走向安全科学

客座编辑导言 | 慕尼达 P. 辛 | 2013 年 1 月

“我们遇到了敌人，他就是我们自己”

沃尔特·凯利，《Pogo》

过去数十年，安全研究获得了越来越多的关注和资助。尽管付出了大量努力，但是目前的安全实践尚未脱离“头疼医头，脚疼医脚”的套路：发现缺陷、打个补丁、再找缺陷……如此反复。这种就事论事的方法有时称为“工程”，当然这仅仅是从针对具体问题开发专门解决方案这个狭义角度而言的。

不同于以往的工程化方法，过去几年安全研究界出现了发展安全科学的势头。美国国家科学基金会和美国国防部等主要资助机构启动了一些项目，专门支持把安全研究提升为一门科学。这些项目背后的动机是建立一套具有较强理论和实证基础的系统化知识体系，从而使得信息系统安全工程不仅可以抵抗已知攻击，还能抵御未预料到的攻击。一个让人引颈以待的愿景是寻求度量标准，例如描述一个系统在哪些情况下、面临什么样的威胁时安全性到底如何。

部分挑战源于如下事实：计算不是一门自然科学，这一点看来让计算机科学家产生了不少焦虑和反思。根据赫伯特-西蒙（司马贺）数年前的洞察，计算科学是一门人工科学。作为人工科学，计算不仅需要原理，还需要通过实证调查对知识进行系统化的方法，尽管这与物理学原理或生物学调查并不相同。不同于对自然世界做预测，我们要对 IT 的表达、架构以及实施（该信息安全系统的）组织做出断言。

开放系统

安全与计算的明显不同包括两个方面。首先安全从根本上不能脱离人：它不仅关注人，而且我们自身就是其中的活跃角色。正因为认识到人是安全中的活跃因素，才导致引

入心理学的洞见来理解人们如何概念化私人信息、为什么他们容易受到某种形式的攻击，以及如何根据人类注意力和认知能力的局限性来协助他们应对威胁。

另一方面，安全从根本上讲是一个开放系统。如果我们可以精确限定一个系统，那么除了确保正确性和完整性，就没有其它安全挑战，因为这种情况下，任何入侵都会违反某些假设。系统的开放性意味着参与者及其行为事先不可知。然而，计算学科一直强烈偏向于处理封闭系统。的确，在我们的语言中，一个根深蒂固的观念是“系统”总是明确限定的，我们谈及“系统”时，老像是在议论一个我们可以随意处置的盒子。在我们的想象中，用户是呆在外面与系统进行交互的。

规范：一种新看法

上述情况让我认识到可把系统和安全的规范性做为我们所寻求的安全科学的基础。具体来说，当我们在更宽的视角考虑系统时，我们应该将用户和破坏者都视为系统的必要组成部分。即，系统的安全性并不在它的周边，而正在它的核心。于是，一个系统对应于一个社会，无论是整个人类社会，或者更常见的，是一个适当的微型社会。安全性就是这个社会系统的规范，所谓安全出了问题，就是违反了某些规范。

重要的是—尤其是从安全立场来看—这些规范并不是泛泛的条件，比如发生了好事（处于活跃状态），或没发生坏事（处于安全状态）。对于由单方拥有的单一系统，而且是拥有方从自己的视角运作时，抱有这样的传统观念未尝不可。但当我们将目光移到开放系统，一般性约束就不是那么有意义了：是好是坏取决于你在问谁。此外，我们必须把规范建立在可审计概念基础上，因此，当规范被违反时，我们知道是谁干的。

理解这样的规范对安全科学的清晰表述至关重要。特定的属性可通过对这些规范的推想与确保来证明。我们可以进一步量化这些规范的预期成败来形成特定的度量标准。

一字箴言

精确定义的概念是科学的基本要素，虽然往往发展比较慢。实验和观测都是建立在相应概念的基础上。举例来说，今天测量质量和动量已是常识，但中世纪的学者，甚至像伽利略这样早期的科学家，对这些概念并不清楚。伽利略的前辈们谈论的原动力（impetus）概念，今天已经不再作为一个技术概念而存在，虽然从质量、动量和动能等现代概念中也还能看到它的影子。这让我不由自主地想到安全科学目前尚处在前伽利略阶

