关乎你、我、他的生存和安危

漏洞

齐向东 著

VULNERABILITY

About You and Me
About Survival and Safety

同济大学出版社
TONGJI UNIVERSITY PRESS

关乎你、我、他的生存和安危

漏洞

齐向东 著

VULNERABILITY

About You and Me
About Survival and Safety

同济大学出版社
TONGJI UNIVERSITY PRESS

图书在版编目(CIP)数据

漏洞 / 齐向东著. —上海：同济大学出版社，2018.8
ISBN 978-7-5608-8075-4

Ⅰ. ①漏… Ⅱ. ①齐… Ⅲ. ①计算机网络-网络安全-研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第180847号

漏洞

齐向东 著
出版策划人 李 舒
出 品 人 华春荣 责任编辑 卢元姗 熊磊丽
责任校对 徐逢乔 封面设计 钱如潺

出版发行 同济大学出版社 www.tongjipress.com.cn
(地址：上海市四平路1239号 邮编：200092 电话：021-65985622)
经 销 全国各地新华书店
排版制作 南京展望文化发展有限公司
印 刷 浙江广育爱多印务有限公司
开 本 787mm×1092mm 1/16
印 张 20.75
字 数 415 000
版 次 2018年8月第1版 2018年8月第1次印刷
书 号 ISBN 978-7-5608-8075-4

定 价 49.00元

齐向东

360公司创始人、360企业安全集团董事长。长期从事网络空间安全领域的先进理论、技术研究工作，牵头开展了十余项国家、地市级网络安全重大课题研究。

他领导创造了360杀毒的整体技术体系，主导了云防护、人工智能杀毒引擎等突破性技术问世，为亿万用户提供了国际领先的安全防护，使我国成为全球恶意软件感染率最低的国家。

2015年，他带领360企业安全集团创新提出“数据驱动安全”理念，在态势感知、追踪溯源等方面实现突破，开发出了一系列“安全+互联网”的创新解决方案。2017年，他担任大数据协同安全技术国家工程实验室主任，带领团队在数据防泄露、系统漏洞分析、安全协同分析等国家急需的技术领域取得了一系列成果，引领了国内技术发展方向。

前　言

前不久，在新员工入职360企业安全集团的训练营开营仪式上，我分享了一个感受：人生就是不断“二选一”的过程，每个看似无关紧要的“二选一”都会改变你以后的人生轨迹。

回首我自己的经历，在学生时代，我选择了每天比别人多学五小时，成为优秀的毕业生，摆脱了农民的宿命。参加工作后，我选择了没有怨言的付出，成为当时新华社里最年轻的局级干部之一。互联网大潮初起之际，我辞职下海，没有选择在大公司当高管，而是选择了与周鸿祎共同创办360。

这十几年，中国互联网产业飞速发展，我一直在思考和探索一个问题，是什么推动了互联网产业的发展？

不满足现状矛盾的渴望，推动互联网应用的发展。十九大报告指出，我们现在社会的主要矛盾是人民日益增长的美好生活需要和不平衡不充分的发展之间的矛盾。互联网应用的发展正是解决不平衡不充分发展的问题，搜索、移动支付、电子商务……一系列互联网应用的出现，解决了信息不对称的问题，提高了效率，美好了人们的生活。

不满足技术缺陷的渴望，推动互联网技术的飞跃。互联网的很多技术，都是基于对缺陷的改进，是不断快速迭代的发展过程。就拿360来说，每一代技术的创新，都是在与网络攻击浪潮的攻防对抗中产生的。病毒的大规模增长，黑名单的瞬息万变，推动我们创新了“白名单”的第二代网络安全技术；APT攻击逐渐成为网络攻击主流，“白利用”攻击手段的多样化，推动我们创新了“查行为”的第三代网络安全技术。

不满足制度欠缺的渴望，推动互联网规则的完善。回想一下，欧盟《通用数据保护条例》的实施、我国网络安全法的出台、电子商务法的拟出台……一系列法律和规章，都是针对在经济社会发展中遇到的制度缺陷所采取的补救措施，规则的完善将推动互联网产业更健康地发展。

发展的路上有光明，也有阴影的存在。很多人背离了初心，利用手中掌握的技术、制度的漏洞，变得不择手段，网络“黑产”的规模正在指数级地快速增长，影响社会和人民稳定生活的高级别网络攻击正在不断发生。同时，在我们貌似强大的背后，也存在着自主信息技术的隐忧，与美国的贸易摩擦，戳穿了虚假的繁华。

