文章编号：1672-5913(2015)22-0009-03
中图分类号：G642

网络工程专业学生的网络系统安全保障能力培养

徐　明，徐　建，吴　铤，郑　宁
（杭州电子科技大学 计算机学院，浙江 杭州 310018）

摘　要：针对当前网络工程专业学生网络系统安全保障能力培养中普遍存在的理论与实践脱节、知识体系没有体现出专业特点等问题，文章分析网络工程专业学生网络系统安全保障能力培养的现状和能力构成，并以杭州电子科技大学网络工程专业为例，阐述如何以目标、需求和能力为导向，设置网络系统安全保障能力相关课程、知识点和实践教学体系。

关键词：网络工程专业；网络系统安全保障；能力培养
DOI:10.16512/j.cnki.jsjjy.2015.22.003

0　引　言

没有网络安全就没有国家安全。国家重要信息系统及基础设施的建设和维护需要一支具有较高网络系统安全保障专业知识的队伍。伴随着信息技术的迅速发展，社会对具备网络系统安全保障能力人才的需求一直呈上升趋势。

目前，我国网络工程专业人才培养正处在从知识传授向能力培养与素质提高的转变过程中，以学生为中心，以目标、需求和能力为导向的教育理念已经得到广泛认可。网络系统安全保障是网络工程专业人才的主要能力之一[1]，但网络工程专业在网络系统安全保障能力培养方面普遍存在一些问题，如理论与实践脱节，解决实际问题的能力不足，对应的课程、知识点与实践环节不符，与其他相关专业没有差异化等[2]。

1　网络工程专业学生网络系统安全保障能力培养的现状分析

网络工程专业是依托于计算机科学与技术专业发展起来的。网络工程专业的人才应该具备计算机类专业人才的四大基本能力：计算思维、算法设计与分析、程序设计与实现和系统能力[3-4]。网络工程专业人才的专业能力可以进一步细化为：网络协议分析设计与实现、网络设备研发能力、网络应用系统设计与开发能力、网络工程设计与实施能力、网络系统管理与维护能力、网络系统安全保障能力等[1]。因此，网络系统安全保障能力是网络工程专业有别于其他计算机类专业的一个重要能力。但在目前的现实情况下，大家对网络工程专业和其他相关专业在专业能力构成上的差异认识不够，很多学校不同专业在网络系统安全保障能力培养方面存在同质化现象。

在专业知识体系上，网络系统安全保障知识领域的核心知识单元应有：信息安全基础、安全模型、加密、认证、数字签名、安全协议、防火墙、入侵检测系统、漏洞检测与防护、安全评估与审计等[1]。从知识体系上来看，网络工程专业中的网络系统安全保障知识基本上是信息安全专业中密码学、网络攻防技术及信息系统安全领域基础知识的综合，具有内容多、涉及面广的特点。另外，目前的知识体系主要从防御角度出发，攻击和渗透的知识还很欠缺。如何在确保知识体系覆盖完整的条件下，突出网络工程专业的特色，是一个尚待深入研究的课题。

在课程体系结构上，网络系统安全保障能力对应的网络安全课程，对网络工程、信息安全和信息对抗专业来说是主干课程，而对计算机

基金项目：浙江省“十二五”普通本科高校新兴特色专业项目——网络工程（重点方向：网络安全）（浙教高教[2014]110 号）；国家自然科学基金项目（61070212、61003195）；浙江省自然科学基金重点项目（LZ15F020003）。
第一作者简介：徐明，男，教授，研究方向为网络与信息安全，mxu@hdu.edu.cn。

类其他专业来说，往往是扩展课程；信息安全专业和信息对抗专业一般将其细化为至少 4 门主干课程，如密码学、网络安全、信息系统安全和信息内容安全。网络工程专业需要强化网络安全课程，并开设相应的扩展课程，以完善网络系统安全保障课程体系的完整性。

