

Research on Enterprise Cooperation of “Information Security Technology” Course

Chengshu Zhang, Jie Lin

Shanghai Institute of Technology, Shanghai
Email: zcs@sit.edu.cn

Received: Apr. 4th, 2019; accepted: Apr. 19th, 2019; published: Apr. 26th, 2019

Abstract

Information security is an important branch of computer science technology. Based on the cooperative construction with enterprise in “information security technology” course, this paper discussed the teaching reform from different aspects: teaching content, teaching form and practice effort. During the practice and implement, we also recorded and tried to make it better.

Keywords

Cooperation with Enterprise, Information Security Technology, Reform in Education

信息安全技术课程校企合作中的教学改革探索

张成姝, 林捷

上海应用技术大学, 上海
Email: zcs@sit.edu.cn

收稿日期: 2019年4月4日; 录用日期: 2019年4月19日; 发布日期: 2019年4月26日

摘要

信息安全是计算机专业技术中的重要分支, 本文以“信息安全技术”课程与企业合作建设为基础, 从教学内容、教学形式和实践环节各方面进行了教学改革的有益探索, 并在实践中加以实施和改进。

关键词

校企合作, 信息安全技术, 教学改革



1. 绪论

在高等教育中, 产学研结合、校企合作是以社会和职业需求为导向进行人才培养的重要机制。利用学校和企业两种不同的教育环境和教育资源, 采用课堂教学和课外实践有机结合的教学模式, 来培养适合用人单位需求的应用型人才。目前我国校企合作的主要模式是以学校为主导的合作模式, 合作的深度和广度结合实际条件会有较大的变化[1]。本文以我校开展的“信息安全技术”课程校企合作为蓝本, 在校企合作中深化教学改革研究, 尝试探索一条适用于应用型本科院校的教学之路。

由于我校是以培养应用型技术人才为目标的本科院校, 因此比较重视学生的实践和动手能力, 并在教学计划中设置了较多的实践课时。但是由于目前尚未建设形成独立的信息安全专业, 只为计算机科学与技术专业的学生开设了“信息安全技术”课程, 课时也比较少, 只有 40 课时, 如何合理规划和安排 40 学时, 既讲授信息安全中不可缺少的算法理论知识, 又要教会学生操作常见的信息安全工具, 是课程教学中必须考虑的重要问题。此外, “信息安全技术”课程的特点是理论知识艰深, 加解密算法复杂, 而实践中又需要切实可行的方法来保障公司或个人的信息安全。这也容易导致按照常规教学方法老师讲学生听, 上完不会做的没有用的结果。因此急需探索本课程的教学改革, 寻找适合课程的教学之路。我校从开设本课程至今, 采用了校内教师与企业合作培养办学的模式, 取得了一定的成效。

2. 教学内容和形式的改革

“信息安全技术”课程一般建议开设在计算机科学与技术专业本科二年级下学期或三年级上学期, 此时学生已学完了部分专业课如数据结构、程序设计等课程, 具有一定的编程能力和专业知识储备, 但是对于信息安全保障的意识还比较薄弱。由于“信息安全技术”课程内容极其丰富, 特别是在软件攻防方面, 以往更多是靠老师自行在实践中的摸索得出一定的经验后教给学生, 因此存在着比较强的个人色彩, 也不适应专业化的大班教学。走校企合作之路, 第一步就是分析教学内容, 哪些是适合本科课堂内教授, 哪些是需要在实践中掌握的。经过筛选, 对于密码学基础的理论知识, 所有需要掌握的加解密算法都可以由校内教师在课堂上讲解, 充分发挥校内教师擅长理论讲解清晰的特长。而实验部分则采用由与我校合作的相关企业提供实验要求, 在校内专用机房开设实验项目, 企业教师前来授课的模式。由于这些合作企业在学生四年级毕业实习阶段还会提供部分岗位, 并择优录用, 因此企业方也希望培养出符合生产实际需要的合格学生留用。在本科三年级的“信息安全技术”课程中, 企业就带着生产岗位明确的培养目标, 有针对性地开设实验项目, 以便这些学生在毕业实习环节可以直接进入企业各个岗位实战。例如如果企业更关注无线网络安全问题, 那么此项实验可以多一些课时, 如果企业是研究物联网或智能家居的, 可能需要安排远程监控的实验项目。表 1 就是校企合作后撰写的一份授课计划简表, 课程安排的授课内容和课时如表中所示。需要注意的是, 每次授课计划和内容都会随着合作企业的要求而变动和更新, 也就是每学期学生学习此课程的内容会动态变化, 这也是开设校企合作课程后符合计算机学科不断发展的趋势, 所带给学生的有益之处。