没有安全的环境、载体、制度和保障，我们只是在透支互联网的价值，终将成为水中月、镜中花。

2015年，我创办了360企业安全集团。这是我人生中再一次重要的“二选一”。第四次工业革命的浪潮将把人类社会带进智能时代，现在我们所使用和遵循的传统IT的方法，都将成为过去时。在以往的信息化建设时代，发展是主，安全是辅。但在人工智能时代，人工智能、大数据、物联网是基础，安全成为发展的前提。人们的衣食住行都在被快速网络化，更重要的是，水电、煤气、地铁等关键信息基础设施全部联网以后，攻击者不费一枪一炮，通过网络攻击就可以战胜一个国家，这将是未来战争的形态。可以说，没有网络安全，就没有一切。

“有道无术，术尚可求，有术无道，止于术。”如果说，网络安全是互联网发展的“道”，漏洞则是互联网安全的“术”。

要谈网络安全，必须说清漏洞。若只谈漏洞，则不知言之所谓。本书从漏洞入手，谈网络安全，谈360企业安全集团的价值观。

齐向东

2018年7月6日

目　录

前言　/ 001

第一章
善与恶　漏洞是造成危害，还是推动进步　/ 001

第一节　漏洞，源自人性的缺陷　/ 002
◎ 天生缺陷，难免漏洞　/ 002
◎ 漏洞不等同于缺陷　/ 010
第二节　一切漏洞皆被利用　/ 011
◎ 缺陷是怎么被利用的　/ 011
◎ 内部威胁是最大的危害　/ 020
第三节　左右互搏的自我革新　/ 027
◎ 利用与反制，永无止境　/ 028
◎ 博弈催生创新，矛盾推动进步　/ 032

第二章
黑与白　是“黑产”魔高一尺，还是“白产”道高一丈　/ 035

第一节　网络黑色产业　/ 036
◎ 光明背后的阴影　/ 036

◎ 传统犯罪网络化 / 037
◎ 网络犯罪花样化 / 043
◎ “黑产”的四大趋势 / 058
第二节 网络白色产业 / 062
◎ 漏洞挖掘是“白产”发展的核心技术 / 063
◎ 漏洞防护是“白产”快反的高级手段 / 063
◎ 漏洞平台是“白产”打黑的基础设施 / 064
◎ 攻防大赛是“白产”聚智的重要平台 / 065
◎ 安全众测和实战攻防演习是“白产”推广的重要途径 / 066
◎ “白产”的三大趋势 / 067
第三节 打造凝聚“白产”力量的平台 / 070
◎ 办法总比困难多，向安全从业者致敬 / 071
◎ 永不落幕的盛会，产业趋势的风向标 / 073

第三章
权杖之手 黑客是以武犯禁，还是侠之大者 / 075

第一节 黑客演化史 / 076
◎ 20世纪60—70年代：黑客诞生 / 076
◎ 20世纪80—90年代：黑客的分水岭 / 077
◎ 21世纪前十年：“新”黑客崭露头角 / 079
第二节 最牛的黑客传奇 / 080
◎ 世界上一“黑”成名的黑客 / 080
◎ 我身边的黑客 / 086

◎ 著名的黑客组织 / 091
第三节 黑客的宿命与使命 / 097
◎ 从幕后到台前 / 097
◎ 全民皆黑客 / 098
◎ 黑客精神与黑客使命 / 101

第四章
智能时代 新技术是漏洞帮凶,还是克星 / 105

第一节 “智能生活”的便利与威胁 / 106
◎ 当威胁就在身边 / 106
◎ 当科幻成为现实 / 109
第二节 智能时代的工业物联网安全 / 112
◎ 什么是工业物联网 / 114
◎ 工业物联网遭攻击的典型案例 / 117
◎ 工业物联网面临的安全挑战 / 123
◎ 工业物联网安全的四大趋势 / 127
第三节 云计算的安全困扰 / 129
◎ 云的传统安全威胁 / 130
◎ 云计算的新安全威胁 / 131
◎ 云建设需要形成三方制衡机制 / 133
第四节 人工智能技术在安全中的应用 / 136
◎ 什么是人工智能 / 136
◎ 人工智能在安全防护中的应用 / 139

◎ 智能时代解决安全问题的方法论 / 142

第五章
网络战场　漏洞是癣疥之疾，还是堪比核武器 / 145

第一节　网络战：愈发重要的战争类型 / 145
◎ 美国网络司令部升格获权“先发制人” / 146
◎ 什么是网络战 / 147
◎ 曾经发生过的网络战 / 148
◎ 网络军备竞赛向全球蔓延 / 156
◎ 网络战的六大特点 / 165
第二节　APT攻击——网络战争最常用的攻击方法 / 170
◎ 针对性、持续性是APT的显著特点 / 170
◎ 我们所经历的APT / 172
第三节　漏洞的储备与利用是军事现代化的必备能力 / 177
◎ 漏洞已经具备武器属性：网络武器仅次于核武器 / 177
◎ 漏洞的储备利用之战已经打响 / 179
◎ 实战与演练：网络安全靶场 / 182
◎ 军民融合：凝聚网络空间多元力量 / 185

