Vocational Education 职业教育, 2016, 5(4), 79-83
Published Online October 2016 in Hans. http://www.hanspub.org/journal/ve
http://dx.doi.org/10.12677/ve.2016.54015

Hans汉斯

Course Construction of Mainstream Operating System Security

Juan Wang[1,2]

[1]Computer Science Department, Wuhan University, Wuhan Hubei
[2]Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan Hubei
Email: jwang@whu.edu.cn

Received: Sep. 30th, 2016; accepted: Oct. 17th, 2016; published: Oct. 20th, 2016

Abstract

Operating system is the core of the information system, and the operating system security is the core of information system security. In 2014, the Information Security Professional Education Steering Committee under Ministry of Education issued a new version of the information security major guide specification. The course of Mainstream Operating System Security has been added in the new guide specification. However, currently it lacks operating system security curriculum. In 2014, the course has been opened in Wuhan University. Furthermore, we have been exploring and practicing in the course of construction and have established the course knowledge system including operating system security architecture, analysis of operating system security mechanism, kernel vulnerabilities and operating system security evaluation. In this paper, the relevant contents and teaching experience of the course construction are given.

Keywords

Operating System, Security, Course Construction, Teaching Quality

主流操作系统安全课程建设

王　鹃[1,2]

[1]武汉大学计算机学院，湖北 武汉
[2]空天信息安全与可信计算教育部重点实验室，湖北 武汉
Email: jwang@whu.edu.cn

文章引用: 王鹃. 主流操作系统安全课程建设[J]. 职业教育, 2016, 5(4): 79-83.
http://dx.doi.org/10.12677/ve.2016.54015

收稿日期：2016年9月30日；录用日期：2016年10月17日；发布日期：2016年10月20日

摘　要

操作系统是信息系统的核心，而操作系统安全也是信息系统安全的核心。2014年教育部高等学校信息安全专业教学指导委员会颁布的新版信息安全专业教学大纲中增设了《主流操作系统安全》课程。然而，当前国内外并未形成较完整的操作系统安全课程教学体系。武汉大学于2014年开设了主流操作系统安全课程，并在课程建设中不断的探索与实践，初步建立了以操作系统安全架构、操作系统安全机制分析、内核漏洞攻防、操作系统安全测评为基本内容的课程知识体系。本文给出了主流操作系统课程建设的相关内容及教学体会。

关键词

操作系统，安全，课程建设，教学质量

1. 引言

操作系统是信息系统的核心。操作系统管理着计算机系统的硬件、软件及数据资源，控制程序运行，为其它应用软件提供支持，让计算机系统所有资源最大限度地发挥作用，提供各种形式的用户界面，使用户有一个好的工作环境，为其它软件的开发提供必要的服务和相应的接口等。

操作系统安全[1]也是信息系统安全的核心。2014 年教育部高等学校信息安全专业教学指导委员会颁布的新版信息安全专业教学大纲中增设了《主流操作系统安全》课程。然而，当前国内外并未形成较完整的操作系统安全课程教学体系。武汉大学于 2014 年开设了主流操作系统安全课程，并在课程建设中不断的探索与实践。经过三年的课程教学，目前初步建立了以操作系统安全架构、操作系统安全机制分析、内核漏洞攻防[2] [3] [4]、操作系统安全测评为基本内容的课程知识体系。

2. 主流操作系统安全课程建设

主流操作系统安全课程的学习目标是使学生能够深入了解和掌握目前主流操作系统，如 Windows、Linux 和安卓操作系统的安全架构、原理和机制，并结合操作系统内核攻防实践[5]，使学生具备使用和设计操作系统安全架构和机制的基本方法和技能。

1、教学要求

通过本课程的学习，学生在理论知识和实践技能上应达到以下要求：

(1) 了解操作系统安全架构设计及原则

(2) 掌握 Windows 操作系统的安全架构、原理和机制

(3) 掌握 Linux 操作系统的安全架构、原理和机制

(4) 掌握安卓操作系统的安全架构、原理和机制

(5) 了解和掌握对操作系统内核进行攻击的常用方法

2、课程内容与学时分配

(一) 课程的主要内容、重点及难点

本课程的主要教学内容包括主流操作系统介绍、操作系统安全架构设计及原则、Windows 操作系统的安全架构、原理及机制、Linux 操作系统的安全架构[6]、原理及机制和安卓操作系统的安全架构、原

理及机制，其中操作系统安全架构设计及原则、各主流操作系统的安全架构和原理是本课程的重点，主流操作系统内核安全机制、内核攻防技能是本课程的难点。

(二) 课程内容与学时分配

主流操作系统安全课程内容与学时见下表 1。

(三) 课程实验

针对主流操作系统的教学目标和教学内容，依照理论与实践结合的教学理念，我们精心组织了十二个课程实验。通过这些实验，提高学生动手实践技能。具体内容如下表 2。

3. 主流操作系统安全课程教学体会

主流操作系统安全作为一门新的课程，目前在教学中还存在很多问题。

(1) 缺乏合适的教材操作系统安全[7]内容以前都是作为操作系统课程的一章内容介绍，主要是简单的介绍操作系统的安全问题。现在该内容作为独立的一门课程，目前国内外都缺乏合适的教材，包括实验指导教程。

Table 1. Mainstream operating system security course content and hours
表 1. 主流操作系统安全课程内容与学时

