网络空间安全丛书

网络空间安全真相：

破除流传已久的行业谬误与偏见

尤金·H. 斯帕福德(Eugene H. Spafford)

[美] 利·梅特卡夫(Leigh Metcalf) 著

乔赛亚·戴克斯特拉(Josiah Dykstra)

张　妤　刘海涛 译

清華大學出版社

北　京

北京市版权局著作权合同登记号 图字：01-2023-2112

图书在版编目(CIP)数据

网络空间安全真相：破除流传已久的行业谬误与偏见 / (美)尤金·H. 斯帕福德(Eugene H. Spafford)，(美)利·梅特卡夫(Leigh Metcalf)，(美) 乔赛亚·戴克斯特拉(Josiah Dykstra)著；张妤，刘海涛译. —北京：清华大学出版社，2024.5
(网络空间安全丛书)
书名原文：Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us
ISBN 978-7-302-66093-4

Ⅰ. ①网… Ⅱ. ①尤… ②利… ③乔… ④张… ⑤刘… Ⅲ. ①计算机网络－网络安全 Ⅳ. ①TP393.08

中国国家版本馆 CIP 数据核字(2024)第 072566 号

责任编辑：王　军
封面设计：孔祥峰
版式设计：思创景点
责任校对：成凤进
责任印制：丛怀宇

出版发行：清华大学出版社
网　　址：https://www.tup.com.cn，https://www.wqxuetang.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-83470000　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：河北鹏润印刷有限公司
经　　销：全国新华书店
开　　本：170mm×240mm　　印　　张：18　　字　　数：450 千字
版　　次：2024 年 6 月第 1 版　　印　　次：2024 年 6 月第 1 次印刷
定　　价：98.00 元

产品编号：101781-01

序　言

当 Eugene H. Spafford 请我为本书写序言时，我要求先看看这本书的部分内容。首先，我阅读了目录，并被作者介绍误区的有趣方式所吸引和逗乐。然后，我觉得他们应该把书名改为《网络空间安全真相》。本书的前言清晰明了，语言朴实无华，风格独特，自嘲中不失幽默，情感真挚，令人破防，有助于读者接受自己可能已经被误区和对误区的理解所迷惑的事实(好吧，我想这种写作网格可能会过时，但它太吸引人了)。

撇开玩笑不说，这是一本重要的书。网络安全往往与人们在使用哪些软件、采用哪些做法，以及坚持哪些安全信念方面的决定和选择有关。作者清晰地解释了人们可能被误导的原因，这有助于使本书更有效。当他们指出每一个关于网络安全的误区时，让你有一种优越感——“有些人竟有这种愚蠢的想法，真是讽刺！”你会觉得自己永远不会上当受骗，不知何故，这让每个案例都更加令人难忘。

这种风格让人想起 C. S. Lewis 的著名作品《魔鬼的秘密来信》(*The Screwtape Letters*)，在这本书中，一位资深的撒旦诱惑者教导年轻门徒 Wormwood 引导人类远离善良，并使其行为合理化，以证明其正当性。安全上网是一个严肃的问题。互联网和由所有可编程对象组成的更广泛“网络空间”不仅会因为蓄意的恶意行为而变得危险，也会因为程序员、网络运营商和其他人所犯的错误而变得危险。

我一直认为，问责制和管理机构是保持在线、网络空间环境安全的关键。必须能够查明不良行为者并追究责任。这将需要穿透匿名面具的能力和国际合作，因为网络空间与互联网一样，在正常运行过程中会跨越国界。管理机构至关重要。网络空间的参与者必须拥有必要的保护工具，包括追查那些从事有害或犯罪行为的人的法律机制和协议。

批判性思维是最强大的防御工具之一。本书主要介绍如何以批判性思维看待网络空间的风险。这需要付出努力，不是免费的午餐。坏人利用人类的弱点，可悲的是，这包括我们助人为乐的天性。许多骗局都利用了这些和其他积极的社会情感。本书让人们有能力识破这些骗局，还提供了更安全的做法，如双因素或多因素身份验证、使用加密技术、备份和冗余。在 21 世纪复杂的网络空间中，出错的方式有很多，需要结合个人、企业和政府的实践来防范风险。通常情况下，有备才能无患。

读一读这本书，在某些地方会心地笑一笑，并学以致用。你不会后悔的。

Vint Cerf，互联网之父

前　言

假设有一家名为 GoodLife Bank 的中型地方性银行，有 12 个实体分行，可提供在线银行服务，并有 325 名员工。该行首席信息安全官 Terry 想对银行员工进行行为监控，但首席执行官 Pat 表示反对。Pat 说：“员工都是好人，他们以前从未窃取过银行的钱，而且我们以前也从未进行过这种监控。将来也不会出现问题，没有必要浪费钱。”

另外假设，有一个名为备份信息部门(DRID)的政府部门，隶属于宣传部(APB)。在员工会议上，新上任的首席信息官询问 DRID 主管 Chris，部门内除了实施美国联邦信息安全管理法(FISMA)的最低标准外，还采取了哪些安全措施。Chris 回答说：“不需要，因为没有人想窃取我们的东西，而且我们也没有别人想要的东西”。

Pat 和政府机构的 Chris 两人都陷入了网络安全的误区。本书中会使用这些虚构(但具有代表性)的机构和人员，因为他们代表了本书需要提及的常见观点和理念。

在网络空间安全专业和应用中，需要掌握许多知识才能有所成就。这些知识可以通过正式教育和实践学习等多种形式来获取。例如，若要保护计算机免受数字威胁，则需要了解硬件和软件的工作原理，应采取哪些防御措施来阻止特定威胁而不是其他威胁，以及如何识别出现错误的情形。但网络安全领域存在一种潜在危险，即在没有依据的情况下，将传统经验或看法作为真理传承。虽然网络安全是一门不断发展的学科，但当有人质疑某种方法时，仍会听到“一直都是这样做的”的说法。人类大脑天生抵制变化，因此需要努力摒弃陈旧的错误观念。

许多文化内容以谚语和故事的形式进行流传。历史和传统是人类故事的核心，但是这些告诉人们应如何做的处世名言不一定真实可靠。民俗和民间传说有时只是用来证明我们已经做了什么或相信了什么，而不是有依据的行动准则。例如为什么在寒冷的天气里出门时需要戴帽子？有人告诉你是因为 90%的体温是从头部散发出去的，如果不想感冒，最好戴上帽子。这种说法听起来很有道理。但正确吗？不一定！[1]

有些谬论比其他观点更具迷惑性，更为普及与持久，因此很难被改变。例如，第 8 章将讨论用户是“最薄弱的环节”的观点。很多人都持这种观点，但这是带误导性的错误观点。

网络安全应是有效、公开和合理的。根据经验，人们经常受到偏见或误解的影响而做出错误或次优的选择。少数情况下，人们知道危险但继续前行。不知情和被误导之间有重要的区别。本书的主要目的不是讲授新技术概念(但附带这个效果)，而是聚焦于人们已知的知识领域。

---

1 身体任何未被遮盖的部分都会使你失去热量。全身赤裸但戴着帽子，会比全身穿戴整齐只光着头更快被冻僵。详细内容可参见[1]。

人们对什么是正确的最佳安全实践存在疑惑，但对糟糕的安全实践(如重复使用密码)却经常意见一致。当然这些糟糕的做法可能并非一直很差，取决于具体参数和条件。许多糟糕的做法听起来合乎逻辑，对网络安全领域的新手来说尤其如此；即使它们并非正确，但仍会被采纳并重复使用。例如，为什么用户不是最薄弱的环节？本书能帮助你更清楚地思考网络安全问题。

本书直面几十年来积累的民间传说误区，希望读者能够在现实的基础上做出更好的选择。无论网络安全民间传说误区是如何开始的，以及如何传播的，我们都认为人们有良好的意愿，并没有故意试图误导信息。误区不是谎言或故意的误导，误区是关于某些事实或现象的信仰的故事。本书的目标是在一直存有陷阱的地方纠正错误。

本书还想消除人们在面对复杂情况或新情况时产生的偏见。使用探索的方法来做决策，但经常对结果带有偏见。有许多方法适用于日常情况，但计算方法是复杂的，并且对手的行为经常不符合典型的心理模型。了解偏见可能导致的错误决策是很有价值的。

本书的目的不是指责人们的不当行为！并不是每个人都会掉进陷阱，因为有人只相信清单上的某个特定的误区。本书讨论的某些概念可能曾经是正确的，但安全领域在不断进步，环境也在变化。太多人认为网络安全只与技术有关，但事实并非如此。举个例子，尽管人在网络安全方面发挥着重要作用，但许多计算机科学专业的课程都不包括心理学必修课。

如果你从未接触过本书中描述的逻辑谬论和认知偏见，当你在日常生活中听到错误观点时，不要贬低任何人。相反，请根据本书的建议，从另一个角度理解。我们以谦逊的态度为你呈现本书。我们以前犯过的错，以后还会再犯。[1]通过这本书我们都学到了新东西！

可以明确的是，很久以前我们了解到的有关网络安全的一切并非都是错误的理念或想法。在 20 世纪 90 年代，SSL/TLS 被认为是不必要和不重要的。这不是误区，对许多企业来说，这是当时的现状。但现在，它变得异常重要，不可或缺。

曾经的网络安全误区

几十年前，一个常见的误区是，反病毒公司制造并发布恶意软件，这样用户就需要购买他们的产品。人们普遍认为反病毒公司人为地制造了需求及解决方案，但这不过是一种阴谋论(这也是 David Gerrold 在 1972 年创作的科幻小说 *When HARLIE Was One* 的情节之一)。

现在不再经常听到这个谬论了。为什么呢？它似乎已经自行消失。如今，大多数人都认识到反病毒软件对于保持良好的网络安全是必要的。有证据表明罪犯、破坏者制造了恶意软件，但没有证据表明反病毒公司正在这样做或者曾经这样做过。

1 好吧，本书的三个作者中至少有两个可能是。

20 世纪 90 年代，这个误解进入鼎盛时期，那么这个误解是如何被解开的？

- 寻找支持这个误解的证据或深入调研是第一步。有人确实进行了调查，但没有发现任何证据。这些结果并没有让这个误解完全消失，但确实削弱了这一说法的真实性。寻找证据是本书建议的验证其他误解的常见手段。
- 考虑备选的解释和动机，应用奥卡姆剃刀原则：优先使用最直接和最简单的解释。反病毒软件公司要编写病毒，就必须让所有员工守口如瓶，因为如果真相泄露，将毁掉整个业务。同时，为了表明不知道内幕，还需要偶尔放过一些病毒(或在内部放松查杀它们)。此外，还需要雇用演员参加会议，并在网上发布关于“他们”编写病毒软件的帖子。这比与公司无关的无赖作者制造病毒更简单、更有可能吗？

本书将揭开误区的真相，但世界上不会没有谬论，因为人类倾向于创造谬论来解释经验。特别是在进化出快速处理信息的能力后，在无法立即解释某些事情时，我们会构思出一个答案。

未来，误区或谬论可能会变得更加普遍并且更具挑战性。人们可以获取越来越丰富的信息，包括错误信息。我们已经看到了荒谬甚至具有破坏性的错误观点在传播，包括一些关于高空飞行物痕迹、疫苗和太空生物渗透政府的谬论。对于许多人来说，确定什么是真实可信的越来越困难。这就是为什么无论是在网络安全领域还是在其他领域，所有人都需要具备发现谬论的技能，以及纠正它们的技巧。

读者对象

本书主要面向网络安全专业人员和业余爱好者，包括学生、架构师、开发人员、分析师和决策者。当误区被揭穿时，现有的信息安全专业人员可以通过改进网络安全来受益。通过阅读本书，那些刚踏入这个领域的人将更好地理解上下文中的民间传说并预防错误；对于有经验的从业人员，将为他们的技术和方法提供新的灵感，并告诉他们如何避免不经意间陷入破坏良好网络安全的陷阱。本书还指出更有经验的从业人员如何帮助指导其他人。

如果你不是网络安全领域从业人员，这本书仍然适合你。网络防护与每个人有关，肯定也包括你，特别是，决策者和商业领袖需要对网络安全有准确的了解：这些人通常负责接受风险或管理风险，这是整本书的关键内容。

本书并不假定读者在特定领域有特定的职务、经验或深厚的技术知识，只假定他们有鉴别能力、思想开放，并对本书的主题领域有一定的了解。书中提供了参考资料，并在末尾提供了参考资料的清单，我们相信，如果读者需要更多信息，这些资料会有

