorobogatov，“半侵入式攻击 硬件安全分析的新方法”，博士论文，2004 年；剑桥大学技术报告 630，2005 年；在 http://www.cl.cam.ac.uk/techreports/

UCAM-CL-TR-630.html

[1770] SP Skorobogatov，“闪存设备中的数据残留”，CHES 2005，第 339-353 页

[1771] SP Skorobogatov，“光学增强位置锁定功率分析”，CHES 2006，第 61-75 页

[1772] SP Skorobogatov，“防篡改和物理攻击”，密码硬件、侧信道和故障攻击暑期学校，2006 年 6 月 12 日至 15 日，比利时新鲁汶； http://www.cl.cam.ac 上的幻灯片。英国/~sps32

[1773] SP Skorobogatov，“硅芯片上的光学监控：您的加密密钥可见”，安全小组研讨会，2009 年 10 月 13 日，幻灯片 https://www. cl.cam.ac.uk/~sps32/

[1774] SP Skorobogatov，“闪存‘碰撞’攻击”，CHES 2010

[1775] SP Skorobogatov，C Woods，“突破性的硅扫描发现军用芯片门”，CHES 2012

[1776] SP Skorobogatov，“安全性、可靠性和后门”，安全小组研讨会，2013 年 5 月 13 日，幻灯片位于 https://www.cl.cam.ac.uk/~sps32/

[1777] SP Skorobogatov，“通往 iPhone 5c NAND 镜像的坎坷之路”，arXiv:1609.04327，2016 年 9 月 14 日；并查看 https://www.cl 上的项目页面。 cam.ac.uk/~sps32/5c_proj.html

[1778] SP Skorobogatov，“无内胎胰岛素泵的深浸拆卸”，arXiv:1709.06026 (2017)

[1779] SP Skorobogatov，“微探针如何攻击加密内存”，Euromicro 数字系统设计会议论文集，AHSA 2017

特别会议 (2017)

[1780] SP Skorobogatov，“硬件安全：当前挑战和未来方向”，IC 硬件分析研讨会，NTU，新加坡 2018 年 http://www.cl.cam.ac.uk/~sps32

[1781] SP Skorobogatov，“硬件安全是否为意外发现做好了准备？”，2018 年 IEEE 集成电路物理和故障分析国际研讨会，第 1-4 页

[1782] SP Skorobogatov，RJ Anderson，“光学故障感应攻击”，密码硬件和嵌入式系统研讨会（CHES 2002），Springer LNCS v 2523 第 2-12 页；在 http://www.cl.cam.ac.uk/~sps32

[1783] SP Skorobogatov，C 伍兹。 “眨眼间：你的 AES 就消失了关键” IACR 预印本 2012/296

[1784] B Skyrms，“社会契约的演变”，剑桥大学出版社 (1996)

[1785] R Sleevi，“生态系统出了什么问题”，CA Browser (2014)，https://cabforum.org/wp-content/uploads/论坛 CABF45-Sleevi-Whats-Wrong-With-the-Ecosystem.pdf

[1786] R Sleevi，“维持数字证书安全”，谷歌安全博客 10 月
28 2015

[1787] P Slovic、ML Finucane、E Peters、DG MacGregor，“理性演员还是理性傻瓜？ A ect Heuristic
对行为经济学的影响”，http://www.decisionresearch.org/pdf/dr498v2.pdf；启发式与偏见：
直觉判断的心理学，CUP (2002) pp 397–420 中的修订版本为“The A ect Heuristic”

[1788] A Smith，“对国家财富的性质和原因的调查”，
1776；在 http://www.econlib.org/LIBRARY/Smith/smWN.html

[1789] A Smith，“新的假 20 英镑纸币‘欺骗店员然后在一周内剥离 ’”，Metro，2018 年 11 月 15 日

[1790] B Smith，“Facebook 与唐纳德特朗普的交易是什么？”纽约时报 2020 年 6 月 21 日

[1791] B 史密斯，“一周老好莱坞终于，实际上死了”纽约
时代 2020 年 8 月 16 日

[1792] C Smith，《汽车黑客手册》，无淀粉出版社，2016 年

[1793] E Smith，“令人难以置信的数字版权管理技术史”，
副 2017 年 10 月 19 日

[1794] RE Smith，“构建高保证邮件防护”，第十七届全国计算机安全会议，10 月 11 日至 14 日，马里兰
州巴尔的摩； NIST 出版的论文集 (1994) pp 247–253

[1795] S Smith、S Weingart，“构建高性能、可编程安全协处理器”，IBM 技术报告 RC 21102，可通过
http://www.ibm.com/security/cryptocards/ 获取

[1796] P Smulders，“通过接收 RS-232 电缆的电磁辐射来窃取信息的威胁”，载于 Computers &
Security v 9 (1990) pp 53–58

[1797] T Snoke，“NTP 服务的最佳实践”，SEI 博客，2017 年 4 月 3 日

[1798] T Snyder，“通往不自由之路”，Bodley Head 2018

[1799] A Soltani、R Calo、C Bergstrom，“接触者追踪应用程序不是解决 COVID-19 危机的方法”，
TechStream，2020 年 4 月 27 日

[1800] O Solon，“NHS 患者数据在线公开”，3 月 3 日连线
2014

[1801] D Solove，“隐私分类法”，宾夕法尼亚大学法律评论 v 154 no 3 (2006) pp 477–560；在 http://
papers.ssrn.com/abstract_id=667622

[1802] R Sommer，V Paxson，“封闭世界之外：关于使用机器
学习网络入侵检测”IEEE 安全与隐私研讨会（2010 年）

[1803] DX Song、D Wagner、XQ Tian，“击键和 SSH 定时攻击的定时分析”，第 10 届 USENIX 安全研讨
会论文集（2001 年）

[1804] R v Department of Health, ex parte Source Informatics: [2000] 2 WLR 940。

[1805] 西南泰晤士河地区卫生局，“伦敦救护车服务调查报告”（1993 年），网址为 http://www.cs.ucl.ac。英国/员工/A.Finkelstein/las.html

[1806] E Spa ord，“互联网蠕虫程序:分析”，《计算机通信评论》v 19 no 1（89 年 1 月)第 17-57 页

[1807] A Sparrow，“NHS 患者记录可能与私营公司共享”，卫报 2011 年 12 月 4 日

[1808] J Specht，“充足的代价:牛肉如何改变美国”卫报 2019 年 5 月 7 日和“红肉共和国”,普林斯顿大学出版社 (2019)

