前　言

笔者在普渡大学读博士期间，耳濡目染，除了在研究方面，在教育方面也有幸受到不少优秀教授的影响。当笔者 2001 年在雪城大学（Syracuse University）开始教学生涯时，很多潜移默化带来的理念就自然在自己的教学中体现出来，其中最大的一点就是理论与实践相结合。这看似老生常谈，但真正做到却不容易。教理论易，教实践难，设计一套动手实践的教案则更难。没有有效的动手实践，理论与实践相结合就是一句空话。

在普渡大学读书时，笔者学习过的操作系统、编译原理和网络等课程都有非常好的教材，并且每门课程都有精心设计的动手实践环节。这些教材不仅讲授抽象的理论，而且结合了很多与实践密切相关的内容，让学生边学边做，既能学到系统的知识，又能通过实践加深对知识的理解。遗憾的是，在计算机安全领域，能够做到理实交融的教材并不多。从 2001 年开始教学后，笔者陆续使用过一些教材，但都不满意。笔者一直在教学中贯彻理实交融的理念，但不是按照任何一本书来做的。笔者也曾想自己编写一本教材，但当时没有太多的教学经验，对计算机安全的理解和领悟也还没有达到能够随心所欲写作的地步，因此第 1 章还未写完，就觉得写不下去了，即使再写下去，也未必能超越其他的教材。于是搁笔，这一搁就是十几年。

这十几年虽然没能写出教材，但笔者精心设计了 30 多个动手实验，除了自己使用之外，还免费提供给其他教师和学生使用。这些实验弥补了已有教材在实践方面的不足。笔者联系了几乎所有比较有名气的计算机安全方面教材的作者，授权他们免费使用这些实验作为教材的辅助材料。在设计这些实验的过程中，笔者也加深了对计算机安全的领悟，很多看似独立的知识点也因为从这些实验中得到的经验逐步在脑海中形成知识体系。

同时在这十几年中，笔者在教学方面也渐渐成熟，掌握了如何循序渐进地把较难的内容讲清楚讲透彻，如何把实践结合到教学中，如何通过比喻让学生更好地理解抽象的概念和原理，如何举一反三，如何把相关知识点串联起来，如何从不同角度出题看学生是否真正理解了某个知识点，等等。这些积累，使笔者在计算机安全教学方面渐渐形成了一套自己的体系，一套与别人不同、自始至终贯彻理实交融理念的教学体系。

2015 年，笔者突然意识到，如果把上课的内容与设计的 30 多个实验结合起来写成一本教材，将来就可以按照这本教材来上课，另外这些积累下来的经验也许会对其他教师有借鉴作用。从那一刻起，笔者开始奋笔疾书。而且因为有了多年的积累，在写作时总有一

种左右逢源的感觉，不再像十几年前那样不知从何下笔。2017 年 10 月，笔者终于完成了教材的写作，并通过自我出版平台出版了教材的英文版。一年之内，将近 60 所学校开始使用这本教材。在过去的一年中，在浙江大学同人的鼎力帮助下，这本书的中文版终于面世了。这并不是单纯的翻译。在撰写中文版教材的过程中，笔者同时在准备英文版教材的第二版，因此本书中加入了不少未在英文版中出现的新内容，这些内容将来会被翻译成英文，出现在英文版的第二版中。

• 本书特点

本书的第一个特点是理论与实践相结合。对于每个书中涉及的理论，本书都使用了一系列实验帮助读者加深对理论的理解，目的是让读者得到亲身体验，而不仅仅是从字面上获取知识。在这些实验中，有些是几分钟即可完成的小实验，有些则是需要花费较长时间、比较复杂的实验。例如，在介绍一个攻击时，本书不仅仅是讲解攻击的原理，更重要的是使读者了解攻击过程，并指导读者在本书提供的实验环境中亲自动手发动这个攻击。在介绍安全机制，例如防火墙和虚拟专用网（VPN）时，本书会指导读者亲自动手开发一个小型的防火墙或 VPN，而不只是简单地介绍一些抽象的原理。