内容	学时(理论)
操作系统安全设计原则	3
操作系统内存保护机制	9
操作系统内核安全	9
操作系统访问控制机制	6
安卓安全框架、原理及机制	6
总结和复习	3
合计	36

Table 2. Mainstream operating system security course experiment
表 2. 主流操作系统安全课程实验

序号	实验内容
实验一	Linux 系统的基本操作
实验二	Linux 文件权限
实验三	Linux 系统用户密码机制
实验四	操作系统内存分配及缓冲区溢出
实验五	ALSR 及绕过方法
实验六	Windows 内核结构分析
实验七	Linux 内核架构分析
实验八	Linux 基本访问控制实现机制
实验九	Selinux
实验十	Capability
实验十一	操作系统内核漏洞
实验十二	安桌 Rooting

(2) 与其它课程的联系

操作系统安全与操作系统课程、信息系统安全、软件安全课程都存在交叉点。与操作系统的交叉点主要在操作系统安全机制介绍中，要求学生要了解操作系统基本原理；与信息系统安全课程的交叉点在访问控制机制部分，目前大部分信息系统安全课程中介绍了访问控制原理；与软件安全课程的交叉点主要在内存保护和内核漏洞部分，软件安全课程中会涉及到这些内容的一部分。因此，如何较好的联系这些课程，同时找出不同点，结合操作系统安全课程的特点加以区分，是讲授该课程时需要认真设计和考虑的。

(3) 缺乏开放的课程实验平台

主流操作系统课程需要学生能够分析操作系统中安全机制的部分源代码，同时掌握操作系统内核的漏洞和利用方法，因此对学生的实践能力要求比较高。然而，目前缺乏支撑该课程的开放实验平台。该平台需要提供实验环境，并允许教师和学生在其中添加新的实验内容，基于互联网和群体智慧，不断完善和扩充课程的实验内容。目前该课程的实验还是基于独立的虚拟机完成，不便于后续学生的学习，和课程实验内容的共享和扩展。

4. 提高教学质量的探索

为了达到课程设置的目的、提高教学质量，作者依据“主流操作系统安全”课程的特点，对该课程的教学方式方法进行了有益的研究和探索并取得了一些经验，现列举如下：

(1) 以问题为导向，开展启发式教学

传统的填鸭式教学方法，单纯地给学生灌输大量的概念和相关内容，不能充分地调动学生们的积极性。为增强教学效果，我们采用以问题为导向的启发式教学方法。在内容讲解的过程中，结合一些实际案例，引导学生分析导致这些问题的原因，一步步地讲解相关内容原理，从而提高学生们分析问题，解决问题的能力。例如在讲解操作系统内存安全内容时，我们精心设计了内存溢出的案例，通过 OllDbg, 一步步的引导学生分析溢出现象，从而理解缓冲区溢出的根本原理。

(2) 通过课堂展示，提高学生自主性和积极性

主流操作系统课程是一门实践性非常强的课程，要求学生具有较强的实际动手能力。同时，操作系统安全版本不断更新，漏洞层出不群，一些内容很容易就过时了。因此，在课程教学中，我们要求学生以主流操作系统漏洞利用和防御为主线，查找和分析最新的内核漏洞攻击方法，并以小组的形式进行课堂展示，同时要求给出可能的防御措施。课堂展示的内容会被录制视频，在云盘上分享。经过三年的实践，该方法得到了同学们的认可和欢迎，极大的提高了学生们的积极性和主动性，也给课程输送了更多的新鲜血液，并提高了学生们团队合作及动手能力，促使他们更加深入地理解操作系统安全问题。

(3) 建立课程漏洞库

信息安全是一门具有对抗性质的学科。只有深入的了解了攻击技术和原理，才能够制定出更好的防御措施。目前虽然有 CVE [8]、Exploit-db 等安全漏洞库，但这些平台涵盖的漏洞十分广泛，没有针对操作系统的安全漏洞库，也缺乏对这些漏洞的分析和分类。对于主流操作系统安全课程而言，我们依托该课程，建立了操作系统漏洞库。学生们可以分析目前操作系统的各种安全漏洞，并给出分析报告。通过云盘在班级内分享，以方便学生们了解最新的漏洞，学习最新的攻防技能。

5. 结语

主流操作系统安全是一门很新的课程，同时作为信息系统安全的核心，它又是非常重要的一门课程。我们在近三年的教学中，依据该课程的特点，建立了该课程的教学体系。同时，也在教学实践中总结了

相关的经验和教学体会，希望能够对该课程的教学和进一步完善起到抛砖引玉的作用，共同构建国内外领先的主流操作系统安全课程教学体系。

参考文献 (References)

[1] 刘克农, 冯登国, 主编. 安全操作系统原理与技术[M]. 北京: 科学出版社, 2004.

[2] 王清, 主编. 0day 安全: 软件漏洞分析技术(第二版)[M]. 北京: 电子工业出版社, 2011.

[3] 王爽. 汇编语言入门(第二版)[M]. 北京: 清华大学出版社, 2008.

[4] 温玉杰, 译. Intel 汇编语言程序设计(第五版)[M]. 北京: 电子工业出版社, 2007.

[5] SEED. http://www.cis.syr.edu/~wedu/seed/index.html

[6] 陈利君. Linux 内核设计与实现[M]. 北京: 机械工业出版社, 2006.

[7] 卿斯汉, 主编. 操作系统安全[M]. 北京: 清华大学出版社, 2004.

[8] 国家漏洞数据. https://web.nvd.nist.gov