段。我们应该提出并通过各种方式完善我们的假设，并且尽可能地开展测量，我们应该记住，我们所测量的有可能对安全科学至关重要——就像原动力对现代物理学那样关键。

本月主题

安全是一个庞大的领域，安全科学也涵盖很多方面。下面选择的代表论文反映了我对专家和规范性关注的偏好，也代表了我希望这个领域应该的发展方向。

在《论对手模型和组件安全》一文中，Anupam Datta 和他的同事们直面的挑战是确定系统是否满足特定类型的安全属性(security properties, 又称为 safety properties)，从而保证在计算中不发生坏事。在他们的系统模型中有两类组件：可（正确地）信赖组件和对抗者。对抗者可能以任意次序调用资源接口，而可信任组件只以适当的方式调用。

回想一下 CAPTCHA 这类网站常用的小挑战问题：用户要想执行某些步骤，例如创建一个帐户，必须先解决它。其背后的思想是，这种小挑战问题（如识别扭曲的字母）人很容易解决，但对电脑来说却很难，这样就能抵御机器攻击，例如创建虚假帐户。《人在解决 CAPTCHA 问题方面表现如何？》一文中，Elie Bursztein 和他的同事们评估了各种常用 CAPTCHA 的有效性，发现它们对用户的难度往往比设计者预想的要大。

处理开放系统的核心观念是身份。Elisa Bertino 的《赛博空间中的可信身份》对数字身份以及如何创建和共享身份的当前观点进行了简要综述。

《风险可知访问控制中的责任》采用了规范性方法，Liang Chen 和他的同事介绍了一种将风险评估引入决策的方法。特别地，他们的方法支持在必要时可以违反规则，只要责任方承担事后收场的责任。例如，当遇到紧急情况却没有医生做决定时，护士可以得到开药授权，只要护士能够在一定时间内提供必须这么做的理由。

在《一种面向在线社交网络访问控制的用户行为为中心的框架》一文中， Jaehong Park 和他的同事们介绍的方法将用户的主要行为从管理行为（用户自己执行或由其代表执行）中分离出来。这种方法的主要动机是有助于表达和执行那些反映了用户喜好的规则，包括他们如何与他人互动，他们希望如何调节他人的互动，例如父母控制孩子与他人交往的规则。

深入探索

除了上面的文章，有兴趣的读者可以参考以下资源。

- 美国国家安全局的《下一波（Next Wave）》杂志就赛博安全出了一个专辑。Roy Maxion 以自己的键盘生物识别研究为例的论文《**让实验独立**》，尤其值得一读。
- Bruce Schneier 的新作《说谎者和局外人：建立社会健康发展需要的信任》(Wiley, 2012)从规范性的观点看待安全，这和我前面提到的思路相仿。Paul Wallich 在《**IEEE Spectrum》上对 Schneier 大作的书评**生动地介绍了其中的观点。
- Carl Landwehr 等在**《隐私和赛博安全：新百年》**对安全和隐私进行了回顾和展望。美国国土安全部发布了更广泛的**《赛博安全研究路线图》**，点出了安全科学需要致力应对的一些关键挑战。

致谢

感谢 Amit Chopra 和 Laurie Williams 的宝贵意见。感谢美国陆军研究办公室的安全科学微实验室基金的支持。

慕尼达 P. 辛（Munindar P. Singh）是美国北卡罗莱纳州立大学计算机科学系教授。他的研究兴趣包括多代理体系统和面向服务的计算的研究，后者注重于从规范的角度对信任和隐私进行研究。慕尼达 1999 年至 2002 年担任《IEEE 互联网计算》总编，也是其它几个编辑委员会的成员。他是 IFAAMAS（自主代理与多代理系统国际基金会）的创始理事。慕尼达的研究成果曾获得美国陆军研究实验室、美国陆军研究办公室、思科、DARPA、爱立信、IBM、英特尔、海洋学联合研究所、美国国家科学基金会和施乐公司的各种奖励和资助。他已经指导 17 名学生获得博士学位。慕尼达是 IEEE 会士。他的电邮是 singh@ncsu.edu。

（黄铁军 译）