第六章
新战力　数据驱动安全 / 189

第一节　不断被刷新的网络安全定义 / 190

◎ 网络安全的定义需要不断刷新 / 190
◎ 网络安全的判断标准 / 191
◎ 网络安全相关的理论发展 / 191
第二节 网络安全的新常态 / 193
◎ 漏洞军火化、军火民用化 / 193
◎ 网络攻击产业化、犯罪集团化 / 194
◎ 态势感知智能化 / 194
◎ 应急响应小时化 / 195
◎ “等保”法制化 / 195
◎ “重保”常态化 / 196
第三节 网络安全的终极目标是保护大数据 / 197
◎ 大数据代表着未来 / 197
◎ 大数据是“大熊猫”，需要被重点保护 / 199
第四节 数据驱动的安全创新 / 201
◎ 大数据驱动安全可“预期” / 201
◎ 大数据是解决安全漏洞的“药方” / 202

第七章
新战具 第三代网络安全技术 / 215

第一节 互联网的“基因病变现象”：漏洞的四个假设 / 215
◎ 假设系统一定有未被发现的漏洞 / 216
◎ 假设一定有已发现但仍未修补的漏洞 / 217
◎ 假设系统已经被渗透 / 219

◎ 假设内部人员不可靠 / 221
第二节 网络安全技术的变革：从“查黑”到“查行为” / 223
◎ 第一代技术：“查黑” / 224
◎ 第二代技术：“查白” / 225
◎ 第三代技术：“查行为” / 227
第三节 第三代网络安全技术的大数据观 / 228
◎ 以空间换时间 / 228
◎ 以算力提战力 / 229
◎ 以已知求未知 / 230

第八章
新战术 安全从0开始 / 233

第一节 从“五段论”看网络安全市场前景 / 234
◎ 架构安全 / 235
◎ 被动防御 / 236
◎ 积极防御 / 237
◎ 威胁情报 / 238
◎ 进攻反制 / 240
◎ 未来的网络安全市场 / 241
第二节 “三位能力”系统是安全从0开始的最佳实践 / 244
◎ 低位能力——安全体系的“五官和四肢” / 245
◎ 中位能力——安全体系的“心脏” / 245
◎ 高位能力——安全体系的“大脑” / 246

◎ 数据驱动安全的“三位能力”联动系统 / 247
第三节 漏洞的“一体化”治理之道 / 248
◎ 漏洞是有优先级的 / 249
◎ 漏洞治理的四个环节 / 250
◎ 漏洞治理的响应等级 / 254
◎ 漏洞治理的关键 / 258
◎ 漏洞治理中未来可能的问题和关注点 / 259

第九章
新战法 人是安全的尺度 / 261

第一节 漏洞攻防是人海战 / 261
◎ 再聪明的机器,也不能取代人 / 262
◎ 人+机器,能极大提高战斗力 / 263
第二节 再先进的防护技术也不能代替运营和响应 / 265
◎ 安全运营需要更多干“脏活累活”的人 / 265
◎ 用全新模式培养网络安全运营人才 / 266
第三节 网络安全靠人民 / 267
◎ 共治:发动人民群众治理网络安全问题 / 268
◎ 补天:汇聚和动员民间“白帽”黑客力量 / 270

第十章
新方略　没有网络安全就没有国家安全　/ 275

第一节　国家网络安全的外部威胁：网络恐怖主义　/ 276
◎ 互联网成为恐怖主义的主战场　/ 276
◎ 网络恐怖主义：把计算机与电信网络作为犯罪工具　/ 278
◎ 网络恐怖主义活动类型：利用监管漏洞和技术漏洞　/ 279
◎ 应对网络恐怖主义：技术、人才与合作机制　/ 282
第二节　我国网络安全建设的三大保卫战　/ 285
◎ 关键信息基础设施的保卫战　/ 285
◎ 网络安全态势感知能力的保卫战　/ 287
◎ 核心技术自主创新的保卫战　/ 290
第三节　“一法二条例”保障国家网络安全措施落地　/ 291
◎ “一法二条例”为网络安全建设加装了新动力　/ 291
◎ 关键信息基础设施清单　/ 296
◎ 新等级保护制度2.0的精彩之处　/ 297
◎ 网络安全人才的春天　/ 298
第四节　建立现代政企网络安全防护体系　/ 299
◎ 树立正确的现代网络安全观　/ 300
◎ 建立数据驱动的协同联动防御体系　/ 302
◎ 建立有效的网络安全应急响应体系　/ 302
◎ 专业的安全服务是保障安全的关键　/ 303