[1809] M Spectre，“指纹会撒谎吗?法医证据的黄金标准正在受到挑战”,纽约时报,2002 年 5 月 27 日

[1810] MA Spectre、J Koppel、D Weitzner，“选票在区块链之前被破坏:Voatz 的安全分析,美国联邦选举中使用的第一个互联网投票应用程序”,2020 年 2 月 13 日

[1811] R Spencer、S Smalley、P Loscocco、M Hibler、D Andersen、J Lepreau，“The Flask 安全架构:对不同安全策略的系统支持”,第 8 届 USENIX 安全研讨会论文集（1999 年)第 123-139 页

[1812] C Spensky、J Stewart、A Yerukhimov、R Shay、A Trachtenberg、R Housley，RK Cunningham，“SoK:移动设备上的隐私 这很复杂”隐私增强技术论文集 2016 年第 3 期

[1813] “Tip von Urmel”,载于 Der Spiegel,1995 年 9 月 11 日

[1814] J Spolsky，“签发护照会让微软成为一个国家吗？”在 http://joel.editthispage.com/stories/storyReader$139

[1815] N Springer，“当应用程序获取您的医疗数据时,您的隐私可能会消失 With It”,纽约时报,2019 年 9 月 3 日

[1816] S Stamm、Z Ramzan、M Jakobsson，“Drive-By Pharming”,印第安纳大学计算机科学系技术报告 TR641,2006 年

[1817] M Stamp,RM Low，“应用密码分析”,Wiley 2007

[1818] T Standage，“维多利亚时代的互联网”,凤凰出版社（1999）

[1819] F Stajano,RJ Anderson，“The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks”, in Security Protocols – 7th International 研讨会”,Springer LNCS 1796 第 172-182 页

[1820] F Stajano、P Wilson，“了解诈骗受害者:系统安全的七项原则”,剑桥大学计算机实验室技术报告第 754 号（2009 年）

[1821] S Staniford、D Moore、V Paxson、N Weaver，“闪存的最高速度蠕虫”,在 WORM04

[1822] “计算机芯片在碳粉盒中的使用及其对售后市场的影响:过去、现在和未来”,Static Control, Inc.,以前位于 http://www.scc-inc.com/special/oemwarfare/whitepaper/默认。 htm,通过 www.archive.org 检索

[1823] N Statt，“Android 版 Fortnite 将为 Epic 的网站放弃 Google Play 商店”，The Verge，2018 年 8 月 3 日

[1824] WA Steer，“VideoDeCrypt”，位于 http://www.ucl.ac.uk/~ucapwas/vdc/

[1825] P Stein、P Feaver，“确保控制核武器”，CSIA 偶尔论文编号 2，哈佛大学 1987 年

[1826] J Steiner、BC Neuman、JI Schiller，“Kerberos：开放网络系统的身份验证服务”，USENIX（1988 年冬季）；“RFC”中的第 5 版 1510：Kerberos 网络身份验证服务 (V5)

[1827] N Stephenson，“雪崩”，Bantam Doubleday Dell（1992 年）

[1828] M Stevens、E Bursztein、P Karpman、A Albertini、Y Markov、A Petit Bianco, C Baisse，“宣布第一次 SHA1 碰撞”，谷歌安全博客（2017 年 2 月 23 日）

[1829] DR Stinson，“密码学 理论与实践”，CRC 出版社（1995 年）

[1830] M Stoller，“缺席所有权：亚马逊、Facebook 和谷歌如何破产 Commerce Without Noticing”，BIG by Matt Stoller 2020 年 7 月 28 日

[1831] B Stone，“亚马逊从 Kindle 上删除奥威尔书籍”，纽约时报 2009 年 7 月 17 日

[1832] B Stone-Gross、T Holz、Gianluca Stringhini 和 Giovanni Vigna，“垃圾邮件的地下经济：僵尸主机对协调的看法 大规模垃圾邮件活动”，USENIX 大规模利用和新兴威胁研讨会 (LEET) (2011)

[1833] PO Stoutland，S Pitts-Kiefer，“新网络时代的核武器”，核威胁倡议 (2018)

[1834] O Storbeck、T Kinder、S Palma，“安永 3 年未能检查 Wirecard 银行对账单”，《金融时报》，2020 年 6 月 26 日

[1835] S Stover、D Dittrich、J Hernandez、S Dittrich，“风暴分析和 Nugache 特洛伊木马：P2P 就在这里”，;登录 2007 年 12 月

[1836] J van der Straaten，“所以你认为数字化是未来?你的互联网数据正在腐烂”，Researchgate，2019 年 5 月

[1837] R Strehle， Verschlusselt – Der Fall Hans Buhler ¨ ，韦德出版社 (1994)

[1838] E Strickland，“专家问题声称 St. Jude Pacemaker 是被黑”，IEEE Spectrum 2016 年 9 月 2 日

[1839] DH Strobel、B Driessen、T Kasper、G Leander、D Oswald、F Schellenberg，C Paar，“发烟酸和密码分析：克服密码分析的便捷工具 数字锁定和访问控制系统”，Crypto 2013 第 147-164 页

[1840] A Stubblefield、J Ioannidis、A Rubin，“使用 Fluhrer、Mantin 和 Shamir Attack to Break WEP”，在 ISOC 2002 中

[1841] C Stupp，“欺诈者在异常网络犯罪案件中使用人工智能模仿 CEO 的声音”，《华尔街日报》，2019 年 8 月 30 日

[1842] G Suarez-Tanguil、G Stringhini，“Android 恶意软件生态系统中八年的 Rider Measurement”，IEEE Transactions on Dependable and 安全计算 (2018)

[1843] Suetonius (Gaius Suetonius Tranquillus)， Vitae XII Caesarum ，Philemon Holland 于 1606 年将其翻译成英文为“History of twelve Caesars”；纳特 (1899)

[1844] T Sugawara、B Cyr、S Rampazzi、D Genkin、K Fu，“光命令：对语音可控系统的基于激光的音频注入攻击”，https://lightcommands.com，2019 年 11 月 11 日

[1845] J Suler，“在线抑制效应 ect”，CyberPsychology & Behavior （2004 年 7 月）

[1846] SC Sundaramurthy、M Wesch、XM Ou、J McHugh、SR Rajagopalan、AG Bardas，“人类是动态的 我们的工具也应该是动态的”，互联网计算第 21 期（2017 年 5 月至 6 月）第 40-46 页

