前　言

龚晓锐[1,3], 张　超[2]

[1]中国科学院信息工程研究所 北京 中国 100093
[2]清华大学 北京 中国 100000
[3]中国科学院大学 网络空间安全学院 北京 中国 100049

网络空间安全的核心是攻防能力的较量, 在道高一尺魔高一丈的斗争中, 只有掌握了各类高超的攻击技术, 才能在防御中立于不败之地。本期专题旨在总结网络攻防领域主要分支的技术发展, 介绍几个代表性方向的最新研究成果, 帮助读者把握攻防技术前沿, 为更好地实施网络防御提供指引。

网络攻防是一个双方博弈过程, 有效的防御技术必须要跟上攻击技术的发展, 了解攻击技术的机理至关重要。攻击技术主要分为软件/系统级攻击和网络级攻击两大类。软件/系统级攻击关注的是针对单个软件、单个系统的攻击技术, 主要围绕软件漏洞挖掘以及系统机制及特性的利用。本期专题向读者推荐一篇涉及软件漏洞挖掘的文章, 面向有源代码的软件, 使用代码的结构信息进行智能化漏洞挖掘, 所考虑的结构信息是抽象语法树(Abstract Syntax Tree, AST), 并引入神经网络模型学习 AST 的语法表征。

攻防对抗无处不在的思想也在本刊中也得以体现, 神经网络模型一方面能够用于漏洞挖掘, 另一方面也成为了被攻击的对象。本刊另一篇软件/系统级攻击技术方面的文章, 讲解的就是深度学习中的中毒攻击方法, 作者分析了此类攻击存在的可能性,并研究了现有的针对这些攻击的防御措施, 让读者对神经网络模型的攻击面有了一个较为清晰的认识。

软件漏洞的不可避免性决定了防守方不能一味把精力放在漏洞消除方面, 我们必须承认系统“带洞运行”的现实。有漏洞的情况下如何防止攻击, 这正是漏洞利用缓解技术要解决的问题。随机化技术和完整性校验技术是该方向两个重要的分支, 本刊推荐的两篇文章, 分别在指令随机化和控制流完整性校验方向提出了新的方法。除了技术创新外, 这两篇文章所代表的还有一个重要思路, 那就是当前防御机制的发展趋势是要逐步由被动走向主动。

网络层面的攻击技术建立在软件/系统层面的攻击技术之上, 关注点是如何将网络中的一系列薄弱点连接起来形成杀伤链。本刊在这个方向为读者推荐的两篇文章, 第一篇提出了一种模拟真实网络渗透场景的安全竞赛, 让读者了解攻防整体过程, 以及攻防演练场景的构建方法; 第二篇针对的是网络层面典型攻击之一的资源消耗型攻击, 讨论了在 SDN 场景下的关键资源以及针对这些资源的多种攻击形式。

网络攻防的双方博弈是一个不对称博弈, 攻击方只需突破一个点即可达成目标, 而防守方则要对所有攻击面进行防护。并且攻击方处于主动地位, 防守方处于被动地位, 这就导致防守几乎成为一项不可能完成的任务。攻击发现是扭转这一被动局面的关键技术, 传统的入侵检测技术在经历了约 20 年的发展后, 到达了一个什么样的状态, 前景如何？除了入侵检测我们还有哪些可用的技术？在攻击发现方面本刊向读者推荐3篇文章, 分别讨论入侵检测技术发展、恶意软件检测以及物联网蜜罐技术, 文章中提出一些新的思路, 让读者能够了解本领域的发展前沿。

本刊组稿经历了较长时间, 我们要特别感谢《信息安全学报》编委会对本期专题工作的信任和指导, 感谢编辑部各位工作人员从征稿启事发布、审稿专家邀请至评审意见汇总、论文定稿、修改、校对和出版所付出的辛勤工作和汗水, 非常感谢专题评审专家及时、专业、细致的评审。我们还要感谢向专题踊跃投稿的各位作者。

最后, 感谢本期专题的读者们, 希望专题能够有助于你们的技术研究工作。