帮助。专业人士的两个特点是终身学习和在接收新信息后质疑当前的理念；与政治领域不同的是，当有人形成新的观点时，通常都具有积极意义！[1]

三位合著者——他们分别在学术领域、工程领域和政府机构工作——都研究并撰写了关于网络安全和计算机科学的文章。科学可以通过使用标准化的方法和产生有效的证据来更新、验证及消除网络安全的神话。工程学可以利用科学来创造更强大、更可靠的产品。作者们在科学和工程领域工作，在网络安全设计和研究、事件响应、取证以及其他方面的工作年限加起来接近一个世纪。在职业生涯中，他们看到网络安全领域的从业者因为神话和误解而屡屡犯下本可避免的错误。写这本书正是为了教育学生和从业人员；相信这是第一本将这些信息整合在一起的书。

黑客的误区与传说

敏锐的读者会注意到，在这本关于网络安全的书中，使用“黑客”这个词时是很慎重的。尽管黑客最初用于标识熟练的技术爱好者，但不幸的是，现在它的负面含义已经使这个词面目全非。我们支持黑客的这个词的正面含义，所以使用“对手”或“攻击者”这些词来描述那些带有恶意的人，或者使用“恶意网络行为者”(malicious cyber actor)这一短语，这是 2011 年左右在美国政府出版物中出现的术语。我们也使用“坏人”(bad guy)一词来指一般的恶意网络行为者；这种用法不分性别，“好人”(good guy)也是如此。

黑客并不是唯一的在网络安全中被赋予负面含义的用语。正如在即将讨论的几个误区中看到的，“用户”这个词被不尊重和蔑视地使用。我们鼓励人们对这一问题保持警惕，在使用中进行澄清，或者使用其他替代用语。

误区的起源

在探讨并消除误区之前，应了解它们的起源以及它们为何如此顽固。一个原因是，技术和威胁在变化，但教育却迟迟不能跟上。除非人们认真对待持续教育，否则当旧的真理变成新的误区时，就很容易落伍。很多时候，当工作量很大，事情发展很快的时候，教育就被放在了较低的优先级。

所有群体中都不同程度地存在误区和错觉。任何个人或组织都不能幸免，即使是网络安全专家。这里有三个例子：

- 2017 年 Pew 研究中心对美国成年人进行的关于网络安全主题的 13 个问题的调查中，大多数人只能正确回答其中两个问题。只有 54%的人能够识别网络钓鱼攻击的例子。[2]

1 见[2]。

2 见[3]。

- 在对 25 名至少选修过一门网络安全课程的学生的访谈中，研究人员发现了四个共同的主题：过度概括、混淆概念、偏见和不正确的假设。例如，许多学生过度概括并形成错觉，认为加密可以实现保密性之外的其他属性：防止操纵、防止盗窃和确保可用性。研究人员将这些错误观点归咎于在网络安全领域缺乏经验。[1]
- 对一所大学的 20 名非专业人员和网络安全工作人员的研究显示，教职员工对网络安全都存在误解。例如，一些员工认为，链接比附件更危险，因为单击它们会自动损害计算机，而其他员工则认为，如果不安装附件，那么附件是无害的。[2]

误区与迷信的区别

这本关于误区和错觉的书可能会让你想知道它们与迷信的关系。

在有记载的历史中，迷信已经渗透到人类生存的每一个方面，从体育到天气，再到医学。也许你有一双幸运的袜子，或者避免使用数字 13 或 666。也许你相信扫把星或诅咒。从形式上看，这些都是神奇思维的例子。

数字生活也不能幸免于神奇的思维。今天，我们有一个仪式，关闭我们手机上的所有后台应用程序，或重新启动计算机，以“优化它们的性能”[3]。

根据《魔幻思维的七大法则：如何通过非理性信仰保持快乐、健康和理智》一书的作者 Matthew Hutson(马修・霍斯顿)的描述，神奇思维帮助人们理解非理性的世界，给人们带来舒适感、能动性和掌控感。第 3 章会再次讨论神奇思维这个话题。

误区和迷信是不同的。误区是不正确的事情或错误解释所观察到的现象，而迷信是基于超自然的信仰。金鱼有 3 秒钟的记忆是一个误区，敲击木头可以抵御厄运是一种迷信。举一个与计算机有关的例子，20 世纪 80 年代的许多孩子相信，对着游戏卡吹气可以解决灰尘问题。取出游戏卡，对着它吹气，然后重新插入，往往能解决“启动时设备接触不良”问题。是灰尘导致了问题的解释是一个误区。如果他们认为墨盒被鬼魂入侵，把它取出来并举办驱魔仪式，然后重新插入，那就是迷信了。无论哪种方式，取出和重新插入的行为都能解决这个接触不良的问题，并强化这种信念。

本书关注的是误区，而不是迷信。如果认为把水晶粘在笔记本电脑上，并根据星座部署防火墙规则，就能保证系统安全，那么本书不适合你。而是，我们建议你部署良好的备份系统并购买保险。

一些读者可能会想：“等一下，那宗教呢？”本书不打算以任何方式对宗教问题发表意见。迄今还没有看到任何经同行评审的、可复现的研究，能证实祈祷

1 见[4]。

2 见[5]。

3 关于更多奇特的技术行为，请参阅 Nova、Nicholas、Miyake、Katherine、Chiu、Walton、Kwon、Nancy 合著的“Curious Rituals: Gestural Interaction in the Digital Everyday (2012)”，网址为[6]。

可以影响安全事件导致的宕机时间。此外，如果认为计算机中心受到恶魔攻击，本书也不会帮助你——烧鼠尾草和雇用驱魔人，请不要感到惊讶，这两者都没有任何用处。

基本观点

作者根据自己的经验、研究成果和同行的意见撰写本书。有些基本观点是所有内容的基础，希望能将它们作为在安全领域组织工作的原则。

首先，网络安全不只是保护计算机和网络。网络安全用于保护支撑社会的技术和数据。计算机不是一个独立的学术研究领域，而是一个支持和促成现代生活的技术领域。计算机用于银行、公用事业系统、商业、学校、执法机构、医疗、娱乐等。生活依赖于计算机系统的正确运行。如果计算机停止工作，公民在社会中互动的能力就会消失，而且往往是以突然和意外的方式消失。因此，当提及击退计算机攻击或保护计算机时，不仅针对计算机和网络，从根本意义上说，是指保护社会和文明生活。

其次，网络安全涵盖了计算机，但主要涉及人。人为计算机编程，设计和制造计算机，购买计算机并部署它们。是的，人也会滥用计算机。不应该忽视这样一个事实：计算机是人使用的工具，是为人准备的，是由人制造的。解决网络安全问题需要关注人及人的行为。

最后，有时计算机会出现故障。事实也是如此，人也会犯错。通常情况下，计算机出现故障是因为设计或运行计算机的人出现了错误或疏忽；计算机硬件已经变得越来越可靠。不应该试图通过指责计算机来为计算机系统的不良行为开脱，如 “计算机决定的”或“计算机犯的错”。这些问题通常是编写软件、输入数据或操作系统的人的错误。使用人工智能(AI)和机器学习(ML)的系统也是如此——问题在于这些系统是如何训练的，以及谁决定采用它们的输出。在每种情况下，都是人承担责任。当一辆汽车闯红灯时，常规做法是把责任归咎于司机，而不是车辆或灯光。

本书的路线图

本书分为四部分——普遍性问题、人的问题、背景问题和数据问题——提出了 175 个以上的谬论、偏见和误解。章节按主题组织，将类似的误区组合在一起。这些章节可以独立阅读或连续阅读。各章中的标题确定了具体的误区或主题。每一节解释一个误区或错误概念，给出实践中的例子，并讨论如何避免。有些章节是技术性的，如关于漏洞、恶意软件和取证的章节。其他章节则描述了网络安全是如何被思维和决策所影响的，比如关于逻辑谬误和沟通的章节。书中材料包含具体的技术安全建议——大

部分项目都是关于人们的看法、决定和行动。这是因为，正如我们所指出的，大多数网络安全问题是由人造成的。[1]

许多书都讨论了如何构建技术解决方案，通常是对根本问题打补丁(往往是不完美的)。而本书的目的是帮助你解决根本问题。

附录 A 提供了文中使用的概念和术语的简短解释。例如，如果对防火墙或 log4j 漏洞不熟悉，可在附录 A 中阅读简短的解释。要提醒的是，这些解释并不是作为教程！附录 A 只是为了帮助读者理解材料，并掌握基本思想。因此，如果遇到一个不认识的术语，请在附录 A 中寻找。可能会有，但不一定。

网络安全，以及一般的计算机领域，充斥着各种首字母缩写词。本书努力将每一个首字母缩写词在第一次使用时展开；然而，也可能存在一个陌生的首字母缩写词，读者在读过几章后就不再记得了。因此，附录 B 提供了一个缩写词表，如果遇到一个不熟悉的缩写词，可从中找到该术语的全称。如果这仍然是一个谜，建议使用你最喜欢的搜索引擎来获得一些额外的背景信息。

附录 C 提供了一些参考资料供进一步探讨：书籍、学术论文、报告和标准文件。这些资料按章节进行编排，与本书各章对应。本书的目的是提供可以进一步探索的起点，正如第 1 章中所指出的，网络安全是一个奇妙的旅程，而不仅仅是一个目的地！

附录 D 是 Links 文件。在阅读正文的过程中，不时会看到网址编号，形式是[*]，即放在方括号中编号。这些链接统一放在 Links 文件(可扫描封底二维码下载)中。例如，在第 1 章中遇到[1]时，可访问 Links 文件中标题“第 1 章”下的第 1 个链接。

各章中穿插了原创的手绘插图，为各种误区提供了轻松的视角。这些图片展示了谬论的精髓，也会给人们带来欢乐，它们是对文字的异想天开的补充。

1 见[7]。

目　录

第 I 部分

普遍性问题

第 1 章

什么是网络空间安全

停泊在港口的船是安全的，但这并非造船的目的。
——John A. Shedd

如果你正在阅读本书，说明你对网络空间安全感兴趣。本书提出了一些想法并总结了经验与教训，涉及计算机领域(还有一些其他领域)中常见的主题。不过，本书还是以网络空间安全为主。无论你是学生、从业人员、行政人员、监管人员还是道德黑客，本书介绍的内容都会与你的工作有关联。

本章将探讨为什么人们对网络空间安全这个广泛的概念的理解充满了误区，为什么这个术语没有被很好地定义，以及为什么没有采用合理的方法来评价网络空间安全。

1.1 误区：每个人都知道“网络空间安全”的定义

虽然这看起来很无聊且很平常，难道不是所有人都应该知道网络空间安全的定义吗？

可能让你感到惊讶的是，即使是专家，对“安全”的认识也有分歧。最突出的原因是，对于什么是网络空间安全，并没有一个普遍接受的、精确的定义！对于这样一个备受关注并且已进行近六十年研究的领域，这似乎是不可想象的，但这是事实！

先从“网络空间安全”(cybersecurity)开始，这个词有什么含义呢？直接的答案是“关于 cyber 的安全”(security of. . . cyber)。很多人抛出“cyber”这个前缀来描述计算和网络，以及“cyberspace”(赛博空间)、“cyberpunk”(赛博朋克)和“cybercrime”(赛博犯罪)。首先，“cyber”到底是什么意思？

能找到的大多数参考资料都与数学家 Norbert Wiener 在 1948 年创造的“控制论”(cybernetics)这一用于描述通信和控制研究的词有关。“cyber”可能来自希腊语的

“kybernetes”，大致意思是总督、督导。1982 年，William Gibson 提出了“cyberspace”一词，指的是可在线体验的网络与计算机的虚拟空间。在科幻小说中使用这个词之前，还没有人用 cyber- XXX 来描述安全或在线事物。

1960—1990 年，人们大多谈论“计算机安全”(computer security)、“通信安全”(communications security)、“信息安全”(information security)、“网络安全”(network security)和“数据安全”(data security)。这些术语描述相当紧凑，但在讨论全面的安全时，变成了“计算机、通信、信息、网络和数据安全”，显得很冗长。不仅每次提及该领域时要打很多字，而且没有一个好的缩写作为替代。