[1847] D Sutherland，“信息模型”，第 9 届全国计算机安全 会议 (1986)

[1848] T Swarbrick，“我们的国家安全委员会是个笑话”Unherd 2020 年 5 月 20 日

[1849] L Sweeney，“编织技术和政策共同维护机密”，载于《法律、医学和伦理学杂志》第 25 卷第 2-3 卷（1997 年）第 98-110 页

[1850] L Sweeney、JS Yoo、L Perovich、KE Boronow、P Brown、JG Brody，“ 回覆 HIPAA 安全港数据中的识别风险：一项环境健康研究数据的研究”，技术科学 2017082801 (2017)

[1851] F Swiderski、W Snyder，“威胁建模”，Microsoft Press 2004

[1852] P Swire，“隐私、安全和机密商业信息的有效保密”，布鲁金斯-沃顿商学院金融服务论文（2003 年），网址为 http://ssrn.com/abstract=383180

[1853] P Swire，“出于安全和竞争原因的披露理论：开源、专有软件和政府机构”，载于《休斯顿法律评论》第 42 期第 5 期（2006 年 1 月）第 101-148 页；在 http://ssrn.com/abstract_id=842228

[1854] 赛门铁克，“赛门铁克互联网安全威胁报告 – 2007 年 1 月至 6 月 7 日第 12 期趋势”，网址为 www.symantec.com/threatreport/

[1855] 可用隐私和安全研讨会，http://cups.cs.cmu.edu/soups/2007/

[1856] J Szczesny，“戴姆勒同意为美国公司支付超过 22 亿美元的数十亿美元柴油和解”，底特律局，2020 年 8 月 14 日

[1857] C Szegedy、W Zaremba、I Sutskever、J Bruna、D Erhan、IJ Goodfellow、R Fergus，“神经网络的有趣特性”，arXiv 1312.6199 (2013)

[1858] A Tang、S Sethumadhavan、S Stolfo，“CLKSCREW：揭露危险 Security-Oblivious Energy Management”，Usenix Security (2017)

[1859] S Tajik、F Ganji、JP Seifert、H Lohrke、C Boit，“激光故障攻击
物理上不可克隆的函数”，FDTC 2015

[1860] AS Tanenbaum，M van Steen“分布式系统”Prentice Hall（2002 年）

[1861] T Tanielian，LH Jaycox，“无形的战争创伤”，兰德公司，2008 年；第 128、436 页

[1862] C Tarnovsky，“复杂的百万美元黑客发现一系列智能卡中的弱点”，https://youtu.be/2td3-sWsiKg；和
“暴露智能卡的深度安全元素”，https://youtu.be/-vnik_iUuUs，均在 hardwear.io (2019)

[1863] C Tavris，E Aronson，“犯了错误 但不是我犯的”，Harcourt 2007

[1864] J Taylor，“在银行、英国警察和国防公司使用的生物识别系统中发现的重大漏洞”，《卫报》，2019 年 8
月 14 日

[1865] J Taylor、MR Johnson、CG Crawford，“DVD Demystified”，第三版，
麦格劳-希尔 2006

[1866] J Tehranian，“从容应对版权改革：弥合法律/规范差距”，2007 年犹他州法律评论，网址为
www.turnergreen.com/publications/Tehranian_Infringement_Nation.pdf

[1867] J Temperton，“塞拉菲尔德内部：英国最危险的核设施如何清理其行为”，《连线》杂志，2016 年 9 月 17
日

[1868] S Tendler, N Nuttall，“黑客在 Yard 的电话上花费了 100 万英镑”，载于 The
泰晤士报，1996 年 8 月 5 日

[1869] T Tengs、M Adams、J Pliskin、D Safran、J Siegel、M Weinstein、J Graham，
“五百种拯救生命的干预措施及其成本效益”，风险
分析 v 15 第 3 期（1995 年）第 369–390 页

[1870] “特斯拉之死”，https://www.tesladeaths.com/，2020 年 6 月 23 日

[1871] E Tews，“DECT 安全分析”，博士论文，达姆施塔特，2012 年

[1872] E Tews、JW¨alde、M Weiner，“Breaking DVB-CSA”，西欧
研讨会，WEWoRC 2011

[1873] E Tews、RP Weinmann、A Pyshkin，“在不到 60 秒内破解 104 位 WEP”，Cryptology ePrint archive，
2007 年 4 月；在 http://eprint.iacr。组织/2007/120.pdf

[1874] RH Thaler，“行为不端：行为经济学的形成”，Penguin
2016年

[1875] RH Thaler，“轻推，而不是污泥”，Science v 361 no 6401 (2018) p 431

[1876] R Thaler，C Sunnstein， Nudge ，Penguin 2009

[1877] L Thalheim、J Krissler、PM Ziegler，“身体检查 – 生物识别访问保护设备及其测试程序”，c 杂志，
2002 年 11 月，第 114 页，网址为 http://www.heise.de /ct/英文/02/11/114/

[1878] H Thimbleby，“提高医疗设备和系统的安全性”，IEEE
医疗保健信息学国际会议 (2013)

[1879] H Thimbleby，“更安全的用户界面:改进数字输入的案例研究”，IEEE Transactions on Software Engineering v 41 no 7 (2015) pp 711–729

[1880] DR Thomas、AR Beresford、A Rice，“Android 的安全指标生态系统”，智能手机和移动设备的安全和隐私研讨会设备，2015 年，第 87-98 页

[1881] TL Thomas，“龙字节:中国信息战理论与实践”，外国军事研究办公室，堪萨斯州利文沃思堡，2004 年

[1882] K Thomas，A Moscicki，“新研究:基本帐户卫生在防止劫持方面的效果如何”，谷歌安全博客，2019 年 5 月 17 日

[1883] K Thompson，“Reflections on Trusting Trust”，ACM 通讯 v 27 no 8（8 月 84 日)第 761-763 页;在 http://www.acm.org/classics/sep95/

[1884] R Thompson，“Google 赞助商链接不安全”，漏洞利用预防实验室，2007 年 4 月 24 日，网址为 http://explabs.blogspot.com/2007/04/google-sponsored-links-not-safe.html;另见 J Richards，“黑客劫持 Google AdWords”，泰晤士报，2007 年 4 月 27 日

[1885] SA Thompson、C Warzel，“1200 万部手机，一个数据集，零优先级 vacy”，纽约时报，2019 年 12 月 19 日

[1886] I Thomson，“谈论意想不到的后果:GDPR 是身份窃贼获取欧洲人数据的梦想门票”，载于 The Register，2019 年 8 月 9 日