本书中的大部分实验都基于笔者花费 16 年心血设计的 SEED 实验，这些实验已经在世界各地被广泛使用。截至目前，大约有 65 个国家的 800 多所学校在使用这些实验，包括大学、专业技校，甚至一些高中。所有这些实验都可以在笔者的 SEED 网站（https://seedsecuritylabs.org）免费下载。读者在学习完每一章后，都可以找到一个对应的 SEED 实验，通过这些实验巩固对书中知识的理解。书中所有的实验都可在由笔者提供的 Ubuntu 16.04 虚拟机映像中进行。该虚拟机可以从 SEED 网站下载。实验所需要的一切环境已经在虚拟机中安装和配置好了，读者只需下载这个免费的虚拟机并在 VirtualBox 中运行，即可开展书中设计的各种实验。笔者将每隔几年定期升级虚拟机映像。

本书的第二个特点是注重知识体系的建立。计算机安全中的不少攻击和防御方法表面上看起来不同，但如果深入研究的话，会发现它们其实是相似的或有关联。有些内容看起来相似，本质上却有所不同。这就是知识点的相关性。只有将不同的知识点联系起来，读者才能在脑海中形成知识体系。这是学习的更高境界，也是一个好的教育者希望学生真正学到的。因此，本书不希望成为一本计算机安全方面的“百科全书”，而是希望帮助读者建立完善的知识体系。例如，在介绍完 SQL 注入攻击后，本书将几个注入攻击放在一起，讨论它们共同的根本原因，并解释为什么针对它们的防御措施在本质上是相似的。计算机安全知识更新很快，每天都有新的漏洞和攻击出现。有了扎实的知识体系，读者就不会疲于学习这些新知识，因为很多东西万变不离其宗。

本书的第三个特点是深入细节、讲解透彻。计算机安全虽然涉及不少理论，但并不是一门理论学科，而是一门和计算机系统密切相关的学科。不少教材在介绍计算机安全原理

时只停留在理论层面，很多计算机系统的相关细节都被抽象掉了。这就导致很多人只懂理论，不会实践，因为有太多的细节不清楚。笔者本人在刚当教授时也犯过这种错误。当讲完缓冲区溢出的原理后，安排学生花一周时间完成攻击实验，结果一个多月过去了，也没有几个学生能够完成。后来发现原因不在学生身上，因为其中涉及了太多的细节。一个细节没搞清楚，攻击就无法成功。没有正确的引导，大部分初学者很难琢磨出全部细节。即使是有能力的学生，也需要花很多时间，走不少冤枉路。虽然走冤枉路也是一个学习的过程，但是如果能对学生进行正确引导，他们学习的效率就会大大提高。为了达到这个目的，本书在细节上绝不吝惜笔墨，在介绍一个知识点时，会循序渐进地把它讲解透彻。例如，对于缓冲区溢出，一般课堂上 30 分钟就可以讲完，本书却用了整整两章，从数据在计算机内存中是如何分布的，到攻击的原理和难点，如何克服难点，如何进行防范，以及如何攻破某些防范措施等，通过循序渐进、由浅入深的方法将整个过程讲得清清楚楚。

• 内容结构

本书分为三大主题：软件安全、Web 安全和网络安全。软件安全和 Web 安全涵盖了一些众所周知的漏洞以及一般软件和 Web 应用程序面临的攻击，包括最近的一些攻击，如 Shellshock 和 Dirty COW 攻击。通过学习这些主题，读者可以理解为什么计算机或程序会受到攻击，这些攻击的原理是什么以及如何编写更好的程序，从而使得程序对攻击免疫或更具弹性。网络安全部分重点介绍与因特网（Internet）相关的安全原理。这部分不仅涵盖一些众所周知的互联网攻击，也包括重要的防御机制，如防火墙、虚拟专用网（VPN）和公钥基础设施（PKI）等。