20 世纪 80 年代末，美国参议院就政府系统的安全问题举行听证会时，据说一名工作人员想出了缩写词 cybersecurity。对参议员们来说，这个词很新颖，也许这就是它流行起来的原因——这让当时在这个领域工作的许多专业人员(以及此后的许多人)感到失望[1]。“cyber”这个术语并不那么准确，而且很容易让人忽略计算机和网络之外，还有数据、流程、人员和策略等内容。新颖性可能是它流行起来的原因，特别是在那些想获得客户关注的销售人员中备受欢迎(第 8 章将讨论术语的重要性)。

“cyber”意味着——计算机、网络、数据、通信，以及机器人、传感器、控制系统和人工智能[2]。

那么“安全”意味着什么呢？安全指采取行动来保护系统，以确保系统的安全。网络空间安全没有一致同意的正式定义。例如，在线朗文词典[3]将网络空间安全定义为“为保护计算机信息和系统不受非法侵害所做的事情”。这个定义省略了访问控制、检测非犯罪性滥用、事件响应及保护网络等内容。

NIST(美国国家标准与技术研究所)对网络空间安全的定义更为宽泛：“网络空间安全是对计算机、电子通信系统、电子通信服务、有线和无线通信，以及所包含的信息加以保护、防止损害及损害后恢复，以确保其可用性、完整性、可认证性、保密性和抗抵赖性。”[4]美国国防部 DoD8500.1 策略中使用了相同的定义，但并非所有美国联邦机构都使用这一定义。NIST 在文件中至少使用了三个以上其他的定义，进一步混淆了其确切的含义。一些其他安全定义如下：

- 系统资源不会被未经授权地访问，也不会被未经授权或意外地改变、破坏或丢失。[5]
- 通过预防、检测和应对攻击来保护信息的过程。[6]

---

1 Spafford 博士曾与参议员 Sam Nunn 谈过这个问题，表示对这个词持保留意见。这位参议员告诉 Spafford：“在这个问题方面与一位美国高级参议员争执，你必输。”

2 在哲学领域，“人工智能”和“机器学习”这些术语也不受欢迎。学者们对“智能”没有良好的定义，也不了解意识和学习。这些术语已经成为“通过反复海量输入，以建议的定向选择方式加强操作而开发的算法和系统”的简称。必须承认，系统似乎比某些现任国会议员更聪明，但我们不会给系统贴上智能的标签。如果想进一步探索这个话题，请咨询一些心理学家、神学家和哲学家。

3 见[1]。

4 见[2]。

5 见[3]。

6 见[4]。

- 保护与互联网连接的系统(如硬件、软件和数据)，防止受到网络威胁。[1]
- 旨在确保人员、数据和基础设施免受各种网络攻击的技术、服务、战略、实践、策略。[2]

国家安全局(NSA)Rob Joyce 在 2019 年提出了一个更简洁的定义：“网络空间安全是确保信息和基础设施免受盗窃、操纵和破坏的所有一切。”这留下了很多可以解释的地方；更接近大多数人在提到网络空间安全时所想到的。沿着这条道路走得更远的是 1990 年 Garfinkel 和 Spafford 的定义：“如果一台计算机是可靠的，而且软件按预期运行，那么这台计算机就是安全的。”[3]

误区：每个人都理解“被黑”是什么意思

当有人说他们被黑客攻击了，这是什么意思？与“网络安全”的定义模糊类似，“被黑”这个名词，不同人有不同看法。你或许会在朋友或同事的朋友圈上看到他们发布的“我的账户被黑了!”这样的信息。一些系统管理员甚至认为登录失败也是被黑了。

在一项关于 Twitter 上受害情况的调研中，研究人员发现，这些报告中有 43%与社交媒体账户有关，32%与网络游戏有关。不良后果中最常见的是账户丢失(27%)，其次是设置被更改(18%)和收到垃圾邮件(16%)。因此，说自己“被黑”的人一般只是不能进入自己的账户。但这一定是未经授权的访问吗？如果你把自己的 Netflix 密码告诉了你的妹妹，而她改了密码，这是不是未经授权？你是否被“黑”了？

网络安全专业人士倾向于使用事件、漏洞或攻击这些名词，而不是“黑客事件”这个词。这些名词一般描述的是恶意事件发生之后的问题，比如攻击者获得了未经授权的访问或窃取了数据，而不是描述失败的尝试。

本书将对“并非所有事件都有相同后果”这个主题进行更深入的讨论。这意味着，并非所有的“被黑”事件损失同等糟糕。例如，一个攻击者猜中了你在咖啡俱乐部的会员密码，然后“黑”掉了账户中的 20 美元余额。这与将公司的知识产权发送给另一个国家的竞争对手这样的高级持续性威胁(APT)，或控制大学网站这样的“被黑”事件有着完全不同的损失。

为什么定义很重要？部分原因是为了确定我们谈论的是相同的概念。定义指标也至关重要，这些指标能够衡量控制措施的有效性，并可相互比较，评估控制措施的经济效益。

总之，如果没有一个公认的定义，其他一切都不精确。

---

1 见[5]。

2 见[6]。

3 译者注：为了避免过度赘述，后续将“网络空间安全”简称为国内惯用的“网络安全”。

1.2　误区：我们可以衡量系统的安全性

网络安全专业人员对回答“我们有多么安全”这类问题感到很为难[1]。提出这个问题的人往往认为会得到直接且完美的答案，比如回答 90%的安全性或非常安全。而专业人员感到为难，因为这不是可以准确量化的。他们希望这个问题可以问得更精确。

人们仅仅想通过一个数字表明系统的安全程度。他们用这个数值说明：“我们的安全程度为 5，很安全!”这样可以让他们自己感觉良好，或可以放心地宣传。

然而，没有一个良好的定义，就不会有良好的衡量标准。对于科学家和工程师来说，衡量标准很重要！正如 Lord Kelvin 所写：“当你能测量你所讲的东西，并用数字来表达时，你就对它有所了解；但当你不能测量它，不能用数字来表达时，你对它的认知就很浅薄，不能令人满意。”[2]

“等等!”有些人可能会说，“那传统的 C-I-A 标准呢？”在计算机科学教科书和课堂上，保密性、完整性和可用性是网络安全的基本组成要素，但这些也是选得不好的衡量标准。例如，如何表示完整性的维度？如何提高 2 个衡量单位的保密性？3 个衡量单位的保密性是否比 2 个衡量单位的可用性更重要？此外，C-I-A 不是互不影响的属性：如果数据被覆盖(很差的完整性控制)，可用性也没有了。

C-I-A 模型的缺点并不是最近才被意识到的。Donn Parker 开发了 Hexad 模型[3]，增加了三个属性(可控性、正确性、实用性)，John McCumber 开发了 Cube 模型[4]，以更好地将控制集中在目标上，以及区分数据是静止状态还是在传输中。这些只是其中一些模型！这些模型并未解决根本问题，这些问题的根源在于没有对“安全”有一个良好的定义。

这些变得复杂，是因为在大多数实践中没有反映出来的两个事实：①系统不可能安全地抵御所有威胁，并保持高效可用；②所有安全性都与安全策略相关。

第一个事实比较容易说明。试想一下，该如何保护个人计算机不受来自可能毁灭地球的小行星的撞击、来自北大西洋公约组织(NATO)部队的全面网络攻击，以及来自搭载了具有心灵感应能力的蜥蜴人[5]的不明飞行物(UFO)的入侵。

第二个事实是关于定义要保护什么以及要防御什么。情况和环境不同导致策略的不同。如果是一名研究生，可能不在乎保存在家用计算机里面的巧克力曲奇配方；但如果是一个小精灵，在空心树上经营着一个烘焙食品帝国，可能会非常关心保护曲奇配方！在这两种情况下，即使是相同的计算硬件，相同的底层操作系统(OS)，也许甚至是相同的配方，但面临的风险和需要的安全策略绝对不同！如图 1.1 所示，一个尺

---

1 关于这个问题的冗长例子，请看@Accidential CISO 在[7]上发布的对这个问题的回答。

2 Popular Lectures and Addresses,“Electrical Units of Measurement”，1883 年。

3 DonnParker，*Fighting Computer Crime*，1998 年。

4 John McCumber，*Assessing and Managing Security Risk in IT Systems: A Structured Methodology*，2004 年。

5 蜥蜴人有敌意的概率很小；请参考[8]。然而，如果他们不喜欢猫咪视频，我们就完蛋了。

码的衣服并不适合于所有人。

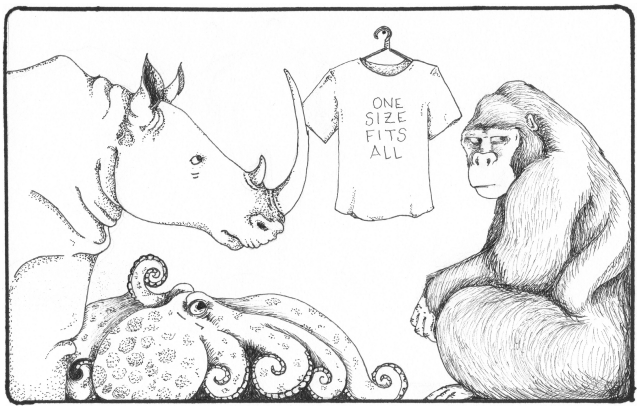

图 1.1　安全必须适合各种用户和情况

将家用计算机、银行用计算机与白宫情报室使用的计算机进行比较时，安全策略的差异性也会凸显出来。这些差异性还与风险问题(系统受到攻击的可能性有多大？被谁攻击？)和后果(曲奇配方的丢失是否等于银行资产负债表被修改？)息息相关。这反过来又导致人们在控制措施、应对策略和恢复机制上花费的时间、资金及努力有所不同。我们不能在同一安全级别上保护每个系统！保护研究生的曲奇配方免受网络犯罪团队的盗窃，是在浪费时间和金钱，但小精灵权衡利弊后，看法会与研究生不一样。

这种观点很早就被提及。一个不太为人所知的 RFC(Request for Comments，征求意见稿)中收藏了这一观点。隶属于 IETF 的 RFC 是单独编号的出版物，里面包含各种互联网标准、想法和偶尔的幽默。例如，RFC 1034 中描述了关于支撑互联网的域名和域名系统(DNS)的相关内容。互联网安全(Internet security)术语表收编在 RFC 4949[1]中，是一本引人入胜、内容丰富的读物，包含了“端口扫描”和“漏洞”等术语的定义，还收编了 Robert H. Courtney 在几十年前定义的 Courtney 定律。

Courtney 定律

Robert H. Courtney Jr.提出的系统安全管理原则如下。

- Courtney 第一定律：除非在特定应用程序和环境下，否则不能对系统的安全性给出任何实质性评论。
- Courtney 第二定律：永远不要让安全支出额度超过安全隐患的损失额度。
  - 第一个推论——完美的安全性需要无限的代价。
  - 第二个推论——不存在零风险这回事。
- Courtney 第三定律：对于管理问题，没有技术解决方案；但对于技术问题，有管理解决方案。

Courtney 是网络安全领域的先驱者，非常了解当前所取得成就的局限性。他提出

1 RFC 可通过[9]找到。

的 3 条定律丰富了网络安全的内涵，网络安全从业人员都应该了解这 3 条定律。

1.2.1　信任与风险

请注意，Courtney 提到了“风险”。那些深入研究过该领域的人通常更喜欢谈论信任、风险，而不是安全性。人们试图测量系统的可信任度来应对风险。网络安全领域最具影响力的文件之一是 TCSEC(可信计算机系统评估标准)，由于其封面的颜色为橙色，通常也称为“橘皮书”，由美国国家计算机安全中心于 1983 年发布，描述了如何构建信任度不断提高的计算机。[1]人们很早就认识到可信任度是安全级别，应该增加对系统的信任，使其按照安全策略运行并将风险降到最低更有意义。

当安全评级不再安全时

微软的服务器操作系统 Windows NT 曾获得橘皮书 C2 级认证，这让微软感到自豪。[2]当时，这对非军事系统来说是一个重要的评级。这说明 Windows NT(特定配置时)适用于更高要求的环境。为使 Windows NT 获得 C2 认证，微软甚至允许认证人员对源代码进行访问，这算是一个重大新闻事件了。