[1887] S Thrun、M Montemerlo、H Dahlkamp、D Stavens、A Aron、J Diebel、P Fong、J Gale、M Halpenny、G Ho mann、KL Oakley、M Palatucci、V Pratt、P Stang、S Strohband、 C Dupont、LE Jendrossek、C Koelen、C Markey、C Rummel、J van Niekerk、E Jensen、P Alessandrini、G Bradski、B Davies、S Ettinger、A Kaehler、A Nefian、P Mahoney，“斯坦利:获胜的机器人DARPA Grand Challenge”，Journal of Field Robotics，Springer Texts in Advanced Robotics v 36，第 1-43 页;在 https://robots.stanford。 edu/papers/thrun.stanley05.pdf

[1888] Y Tian、C Herley、S Schechter，“停止猜测:使用猜测的密码来阻止在线猜测”，EuroS&P 2019

[1889] TimeWarner，“Carmine Caridi，电影学院会员，因非法复制而交出颁奖放映员，被勒令向 Warner Bros. Entertainment Inc. 支付 300,000 美元。”，2004 年 11 月 23 日，http://www.timewarner.com /corp/newsroom/pr/0,20812,832500,00.html

[1890] AZ Tirkel, GA Rankin, RM van Schyndel, WJ Ho, NRA Mee, CF Os borne, “电子水印”, in Digital Image Computing, Technology and Applications (DICTA 93) McQuarie University (1993) pp 666–673

[1891] MW Tobias，“锁具、保险箱和安全 国际警察参考资料”（第二版，2000 年），网址为 https://www.securitylaboratories.org/

[1892] MW Tobias，“在五秒或更短时间内通过碰撞打开锁:这真的是对人身安全的威胁吗？”，2006 年，网址为 https://www. securitylaboratories.org/

[1893] MW Tobias，“撞锁 美国的法律问题”，载于 https://www.securitylaboratories.org/

[1894] MW Tobias，“Medeco M3 遇到回形针:这把锁的安全性是否存在风险？”（2007),在 https://www.securitylaboratories.org/

[1895] C Tomlinson，“关于锁构造的基本论文”,1853 年（摘录）,位于 http://www.deter.com/unix/papers/treatise_locks.html

[1896] TT 工具，“麻省理工学院开锁手册”,1991 年;在 http://people.csail。 mit.edu/custo/MITLockGuide.pdf

[1897] R Torrance、D James，“IC 逆向工程的最新技术”，CHES 2009 第 363–381 页;也在 DAC 11 第 333–338 页

[1898] MA Toy，“中国黑客入侵电影节网站”,悉尼先驱晨报 7 月 26 2009

[1899] F Tram`er、P Dupr´e、G Rusak、G Pellegrino、D Boneh，“AdVersar ial:感知广告拦截遇到对抗性机器学习”,arXiv:1811.03194,2019 年 8 月 26 日

[1900] F Tram`er、N Papernot、I Goodfellow、D Boneh、P McDaniel，“可转移对抗样本的空间”,arXiv 1704.03453 2017 年 4 月 11 日

[1901] F Tram`er、F Zhang、A Juels、MK Reiter、T Ristenpart，“通过预测 API 窃取机器学习模型”,arXiv 1609.02943 2016 年 10 月 3 日

[1902] A Travis，“跟踪失败的寻求庇护者的语音 ID 设备”,载于《卫报》2006 年 3 月 10 日

[1903] A Travis，“恐怖嫌疑人因篡改‘错误’标签而被清除”,载于 The 卫报 2013 年 11 月 1 日

[1904] A Travis，“逃离罩袍清真寺的人正处于反恐行动中限制”,《卫报》,2013 年 11 月 5 日

[1905] I Traynor，“欧盟警方同意使用 DNA 数据库”,《卫报》,2007 年 6 月 13 日;在 http://www.guardian.co.uk/international/story/0, ,2101496,00.html

[1906] P Trimintzios、C Hall、R Clayton、R Anderson、E Ouzounis，“互联网互连生态系统的弹性”,ENISA，2011 年 4 月 11 日； WEIS 2011 上发布的删节版

[1907] A Troianovski，“不仅仅是危机:冠状病毒是对普京安全的考验州”,纽约时报,2020 年 3 月 19 日

[1908] E Tromer，“基于硬件的密码分析”,博士论文,魏茨曼科学研究所（2007 年）,网址为 http://www.wisdom.weizmann.ac.il/~tromer/papers/tromer-phd-dissertation .pdf

[1909] C Troncoso、G Danezis、E Kosta、B Preneel，“PriPAYD:隐私友好的按需付费保险”,电子社会隐私研讨会（2007 年）,网址为 https://www.cosic .esat.kuleuven.be/publications/article-944.pdf

[1910] C Troncoso、M Isaakidis、G Danezis、H Halpin “系统化去中心化和隐私:15 年研究和部署的经验教训”隐私增强技术论文集 2017 v 4 307–329

[1911] Z Tufekci，“扎克伯格所谓的隐私转变”,纽约时报 2019 年 3 月 7 日

[1912] JD Tygar、BS Yee、N Heintze，“加密邮资邮戳”，亚洲版
96（Springer-Verlag LNCS v 1179)第 378-391 页，CMU 技术报告 CMU
CS-96-113

[1913] D Uberti，“Facebook 在克赖斯特彻奇之后与白人至上主义恐怖分子开战。它会起作用吗?副 2019 年 10 月
3 日

[1914] R Uhlig，“BT 承认 sta 可能会摆弄系统以赢得协和飞机之旅”，
在每日电讯报 (23/7/1997)

[1915] ukcrypto 邮件列表，位于 http://www.chiark.greenend.org.uk/mailman/
列表信息/ukcrypto

[1916] Underwriters company tory，https://www.company-histories.com/ 实验室 他的
Underwriters-Laboratories-Inc-Company-History.html

[1917] N Unger、S Dechand、J Bonneau、S Fahl、Hg Perl、I Goldberg、M Smith，
“SoK:安全消息”，IEEE 安全隐私，2015 年

[1918] J Ungoed-Thomas，A Lorenz，“法国人为 10 亿英镑的坦克交易玩脏东西”，载于
星期日泰晤士报 2000 年 8 月 6 日

[1919] 英国政府，“e-commerce@its.best.uk”，网址为 http://www. e-envoy.gov.uk/2000/strategy/
strategy.htm