本书并非要涵盖所有攻击或安全措施，它涵盖的主题是在计算机安全的基础理论方面有代表性的。还有一些主题，如加密、系统安全和移动安全等，会在后续版本中增加。本书的内容足以满足计算机安全和网络安全基本课程的需要。例如，笔者的两门课程（Computer Security 和 Internet Security）使用的就是这本教材中不同章节的内容。这两门课程同时面向本科生和研究生，但对他们的要求不同。虽然有些章节依赖于前面的章节，但大多数章节都是独立的，可以独立阅读。以下是各章节之间的部分依赖关系。

第 1 章（Set-UID 特权程序原理及攻击方法）是大多数章节的基础。本章介绍 Set-UID 机制的工作原理并给出一个可以针对此类特权程序攻击的概述。虽然还有许多其他类型的特权程序，但本书使用这种类型的程序解释各种攻击的工作原理。

第 2 章（通过环境变量实现攻击）是第 3 章（Shellshock 攻击）的基础。

第 4 章（缓冲区溢出攻击）是第 5 章（Return-to-libc 攻击）的基础，Return-to-libc 攻击攻破了缓冲区溢出攻击的一个防御机制。

第 7 章（竞态条件漏洞）和第 8 章（脏牛竞态条件攻击）都与竞态条件漏洞有关，建议读者先阅读第 7 章，因为它更容易理解。

第 12 章（数据包嗅探和伪造）是本书中涉及的大多数网络攻击的基础，因此在阅读网络安全部分之前应该先阅读该章内容。

第 18 章（公钥基础设施）是第 19 章（传输层安全）的基础。

• 关于 SEED 实验

“我听过了，我就忘了；我看见了，我就记得了；我做过了，我就理解了”这句名言，来自于蒙特梭利教学法的创始人玛利亚 蒙特梭利，我们的祖先孔子和荀子也说过类似的话。这句话一直是许多教育者的座右铭，他们坚信学习必须和实践相结合，对于计算机安全教育尤其如此。16 年前，笔者将这个座右铭铭记于心，渴望成为计算机安全领域的好教师。笔者在网上搜索，寻找可以用于课程的动手实验。笔者只能找到有限的一些实验，这些实验来自不同的地方，内容不一致，并且涵盖的范围很窄，实验环境也不易搭建。

于是笔者决定自己开发一系列动手实验，希望涵盖广泛的安全主题；这些实验不只是为了笔者自己使用，也是为了众多和笔者拥有同样教学理念的教师使用。所有实验都应该基于一个统一的环境，这样学生不需要花太多时间为不同的实验学习新的环境。此外，实验环境应该易于搭建且成本低廉，这样更多的教师和学生能从中获益。

上述想法获得了美国国家科学基金会（NSF）的资助（74 984 美元，奖项编号 0231122），于是，笔者从 2002 年起开始了这个旅程。笔者将该项目命名为 SEED（取 SEcurity EDucation 两个单词的各前两个字母）。2007 年该项目又一次获得 NSF 资助（451 682 美元，奖项编号 0618680）。到 2010 年，在笔者和 20 多名学生的努力下，开发了 30 多个 SEED 实验，涵盖许多安全主题，包括漏洞、攻击、软件安全、系统安全、网络安全、访问控制、加密、移动安全等。大多数 SEED 实验经历了多次试用和改进。

SEED 项目非常成功。截至目前，全球有 800 多名教师告诉笔者，他们已经使用了一些 SEED 实验。为了帮助其他人更好地使用 SEED 实验，NSF 在 2014 年给了笔者另一笔资助（863 385 美元，奖项编号 1303306），用来每年举办两期培训班，资助那些有兴趣的教师来参加培训（主要面向美国的教师，但也有来自其他国家的教师自费参加）。每年约有 70 多名教师参加，到目前为止，已经培训了 300 多名教师。2010 年 9 月，美国国家科学基金会的 TUES/CCLI 部门在给美国国会的报告中，选了 17 个项目来代表美国本科 STEM 教学的杰出工作，SEED 项目很荣幸地入选。2017 年，因为 SEED 实验的影响，笔者被第 21 届信息系统安全教育学术讨论会授予“学术领导”奖。