从表 1 中还可以看出课程在讲授密码学基本原理只占用了总课时的 1/4 左右时间, 而将更多的课时分配给企业教师在专用机房讲授网络安全技术、软件安全技术(包括系统软件安全和应用软件安全)等各方面的信息安全应用技术, 并在课程最后精心安排了 2 天完整的企业现场教学, 通过学生进驻企业,

Table 1. “Information security technology” course school-enterprise cooperation teaching plan**表 1.** “信息安全技术”课程校企合作授课计划

章节	内容	课时	授课地点	讲授人	
第一部分 密码学基础	1、古典密码学	2	校内多媒体教室	校内教师	
	2、对称加密体制	4			
	3、非对称加密算法	4			
第二部分 网络安全技术	1、网络攻击技术	2	校内实验专用机房	企业教师	
	2、网络入侵检测技术	4			
	3、无线网络安全技术	4			
第三部分 应用安全技术	1、软件漏洞与软件安全监测	4	校内实验专用机房	校内教师	
	2、Web 安全与认证技术	2			企业教师
	3、计算机病毒与防范	4			
第四部分	信息安全技术解决方案实例	12	企业现场	企业教师	

切身体会各个公司是如何应对信息安全问题的。相信这样的授课内容和方式会给学生留下非同寻常的记忆,对于将来工作中面临的实际信息安全问题有了及早的准备和思考。

此外,由于当前网络的普及和信息技术的发展,使得每个人都有机会接触到各种各样的信息安全问题,可能学生遇到过的信息泄露问题老师还没有遇到过,难免不会处理。因此校企合作的第二步就是引进企业教师参与教学环节,补充工作实践中面对的真实案例,编写合适的实验指导书内容供学生练习。由于信息安全的实验项目可能对实验环境造成较大影响甚至损失,所以征得学院领导的同意和支持后,利用校内机房开设出“信息安全技术”专用实验平台,在这个相对封闭的实验环境下让学生尝试各种网络攻击手段,再利用各种网络防御技术检测和抵御,从而模拟出真实环境下的攻防技术。这种教学形式也极大地吸引了学生的兴趣,有的学生甚至在课后多次前往专用机房想方设法与对手进行攻防较量,取代了游戏世界的满足感。目前有部分软件是由企业购买和提供,安装在校内机房,这也是进行校企合作课程建设后所带来的直接收获。所以说,“信息安全技术”课程的特点非常适合于进行校企合作课程建设。

3. 实践教学的改革

在确定教学内容和授课计划之后,校内教师和企业教师提前进行了充分的沟通,对各自负责的部分编写全新的教案和课件。考虑到本科教学和企业实践的不同特色,因此安排了密码学原理部分、操作系统安全部分、计算机病毒和防范可以在校内由专业教师课堂教授,而网络安全技术和信息安全技术方案综合实例则由企业教师在专用机房里边演示边讲授,并提供学生动手演练的机会(表 2)。特别是课程最后由企业提供的现场实践,在真实环境下为学生解析信息安全实际案例,企业的每位带教老师都参与进来,为学生答疑解惑,这对企业和校内教师的素质都提出了较高的要求,也迫使校内教师迅速成长,提高业务水平。因此本课程的校企合作实施过程中要特别注意学生以小班教学为佳,人数控制在 20 人左右为宜,可以分批前往企业实践基地。

由于信息安全技术是一门既注重理论基础又需要紧密结合实践的课程,所以课程中的实践环节安排分外重要,每学期结合不同的企业需求可以考虑挑选不同的实验项目,而且企业老师编写的实验指导也会根据实践中遇到的问题而修改。例如有一届学生当时在上机过程中企业老师指导学生访问了信息安全行业内大名鼎鼎的乌云网,并为学生讲解了该网站如何分析和破解企业网站中存在的漏洞,但是没有经

过多久, 乌云网已经因为各种原因而消失。这个案例也有力地向学生说明了信息安全技术是把双刃剑, 合法合理地利用技术保障企业与个人的安全并非易事。在信息安全技术课程的校企合作建设中, 企业教师参与安排上机实验和参观实践, 学校机房提供相对封闭的实验环境, 以防实验中的不慎造成损失和破坏。表 2 是课程中的参考实验项目。在每个实验项目中都会有丰富的实验内容, 例如在网络技术实验中, 学生可以在受保护的机房实验环境中尝试端口攻击, SQL 注入攻击、木马攻击、XSS 跨站攻击等多种手段。

Table 2. “Information security technology” course school-enterprise cooperation experimental project
表 2. “信息安全技术”课程校企合作实验项目

