第29章

超越“计算机说不”

在本世纪初,安全技术是一个由相互怀疑的岛屿组成的群岛 密码学家、操作系统保护人员、防盗警报行业,一直到制作钞票墨水的化学家。

我们都认为世界在我们的岸边结束了。到 2010 年,安全工程已成为一门成熟且不断发展的学科;当从业者意识到我们必须超越我们的舒适区时,这些岛屿被桥梁连接起来。

不想了解数字水印的钞票墨水化学家,以及只会谈论机密性的密码学家,逐渐被边缘化。

现在,到了 2020 年,每个人都需要有一个系统的视角,以便设计出可以有效集成到实际产品和服务中的组件。由于这些被真实的人使用,而且通常在全球范围内使用,我们的领域也包括人文和社会科学。

安全工程旨在确保系统在面对从轰炸机到僵尸网络的各种恶意攻击时具有可预测的可靠性。随着攻击从硬技术转移到使用它的人,系统还必须能够抵御错误、意外甚至胁迫。因此,对人员工、客户、用户和旁观者 的现实理解是必不可少的;人、制度和经济因素与技术因素一样重要。真实系统提供可靠性的方式变得越来越多样化,保护目标不仅更接近应用程序,而且可能微妙而复杂。目标之间的冲突很常见:一位校长想要问责制,而另一位校长想要否认,很难同时取悦他们。

从 2001 年开始,我们开始意识到许多持续的安全失败本质上是激励失败;如果 Alice 守卫一个系统而 Bob 为失败付出代价,那么你可能会遇到麻烦。这导致了安全经济学的发展,这本书的第一版有助于催化。 2008 年的第二版记录了故障如何也越来越多地与可用性有关,此后的十年见证了对安全心理学的大量研究。

那么接下来呢?作为本书的结论,我想强调三件事。

第一,复杂性。计算机科学花了 70 年的时间设计了一系列令人印象深刻的工具来管理技术复杂性,但我们现在正在努力应对社会复杂性。我们可以对汽车进行编程,使其在高速公路或沙漠中自动驾驶得相当好,但我们无法应对拥挤的城市街道以及所有那些难以预测的人。我们可以加密消息或从数据库中删除人名,但我们无法阻止社会结构的显现。欺负人是有限度的; “电脑说不”是快速失去客户的方法。仅仅研究计算机系统如何与人类交互是不够的;我们需要弄清楚它如何与许多互动的人一起工作。

第二,可持续性。当我们将软件放入所有东西并在线连接所有东西时,我们必须给软件打补丁并维护服务器。对于汽车、起搏器和变电站等耐用品,我们可能必须维护软件 20 年甚至 40 年。我们不知道如何做到这一点,如果我们不破解它,那么我们的自动化对我们星球的未来来说将是个坏消息。所谓的“智能”设备通常只是当“计算机拒绝”时必须尽快丢弃的东西。

第三,政治。安全不是一个标量,而是一种关系。这不是您撒在系统上的某种魔法仙尘,而是关于这些系统如何发挥作用的。当“电脑说不”时,谁输谁赢?社交网络用户获得隐私权,还是广告商获得访问权?它是如何被用来将金钱转化为政治权力的?如果人们想要可靠的互联网或低网络犯罪率等公共产品,如何在全球范围内提供这些产品?

技术已经完全改变的十年来网络犯罪的稳定性表明,它从根本上与技术无关。技术垄断的持续存在引发了其他问题,如技术与社会如何共同进化,以及权力的本质。当 Facebook 成为政治言论的仲裁者,当苹果和谷歌可以制定冠状病毒接触者追踪政策,当亚马逊、微软和谷歌制定面部识别政策(中国境外)时,我怀疑技术人员应该开始阅读政治学,以及经济学和心理学。

未来十年最棘手的问题可能是治理。

正如个人可以通过经验学习一样,我们的社会也可以学习和适应。民主是实现这一目标的关键机制。因此,工程师可以做出贡献的一个重要方式是参与政策辩论。我们越多地参与技术在复杂性、可持续性和权力性质方面提出的问题,我们的社会就会越快地适应这些问题。