对微软来说，C2 级别是终极目标；公司可以在营销材料中吹嘘，可以放烟花庆祝！对于安全专家来说，则恰恰相反。[3]一位安全专家证明，仍然可能在未经授权的情况下访问 NT 系统上的“安全”文件，甚至可将其删除。评为 C2 级别不足以使系统变得更加安全。客观地说，橘皮书标准的制定者并没有声称 C2 是安全的。C2 是指系统的可信任程度，还有几个可信级别高于 C2。这就是为什么专家们当时并不认为 C2 是一件大事；如果有人真的想尝试通过认证的话，烤面包的烤箱也可能被认证为 C2 级别。

尽管信任与安全性相互关联，但有时会混淆两者。以 SSL/TLS[4]为例，用户可以在访问银行网站时，在浏览器中寻找带“锁”的图标。用户探索出这个办法来判断网站是合法的，而不是网络钓鱼网站。但这不一定正确，如图 1.2 所示。[5]TLS 虽然提供安全的会话连接，但会话仍可能与不可信的攻击者相连。这说明了定义“安全”的困难：在某种意义上网络连接是安全的，但实际会话不是。

1 关于橘皮书的更多信息，可在附录 A 中找到。

2 C2 是 TCSEC 中描述的信任级别评级。另请参阅附录 A 和[10]。

3 见[11]。

4 SSL 是最初的协议，但被发现存在缺陷。TLS 是当前使用的协议。

5 有关网络钓鱼的更多信息，请参阅附录 A。

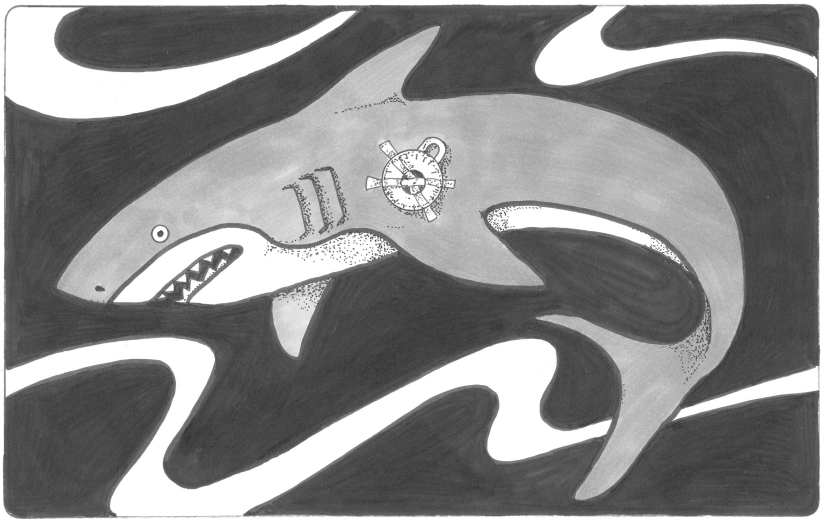

图 1.2　带“锁”的图标并不一定意味着没有风险

重要的是，正如 Courtney 第二定律的推论所指出的那样，没有办法消除所有的风险。例如，强密码降低了攻击者非法访问账户的风险，但所有密码最终都可以使用暴力手段破解。很难量化我们面临的风险有多大，网络安全措施在多大程度上降低了风险。另外，网络安全受太多约束，从而降低了有效使用技术的能力。风险管理是一个从没有到完备的过程，而这个过程中零风险是不可能实现的。

1.2.2　关于威胁

阅读本章前面关于安全的定义时，你是否注意到其中一些定义提到了威胁？这是定义安全的另一种方式。

基于威胁的安全和基于风险的安全之间有着巨大的区别。“防火墙可以防止网络攻击”与“防火墙可以降低网络攻击的风险”大相径庭。Bruce Schneier 在他的一本加密算法书中总结了这一区别：“避免威胁是非黑即白的，即要么避免威胁，要么不避免。避免风险是持续的：有些风险我们可以接受，有些风险我们不能接受。”[1]风险管理的最终状态不是消除风险，就如同要设法降低开车时受伤或死亡的风险，但不可能为零。

尽管有流行的十大安全建议和最佳实践清单，但没有一个公认的数值可以准确地说明更新程序、部署防火墙或安全培训能降低多少风险。这些措施在一定程度上有效，但剩余风险在 0～100%的巨大范围内仍是模糊的。如果能给它一个具体数字就完美了，但实际上做不到。

1 见[12]。

1.2.3　关于安全策略

安全策略中定义了安全态势和风险承受能力的差异。安全策略有助于定义建立和运营组织网络安全制度所需的资产、权限、标准及其他方面。许多大型机构都有结构化的、书面的安全策略。[1]

安全策略的相对性是造成网络安全复杂性的因素之一。很少有机构拥有可直接应用于开发、采购和运营计算资源(或“cyber 网络空间资源”)的总体安全策略。大多数机构只有一个“任何人都不可对系统执行未经授权的操作”的安全策略，并依靠现成的产品来执行；然而，很少有产品被精心设计和定制来支持所有的安全策略。毕竟，供应商的重点是赚取利润，而不是耗费无限的资金来支持每一种安全策略和防御措施。

这与 1985 年最受欢迎的一个观察结果类似：“通用的程序不可能有错误；错误只是意外。”[2]是的，大多数“错误”和“弱点”都不是缺陷——它们只是意外，因为它们发生在没有特定配置安全策略的系统中。如果没有安全策略，并且运行的软件从未按照安全策略明确地设计和定制，怎么会有安全漏洞呢？

考虑到供应商编写正确无误的程序比较困难，以及因市场驱动而不断增加新功能，为原有支离破碎的代码增加越来越多的复杂性以驱动新的销售这些因素，人们无法避免“意外”。提倡及时性、DevOps 和敏捷代码开发的趋势带来的精简设计，导致了“意外”。其出发点是编码人员可以快速解决问题，但快速解决不等于质量保证。就像以每小时 110 公里[3]的速度行驶在高速公路上的车，车的确开得很快，一闪而过，在你需要下车之前一切都很好。当你需要停车时，才发现这辆车是没有刹车的。打补丁可能让下一次迭代的汽车模型变得更好，但对于你和在你前面驾驶相同车型的人来说都不会受益。打补丁的简易性或速度，与良好的安全性是不一样的！代码生成的速度再快也不能替代经过深思熟虑的全面设计。

1.2.4　结论

安全与风险管理紧密交织在一起，而风险管理又与策略有关。我们需要保护重要财产，防止潜在的危险、伤害或损失。房门有锁，以保护里面的人和物品。如果我们关心饼干配方的隐私并保护银行账户中的资金，那么需要稳定可靠的网络安全。

那么，安全策略能带来什么呢？它带来的不是安全本身，而是建立信任和确保系统安全的过程。安全策略让人们有信心相信现有的机制可以安全运行，根据安全策略制定的支持和预防措施可以增强运营能力；还可以根据安全策略进行定期检查以弥补差距与不足。所有工作都必须在预算范围内，只能使用最便宜的软件，而这些软件往

1 如果你的组织没有安全策略，你应该创建并完善它。这是一件有益的事情。

2 Young, W. D., Boebert, W. E., and Kain, R. Y., *Proving a Computer System Secure.*

3 本书将使用公制单位。也欢迎你使用英制单位。

往由软件安全工程方面接受过最少培训(或没有接受过培训)的人所编写，并且运行在只为电子表格和视频游戏做过优化的架构及硬件上。在这种频繁出错和失败的环境中，出现意外理所当然。

安全领域最大的误区是：人们都知道什么是网络安全，这是一个可以实现的目标，而且现有技术已经足够了(本书不再试图解释为什么安全性、准确性和隐私也是难以实现的，原因大致相似)。

1.3　误区：网络安全的首要目标是确保安全

有一种看法，特别是在网络安全专业人士中，认为人们为了网络安全而网络安全。他们说，一旦用户感到安全，所有的感觉都会很棒！必须继续工作，直到用户和系统安全为止；或者至少感到安全为止。这个目标对许多人来说听起来是正确的，但它是被误导的。

事实上，网络安全不是首要目标；网络安全的目标是最大限度地支持用户完成任务，实现目标。人们和组织可以通过安全来达到保护的目的，但首要目标是完成用户的任务。用户希望在网上购买物品并与朋友共享照片，医院希望处理医疗问题，玩家想玩游戏，精灵想做饼干。用户的主要目标是娱乐、医疗保健和在线分享宠物视频。网络安全通过保护用户和活动免遭不幸与损失来支持实现这些目标。

忽视或规避安全的一个原因是它干扰了主要目标。这就是为什么当计算机运行缓慢，人们却想玩游戏时，会禁用反病毒软件的原因。当开发人员和工程师以牺牲主要目标为代价来优先考虑安全性时，往往会适得其反，导致人们禁用或绕过该保护。

例如自动软件更新。由于软件很复杂，并且是易犯错误的人所创建的，通常构建得很差，需要持续的错误修复和功能更新。因此早期用户必须主动检查更新是否可用，并手动安装。因为这不是大多数人的优先事项，所以用户没有检查或安装更新。包括微软、苹果和谷歌在内的供应商认为，当软件在没有用户干预的情况下自动安装更新时，系统会更安全，大部分用户也就不用再费心了。这也产生了意想不到的效果，一些用户认为他们所有的软件都是自动更新的，所以不再检查这些事情。

为了避免安全是首要目标的误区，网络安全专业人士必须更好地了解用户和背景情况。观察用户如何在自然环境中完成主要任务。然后，在考虑网络安全措施时，要仔细考虑对用户的影响。他们每次登录或浏览网页时都会受到干扰吗？付出痛苦或不便的代价值得吗？2019 年，研究人员研究了数据泄露安全措施与医院护理质量之间的关系。他们想知道，由于数据泄露后网络安全事件往往会增加，从患者到达急诊室到接受心电图检查的时间是否会增加？研究显示，在数据被泄露后的三年里，额外增加了 0.5～2.7 分钟，这表明网络安全事件可能减缓了访问健康记录以及下单、审查和执

行心电图的能力。[1]等待时间越长，死亡率越高。

不要专注于最大限度地提高安全性。应该采取适当的安全措施来支持用户实现主要目标。

1.4　误区：网络安全是关于显而易见的风险

想象一下，你正在参加一个类似于《家庭纠纷》的电视节目。在通常的设置中，你会被提示：“我们向 100 位网络安全专业人士提问，最常处理的风险是什么？”你猜测前五个最常见的答案是什么？恶意软件？密码泄露？无论它们是什么，被调查的答案可能不会让你吃惊。

但网络安全并不总是关于表面的风险，并不总是关于计算机本身，其他事情也会影响人们所关心的最终结果。

培训费用不仅高昂而且不能消除风险。例如，Gartner 指出，在没有网络钓鱼培训的情况下，人们单击网络钓鱼链接的比例为 20%，但每年的培训后的单击率仍在 10%左右。[2]与培训成本相比，我们愿意接受多低的单击率(当然，这是假设每次单击都有相同的风险)?

