

新工科背景下嵌入式信息安全专业建设探究

柳亚男^{1,2}, 邱 硕^{1,2}

(1. 金陵科技学院网络安全学院, 江苏 南京 211169; 2. 金陵科技学院软件工程学院, 江苏 南京 211169)

摘 要: 以培养高层次应用型信息安全人才为目标, 在“新工科”的背景下, 针对嵌入式信息安全专业建设展开思考并提出以下方案: 制定定向特色课程体系, 开展校企合作的多元化教学模式, 强化实训实践等。该方案注重将学校资源和企业资源合理融合和综合利用, 以实现提高学生实践能力和创新能力的培养目标。

关键词: 信息安全; 专业建设; 企业嵌入式; 能力培养

中图分类号: TP393; G642

文献标识码: A

文章编号: 1672-755X(2019)03-0012-04

How to Construct the Enterprise-embedded Information Security Major under the Background of Emerging Engineering Education

LIU Ya-nan, QIU Shuo

(Jinling Institute of Technology, Nanjing 211169, China)

Abstract: With the aim of training high-level applied information security talents and under the background of “Emerging Engineering Education (3E)”, this paper considers the construction of enterprise-embedded information security major and proposes the following plans: making new targeted and characteristic courses system, carrying out diversified teaching mode of school-enterprise cooperation, strengthening training and practice, etc. The program focuses on the integration of school and enterprise resources in order to improve students’ practical and innovative abilities.

Key words: information security; major construction; enterprise-embedded; abilities training

教育部于 2017 年 2 月在复旦大学召开了高等工程教育发展战略研讨会, 会上探讨了新工科的内涵特征与建设发展的路径选择等重要问题; 同年 4 月, 教育部在天津大学召开研讨会, 确立了新工科下的人才培养目标是培养多样化、创新型、卓越的工程科技人才; 同年 6 月, 教育部在北京召开新工科研究与实践专家组成立暨第一次工作会议, 全面启动并部署新工科建设工作。由此, 构建了新工科建设的“三部曲”, 即复旦共识、天大行动和北京指南, 并先后发布了《关于开展新工科研究与实践的通知》、《关于推进新工科研究与实践项目的通知》、《教育部办公厅关于公布首批“新工科”研究与实践项目的通知》等重要指示, 奏响了应用型高等人才培养主旋律, 开拓了工程教育改革新路径。

在此背景下, 深入开展信息安全专业建设的研究与实践具有重要的意义。嵌入式信息安全专业的教学模式, 为高校与业界知名的信息安全企业建立战略合作关系, 将企业的定制化、特色化课程嵌入到原

收稿日期: 2019-08-07

基金项目: 江苏省高等学校自然科学研究面上项目(17KJD520003); 金陵科技学院高层次人才科研启动基金(jit-b-201639, jit-b-201726)

作者简介: 柳亚男(1984—), 女, 江苏连云港人, 讲师, 博士, 主要从事轻量级密码协议、传感器网络密钥管理、组密钥管理等研究。

始课程体系中,以培养应用型、实践型信息安全人才为建设发展目标,这对于高校适应国家经济发展和产业振兴具有重要支撑作用。

1 新工科与信息安全专业关系

清华大学林建教授在文献^[1]中解释,新工科的“新”包含新兴、新型和新生,“工科”是指工程学科。其中,“新兴”指从其他非工科的学科门类孕育、延伸和拓展出来的新技术学科;“新型”指对传统、现有学科进行转型、改造和升级;“新生”指传统工科与其他学科的交叉融合。新工科专业借助智能制造、云计算、人工智能等新兴技术,对传统工科专业进行升级改造。

信息安全专业是研究确保信息安全的科学与技术,是跨越计算机、通信、数学等学科的交叉学科。以培养具有全面信息安全专业知识、解决实际安全问题能力的学生为发展目标。信息安全专业将培养学生在安全运维、安全评估、密码学、安全渗透和攻防、木马和病毒、隐私保护等各方面的理论与实践能力。

信息安全专业特别强调“新”和“实践”,这与“新工科”是一脉相承的关系。

首先,信息安全与“新”技术密切相关。互联网设计之初并未考虑到网络攻击、病毒、木马等安全威胁,因此业界经常称 TCP/IP 协议为君子协议。信息新技术的快速发展一方面提高了互联网的普及度、降低了用户使用门槛,但同时也使网络环境更加鱼龙混杂,并引入大量安全隐患,如蠕虫、病毒、隐私泄露、钓鱼网站等。2007 年的棱镜门事件、2014 年的 iCloud 艳照门事件的曝光,给缺乏安全意识的普通用户上了严肃的一课^[2]。在互联网发展基础之上,21 世纪初诞生了新兴产物——物联网,将用户终端延伸和扩展到了任何物品之间的信息交换和通信。物联网与信息安全相互融合,传感器、RFID 的引入给传统的监控安保、身份识别带来了新技术。区块链技术的提出,给信息安全的研究带来了又一个创新点^[3],应用于金融行业的征信、交易安全、数据安全和用户的隐私安全,解决交易过程的信任和安全问题^[4]。