教学条件上，在网络与信息安全方面比较突出的国内高校主要以密码学领域的科学研究与人才培养见长[5]，缺少网络系统安全保障的师资，特别是缺少既有工程背景和网络攻防实战经验又有高学术水平的师资，导致一些高校网络安全课程的教学质量不高，甚至无法开设，影响了网络系统安全保障能力的培养。网络系统安全保障不仅有理论性，也具有实践性，许多方法和手段需要在实践过程中认识和领会。一些高校的网络工程专业缺少必要的实验条件，有些仅仅进行加密与解密、VPN、入侵检测或防火墙等方面的简单配置性实验，缺少网络对抗等复杂的综合性实验，致使网络系统安全保障实践环节质量不高，影响学生动手能力的培养。

2 网络工程专业学生网络系统安全保障能力构成

网络系统安全保障能力的教育需要以网络系统安全保障知识为载体，通过探讨知识发现问题求解过程，培养学生灵活运用所学知识有效地解决网络系统安全防御、检测、评估、响应等实际问题的能力。

计算机类专业培养学生的计算思维、算法思维、程序思维、系统思维、过程思维、数据思维、人机系统思维等思维能力，而网络工程专业还要培养学生的对抗思维、逆向思维、拆解思维、全局思维等网络系统安全保障所特有的思维能力。网络系统安全保障体系是一个复杂系统，必须从复杂系统的观点，采用从定性到定量的综合集成的思想方法，追求整体效能。从系统工程方法论的观点出发，网络系统安全保障不能简单地采用还原论的观点处理，必须遵循“木桶原理”的整体思维，注重整体安全。

网络系统安全保障的方法论与数学或计算机科学等学科相比，既有联系又有区别，包括观察、实验、猜想、归纳、类比和演绎推理以及理论分析、设计实现、测试分析等，综合形成了逆向验证的独特方法论。

从不同的角度看网络系统安全保障可以得到不同的内涵和外延。从物理域看，是指网络空间的硬件设施设备安全，要求确保硬件设施设备不被干扰、破坏和摧毁；从信息域看，重点是确保信息的可用性、机密性、完整性和真实性；从认知域看，主要是关于网络传播的信息内容对国家政治及民众思想、道德、心理等方面的影响；从社会域看，要确保不因网络信息传播导致现实社会出现经济安全事件、民族宗教事件、暴力恐怖事件以及群体性聚集事件等。

网络系统安全保障涉及网络协议安全及相关技术研究、网络安全需求分析、方案设计与系统部署、网络安全测试、评估与优化、网络安全策略制订与实施等内容。培养网络系统安全保障能力就是培养学生熟悉信息安全基本理论和常见的网络安全产品的工作原理，掌握主流网络安全产品如防火墙、入侵检测、漏洞扫描、病毒防杀、VPN、蜜罐等工具的安装配置和使用，能够制定网络系统安全策略与措施，部署安全系统，同时具有安全事故预防、监测、跟踪、管理、恢复等方面的能力以及网络安全系统的初步设计与开发能力，以满足企事业单位网络安全方面的实际工作需求。

3 网络工程专业学生网络系统安全保障能力课程设置

网络工程专业涉及计算机网络的设计、规划、组网、维护、管理、安全、应用等方面的工程科学和实践问题，其网络安全课程使学生了解网络系统中各种潜在的安全威胁与攻击手段以及针对这些威胁可采用的安全机制与技术。掌握常见的网络安全工具和设备，如防火墙、入侵检测、漏洞扫描等工具的工作原理，学生可以了解网络安全的相关政策法规，并具有网络安全策略与措施制定、安全事故监测等能力。为了保质保量地完成网络工程专业学生的网络系统安全保障能力的培养，可设置相应的主干课程：网络安全技术和网络安全技术实践及扩展课程安全测试与