以确定的成本获得不同的保护水平。想象一下，企业已经投资于技术和流程，以实现其策略所规定的 20 天内修补漏洞的目标。如果企业达到了目标，而漏洞在第 21 天被利用，这就是没有实现承诺的安全目标。如果漏洞利用发生在第 19 天，这是业务决策的结果。

人们经常忘记考虑比安全软件和设备更广泛的观点。这种情况发生在从工程师到高管的每个人身上。组织机构是否有介质处理策略？当计算机死机时，存储空间是否被清除了？另一个问题是疲劳。疲惫和沮丧的用户更容易发生事故与错误。安全策略如何处理这个问题？

网络安全中“显而易见”的风险无疑是可怕的。例如，2021 年 12 月，在数百万网站和应用程序用来记录日志的代码片段中发现了一个新的严重漏洞，称为 log4j。[3]当有人单击网页链接并出现“Page Not Found”错误时，这个有漏洞的软件使 Web 服务器在一个日志文件中记录错误，供系统管理员使用。攻击者立即开始尝试寻找和攻击使用 log4j 的网站与应用程序。许多新闻文章都写到了它的可怕之处；社交媒体对此进行了疯狂报道。这是真正令人担忧的事件，因为攻击者可以通过类似日志机制这样简单的东西轻易获得访问权。开发人员喜欢日志机制，因为可以帮助他们调试程序及审计。攻击者也喜欢它们，因为它们很容易被利用。

---

1 Choi，Sung J.，Johnson，M.Eric 和 Lehmann，Christopher U.，“Data Breach Remediation Efforts and Their Implications for Hospital Quality”，见[13]。

2 Proctor, Paul, “Outcome-Driven Metrics Optimize Cybersecurity Risk, Value and Cost”.

3 关于 log4j 的更多信息，见附录 A。

应该担心任何使用此代码(log4j)的程序，并尽快更新(或禁用)它。等待别人利用这种脆弱性绝对是一个严重错误。

许多攻击并不是源于组织之外。我们将花费大量的时间和精力来清理用到了 log4j 的地方，但内部人员不需要远程代码执行(RCE)程序：他们不在远程，而在本地。根据他们的位置，他们可以做与外人一样多(或更多)的破坏。这可能是无意的或故意的，但内部人士可能很容易搞垮基础设施或泄露数据并将其出售。外部威胁与孩子们小时候被教导的“陌生人的危险”相同。为了安全起见，应避开陌生人和他们的恶意流量。[1]

Jordan(乔丹)是马里兰州繁华郊区的专业网络安全专家，也是社区的活跃志愿者。应当地商会的邀请，Jordan 为企业主制作了题为“网上保护自己的十种方法”的演示文稿。Jordan 的演示以许多人熟悉的方式开始，幻灯片显示了一个穿着连帽衫的人弓着腰坐在电脑前的像素化绿色图像。甚至在说一句话之前，演讲的语气就显得很恐怖，害怕那个神秘的连帽人物！[2]

许多网络安全演讲都是从谈论网络威胁开始的。他们认为，没有什么比教育(恐吓)观众采用更好的网络安全更有用。“你最好选择更好的密码，否则攻击者会偷走你所有的钱！”利用没有根据的即将到来的危险和厄运来散布恐惧是一种心理操纵。广告商利用这种策略来刺激焦虑。还记得“这是你的大脑在吸毒”禁毒电视宣传活动中一个鸡蛋在煎锅里嘶嘶作响的画面吗？对许多人来说，这是一种故意操纵的情感和力量。

网络安全常常让人觉得它被负面影响所掩盖。在学术界和新闻界，如果被认为是批判性的或负面的，那么会被认为更严重。积极性与天真有关，在某些行业可以提高销售额。但我们很少听说在网络安全方面进展顺利！

突出威胁的做法非常频繁，甚至可以用恐惧、不确定和怀疑(FUD)来描述它。在网络安全领域存在大量的 FUD，因为存在大量的不确定性。人们利用这一点来恐吓听众，让他们遵守规则，或者让他们相信最新、最卓越的产品可以阻止 FUD。

突出威胁是否有用？即使有用，它是正确的方法吗？英国国家网络安全中心的第一任首席执行官 Ciaran Martin(西阿兰・马丁)说：“在过去的几年里，我们已经从基于恐惧的网络安全方法转向更务实的方法，努力让人们能够解决问题。”[3]网络安全意识与授权和积极文化密切相关。如果员工一直生活在对网络威胁或错误行为惩罚的恐惧中，会感到不快乐、没有动力，并可能因恐惧而麻木。遗憾的是，责骂和其他令人尴尬的策略至今仍在使用。例如，美国卫生与公众服务部就针对医疗保健数据泄露事件建了一面“耻辱墙”。[4]

是的，这个世界很可怕，但恐吓不是网络安全的主要方法。建议不要将警告和故事当作“简单的 FUD”——这些警告表明有一些事情需要考虑。与其恐惧，不如考虑专注于正能量和稳定、促进创新，以及赋予人们权力的信息和运动。人们希望保护自己，保护他们关心的组织。这是人类的本能。没必要把所有时间都花在谈论这些威胁上。

---

1 同时，忽略那些表明大多数危险来自朋友和家人，而不是陌生人的统计数据。

2 不理解媒体为何喜欢用连帽衫来表示恶意威胁行为者。通常，人们穿上连帽衫是为了保暖，而不代表邪恶。

3 见[14]。

4 见[15]。

1.5　误区：分享更多网络威胁情报可以让事情变得更好

想象一下，一个攻击者将伪装成假发票的恶意 PDF 发送给 GoodLife 银行的 CISO Terry。Terry 和他的员工组成一个有天赋的团队，在识别出潜在的网络钓鱼企图后，分析该文件并创建签名以阻止其他银行员工使用。GoodLife 银行得到了更好的保护，但攻击者只在一家银行对一个用户使用这种恶意 PDF 的概率有多大？GoodLife 如何与其他金融机构甚至地球上的每个人分享这些情报？

网络威胁情报(CTI)是“基于证据的知识，包括背景、机制、指标、影响，以及针对现有或新出现的资产威胁或危害的行动建议。这种情报可以为主体应对该威胁的决策提供信息。”[1]有几十篇研究论文和商业产品专注于共享 CTI。我们有共享威胁信息的服务、邮件列表和组织。人们普遍认为“分享越多越好”。毕竟，更多的信息怎么会对网络安全没有帮助呢？

CTI 是知识，了解威胁与使用这些知识来预防或减轻威胁是不同的。CTI 在付诸实施时才有价值。知道如何说希腊语、下国际象棋或 bad.exe 是恶意软件并不是最终目标，将这些知识付诸实践才是知识的价值所在。

更多的分享不是目标，更好的分享才是最好的。威胁情报有多种形式，其中一种形式是实体认为有恶意的 IP 地址、域或电子邮件地址列表；仅提供这个列表是没有帮助的，因为接收者不知道使用 CTI 的时间或任何相关细节。CTI 添加有关入侵组或活动的背景，可以帮助优先考虑这个威胁是否与我们有关。更好、更复杂的 CTI 还会描述恶意行为。例如，APT29，一个已知的威胁组，通常使用合法凭据和 PS Exec 在网络中移动。这种特定的知识，可以帮助防御者知道应该寻找哪些攻击行为，以及如果发现了该怎么办。

信息共享不是免费的。制作和分发有用的威胁信息需要时间和人力成本，即使 CTI 订阅不收费。CTI 还需要人力和机器资源来获取、部署和监控。CTI 越多，处理成本越高；如果处理成本大于收益，泛滥的 CTI 会导致公司处境不妙。因此，只有使用及时、准确和可操作的高质量 CTI，才能获得更有效的安全。如果必须处理大量垃圾，那么找到金子是很困难的。安全团队应该从跟踪 CTI 如何为业务和安全目标做出贡献开始。

阻止列表(Blocklist)就是 CTI 的一个例子，是一种阻止已知不良 IP 地址、域或恶意软件哈希值的简单方法；这样的列表有几十种，有收费的，有免费的。问题在于，研究表明，这些列表大多数是不同的。[2]要有效地使用阻止列表，我们需要收集所有的列表。是的，就像春节集五福一样，必须都收集齐。这需要时间、空间和处理。

最后，信息共享需要参与者之间的信任。普遍认为，各组织间不共享威胁信息，因为害怕暴露自己系统的弱点以及获取信息的来源和方法。非营利的、基于行业的信息共享和分析中心(ISAC)提供积极且不断增长的可信共享途径。例如，金融服务 ISAC

1 McMillan, Rob, “Definition: Threat Intelligence”，见[16]。

2 见[17]。

中有 70 多个国家的 7000 多名成员合作并共享机密威胁情报。[1]

专注于高质量的 CTI，为你的网络环境带来有效的安全结果。2022 年，Mandiant 发布了 CTI 分析师核心能力框架。其中一项能力是“CTI 分析师应该能够根据对业务的影响来理解和评估威胁情报”[2]，这项技能将有助于抑制为分享而分享的诱惑。如果有效使用，CTI 可以帮助安全团队防御已知威胁。尽管如此，还是应该谨慎，不要在采用未经深思熟虑的策略的情况下不断添加威胁源和 CTI 工具。第 10 章将讨论应用过多工具的陷阱。分享的数量永远不应该是衡量成功与否的最终目标。

持续优先考虑质量，从而获得更好的结果。

1.6　误区：对你重要的事对其他人也重要

Todd Barnum(托德・巴纳姆)的书 *The Cybersecurity Manager's Guide* 的第 1 章标题是“赔率对你不利”。Barnum 承认，对于大多数环境中的管理者来说，“除了你的团队之外，公司里通常没有人太关心信息安全。”即使高层领导说他们关心，但你是否得到了资金和其他资源的支持？我们不赞同没有人关心网络安全的观点，但应该停止期望安全优先事项与其他人的优先事项相一致。

雇用网络安全人员来帮助实现网络安全。这些人因其在保护网络方面的独创性和表现而获得专业奖励，这是真人真事。与其他职业一样，越是专业化，兴趣和关心就越狭隘和具体。恶意软件分析师认为了解恶意软件是网络安全的关键，并寻求获得更多的关注和资源。对于密码学家，恶意软件分析是不错的，但密码学[3]是必不可少的。只有当人们寻求更广泛地扩展保护网络的方法时，才会看到更大的图景，考虑更多的视角。对于污水处理厂的 CEO 来说，网络安全的确不错，但并非首要目标，甚至可能不在前十名之内。

具有讽刺性的是，研究表明，即使是对网络安全有了解的人，行为有时也会表现得比预期更危险。例如，“自称是专家的人报告的安全行为较少，对网络健康的了解也比其他参与者少”[4]。所以，即使是很重要的事情，也可能不会在他们的行为中表现出来！人类是充满矛盾的生物。

如何避免这种误区呢？一定要避免假设。不要假设 CIO 同意立即安装补丁，是否安装请直接寻求 CIO 证实。可能有一些我们不了解的情况导致 CIO 并不同意。例如，安装一个需要重启的补丁可能影响年度股东大会或一个大型营销活动。可能会发现，安装该补丁的结果是批评而非赞美！[5]

1　请访问[18]。目前有 25 个 ISAC 专注于不同的行业。

2　见[19]。

3　当使用 crypto 这个词时，通常指的是密码学，并不是指围绕加密货币的各种方案。

4　Cain, Ashley A., Edwards, Morgan E., Still, Jeremiah D., “An Exploratory Study of Cyber Hygiene Behaviors and Knowledge”.

5　见[20]。

这里的关键想法是需要考虑“背景”。这与前文提到的保护曲奇配方和保护政府系统有关。在一种情况下是真的，而在另一种情况下可能是无稽之谈(或误区)！在计划和执行可能采用的安全策略时，了解背景是很重要的。资源、目标、法律、人员、价值观和历史都是背景的一部分。需要了解这些背景，无论是 CISO 还是 CIO。请注意，本书中谈到的许多其他事情也是如此！

1.7　误区：某产品将确保你的安全

跟我重复一遍：没有任何一种产品能确保安全。这不是网络威胁的现实，也不是网络防御的工作方式。这是一个可爱的梦：找到神奇的产品，哇呀！完全安全了；没有什么可担心了！

人们认为(或者供应商告诉他们要相信)购买某种产品最终会解决他们所有的网络安全问题。产品是什么并不重要，这种看法永远不会实现。云存储？不是。扩展检测和响应(XDR)平台？不是。下一代防火墙(NGFW)？不是。许多单独的解决方案都有自身价值，但没有一个单独的解决方案能够面面俱到。这不仅是因为所有产品都有漏洞，还因为一些问题尚未被发现或还没有被验证。第 11 章将讨论更普遍的密码、补丁和配置错误问题。

一些组织购买了大量产品，认为产品越多就越安全。简单地投入资金购买工具来解决问题，这会导致其他副作用，例如过于关注与其他公司的比较。此外，增加更多的工具可能会降低安全性。[1]竞争对手的新工具很花哨，但并不意味着适合自己。第 10 章将研究更多关于工具的误区。

很多时候，增加产品是事件发生后的一种应激反应。一家公司受到攻击，不是考虑问题的根本原因，而是砸钱来努力防止未来再次出现同样的问题。成语“失马锁厩”说，马匹逃跑后才锁上马厩并不是好的安全方法，它导致了大量的点式解决方案，而不是全面的策略。从考虑将马留在马厩的最佳方式开始，是一种更好的方法。

同样重要的是，要考虑把钱花在了哪里。如果安装了一扇新的马厩门，门上挂满了铃铛和口哨，但马厩本身却在倒塌，那么花费的钱就没有意义。

这不仅仅是企业和网络安全专家的问题。普通人也认为单一的软件应该提供安全保障。此外，他们往往接受电脑中默认的程序，并期望它终身免费。为什么没有一个超强的安全产品、一个终端保护程序来统治它们？现代设备——智能手机、笔记本电脑、服务器、汽车——是复杂的，攻击面是巨大的。没有任何一种网络防御措施可以防止攻击者试图攻击、影响或从系统中窃取数据的所有方式，更不用说预测所有可能出现的新攻击。[2]

