第三篇前言
版

《安全工程》第一版于 2001 年出版，第二版于 2008 年出版。此后发生了几次重大变化。

最明显的是智能手机已经取代了 PC 和笔记本电脑。
世界上大多数人现在都带着一台同时也是电话、相机和卫星导航的计算机；在这些神奇设备上运行的应用程序已经取代了我们十年前构建的许多东西。出租车现在由叫车应用程序而不是出租车计价器收费。银行业已基本在线，手机开始取代信用卡。节能不再是您的电表与您的供暖系统通话，而是两者都与您的手机通话。社交网络已经占据了很多人的生活，推动了从广告到政治的方方面面。

一个相关但不太明显的变化是转向大型集中式服务器场。
敏感数据已从学校、医生办公室和律师事务所的服务器转移到云服务提供商。许多人不再在笔记本电脑上使用文字处理软件写作，而是在 Google Docs 或 Oce365 上写作（我在 Overleaf 上写作）。这有后果。安全漏洞的发生规模在 20 年前是任何人都无法想象的。泄露数千万个密码或信用卡几乎已成为家常便饭。在 2013 年，我们发现在未经患者同意的情况下，价值 15 年的英国医院病历被卖给了全球 1200 家组织（患者仍然可以通过邮政编码和出生日期进行识别）。

过去十年中最大的游戏规则改变者可能是斯诺登泄密事件，也是在 2013 年，当时超过
50,000 份关于美国国家安全局信号情报活动的绝密文件被泄露给了媒体。政府监控的规模和侵入性甚至让愤世嫉俗的安全工程师感到惊讶。

这给我们带来了第三大变化，即对安全威胁有了更好的理解。除了了解西方情报机构的能力和优先事项外，我们对中国人、俄罗斯人甚至叙利亚人的所作所为也有相当好的了解。

钱在哪里，骗子也会跟到哪里。过去十年还出现了网络犯罪生态系统，恶意软件编写者提供了破坏数百万台机器的工具，其中许多机器被用作犯罪基础设施，而其他机器则以各种方式被破坏以欺骗用户。我们在剑桥有一个研究这个的团队，还有几十个

全球其他研究小组。网络犯罪的兴起正在改变警务和其他国家活动:加密货币不仅使编写勒索软件变得更容易，而且破坏了金融监管。然后是网络欺凌等个人威胁,这些威胁通常低于刑事起诉的门槛,但会造成真正的痛苦,社交网络使这些威胁变得更容易,而且发生的规模如此之大。

因此,网络危害现在涉及从银行和军队到学校教师的各种各样的人。衡量这些危害的成本以及我们为减轻这些危害而采取的措施的有效性变得越来越重要。

有些变化会让十年前读过我的书然后被单独监禁十年的人感到惊讶。例如,尽管 40 年来受益于美国政府数十亿美元的资金,多层次安全行业仍处于垂死状态;五角大楼的整个信息安全理念 强制架构阻止信息从绝密到机密再到机密再到非机密 已被放弃,因为它不可行。尽管架构仍然很重要,但重点已转移到生态系统。鉴于漏洞无处不在,漏洞利用不可避免,我们最好善于发现漏洞,修复漏洞并从攻击中恢复。游戏不再是可信系统,而是协调披露、DevSecOps 和弹性。

未来会怎样?一个可能的游戏规则改变者是,当我们将软件放入汽车和医疗设备等安全关键系统中,并将它们连接到互联网时,安全和安保工程正在融合。这导致了真正的压力;安全工程师可以快速修复错误,而安全工程师则喜欢根据变化缓慢（如果有的话)的标准严格测试系统。一个棘手的问题是我们将如何修补耐用品。目前，您的手机可能会获得三年的安全补丁,您的笔记本电脑可能会获得五年的安全补丁;在那之后你应该买一个新的。但是汽车平均可以使用 15 年,如果我们突然要求我们在 5 年后报废它们,那么环境成本将是无法接受的。那么请告诉我,如果您现在正在为 2022 年推出的汽车编写导航软件,您将选择哪种工具链来确保您能够在 2032 年、2042 年和 2052 年继续发布安全补丁?

最后,政治环境发生了翻天覆地的变化。几十年来,政治领导人一直认为技术政策是为 anoraks 准备的,并且通常采取阻力最小的路线,但俄罗斯干预英国脱欧公投和特朗普大选的报道真正引起了他们的注意。失去工作的前景可以很好地集中思想。立法者的密切关注正在改变游戏规则,首先是更严格的规则（例如欧洲的通用数据保护条例）,其次是软件和在线连接进入已经受到安全监管的产品,从汽车和铁路信号到儿童玩具.

安全工程师今天要问的问题与十年前一样:我们要防止什么,所提议的机制是否真的有效?但是,我们现在工作的范围要广得多。

几乎所有的人类生命都在那里。