[1920] 英国护照服务处，“生物识别注册试验报告”，2005 年 5 月;在 www.passport.gov.uk/downloads/
UKPSBiometrics_Enrolment_Trial_Report.pdf

[1921] 联合国欧洲经济委员会，“关于在网络安全和网络安全管理系统方面批准车辆的统一规定的新联合国条例提
案”，ECE/TRANS/WP.29/2020/REVISED

[1922] M Untersinger, J Follorou, “EncroChat, cette myst´erieuse soci´et´e tech
nologique pris´ee par le crime organis´e”，世界报，2020 年 8 月 3 日

[1923] UPI 新闻专线，俄克拉荷马州发行，1983 年 11 月 26 日，塔尔萨，
俄克拉何马州

[1924] 美国陆军，“TM 31-210 简易弹药手册”，1969 年，http://cryptome.org/tm-31-210.htm

[1925] 《美国法典》 美国联邦法律，网址为 http://www4.law。
cornell.edu/uscode/

[1926] 美国哥伦比亚特区巡回上诉法院，美国电信协会诉联邦通信委员会和美利坚合众国案，编号 99-1442，2000 年 8
月 15 日，http://pacer.cadc。 uscourts.gov/common/opinions/200008/99-1442a.txt

[1927] 美国法院，“2017 年窃听报告”，网址为 https://www.uscourts。 gov/statistics-reports/wiretap-
report-2017

[1928] 美国移民和海关执法局，“俄罗斯国民承认在跨国网络犯罪组织中的作用，造成超过 5.68 亿美元的损失”，
2020 年 6 月 29 日

[1929] 美国海军，“海军发布菲茨杰拉德号和 USS 的碰撞报告
John S McCain Collisions” NNS171101-07 2017 年 11 月 1 日

[1930] S Usborne，“特斯拉是如何让它的一些汽车在艾尔玛飓风期间行驶得更远的？”，《卫报》，2017 年 9 月 11 日

[1931] S Vaidhyanathan，“Facebook 的新举措与隐私无关。是关于统治”，卫报，2019 年 3 月 7 日

[1932] J Valenti，“Anita Sarkeesian 采访：巨魔 这个词感觉太幼稚了。这是虐待”，《卫报》，2015 年 8 月 29 日

[1933] L van Hove，“电子钱包：（哪条）路要走？”，第一个星期一 v 5 no 7（2000 年 6 月）

[1934] P Van Oorschot、M Wiener，“并行碰撞搜索应用于哈希函数和离散对数”，第二届 ACM 会议
计算机和通信安全第 210-218 页

[1935] R van Renesse，“光学文件安全”（第二版），Artech House (1997)

[1936] R van Renesse，“验证与伪造钞票”，光学安全和防伪技术 II（1998 年），IS&T（The Society for
影像科学与技术）和 SPIE（国际影像学会
光学工程）v 3314，第 71-85 页

[1937] H van Vliet，“软件工程 – 原理与实践”，Wiley（第二版，2000 年）

[1938] R van Voris，“Black Box Car Idea Opens of Worms”，载于法律新闻网络 1999 年 6 月 4 日

[1939] V Varadharajan、N Kumar、Y Mu，“基于安全代理的分布式授权：一种方法”，第 20 届国家信息系统安全
NIST 出版的会议论文集（1998 年）第 315–328 页

[1940] H Varian，“个人隐私的经济方面”，隐私和自我
信息时代的监管，国家电信和信息管理局报告，1996 年

[1941] HR Varian，“中级微观经济学 一种现代方法”（第五届版），诺顿 (1999)

[1942] HR Varian，“新芯片可以严格控制客户”，新
纽约时报 2002 年 7 月 4 日

[1943] H Varian，“管理在线安全风险”，经济科学专栏，
纽约时报，2000 年 6 月 1 日

[1944] H Varian，“新芯片并严格控制消费者，即使他们购买了产品”，纽约时报，2002 年 7 月 4 日

[1945] H Varian，“系统可靠性和搭便车”，Informa 经济学
安全，Kluwer 2004 第 1-15 页

[1946] H Varian，第三届数字版权管理会议的主题演讲，德国柏林，2005 年 1 月 13 日

[1947] M Vasek、J Bonneau、R Castellucci、C Keith、T Moore，“比特币大脑
流失：检查比特币大脑钱包的使用和滥用”，金融
密码学 (2016)

[1948] M 瓦斯，“ Spearmint Rhino 在我十几岁的儿子在家睡觉时拿走了他的钱 – 更多关于膝上
舞俱乐部的抱怨” Bournemouth Daily
回声 2014 年 11 月 15 日

[1949] S Vaudenay，“CBC 填充引起的安全缺陷”，Eurocrypt 2002

[1950] A Vaughan，“英国推出了它知道会失败的护照照片检查程序
深色皮肤”，新科学家，2019 年 10 月 9 日

[1951] W Venema，“墨菲定律与计算机安全”，载于 Usenix Security 96
第 187-193 页

[1952] R Verdult、F Garcia、B Ege，“拆除 Megamos 加密：无线
Lockpicking a Vehicle Immobilizer”，Usenix 2013

[1953] R Verdult、F Garcia，“Megamos Crypto 汽车防盗器的密码分析”USENIX；登录 v 40 第 6 页 17–22

[1954] A Vetterl，“星期四的三篇论文：我们能否正确实现物联网安全？”，
lightbluetouchpaper.org 2020 年 5 月 14 日

[1955] A Vetterl、R Clayton，“Honware：用于捕获 CPE 和 IoT 零日漏洞的虚拟蜜罐框架”APWG 电子犯罪
研讨会
研究（电子犯罪），2019 年 11 月

[1956] “Link 16/MIDS 常见问题”，Viasat，网址为 https://www.
viasat.com/support/data-links/faq

[1957] J Vijayan，“Retail group takes a swivel at PCI, puts card companies on
通知 ”，Computerworld 2007 年 10 月 4 日

[1958] N Villeneuve，“中国的 DNS 篡改”，2007 年 7 月 10 日

[1959] N Villeneuve，“违反信任：对中国 TOM-Skype 平台的监视和安全实践的分析”，信息战监测

2008 年 10 月 1 日

[1960] J Vincent，“欧洲 40% 的‘AI 初创公司’实际上并未使用 AI，
索赔报告”，The Verge，2019 年 3 月 5 日

[1961] B Vinck，“安全架构”（3G TS 33.102 v 3.2.0），来自第三代合作伙伴项目，位于 http://
www.3gpp.org/TSG/Oct_status_list.htm