评估技术。课程涉及的核心知识点如表 1 所示。通过开设安全测试与评估技术，教师引导和培养学生用逆向、对抗和整体思维来学习并思考网络系统安全保障问题。

表 1 网络系统安全保障相关的课程和核心知识点

课程名称	核心知识单元	课时数
网络安全技术	信息安全基础安全，安全模型，加解密、认证、数字签名，安全协议，防火墙，入侵检测系统	51
网络安全技术实践	加解密编程实验，PGP 实验，PKI 实验，VPN 服务器和客户端实验，病毒与恶意代码行为分析实验，Iptables 防火墙实验，Snort 入侵检测实验，以太网网络监听与反监听，端口扫描实验，WinPcap 编程实验，Windows 安全配置实验，Linux 安全配置实验，综合实验	32
安全测试与评估技术	安全测试与评估的基本概念、流程，社会工程学攻击，信息收集，内部攻击，Kali Linux 的安装与使用，Metasploit，缓冲溢出攻击，Shellcode，Web 攻击，数据库安全，逆向分析	40(理论：课内实验 =1:1)

4 培养学生网络系统安全保障的实践和创新能力

实践动手能力是网络系统安全保障能力培养中的重要一环。许多网络信息系统安全保障能力知识点比较难掌握，必须通过实践环节来消化、吸收、巩固和升华，才成为学生自己的技能。为此，我们一方面努力争取解决实验条件，与企业联合共建网络安全教学实验室；另一方面，自主开发实现了一系列的教学演示和实践工具，弥补部分环节难以让学生动手实践的不足。

通过完善的实践体系（包括课内实验、综合实验、创新实践、实习及学科竞赛等），培养学生网络系统安全保障的实践和创新能力。课内实验包括安全测试与评估技术课程的信息收集、内部攻击、Kali Linux 的安装与使用、Metasploit、缓冲溢出攻击、Shellcode、Web 攻击、数据库安全、逆向分析等实验。网络安全技术课程对应的实践课程网络安全技术实践设置了加解密编程、PGP、PKI、VPN 服务器和客户端、病毒与恶意代码行为分析、Iptables 防火墙、Snort 入侵检测、以太网网络监听与反监听、端口扫描、WinPcap 编程、Windows 和 Linux 安全配置等实验；另外还设置了两个综合实验——综合防御实验 (安全配置、防火墙、入侵检测、事件响应) 和综合渗透测试实验 (信息收集、缓冲溢出渗透、权限提升、后门安装、日志清除)。在课内实验和综合实验环节采用分工合作、以强带弱、小组整体与个人测试评分相结合等措施，确保让每个学生掌握相应的网络系统安全保障实践能力。目前，我们正积极与网络安全相关企业建设实习和实训基地，开展社会实习和实践，探索利用社会力量培养实践能力的模式。

专业实践是一门 2 学分的创新实践和实习课程。通过专业实践和毕业设计，学生可以根据自己的兴趣选择网络系统安全保障方面的创新实践拓展和深化。一方面，积极鼓励并组织优秀学生参加全国性和地方性的网络安全技能竞赛；另一方面，让高年级的同学参与教师的网络系统安全保障科研项目中来，让学生在竞争与对抗中和解决实际问题过程中增强自己的动手能力和创新能力，培养学生的自主学习能力和研究能力，激发他们的网络系统安全保障创新思维。

5 结 语

网络系统安全保障能力是网络工程专业能力培养的一个重要环节。我们的工作仅仅是一个尝试性的开始，如何处理与计算机类其他专业、信息安全和信息对抗等相关专业之间的关系，如何评测网络安全能力的培养状况等，有待于未来的进一步研究与实践。

参考文献：

[1] 教育部高等学校计算机科学与技术教学指导委员会.高等学校网络工程专业规范[M]. 北京: 高等教育出版社, 2012: 8-9.

[2] 曹介南, 蔡志平, 朱培栋. 网络工程专业与计算机专业差异化教学研究[J]. 计算机教育, 2010(23): 139-142.

[3] 教育部高等学校计算机科学与技术教学指导委员会.高等学校计算机科学与技术专业人才能力构成与培养[M]. 北京: 机械工业出版社, 2010.

[4] 蒋宗礼. 计算机类专业人才专业能力构成与培养[J]. 中国大学教学, 2011(10): 11-13.

[5] 马建峰, 李凤华. 信息安全学科建设与人才培养现状问题与对策[J]. 计算机教育, 2005(1): 11-14.

（编辑：孙怡铭）