其次,信息安全专业强调“实践性”。信息安全是实践性要求非常高的专业,是涉及计算机、通信、数学、物理、法律、管理等学科的交叉学科^[5]。信息安全专业学生,在具备良好的数学和物理思维基础之上,一方面需要在计算机、通信领域具备较强的动手能力,另一方面要在法律、管理领域具备丰富的实践经验。加强学科所要求的基本修养,使学生具有本学科进行科学研究所需的基本素质,为学生今后的发展、创新打下良好的基础;使学生具有较强的应用能力,具有利用已掌握的基本知识解决实际问题的能力,增强系统应用开发以及不断获取新知识的能力。努力使学生既有扎实的理论基础,又有较强的应用能力;既可以承担实际系统的开发,又可进行科学研究。

2 嵌入式信息安全专业研究内容与目标定位

2.1 信息安全学科的研究内容

随着计算机网络的发展和广泛应用,当今全球几乎所有的计算机系统都已通过网互联起来,并且无论是组织还是个人越来越依赖这些系统存储和传输信息。而病毒、电子窃听和电子欺诈使得网络中的安全问题日趋严重。信息安全学科将针对操作系统、软件与应用、计算机网络、物理硬件等环境下存在的安全问题,以及解决安全问题的各种机制和技术进行深入研究。

信息安全架构涉及三个方面:安全威胁、安全服务和安全机制。

安全威胁主要分为两大类,即被动攻击和主动攻击,如图 1 所示。为防止以上安全威胁,需要提供以下基本安全服务:Confidentiality (保密性)、Integrity (完整性)和 Availability (可用性),三个词简称为 CIA 三元组。

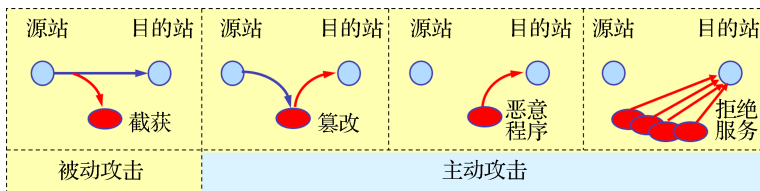


图 1 对网络的被动攻击和主动攻击

X. 800 定义了具体的安全机制,可以分为两类:一类在特定的协议层实现,称为特定安全机制,包括加密、数字签名、访问控制、数据完整性、认证交换、流量填充、路由控制和公证这 8 种;另一类不属于任何协议层或安全服务,称为普遍安全机制,包括可信功能度、安全标志、事件检测、安全审计跟踪和安全恢复这 5 种。根据 X. 800 的定义,安全服务与安全机制之间的关系如表 1 所示,该表详细说明了实现某种安全服务应采用哪些具体的安全机制^[6]。

表 1 安全服务与安全机制之间的关系

安全服务	加密	数字签名	访问控制	数据完整性	认证交换	流量填充	路由控制	公证
对等实体认证	Y	Y	—	—	Y	—	—	—
数据源认证	Y	Y	—	—	—	—	—	—
访问控制	—	—	Y	—	—	—	—	—
保密性	Y	—	—	—	—	—	Y	—
流量保密性	Y	—	—	—	—	Y	Y	—
数据完整性	Y	Y	—	Y	—	—	—	—
不可否认性	—	Y	—	Y	—	—	—	Y
可用性	—	—	—	Y	Y	—	—	—

注:“Y”表示安全机制适合提供该种安全服务,“—”表示安全机制不适合提供该种安全服务。

2.2 嵌入式信息安全专业目标与定位

金陵科技学院网络安全学院嵌入式信息安全专业立足江苏省及长三角地区,根据社会经济发展需要和就业市场需求,力求培养具有扎实的计算机网络安全理论与技术基础的应用型人才,具有较强的实践能力和创新能力,掌握专业网络安全软硬件产品的运维技能^[7]。培养学生在入侵原理与防御技术、网络的病毒防范、网站安全管理、软件开发等方面的实践技能,能够从事防火墙安全策略制定、网络入侵行为识别、网络系统安全改进与优化、安全风险评估与检测、信息安全体系管理等方面的工作。培养具备综合性信息安全工程实施与安全运维能力的应用技术型人才,使之能够满足网络安全 IT 企业、信息应用企业中相关岗位的要求。

3 企业嵌入式信息安全专业建设

如图 2 所示,嵌入式专业教育主要依托校内教学资源并引入产学合作元素,校企对接教育,企业学习依托产学合作方式实现。从第 1 学期开始融入与企业对接的教育内容,并不间断地持续至第 8 学期。