[1962] B Vinck，“合法拦截要求”(3G TS 33.106 v 3.0.0)，来自第三代合作伙伴项目，网址为 http://
www.3gpp.org/TSG/Oct_status_list.htm

[1963] VISA International，“集成电路芯片卡 – 安全指南”
摘要，版本 2 草稿 1，1997 年 11 月

[1964] A Viterbi，“扩频通信 神话与现实”，载于
IEEE Communications Magazine v 17 no 3（1979 年 5 月）第 11-18 页

[1965] PR Vizcaya、LA Gerhardt，“指纹全局描述的非线性方向模型”，模式识别 v 29 no 7（96 年 7 月)第 1221-1231 页

[1966] W Vogels，“AWS 的现代应用程序”，All Things Distributed，8 月 28 日 2019

[1967] G Volovik，“氦液滴中的宇宙”，克拉伦登出版社，牛津 2003年

[1968] L von Ahn，个人通讯，2006

[1969] L von Ahn、M Blum、NJ Hopper、J Langford，“验证码：使用硬人工智能安全问题”，密码学进展 – Eurocrypt 2003，施普林格 LNCS v 2656 第 294–311 页

[1970] A Vrij， 检测谎言和欺骗：陷阱和机会 WiLey 2008

[1971] D Wagner，“一些最近提出的多种模式的密码分析操作”，在第五届快速软件加密国际研讨会上 (1998), Springer LNCS v 1372 第 254-269 页

[1972] D Wagner、I Goldberg、M Briceno，“GSM 克隆”，http://www.isaac。 cs.berkeley.edu/isaac/gsm-faq.html；另见 http://www.scard.org/gsm/

[1973] D Wagner、B Schneier，“SSL 3.0 协议分析”，第二届 USENIX 电子商务研讨会（1996 年），第 29-40 页；在 http://www.counterpane.com

[1974] M Waldman、AD Rubin、LF Cranor，“Publius：一个强大的、防篡改的、抗审查的网络发布系统”，第 9 届 USENIX 安全研讨会 (2000) 第 59-72 页

[1975] J Walker，“IC 外科手术：用最小的手术刀解决问题的核心” em HardwearIO (2019) https://youtu.be/o1We1o3tMWc

[1976] M Walker，“On the Security of 3GPP Networks”，Eurocrypt 2000 邀请演讲，http://www.ieee-security.org/Cipher/ConfReports/2000/CR2000-Eurocrypt.html

[1977] E Waltz，“信息战 原则和操作”，Artech House (1998)

[1978] XQ Wang、YQ Sun、S Nanda、XF Wang，“从镜子看：通过移动配套应用评估物联网设备安全性” Usenix 2019

[1979] XY Wang、DG Feng、XJ Lai、HB Yu，“哈希函数 MD4 的碰撞，MD5、HAVAL-128 和 RIPEMD”，IACR 密码学 ePrint 存档报告 2004/199

[1980] XY Wang、YQL Yin、HB Yu，“对 SHA1 的碰撞搜索攻击”，2005 年 2 月 13 日，http://www.infosec.sdu.edu.cn/sha-1/shanote.pdf

[1981] XY Wang、HB Yu，“如何破解 MD5 和其他哈希函数”，密码学进展 – Eurocrypt 2005，http://www.infosec.sdu。 edu.cn/paper/md5-attack.pdf

[1982] R Want、A Hopper、V Falcao、J Gibbons，“活动徽章定位系统”，ACM Transactions on Information Systems v 10 no 1（92 年 1 月)第 91-102 页;在 http://www.cl.cam.ac.uk/research/dtg/attarchive/ab。
网页格式

[1983] D Ward，“JTRS：今天的警示故事”，Mitre Disrupting Acquisi
化博客 2020 年 4 月 1 日

[1984] R Ward、B Beyer，“BeyondCorp：企业安全的新方法”
;登录：v 39 no 6 (2014) pp 6–11

[1985] WH Ware，“计算机系统中的安全和隐私”，春季联合计算机会议，1967 年第 279-282 页，网址为 https://www.rand.org/pubs/papers/P3544.html

[1986] WH Ware，“计算机系统的安全控制：国防科学委员会计算机安全工作组的报告”，兰德报告 R609-1（1970 年 2 月），网址为 https://www.rand.org/pubs/reports/ R609-1.html

[1987] M Warner，“数字时代的机器政治”，载于《纽约时报》
2003 年 11 月 9 日

[1988] SD Warren、LD Brandeis，“隐私权”，哈佛法律评论系列 4 (1890)，第 193-195 页

[1989] 废弃电子电气设备 (WEEE) 法规 2007

[1990] S Waterman，“分析：俄罗斯-格鲁吉亚网络战存疑”，太空战争
2008 年 8 月 18 日

[1991] M Watson，“卫星导航‘干扰机’威胁到道路收费计划”，载于
汽车快报 2007 年 8 月 8 日

[1992] RNM Watson，“利用内核系统调用包装器中的并发漏洞”，在第一次 USENIX 攻击性技术研讨会 (WOOT 07) 中，网址为 http://www.watson.org/~robert/2007woot/

[1993] RNM Watson，“操作系统访问控制可扩展性的十年”，Communica
ACM v 56 第 2 期（2013 年 2 月）

[1994] DJ Watts，“六度 互联时代的科学”，海涅曼，
2003年

[1995] N Weaver，“我们的政府已将互联网武器化。他们是怎么做到的”，《连线》杂志，2013 年 11 月 13 日

[1996] W Webb，“高科技安全：亲眼所见”，EDN (18/12/97) pp
75–78

[1997] S Weckert，“Google Maps Hacks – Performance Installation，2020”，http：//www.simonweckert.com/googlemapshacks.html，2020 年 2 月

[1998] SH Weingart，“μABYSS 系统的物理安全”，载于 1987 年 IEEE 安全和隐私研讨会论文集，第 52-58 页

[1999] SH Weingart，“攻击和防御调查”，CHES 2000

[2000] SH Weingart，“注意差距：更新 FIPS 140”，夏威夷 FIPS 物理安全研讨会，2005 年;在 http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper18.pdf

[2001] SH Weingart、SR White、WC Arnold、GP Double，“计算系统物理安全评估系统”，第六届年度计算机
安全应用会议 IEEE (1990) pp 232–243

[2002] L Weinstein，“彩色复印件中的 ID 隐私论坛特别报告”，载于隐私论坛文摘，第 8 期第 18 期（1999 年 12 月 6 日），网址为 http://www.vortex。 com/privacy/priv.08.18