1　见[21]。

2　这表明在整体设计和复杂性方面存在问题，应该加以解决，而不是增加更多的安全应用程序；但市场似乎对这一概念没有反应。

要避免这种误区，就必须了解技术的复杂性及其面临的各种威胁。没有任何一种安全产品能够提供足够的控制来降低现有的所有风险，这尤其体现在设计不好、过于复杂和构建不完善的系统中。

1.8　误区：Mac 比 PC 更安全，Linux 比 Windows 更安全

对于某一产品更安全的误区，计算机平台的选择就是一个具体例子。

想象一下，你从事网络犯罪活动，目标是感染受害者并运行加密挖矿的恶意软件。[1]攻破的电脑越多，赚的钱就越多。你创建的恶意软件必须为每个平台单独开发。适用于 Windows 的恶意软件在 Mac 上并不适用，所以要适用于这两个平台就要做更多的工作。对你来说，哪一个是更好的目标？Mac 还是 PC？[2]

抛开可能的相关因素，如拥有 Mac 或 PC 的人的类型，考虑最相关的属性：市场份额。截至 2021 年 6 月，微软以 73%的份额主宰了桌面操作系统市场，macOS 次之，占 16%，再次是 Linux，占 3%。[3]运行 Linux 的人认为他们的电脑更安全。[4]虽然可能如此，但实际上，不应希望攻击者把时间花在如此小的市场份额上。从纯粹的理性(尽管是邪恶的)角度看，犯罪分子应该以运行 Windows 的电脑为目标，因为潜在的受害者更多。

除了市场份额之外，几十年前曾有一段时间，人们对一些软件系统的质量和安全更加关注。从故障发生率的标准看，似乎一种系统比其他系统更有优势；然而，正如本书前言中指出的，事情是变化和发展的。很难断言一个系统比另一个系统对常见的威胁更有免疫力，特别是考虑到各种附加的防御措施。然而，这种看法一直存在。

因此，Mac 和 iPhone 的爱好者不时声称他们的设备比竞争对手更安全。在技术领域有很多竞争和忠诚度问题。很多人对苹果产品有很高的忠诚度，或者反过来说，对微软有很高的忠诚度。你可能还记得 21 世纪初的“Mac 与 PC”的电视广告，暗示 Mac 很酷，PC 很笨拙。[5]你可以有强烈的忠诚度，但不要让它蒙蔽你的眼睛，所有用户和设备都是脆弱的。没有人能够幸免。

此外，Mac 电脑的市场份额持续增长。如果这些用户认为自己天生更安全，就会变得不那么谨慎。攻击者会注意到这一点，并利用过度自信的偏见。事实是 Mac 和 PC 都有漏洞。无论运行 Windows、macOS、Linux 还是其他操作系统，都有风险。在许多社会工程攻击中，比如诱骗人们将密码输入假银行网站，那么运行的操作系统并不重要。所有系统的用户都必须谨慎。

---

1 我们有些调侃地建议，鉴于其对环境的影响，所有加密货币挖矿软件都是恶意软件。

2 攻击者与其他人类相似，都很懒惰。研究人员还研究了网络犯罪的无聊程度，可参阅[22]。

3 可参阅[23]。

4 这样考虑有很多原因，包括可以根据自己的喜好调整更多的安全设置，以及大多数软件是开放源码的事实。关于开放源码的更多信息，可参阅 1.9 节。

5 2021 年，英特尔推出了新的广告，其中曾经出现“我是 Mac 的人，现在更喜欢 PC”。可参阅[24]。

1.9　误区：开源软件比闭源软件更安全

有一种观点认为，让所有人都能看到源代码会减少 bug。与此相关的是，人们认为闭源软件，如微软的 Windows，意味着很少人可以审计、发现和修复漏洞。这并没有使开放源码软件避开严重的问题。然而，开放源码产品使我们更安全的神话依然存在。

2012 年 3 月，一个新的功能 RFC 6520 被添加到极受欢迎的开源库 OpenSSL 中，用于大多数网络服务器和浏览器。RFC 6520 有缺陷，该缺陷在两年内一直没有被注意到。2014 年 4 月，谷歌发现并私下向 OpenSSL 团队报告了该漏洞，六天后发布了修复程序。CVE 2014-0160 更名为众所周知的“心脏出血”。

2022 年 5 月，Python 库 CTX 被劫持和修改，攻击者可以窃取用户的亚马逊网络服务(AWS)密钥。[1]CTX 不是为与 AWS 服务器通信而创建的库。相反，它是一个管理 Python 核心功能(称为字典)的库。该库最后一次由开发人员更新的时间是在 2014 年，所以被大多数人视为稳定而且有用的库。遗憾的是，它被滥用了，有人对它进行了修改。大约在同一时间，人们发现 PHP 中使用的一个流行库也被劫持了。在这两种情况下，代码都是开源的，并且被广泛使用。在这两起事件中，任何人都可以查看源代码，但这并没有阻止攻击的发生。

商业封闭系统是人员付费开发的，无论是否认为这是一件苦差事，他们都会考虑系统安全和稳健的运行。结果可能是代码的漏洞比开源软件(OSS)少。TCSEC 和后续系统的最高级别评估的几个系统，如 Scomp、GH INTEGRITY 和 GEMSOS，都不是 OSS。它们经过了彻底的检查和测试，以提供非常高的运行保证，但不是免费或开源的。

开源可能意味着更快的安全修复，但并非总是如此。当在 OpenSSL 中发现并修复错误时，该修复不会自动传播到每个软件包。如果网站使用 Apache Web Server，Apache 需要合并新的 OpenSSL 库，然后需要更新 Apache 的安装。例如，在“心脏出血”事件发生三年后，仍有超过 14.4 万台面向互联网的网络服务器没有打上针对该漏洞的补丁。[2]简而言之，补丁并不是安全事件的结束，只是清理事件的开始。

开源确实鼓励透明公开和社区投入；然而，因为公开存在，所以并不一定意味着安全专家正在关注它们。有证据表明，有权访问开源代码的人在创建新代码和扩展时比审计现有代码更积极。最近的一项研究表明，开放源码软件开发人员花在提高安全性上的时间不到 3%。[3]他们将安全性工作描述为“令人心碎的家务活，最好留给律师和流程怪胎”，以及“令人难以忍受的无聊程序障碍”。据估计，开放源码程序占当前软件应用程序的 70%，这些结果应该引起特别关注。

避免这种误区意味着接受这样的观点：开源和闭源软件都有漏洞，但某些 OSS 中可能存在更多漏洞。软件开发是困难的，用户必须积极和勤奋地进行修补。

---

1 见[25]。

2 见[26]。

3 见[27]。

1.10　误区：某技术将保证你的安全

一个简单的流程图，从决策点“我需要区块链吗”开始，指向单一的终点“不”。区块链不是每个问题的答案(可能不是任何重大问题的答案)，当然也不是网络安全的完美答案。

云、量子计算、开源智能、区块链、人工智能、机器学习和加密技术作为强大的推动者，可以降低风险并持续推动网络安全的进步。技术在网络防御中发挥着突出且重要的作用，然而，任何技术都能消除网络风险，这是一个误区。小心炒作。

Jackie Fenn 于 1995 年在 Gartner 创造了“炒作周期”一词。她观察到，在新技术最终提供可预测的价值之前，有一条可预测的过度热情和幻灭的道路。该图示涵盖了五个阶段：

(1) 技术触发；
(2) 期望膨胀的高峰；
(3) 幻想破灭的低谷；
(4) 启蒙的斜坡；
(5) 生产力的高原。

炒作周期承认技术的价值，但从不认为技术能解决所有问题。

网络安全的历史上充满了人们曾经认为完美的防御措施。创建地址空间布局随机化(ASLR)是为了防止利用内存损坏漏洞。数据执行预防(DEP)也是如此。它们确实产生了积极影响，并帮助削弱了一些恶意软件。但 ASLR 和 DEP 并没有全面阻止攻击。这些技术无法阻止网络钓鱼和其他社会工程对计算机的影响。此外，攻击者利用面向返回编程(ROP)进行了调整并学会了绕过 DEP 和 ASLR。

这个误区与单一产品会保护我们的误区密不可分。没有任何东西适用于所有威胁和所有环境，而且这些技术和解决方案往往有其自身的弱点。在网络安全世界里，没有什么是完美的。

避免某技术能确保网络安全这一误区的关键是诚实地面对它不能做的事情。不要让这扼杀你对新技术的兴奋感。睁大眼睛进行评估、实验和部署，同时承认仅靠它无法拯救我们。此外，要警惕由此可能导致的任何新漏洞或暴露！

1.11　误区：某流程将确保你的安全

如果产品和技术不能确保安全，那么 DevSecOps(开发安全运营) [1]、Security Chaos Engineering(安全混沌工程)、SAFe Agile(大规模敏捷框架)[2]等流程框架或规则会是解决

1 见[28]。
2 见[29]。

方案吗？为什么？

优化后的安全行为在直觉上让人感觉很有希望。作为一个抽象概念，支持安全的优化流程可以应用于许多场景。就像通过戒烟或开始锻炼来改变生活方式，人们会获得许多好处。

从历史上看，有些流程已经被证明可以减少代码缺陷，但由于需要花费时间和进行人员培训，并未广泛采用。例如，为航天飞机和核电站控制编写的代码几乎没有缺陷。1986 年提出的能力成熟度模型(CMM)是描述软件开发过程的形式化和优化的方法。9 年后提出的人员能力成熟度模型(PCMM)的知名度却要比它低得多。大多数编程人员都对快速性和廉价性感兴趣，而使用可以减少缺陷的流程却与这些特性无关。遗憾的是，使用计算机的公众和许多供应商的想法已经固化为“代码是有缺陷，但开发速度快且成本低！”

强烈推荐优化开发与安全管理流程！使用经过充分验证的流程方法，特别是在大型企业环境中，受益会随着规模的扩大而日益增长。虽然到目前为止，没有正式的研究明确证明敏捷开发、DevSecOps 或任何其他最新的流程框架比原有方法好得多。但这并不意味着不应该使用它们。这只意味着应该理解它们的局限性。许多因素都会影响安全性，因此要证明某个特定的流程是提升的因素并不容易。有时，仅是出于一腔热情而实施新方法的简单行为会让事情看起来更好。使用健全的流程可以控制开发和部署系统的过程。遗憾的是，有很多影响安全的事情是无法控制的。人们无法控制攻击者是否试图对网站发起拒绝服务攻击，再精妙的流程也无法消除供应链攻击。

请记住，企业是基础设施、人员、威胁、资源、时间和资金的组合。对于这些因素的不同组合，有些方法实施效果会更好。不要相信哈佛商学院的研究报告、畅销书籍或会议研讨会中别人的经历会无缝地转化为你自己的经验！

一种误区是，可以从供应商那里购买流程解决方案。最好的情况是，可以使用开源工具帮助实现规则。例如，Netflix 在 GitHub 上发布了 Chaos Monkey(还有许多其他工具)，可支持混沌工程(chaos engineering)。[1]此外，Netflix 还发表了论文，可以测算混沌工程的收益和成本。[2]

1.12　误区：“神仙粉”可以让旧想法焕发新生命

如果了解新技术的唯一途径是通过供应商，那么可能会产生一种误解，认为独一无二的革命性解决方案每天都会出现。毕竟，营销就是推广产品或服务。即使是对旧商品的重新包装，人类也能从中获得生物层面的乐趣。[3]这不是一个反对供应商的误区，

1　见[30]。

2　Tucker, Haley, Hochstein, Lorin, Jones, Nora, Basiri, Ali, Rosenthal, Casey, “The Business Case for Chaos Engineering”.