序号	实验名称	实验学时	实验指导负责教师	实验地点
1	大整数和古典加密设计	2	校内教师	校内机房
2	Simple-DES 加解密程序设计	2	校内教师	校内机房
3	Diffie-Hellman 密钥交换算法程序设计	2	校内教师	校内机房
4	CA 认证与网上支付	2	企业教师	校内机房
5	网络安全防火墙与 VPN 实验	2	企业教师	企业
6	网络入侵与检测实验	2	企业教师	校内机房
7	软件安全实验	2	企业教师	校内机房
8	计算机病毒与防范	2	校内教师	校内机房
9	无线网络安全实验	2	企业教师	校内机房
10	信息安全技术应用案例	6	综合练习	企业

另外, 在校合作课程的开设过程中, 也发现了一些问题。例如企业请来的授课教师往往并不擅长课堂的掌控, 因此课程要求校内教师全程参与, 并配合企业老师共同编写与修订教学课件, 补充案例。在企业现场教学中还要负责学生的安全工作, 因此校内教师必须由经验丰富的高年资教师来承担, 并愿意尝试教学改革的新变化, 在开设校企合作课程的几年时间内, 希望尽快培养出高水平的师资队伍。

在校内讲授课程部分, 也针对应用型人才培养目标进行了教学方法改革。课堂教学中更多地引入了任务驱动模式的教学方法, 由教师引入问题, 安排任务, 学生思考后再讲授解决方法, 这样会更大地激发学生的学习兴趣。例如, 在讲授古典密码学中穿插了影视作品中的加密情节, 引导学生进行密文训练; 在讲解 DES 加密算法时, 考虑到算法实现难度, 特地降低到 8 位简单 DES 算法程序设计, 使得大部分同学都能通过几轮变换后理解对称密钥体制的加密、解密过程。

在课程建设中, 还推荐一部分较为优秀的学生参加了全国计算机等级考试三级-信息安全技术的考试, 为培养合格的信息安全工程师打下基础。特别是在学校的大力支持下, 举办企业赞助命名的信息安全技术竞赛, 通过宣传和参与, 让更多的学生参与进来, 得到了非常好的实训机会。目前本课程的校企合作之路又有了新的方向, 尝试与具有信息安全技术方面强大研究能力与资质的培训中心合作, 为确实具有信息安全方面兴趣和潜力的学生培训, 颁发证书, 继而走出信息安全专业培养的特色之路。

4. 总结

在与企业合作培养掌握信息安全技术的人才过程中, 深深感到随着计算机技术的发展, 各种信息安全问题层出不穷, 仅仅依靠一位老师或者一个案例反复授课是无法应对飞速变化的信息时代的。因此, 博采众家之长, 挑选出既有深厚专业背景和实践经验, 又能将知识转化讲解成易于被学生吸收, 深受学

生喜爱的企业教师, 绝非一朝一夕可以完成的事。在校企合作的过程中, 找到有意愿进行合作的企业, 并且能够坚持为学生的成长辛勤耕耘的企业员工是不容易的。在校企合作的过程中, 有可能遇到员工辞职、企业变动的各种因素, 没有企业的大力支持和企业带教老师对教育行业的热情, 是很难将高校内的一门课程琢磨打造好。经过校企合作建设, 不仅推广宣传了企业, 为企业培养未来的员工, 提高了应用水平, 高校教师也学习和获得了宝贵的实战经验, 更新了知识体系, 学生更是在吸收理论知识的同时学会应用于实践, 受益匪浅, 实现了合作各方的双赢。

校企合作培养信息安全技术方面的专业人才, 是建设信息安全专业的有效培养模式。通过建立 KPI 关键指标考核和评估校企合作课程的建设效果, 是一次用科学的管理方法来控制校企合作课程的有益尝试[2]。这种方法不仅适用于某一门专业课程, 在有条件适合开展校企合作建设的课程范围内都可以考虑。通过校企合作, 完善了课程体系, 提高了教学质量, 帮助学生巩固理论知识, 提升动手能力和实践能力, 实现校企双方的双赢。

基金项目

项目来源: 1011XQ170020-信息安全技术。

参考文献

- [1] 李军锋, 彭冲. 基于 KPI 的高校院系整体绩效考核应用研究[J]. 北京航空航天大学学报, 2011, 24(4): 111-114.
- [2] 王成强. 基于 KPI 的高校实验技术人员绩效考核体系设计[J]. 实验技术与管理, 2009, 157(10): 162-164.

知网检索的两种方式:

1. 打开知网页面 <http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD>
下拉列表框选择: [ISSN], 输入期刊 ISSN: 2331-799X, 即可查询
2. 打开知网首页 <http://cnki.net/>
左侧“国际文献总库”进入, 输入文章标题, 即可查询

投稿请点击: <http://www.hanspub.org/Submission.aspx>

期刊邮箱: ces@hanspub.org