[2003] L Weinstein，“在线病历陷阱”，2007 年 10 月 4 日，网址为：//lauren.vortex.com/archive/000306.html

[2004] K Weise，N Singer，“亚马逊暂停警方使用其面部识别
软件”，纽约时报 2020 年 6 月 10 日

[2005] M Weiss，M Weiss，“对美国电网威胁的评估”，能源，
可持续发展与社会 v 9 no 18 (2019)

[2006] C Weissman，“ADEPT-50 分时系统中的安全控制”，载于 AFIPS 会议论文集，第 35 卷，1969 年秋季联合计算机会议第 119-133 页

[2007] G Welchman，《小屋六层楼》，麦格劳希尔 (1982)

[2008] B Wels、R Gonggrijp，“撞锁”，2006 年，http://www.toool.nl/bumping.pdf

[2009] A Welz，“非自然监视：在线数据如何给物种带来风险”，
耶鲁环境 360，2017 年 9 月，https://e360.yale.edu/features/unnatural-surveillance-how-online-data-is-putting-species-at-risk

[2010] J Werner、J Mason、M Antonakakis、M Polychronakis、F Monrose，“The
最严重的是：针对安全虚拟区域的推理攻击”，ACM Asia CCS 2019 年 7 月

[2011] Western Power Distribution，“智能计量 获取和使用与住宅相关的消耗数据 数据隐私计划”，2018 年 5 月

[2012] A Westfeld、A Pfitzmann，“对隐写系统的攻击”，In Information Hiding (1999)，Springer LNCS v 1768，第 61-76 页

[2013] L Whateley，“有人从我的帐户中偷走了 16,000 英镑，但 Bar clays 不会退还我”，泰晤士报，2011 年 8 月 20 日，网址为 https://www. lightbluetouchpaper.org/2011/12/25/bankers-christmas-present/

[2014] E Whitaker，“在 SBC，一切都与‘规模和范围’有关”，载于《商业周刊》
2005 年 11 月 7 日

[2015] O Whitehouse，“蓝牙：红牙，蓝牙”，CanSecWest/core04，链接自“蓝牙 PIN 破解器：害怕”，网址为 http://www.symantec.com/enterprise/security_response/weblog/2006/ 11/bluetooth_pin_cracker_be_afrai.html

[2016] Z Whittaker，“遇见‘强者’：美国国家安全局被指控窃听两者之间的联系
雅虎、谷歌数据中心”，ZDnet 2013 年 10 月 30 日

[2017] Z Whittaker，“黑客正在从被黑的手机中窃取多年的通话记录
运营商”，Techcrunch，2019 年 6 月 25 日

[2018] A Whitten,JD Tygar，“为什么约翰尼不能加密:PGP 5.0 的可用性评估”,第八届 USENIX 安全研讨会（1999 年)第 169-183 页

[2019] 维基解密，“Vault 7:CIA 黑客工具揭晓”,2017 年 3 月 7 日

[2020] MV Wilkes, RM Needham, The Cambridge CAP computer and its Operating System ，Elsevier North Holland (1979)

[2021] J 威尔金斯，“水星;或秘密和 Swift Messenger:Shewing,How a 人可以在任何距离内以隐私和速度与朋友交流他的想法”,伦敦,里奇·鲍德温 (Rich Baldwin)（1694 年）

[2022] L Wilson，“了解 ISIS 的吸引力”,新英格兰杂志 公共政策 v 29 no 1 (2017)

[2023] C Williams，“加密种子激增盲目记录业务”,载于 The Register 2007 年 11 月 8 日,网址为 http://www.theregister.co.uk/2007/11/08/bittorrent_encryption_explosion/

[2024] TA Williams，“和平的左翼活动家,94 岁,没有犯罪记录,赢得了八年的战斗,从警察‘极端主义’数据库中抹去了他 66 次反战、人头税和学费抗议的细节”,每日邮报2019 年 1 月 24 日

[2025] E Williamson、AJ Walker、KJ Bhaskaran、S Bacon、Chris Bates、CE Mor ton、HJ Curtis、A Mehrkar、D Evans、P Inglesby、J Cockburn、HI Mcdon ald、B MacKenna、L Tomlinson、IJ Douglas， CT Rentsch、R Mathur、A Wong、R Grieve、D Harrison、H Forbes、A Schultze、RT Croker、J Parry、F Hester、S Harper、R Perera、S Evans、L Smeeth、B Goldacre，“安全开放:因素与 1700 万成年 NHS 患者的链接电子健康记录中与 COVID-19 相关的医院死亡相关”medRxiv https://doi.org/10.1101/2020.05.06.20092999 2020 年 5 月 7 日

[2026] B Wilson、J Ho man、J Morgenstern，“对象 De 中的预测不平等保护”,arXiv 1902.11097 2019 年 2 月 21 日

[2027] CL Wilson、MD Garris 和 CI Watson，“Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints”,NIST IR 7110（2004 年 5 月）

[2028] T Wilson，“2005 年 Visa 让 TJX 通过了 PCI”,Dark Reading,2007 年 11 月 12 日,网址为 http://www.darkreading.com/document.asp?doc_id=138838

[2029] H Wimmer, J Perner，“关于信念的信念:错误信念在幼儿对欺骗的理解中的表征和约束功能”，Cognition v 13 no 1 (1983) pp 103–28

[2030] D Winder，“如何从黑客中赚取 100 万美元:认识六位黑客百万富翁”,福布斯,2019 年 8 月 29 日

[2031] FW Winterbotham， The Ultra Secret ,Harper & Row (1974)

[2032] P Woit， 甚至没有错:弦理论的失败和持续统一物理定律的挑战”,Vintage 2007

[2033] 沃尔夫森，“最残酷的骗局”,《信使报》,2005 年 10 月 9 日

[2034] K Wong，“手机欺诈 – GSM 网络安全吗？”,载于计算机欺诈和安全公告（96 年 11 月)第 11-18 页

[2035] N Wong，“法官对司法部的搜索查询说‘不’”，谷歌博客，2006 年 3 月 17 日

[2036] E Wood，“住房设计，一种社会理论”，公民住房和规划
纽约市议会，1961 年

[2037] L Wood，“Security Feed”，载于 CSO，2007 年 4 月 20 日；在 http://www2.
csoonline.com/blog_view.html?CID=32865