本文关于嵌入式信息安全专业建设的具体思考主要包含以下三方面。

3.1 定向特色课程体系

针对信息安全行业不同岗位技能要求,课程体系遵循“通用+特长”的设计思路,通过通用信息安全知识域与特色信息安全技能相结合的培养模式,利用项目驱动的实战技能训练,实现个性化、企业化的定向培养。以满足产业用人需求为导向,开设公共基础课程(包括通识教育课程和工具素质课程)、学科专业课程(包括专业基础课程、专业课程和专业方向课程)、实践实习课程(包括课程设计、综合实习、毕业设计)等多种类型课程,打造定向、完善、统一的信息安全特色课程体系。将产学合作培养机制的起始点由企业前移至校内教学,从校内专业教育阶段就开始定向导入产业元素,有效避免了校内教育与校外培养之间的脱节,实现工程能力的渐进式培育。

3.2 校企合作的多元化教学模式

网络安全学院拟与西普教育、天融信教育等多家业界知名企业在信息安全专业进行课程合作,经深入分析现有课程体系及反复磋商,形成合作方案。坚持人才培养的层次要求和满足个性发展需要,构建科学

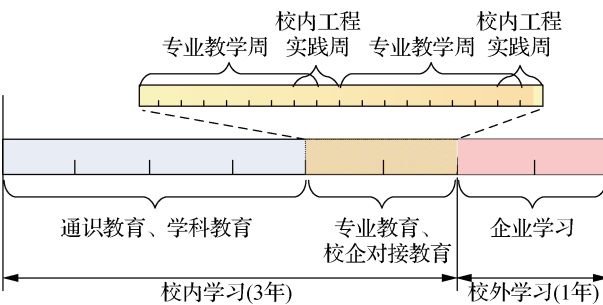


图 2 信息安全专业教育培养方案总体框架

合理的应用型人才理论和实践教学体系。成立校企合作执行委员会或工作委员会,负责校企合作的具体工作,开展信息收集、联系洽谈,负责具体计划制定和实施,推进校企合作向纵深发展。

3.3 强化实训实践

利用校内外资源进行实习实训,培养学生分析问题和解决问题的能力,培养理论联系实际的能力,培养创新能力与创业意识。针对信息安全方向,借助公司科技优势建设校内外实践基地,提出如下方案。

1)校内实训基地建设。基于网络信息安全专业领域课程的多样性,学生实践能力的培养必须具备一些实体软硬件环境,通过构造相关的网络环境、应用环境、攻防情景等线下环节,才能培养学生的实际工程技能。为此,网络安全学院与西普教育、天融信教育共同建立了“信息安全仿真教学实验室”,建设课程实验、综合实训、项目实战等子平台,为学生系统化的网络信息安全知识体系以及实用化的实践能力体系提供良好的软硬件环境支持。

2)校外实训基地建设。在专业课程学习的基础之上,在寒暑假以及最后一学年派遣学生到基地进行实践学习,可以大大提高学生的实践动手能力,还可以让学生近距离接触企业一线工作岗位,为未来的高质量对口就业奠定了基础。实训基地的选址以高新产业园区为主,除具备良好的学习环境外,还拥有便利的住宿和生活条件以及接近网络安全企业的地缘优势。

3)持续提高师资水平。师资队伍建设是保证和提高教学质量的关键,是教学团队建设的中心工作。信息安全人才培养中,建立专业自身的“双师型”教师队伍对于项目的可持续性发展尤为重要。合作企业在为学生提供课程学习、职业发展服务等基础上,通过师资培训、产学研交流、科研成果孵化等多层次服务,建立起与学校、教师之间的交流平台。

4 结 语

嵌入式信息安全人才培养是利用学校和企业两种不同的教育环境和教育资源促进产学研结合的互动共赢模式,是一种以市场和社会需求为导向的运行机制。但两种不同的教育环境和教育资源之间的整合,会因体制、机制、文化的不同而产生一些问题,所以为了促使此项培养模式顺利推行,必须再确立新的不同于高校也不同于企业的体制机制。金陵科技学院网络安全学院通过不断探索、多次走访、反复求证,初步推出以上体制机制改革,并获得实践成效。

参考文献:

- [1] 林健. 面向未来的新工科建设[J]. 天津中德应用技术大学学报, 2017(4): 14 - 15
- [2] FRAGKIADAKIA A G, TTAGOS E Z, ASKOXYLAKIS I G. A survey on security threats and detection techniques in cognitive radio networks[J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 428 - 445
- [3] OLIVIER F, CARLOS G, FLORENT N. New security architecture for IoT network[J]. Procedia Computer Science, 2015, 52(1): 1028 - 1033
- [4] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: using blockchain to protect personal data[C]. New York: IEEE Security & Privacy Workshops, 2015
- [5] 马建峰, 李风华. 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
- [6] 刘建伟, 王育民. 网络安全——技术与实践[M]. 3版. 北京: 清华大学出版社, 2017: 25 - 26
- [7] 中关村网络安全与信息化产业联盟. 2016年全国企事业单位移动信息安全需求调查报告[J]. 信息安全与通信保密, 2017(4): 102 - 105

(责任编辑: 湛 江)