3　Swaminathan, Nikhil, “Our Brains on Marketing: Scans Show Why We Like New Things”.

而是奢侈和密集的宣传或促销(炒作)，是营销必不可少的手段。考虑到史上很少有网络安全从业者愿意研究该领域，这种手段显得特别有效。

这里的误区是，对现有或稍微改进的技术进行重命名、品牌重塑或重新包装，会神奇地使其更有效或更可用，就如撒一把“神仙粉”可以使现有技术脱胎换骨。如果有人试图将防火墙[1]技术改头换面，包装为一种全新的安全产品“数字哨兵”卖给你，你要持怀疑态度。

考虑两个当前的例子：云计算和零信任。[2]这两个短语都被随意使用，因为人们已经相信它们的新颖和神奇。事实上，云计算和零信任自身都是带有“神仙粉”效应的旧技术。毫无疑问，它们是有价值的，但过度夸大使一些人产生了错误的期望。

在现代网络安全中，使用趋势往往与新颖性和价值混为一谈。如果消费者去了解一项技术的来龙去脉，了解技术发展趋势，这件事本身并没有任何问题。然而，如果每个人都在赶时髦谈论这件事，就容易被误导。当普通消费者听到云计算等技术时，它通常已经持续渗透和发展了多年。在 21 世纪初，当 Amazon、Google 和其他公司推出产品时，即付即用的计算服务并没有突然出现。分时共享系统在 20 世纪 60—70 年代开始商业化。今天的云服务是从 20 世纪 70—80 年代在分布式计算方面所做的工作演变而来的。但似乎一夜之间，每个人都在谈论云，就好像这是一个革命性的解决方案，可以满足人们所有的需求！

云计算是一种资源共享形式，允许用户按需使用云服务商提供的资源。如果在线存储文件，可以从第三方处租用存储空间。如今，可以付费请服务商做各种在线操作，包括托管数据库和将语音翻译成文本(如 Siri 和 Alexa)。自助式服务商业模式使得获取和采用这些服务变得几乎无缝衔接。但云服务并非完美，确实有一些缺点需要考虑；例如，牺牲控制权和灵活性换取便利性、供应商封锁问题，对透明度和控制权的限制，以及宕机和泄露问题。某些情况下，云计算可能是正确的选择，但在赶时髦之前要仔细考虑。

零信任是去除隐性信任、完全仲裁及信任隔离的时髦说法，不再使用边界设备隔离等术语。信任存在于许多数字生态系统中，从设备的硬件到连接到软件的网络，以及连接到其他人的在线服务。利用信任是许多破坏网络的安全攻击的根源。攻击者以域控制器为目标，因为域控制器是域内计算机信任的服务器。许多系统所有者还认为，如果有人使用合法的用户名和密码登录，那么他的所有操作都是可信的。当用户登录 GoodLife Bank 应用程序时，因为受到信任，他们可以存款和取款。替代做法应是验证每个操作，包括合法用户可能正在使用不可信的设备这种实际情况。如果用户从新设备或外国访问 GoodLife Bank，那么应该对他们进行仔细检查。最佳做法应该是限制信任，强制实施最小特权，授权访问，并隔离不同信任。[3]

最小的特权、访问的完全仲裁和隔离都是几十年前的旧观念！但多年来，网络安

1 关于防火墙的更多信息，请参阅附录 A。

2 有关这些方面的更多信息，请参阅附录 A。

3 关于零信任的更多信息，请参阅附录 A。

全专业人员一直在推荐这些做法。当前的实现允许持续的分析和调整，提供更细粒度、实时、最小特权的访问。如果你仔细想想，就不存在完全零信任这回事，因为系统需要进行信任身份验证和访问控制；建立在真正零信任基础上的系统将是惰性的。归根结蒂，没有“神仙粉”可以使零信任成为革命性的或者安全需求的神奇解决方案。

1.13　误区：密码应经常更换

密码是几乎每个人都有经验和意见的一个话题。事实上，60 多年后的今天，密码——包括文字、短语和 PIN——仍然是最主要的认证形式。这个方案看起来像一把保护贵重物品的秘密钥匙。事实上，目前已经经历了让用户选择和记住许多密码的危险弊端。几十年来，人们一直承诺会有更加光明的无需密码的未来。2004 年，Bill Gates 承诺密码会消失，因为“密码无法确保安全”[1]。

计算机的密码不像房子的钥匙。没有人让房主挑选房子钥匙上的齿和凹槽，也不需要在每次回家时对其重新构建。然而，用户被要求自行生成并记住数字密码(就像锁的密码)或携带物理令牌。多因素认证是在 20 世纪 90 年代引入的，极大地提高了安全性，但给用户带来了不便。John Viega 在他 2009 年出版的 *The Myths of Security* 一书中说：“尽管如此，但仍没有看到密码的替代方案。”

尽管密码遭到大量滥用，但不太可能很快消失。即使是新手也能理解这种模式，不需要对硬件进行额外投资，并且在适当使用时仍然是一种合理的机制。关键是使用时要了解背景和风险——这是我们反复提及的主题。糟糕的密码选择、密码猜测、拦截/欺骗都是密码方案的潜在问题；然而，在某些情况下，这些不是重大威胁或有缓解措施。有效的身份验证应该不仅仅是高强度计算或对每一种攻击的抵抗。对于网络安全专业人士来说，选择身份验证方案的首要任务是安全，但也应该考虑威胁模型、成本和用户接受度。正如图 1.1 中所指出的，一种方法并不会适合所有情况。

众所周知，100 个字符的密码比 10 个字符的更安全，但如果没有工具帮助(例如密码管理器)，就不可能实际使用。不同的身份验证机制具有不同的加密强度，这不是误区。这里说的强度指的是破坏加密需要的时间和资源。专家指出，密码与生物识别技术的相对强度不仅在密钥上不同，而且在其他方面也有不同的考虑。如果指纹认证器被破坏，就无法更改指纹。与所有网络安全一样，即使加密协议非常出色，在实现算法时也可能出现漏洞。

这并不是说没有致力于改善用户的密码状况。密码表促使人们选择更好的密码。密码管理器代表人们记住强密码。但要改变使用密码的动力，并为其他选择重新配置系统，这是一项挑战。

一种误区是，不熟悉的人无法猜到我们的密码。也许我们最喜欢的球队是利物浦，

1 见[31]。

或者我们的狗叫查理。如果利物浦或查理是我们的密码，即使攻击者无法访问密码表，也可以在不到一秒钟的时间内猜到这些密码，如图 1.3 所示。不要想当然地认为攻击者需要了解个人信息来猜测密码！

图 1.3　强密码难以生成和记忆

另一个误区是密码应该经常更换。研究表明，频繁的更换会对良好的安全性产生反作用，因为这样会导致简化密码或采用变通的方法。类似地，对复杂度的要求，例如需要符号和数字，也导致了更糟糕的密码。现在已经不再建议使用这样的规则。

密码指南的权威来源是 NIST 800-63B(Digital Identity Guidelines，数字身份指南)，最后一次更新于 2017 年 6 月。特别是，附录 A 描述了考虑记忆性秘密强度的问题。NIST 建议，不允许用户从“以前的漏洞库、字典词和用户可能选择的特定词(如服务本身的名称)”中选择密码。

2021 年，微软宣布用户可以免密码登录微软 Outlook 和 OneDrive 的微软账户。[1]为此，用户被邀请使用验证器 App、安全密钥或验证码。这可能是第一个既强大又可用的新身份验证替代方案。密码可能不会永远存在，但不要轻易下注。

1 见[32]。

多因素身份验证(multifactor authentication，MFA)意味着安全

MFA 是一种机制，不仅必须知道一些东西(密码)，而且必须拥有一些东西。必须拥有的东西可能是加密狗、智能手机或系统可用来进行双重检查的东西(如短信验证)。这是一个额外的安全层，所以它必须是安全的，对吧？

如果是短信验证，它可能不安全。如果手机已经有恶意软件，恶意软件可以拦截消息并伪装成实际用户。更不用说，一些要求你使用这种身份验证的地方会通过短信来安装恶意软件。[1]短信在通过网络传输时也是可以被截获的。

1.14　误区：相信和害怕你看到的每一个黑客演示

DEF CON 是一年一度的黑客大会，以最新的爆料和演示而闻名。2010 年，主持人演示了一辆汽车被黑客入侵。2017 年，黑了一台投票机。2020 年，是一颗卫星。这些演示使得节目和故事很精彩，引来大量的掌声(来自其他黑客)，以及广泛的炒作和恐惧(来自公众和媒体)。这就像电影变成了现实！既神奇又可怕，谁不想报道奇妙的事情呢？

网络安全专业人士理解、赞赏和钦佩该领域的新进展，有时甚至欣赏进攻的技巧或新的进攻技术。在公众明白或了解新漏洞之前，就可以看到它们的影响和严重性。参与漏洞赏金计划的供应商通常会要求提供 POC(概念验证)代码，以证明新的漏洞可以被利用。黑客也被要求提供 POC 例子才能受到重视。有一份出版物对此提出了很好的观点：应呈现切实的证据和成果，否则就不值得被认真对待。[2]

然而，有一种误区，认为每一个演示或学术发现都会导致广泛应用。这些演示很有启发性，但往往忽略了现实世界的背景和复杂性。他们经常做出许多假设。投票机和自动取款机都经常被审验，物理保护措施会阻止攻击者实施快速或不被察觉的修改。黑客攻击一台投票机或自动取款机，与破坏一套选举系统或金融系统是完全不同的威胁。

Rowhammer 是一种新颖的攻击技术，[3]甚至很酷。研究人员已经创造了几个 POC 漏洞，但还没有证据表明 Rowhammer 在实际中被使用。

TCP Shrew 是另一种分布式拒绝服务(DDoS)的新型攻击技术。它既酷又可怕，但还没有证据表明它在实际中被使用。漏洞预测评分系统(EPSS)是一套模型，使用威胁信息和现实数据计算漏洞被利用的概率。数以百计的 CVE 对大多数人来说并不是威胁。根据 Kenna 安全和 Cyentia 研究所的数据，只有大约三分之一的 CVE 出现在实际

1 见[33]。

2 见[34]。

3 有关 Rowhammer 的更多信息，请参阅附录 A。

环境中，其中只有 5%取得成功。[1]攻击可以被证明并不意味着它会被使用。

1.15　误区：网络进攻比防御容易

网络安全领域有一个被很多人认可的观点："防御有一个缺点，因为必须防御所有的攻击，而进攻方只需要一个单一的方式。"从表面上看，这似乎是直观的事实。防御许多攻击面意味着资源被分散了。如果所有的进攻资源都集中在单一攻击上，这怎么可能不有利于进攻方呢？

这种观点基于一个硬性的假设前提：网络攻击很容易。正如 Bruce Schneier 所写："与人们普遍看法正好相反，政府的网络受到攻击并不是突然发生的，攻击/防御是平衡的。"[2]虽然大规模网络钓鱼等犯罪攻击无特别针对性，但由于成功率低，仍然会让攻击者付出代价。此外，网络钓鱼邮件只是犯罪分子的一个组成部分，他们还需要特定功能的恶意软件、指挥和控制基础设施，以及被盗数据变现的方法。如今，勒索软件攻击者甚至为受害者提供客户服务和技术支持。[3]

误区：相信在网上看到的每一个网络威胁

虚假和歪曲信息的历史由来已久。早在互联网出现之前，耸人听闻的危险故事就出现在报纸和地摊文学上。如今互联网加重了这种现象。

网络安全也难免受错误和虚假信息的影响。错误信息是指不准确或故意误导的信息，并非有害，但仍可能造成损失。虚假信息是有意歪曲的信息，将虚假信息作为真相传播，目的是造成伤害。在许多高度重视言论自由的地方，传播虚假信息是合法的。这可能导致问题，尤其是对于容易轻信或消息不灵通的人。

人工智能足够先进，可以生成真实但错误的网络威胁情报，足以愚弄专业人士。以下是一个人工智能生成的网络安全错误信息的例子：

"APT33 正在探索对关键基础设施的物理破坏性网络攻击。攻击者在基于网络的航空公司管理界面中注入各种漏洞。一旦成功，攻击者就可以拦截和提取敏感数据，并获得对内容管理系统(CMS)未经授权的访问。"[4]

每个人，包括网络安全专业人士，都必须对接收到的信息保持警惕和审慎，持健康的、合理的怀疑态度。这也很好地说明了信任是至高无上的资产！

康奈尔大学的 Rebecca Slayton 教授认为，现在说进攻有优势还为时过早。[5]她建

1 见[35]。
2 见[36]。
3 见[37]。
4 见[38]
5 Slayton, Rebecca, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment".