参考文献　/ 305

后记　/ 315

Chapter 1
第一章

善与恶
漏洞是造成危害，还是推动进步

在漏洞的海洋里，我们看到的永远只是浪花。

我一直在思考一个问题，什么是推动互联网发展和完善的动力。按照马克思主义的哲学观点，社会基本矛盾是社会进步的根本动力；社会进步是社会本身的自我否定即“扬弃”的过程。

在互联网领域，矛盾体现在哪里呢？体现在技术、设备、制度、行为的缺陷方面，也就是人们常说的“漏洞”。

漏洞有危害吗？答案无疑是肯定的，危害通常就发生在身边，还毫无察觉。

漏洞只有坏处吗？不，它还在推动互联网的革命和进步。

从技术发展的角度来看，人从会使用工具开始，到逐渐掌握各种客观规律，再到今天网络社会的高度发达，人的本质都是在尝试凭借自身的能力和外力工具来补上各种短板，克服漏洞，追求完善。所以，高尔基才说：“人生的意义就在于人的自我完善。”

因此，无论我们是否追求自我完善，无论我们的能力、金钱和社会地位如何，漏洞都会裹挟着我们，左右着我们的生活，时刻与我们相伴。

“一念善，皆是善。一念恶，皆为恶。”凭借掌握的漏洞，有人为恶，有

人行善。人如是，社会也如是。

第一节　漏洞，源自人性的缺陷

曾经有领导问我："漏洞是天生的吗？"我不假思索地回答："是天生的。因为漏洞是客观存在，而且无法消灭干净的。"领导追问："既然是天生的，为什么设计者自己找不出来，需要你们去找？而且，被利用的可以叫漏洞，没被利用，能叫漏洞吗？"这个问题引起了我的认真思考。

天生缺陷，难免漏洞

辞典里对"漏洞"一词的解释有两个：一是小孔、缝隙；二是法律、法令、条约或协议中制订得不周密的地方，破绽。

我对漏洞的理解是：漏洞本质上是被利用的缺陷。就像一条船的船底和船舱门板上都有一个小孔，这两个小孔都是缺陷。其中，船底的小孔会导致进水，最终船毁人亡，所以它就是漏洞。

法律条文里可能有若干缺陷，能被利用的是漏洞，犯罪分子可能凭借漏洞逍遥法外；金融运行体制里也可能有不少缺陷，能被利用的才是漏洞，抓住这个漏洞可能赚得盆满钵满；甚至我们人也是一样，生来有多疑、贪婪等很多缺陷，一旦被利用，就会带来失败和痛苦。

1946年2月，世界上第一台电子数字式计算机埃尼阿克在美国宾夕法尼亚大学正式投入运行，此后万维网逐渐建立，世界开始以一种更紧密的方式联系在一起。与技术相伴随的，是技术中存在的一个个缺陷。

"漏洞"一词，在有了互联网技术后，更多时候是一个被用于计算机领域的专有名词。由于缺陷是天生的，漏洞是不可避免的，因此网络被攻击

是必然事件。

▶ 漏洞——利用人性的博弈

拿破仑曾经说："我是我自己最大的敌人，也是自己不幸命运的起因。"人，与生俱来就有贪婪、自私、猜疑、虚荣、恐惧、固执等弱点，当这些缺陷被利用时，就演变成致命的漏洞。因此，我认为，漏洞存在三个支点：漏洞因人而生，因人心而用，因人性而决定使用之道。

三国时期，魏国派大将军司马懿挂帅进攻蜀国街亭，诸葛亮派马谡驻守失败后，司马懿率兵乘胜直逼西城，诸葛亮无兵迎敌。但他沉着镇定，大开城门，自己在城楼上弹琴唱曲。本就生性多疑的司马懿怀疑设有埋伏，引兵退去。这是《三国演义》第九十五回的故事，是民间著名的空城计故事。诸葛亮正是准确把握了司马懿多疑而谨慎这一心理缺陷，利用主帅的这个心理"漏洞"，使其错误判断了局势。

空城计并非诸葛亮首创，《三国演义》也不是第一本描述这一计策的书。作为心理战的一种重要方式，它源于我国古代的军事杰作《三十六计》。书中第三十一计"空城计"，就是充分利用人的猜疑这一弱点。原文中有一句"虚者虚之，疑中生疑"，说的就是让敌人在疑惑中更加产生疑惑，造成错觉，从而在敌众我寡的情况下惊退敌军的战术。

"心理战"，本质上研究的就是如何充分利用人心理上的缺陷，把其打造成致命漏洞的方法，军事活动中尤为多见。

诸葛亮和司马懿的这一战虽然是虚构的故事，但历史上确有许多真实战例。从我掌握的史料来看，我国历史上第一个使用空城计的例子可以追溯到春秋时期。

春秋时期，楚国的令尹公子元，在哥哥楚文王死后，非常想占有漂亮的