[2038] L Wood，“2019 年全球生物识别系统市场报告：规模预计将从 2019 年的 330 亿美元增长到 2024 年的 653
亿美元”，美国商业资讯，2019 年 11 月 7 日

[2039] Z Wood，“Dixons Carphone 因大规模数据泄露被罚款 A ﹀ c500,000”，这
卫报 2020 年 1 月 9 日

[2040] JPL Woodward，“系统高级和分区模式工作站的安全要求”Mitre MTR 9992，修订版 1，1987 年（也由国防
情报局作为文档 DDS-2600-5502-87 发布）

[2041] “自动取款机 (ATM)（每 100,000 名成年人）”，世界银行，https://data.worldbank.org/indicator/
FB.ATM.TOTL.P5

[2042] B Wright，“对明文签名的判决：它们是合法的”，载于计算机法律和安全报告 v 14 no 6（11 月/12 月 94 日）
第 311–312 页

[2043] B Wright，“电子商务法：EDI、传真和电子邮件”，Little，
棕色 1994

[2044] DB Wright，AT McDaid，“使用来自真实阵容的数据比较系统和估计变量”，应用认知心理学 v 10 no 1 pp
75-84

[2045] JB Wright，“武器化和武器生产及军事使用工作组的报告 基本分类政策审查小组报告的附录 F”，美国能
源部科技信息部（1997 年）， http://www.osti.gov/opennet/app-f.html

[2046] MA Wright，“ATM 系统中的安全控制”，在计算机欺诈和
安全公告，1991 年 11 月，第 11-14 页

[2047] P Wright， Spycatcher – 高级情报人员的坦诚自传
Ocer ，William Heinemann 澳大利亚，1987

[2048] L Wouters，J Van den Herreweghen，FD Garcia，D Oswald，B Gierlichs，B
Preneel，“拆解基于 DST-80 的防盗系统”，IACR Trans actions on Cryptographic Hardware and
Embedded Systems v 2 (2020) pp 99–127

[2049] T Wu，“总开关：信息帝国的兴衰”，
克诺夫 (2010)

[2050] T Wu，“注意力商人：进入我们内部的史诗般的争夺”
Heads ，企鹅兰登书屋 (2016)

[2051] R Wyden，致 John Ratcli e 的信，2020 年 6 月 16 日；来自 S Nicholls 的链接，“如果您对员工共享管理员
密码感到绝望，请往好的方面看。这就是 CIA 级安全”，The Register 2020 年 6 月 16 日

[2052] C Wylie， Mindf*ck ，简介书籍 2019

[2053] K Xiao、D Forte、Y Jin、R Karri、S Bhunia、M Tehranipoor，“硬件木马：十年研究后的经验教训”ACM 电子系统设计自动化交易 v 22 no 1（2016 年 5 月）

[2054] JX Yan， Security for Online Games ，博士论文，剑桥大学 2003年

[2055] JX Yan、A Blackwell、RJ Anderson、A Grant，“密码的可记忆性和安全性 一些实证结果”，剑桥大学计算机实验室技术报告第 500 号；也在 IEEE 安全 & 隐私，2004 年 9 月至 10 月，第 25-29 页

[2056] JX Yan、B Randell，“电脑游戏中的安全性：从乒乓到在线 Poker ，纽卡斯尔大学技术报告 CS-TR-889 (2005)

[2057] JX Yan，B Randell，“在线游戏作弊的系统分类”，第四届 ACM SIGCOMM 网络和系统支持游戏研讨会论文集（2005 年）

[2058] T Yl¨onen，“SSH 互联网上的安全登录连接”，载于 Usenix 安全性 96 第 37–42 页

[2059] G Yuval，“重塑 Travois：30 ROM 字节的加密/MAC”，快速软件加密 (1997)，Springer LNCS v 1267，第 205-209 页

[2060] R Zarnekow、W Brenner，“成本在应用程序生命周期中的分布 多案例研究”，欧洲信息系统会议 (ECIS)，(2005)

[2061] ZDnet，“软件阻止金钱图像”，2004 年 1 月 12 日，http://news. zdnet.co.uk/software/0,1000000121,39119018,00.htm

[2062] S van der Zee、R Clayton、RJ Anderson，“巧舌如簧的天赋：租房诈骗者是否精通说服艺术？” arXiv:1911.08253 (2019)

[2063] S van der Zee、R Poppe、PJ Taylor、RJ Anderson，“冻结还是不冻结：一种检测欺骗的文化敏感动作捕捉方法”，PLOS One 2019 年 4 月 12 日

[2064] K Zetter，“法律风暴之眼，默多克的卫星电视黑客 Tells All”，连线，2008 年 5 月 30 日

[2065] K Zetter，“报告：NSA 利用 Heartbleed 窃取两个人的密码年”，连线，2014 年 4 月 11 日

[2066] K Zetter，“黑客可以向医院药物泵发送致命剂量”，《连线》，2015 年 6 月 8 日

[2067] K Zetter，“深入了解对乌克兰权力的狡猾、空前的黑客攻击 Grid”，载于 Wired，2016 年 3 月 3 日

[2068] K Zetter，“研究人员发现臭名昭著的 Flame 恶意软件的新版本”，连线，2019 年 4 月 9 日

[2069] RS Zhang，XY Wang，XH Yan，XX Jiang，“基于 SIP 的计费攻击 VOIP 系统”，在 WOOT 2007 中

[2070] YQ Zhang、F Monrose、M Reiter，“现代密码过期的安全性：算法框架和实证分析”，ACM CCS（2010）

[2071] YR Zhao、I Shumailov、H Cui、XT Gao、R Mullins、R Anderson，“使用近似时间信息对强化学习代理进行黑盒攻击”，DSN-DSML 2020;还有 arXiv:1909.02918 (2019)

[2072] L Zhuang、F Zhou、JD Tygar，第 12 届 ACM CCS（2005 年)中的“键盘声发射再访”

[2073] P Zimbardo，“路西法效应”，兰登书屋（2007 年）

[2074] Ellie Zolfagharifard，“偷猎者如何使用 INSTAGRAM 寻找猎物：带有地理标记的照片帮助猎人追踪和猎杀老虎和犀牛，”《每日邮报》2014 年 5 月 8 日

[2075] S Zubo ，“监视资本主义时代 在新的权力前沿为人类未来而战”，Profile Books，2019

[2076] M Zviran，WJ Haga，“多级密码技术的比较身份验证机制”，载于 The Computer Journal v 36 no 3 (1993) pp 227–237