议围绕相对效用或价值重新构建对话。将高成本与保护高价值资产联系起来是合理的。此外，如果进攻的价值相对较低，那么进攻就不“受青睐”。例如，分析表明，在 Stuxnet 攻击中，防御的成本可能低于进攻的成本，这与关于网络进攻处于主导地位的主流假设相反。也许最重要的是，美国、以色列和伊朗对伊朗核计划的重视程度似乎远远超过了网络进攻或网络防御的成本，这使得领导人不太关注成本。

这个误区的影响超过简单误解，会导致组织领导人和网络捍卫者感到气馁，觉得自己总是落后，疲于追逐那些“轻松”上阵的攻击者。防御者需要尝试理解攻击者的思想和行为。这就是为什么一些课程向学习网络安全的学生灌输这样的思想：了解攻击者的心态有助于更好地防御。[1]

避免这个误区的关键是，在认为进攻方占优势时要小心。这不是简单的相对成本问题——防御成本应该与受保护的价值适当匹配。

1.16　误区：工业技术不易受攻击

大多数人对信息技术(IT)很了解，因为每天都会看到和使用硬件和软件：手机、平板电脑、电子邮件等。当然，并不是只有这一种技术类别。工业技术(OT)是控制工业设备的硬件和软件，比大多数人意识到的更普遍、更重要。例如，OT 可以打开和关闭工厂中的阀门，或者控制建筑物中的电梯。你可能听说过 OT 的细分领域，即工业控制系统(ICS)和监控与数据采集(SCADA)系统。

网络安全中，IT 和 OT 之间存在明显差异，两者的一个很大的区别是，IT 是以用户为中心，而 OT 是以机器为中心。人与 IT 设备直接互动，如发送电子邮件和写书。OT 系统通常互动性较低，自动化程度较高，因为它们控制着物理世界中的事物，尽管仍需要由操作员编程和监控。

IT 和 OT 十分相似，相同类型的供应商可以同时构建这两者，而相同类型的技能和团队可以同时运营这两者。这一观点越来越正确，但这是最近才发生的变化。IT 和 OT 通常是独立发展的。像通用电气、霍尼韦尔和西门子这样的公司——对许多 IT 用户来说可能不熟悉——使用专有系统为电力公司和其他工业企业生产 OT 平台。这些系统使用的通信和协议是 OT 的“标准”，与 IT 标准不同。例如，智能电表可以测量你家的用电量，并使用开放式智能电网协议(OSGP)将这些信息传送到电力公司。同样，拉斯维加斯 Bellagio 酒店拥有 1000 多个喷泉的表演也是由 Modbus 协议控制的。这些专用协议一直运行良好，直到人们想通过拥有众多恶意用户的互联网访问和控制这类系统。

OT 系统的安全最初并不是一个优先事项，因为威胁模型没有将其包括在内。OT 网络最初是孤立的。这种“空隙”意味着数据无法自动从 IT 网络移动到 OT 网络，因

1 进攻看起来令人兴奋，但吸引学生才是真正的原因。引用 Bear Bryant 的话：“进攻能卖票，但防守会赢得总冠军。”一个精心设计的课程需要更加平衡和微妙的教学方法。

此被认为具有强安全性。现实情况是，为满足某些业务要求，需要在 IT 和 OT 网络之间传输文件，如安装软件补丁或移动配置文件。当网络未连接时，解决方案之一是使用 U 盘复制数据。多年来，攻击者(以及安全研究人员)已经找到了跳过这种空隙的方法：感染 IT 网络上的机器再通过 U 盘进入 OT 网络，甚至可以使用声波或热能在隔离的网络之间进行通信。[1]

IT 和 OT 正在融合，这意味着两者都很脆弱，都需要网络安全。“OT 系统对攻击者来说是孤立的或未知的”是一个误区。

1.17　误区：破坏系统是建立自我形象的最佳方式

有人说，破坏系统在网络中是重要的，尤其是被庞大的黑客行动的荣耀所驱动的破坏。这是一个不幸的误解。其实发现缺陷有时是一门艺术，有时是一项科学，有时是简单的运气，但这通常不是成为专家的关键。

破坏事物的人会得到暂时的认可和宣传，但这不能展示出专业技能和专业知识。也有少量的例外，但解决问题是大多数人所希望的结果，而不是一堆被破坏的代码。具有破坏性的事情看起来既迷人又有趣，但光靠它是不足以建立职业生涯的。打碎一个水晶花瓶对大多数人来说并不难，但只有少数人有能力再做一个。闯入房子只需要用最少的专业知识，但设计和建造房子则需要相当多的技能。考虑到大多数计算机代码的质量，发现缺陷并不是一项巨大的成就，建立能够抵御攻击的系统才是。

一般来说，破坏事物几乎总是比创建或修复更容易，而且大多数网络安全职业都致力于诊断和修复。尽管我们自己有丰富的破坏系统的经验，但还是这样认为。

1.18　误区：因为你能做，所以你应该做

有无数与网络安全相关的活动和行为是合法的，在技术上是可以实现的，却是不可行的。我们能做某事并不意味着我们应该做。我们可以在数据中心大喊“开火”[2]，但我们不能这么做。

首先重申，该领域大部分的从业人员都是基于“信任”，这也延伸到了对人和行业的信任。多数人对二手车销售人员的一般印象总是不太好的，这也许对大多数二手车销售人员不公平，但少数人缺乏诚信，玷污了所有人的声誉。政治家也是如此，在某些地方，执法人员也是如此；少数人的不道德行为会让整个行业的人看起来很糟心，并且不值得信任。书中有几个地方会回到这个主题，并强调专业组织的作用。尽管如

1 参阅 Guri, Mordechai 等人所写的 Bitwhisper: Covert Signaling Channel Between Air-Gapped Computers Using Thermal Manipulations。

2 数据库坏了！有一个 APT 松动了！精灵们已经失去了他们的配方！

此，还是希望这一概念成为讨论的核心：为了网络安全取得成功，为了让网络安全专业人员得到信任，全体需要高度重视道德行为——因为这是正确的做法，而不仅仅是遵守法律或为了方便。这也意味着鼓励他人做正确的事情，谴责不当行为。伤害无辜或危及公众的“绝顶黑客”是不可接受的，无论他多么聪明。

道德挑战

明尼苏达大学被禁止为 Linux 内核做贡献，这件事情始于该校的一项研究。[1]这项研究旨在观察是否可能在修补微不足道的漏洞的同时引入隐蔽的、严重的、新的漏洞。为了证明这种攻击，研究人员将其修改提交给实际的 Linux 内核。值得庆幸的是，该研究包含了防止有缺陷的代码被接受和分发的保护措施。

这引发了网络安全和软件开发社区的强烈反对。许多人认为这是人类欺骗实验。该大学辩称，这项研究不涉及人类，不需要接受 IRB 的审查。

在这个研究案例中，技术上和法律上可以做的事情并不意味着应该这样做。

例如，在美国，法律并不要求负责任地披露漏洞。[2]在主流网络浏览器中发现关键漏洞的安全团队可以在不通知供应商的情况下合法地公开发布该漏洞，但这样做会有广泛利用和泄露漏洞的风险。研究人员可能不会为了自己的利益而利用它，但给其他人留下了机会。为强盗敞开大门几乎和加入抢劫的结果同样糟糕。

道德和伦理与法律是有区别的，但是否应该同时受到法律和道德的限制？许多职业、专业组织和行业都有职业道德规范和职业行为规范。计算机协会(ACM)有一个非常好的守则，[3]第一句话就指出其重要性：“计算机专业人员的行动改变了世界。”该守则阐述了计算机专业人员对公共利益的责任、对社会和人类福祉的关心、对道德实践的责任，以及对隐私的尊重。事件响应和安全小组论坛(FIRST)也有著名的道德准则。[4]

许多获得认可的学术性计算机科学和工程项目都要求进行伦理研究。工程与技术认证委员会(ABET)表示，毕业生将“认识到职业责任，并在网络安全实践中根据法律和道德原则做出明智的判断。”[5]

在大多数研究环境中，机构审查委员会(IRB)审查研究提案，以保护研究对象的权利和福利。如果想通过向人们发送虚假电子邮件来研究网络钓鱼，IRB 将考虑参与者会遭受的潜在危害。

最后，考虑一下其他人会如何看待这样的选择。即使这样做是完全正确的，仍然可能受到很多质疑和抵制。如果这种质疑和抵制成为新闻头条，我们会感到舒服吗？[6]

---

1 见[39]。

2 联邦政府有适用于政府机构和部门的内部披露政策，如漏洞公平裁决计划(VEP)。见[40]。

3 见[41]。

4 见[42]。

5 见[43]。

6 一位前中央情报局官员将其通俗地描述为“华盛顿邮报测试”，参见[44]。

当我们觉得某件事在技术上可行或技术上合法时，应该暂停，并重新审视一下这种行为。

1.19　误区：更好的安全意味着更糟糕的隐私

如果问人们隐私是否重要，无疑会得到热忱的回答：“是!”联合国《人权宣言》中明确提到了这一点。[1]法律界的共识是，美国宪法中隐含了隐私权[2]，几项法律也明确承认隐私权。欧洲颁布了关于隐私的主要法律，其中最著名的是《通用数据保护条例》(GDPR)；然而，与安全性类似，隐私的正式定义并没有被广泛接受。虽然被认为有划时代的意义，但随着时间的推移，不同的社会文化对它的定义也有所不同。

技术在定义隐私和侵犯隐私方面也发挥了作用。窗户、相机和电话的发明都是技术变革对隐私产生影响的例子。计算和网络在这方面继续突破界限。许多与网络安全相关的场所都被贴上了“安全和隐私保护”的标签，使这种联系变得明确。

与此相关的误区是，增加隐私保护会降低系统的安全性，反之亦然。事实并非如此！仔细想想，网络安全的主要驱动因素之一是支持隐私：限制对私人信息的访问。

之所以出现这个误区，是因为在某些情况下，解决安全问题的最直接或最便宜的方案是减少隐私。例如，如果想减少网络钓鱼的机会，需要检查并存储进入企业电子邮箱的所有电子邮件的副本，以牺牲电子邮件隐私为代价捕获网络钓鱼链接。其实还有其他方法，包括允许使用计算能力来增强安全性和保护隐私。例如，可以自动截短电子邮件中的 URL 使其无效，而不必保存记录或让他人阅读内容。

并不存在为了更好的安全而放弃隐私保护的情况。添加日志记录或监控并不是解决问题的唯一方法，尽管这通常是最便宜、最快的方法。“快速、廉价”往往会导致用户群体的隐私逐渐减少。隐私很重要，人们应该有机会对何时、如何，以及是否侵犯他们的隐私，使用一个系统进行确认。公众对 cookie 和在线广告的抵制是对这些问题的认识不断提高的例子。

从事网络安全工作的人应该尽可能保护隐私，而不是减少隐私。当受到 GDPR 等限制时，找到支持而不是规避这些限制的方法是应尽的职业责任。

1　见[45]。

2　不过，美国最高法院最近在 Dobbs 起诉 Jackson 妇女健康组织案中的裁决对这一隐含权利的范围产生了一些怀疑，见[46]。

第2章

互联网的概念

我们急于建造一条从缅因州到得克萨斯州的电报线，但缅因州和得克萨斯州可能没有什么重要的信息需要交流。

——Henry David Thoreau

40 年前，网络安全的书籍只是关注个人计算机的安全。当时没有互联网。之后网络技术不断进步，无处不在，正如 Scott McNeely 所说的：“网络就是计算机。”局域网、广域网、城域网、Wi-Fi、蓝牙、NFC 等连接系统以及系统的系统。在越来越多的情况下，软件和数据都在“外面”的云端，如果没有正常的网络接入，系统就无法按照我们的预期运行。

本书不是一篇关于通信网络的专著，所以不会深入研究通信网络和通信网络安全，只讨论关于互联网和云计算的一些误区和误解。让我们从一个简单的概念开始：什么是互联网？

2.1 误区：每个人都知道“互联网”的含义

在最肤浅和最普遍的层面上理解，互联网是所有计算机系统的集合，它们可以使用通信网络相互沟通。可以有未连接到互联网的网络，这通常被描述为一个“独立的”网络。互联网(和其他通信网络)提供标准化的服务，包括网站和电子邮件。值得注意的是，Web 不是互联网的同义词，它只是其中的一部分。

使用标准化的协议(Protocol)，互联网上的计算机可以相互通信。这些协议定义了交换信息的规则和语法。许多资源的通信网络使用 IP 协议族，如传输控制协议(TCP)、用户数据报协议(UDP)等，还包括仍在使用的 UUCP、Bitnet、DECNET、XNS 和 X.25 等协议。系统可以在同一个物理网络上同时使用 IP 协议及这些协议(尽管已不太常见)。