DOI:10.13878/j.cnki.jnuist.2020.04.003

黄达明[1]　仲盛[1]

本科信息安全教学研究最新进展综述

摘要

随着云计算、移动应用、物联网等技术的不断发展,信息技术已经成为日常生活的一部分.不断浮现的各种安全问题导致整个社会对信息安全专业人才的需求不断增长,而信息安全教育是解决问题的关键.本文从面临的困难、要解决的问题、课程体系建设、教学方法研究、课程实验构建等几个方面系统地介绍了本科信息安全教学的最新研究成果,并指出了信息安全教学研究的未来发展方向.

关键词

信息安全教学;课程体系;课程建设;教学方法

中图分类号 TP309

文献标志码 A

收稿日期 2020-03-22

作者简介

黄达明,男,讲师,主要研究方向为信息安全、数据科学、基础教学.huangdm@nju.edu.cn

仲盛(通信作者),男,博士,教授,博士生导师,研究兴趣包括密码学、博弈论及其在计算机网络、分布式系统中的应用.zhongsheng@nju.edu.cn

1 南京大学 计算机科学与技术系,南京,210023

0 引言

信息技术已经成为日常生活和社会运转的一部分,移动计算被应用到商业、医疗、军事和教育等诸多领域,物联网的广泛建设也使得我们进入万物互联的时代.安全和隐私保护对于所有的信息技术系统和服务都非常关键,但是全球不断出现的有关信息系统和网络的安全攻击和脆弱性事件数量不断上升,提醒我们面临的信息安全形势其实非常严峻.

在现代人使用信息技术如此普遍的情况下,缺少经过良好信息安全教育和训练的人员是导致安全问题频发的主要因素之一,因为信息系统的设计、开发、维护和使用都是由不同角色的人来实施的.应用的多样化使得对软件开发者的要求也越来越高,如果开发者没有受过信息安全方面的训练,那么他们在防止安全问题例如脆弱性时会面临困难.而负责运维的专业人员和使用系统终端的用户如果不具备足够的安全教育和训练,也会导致信息系统和自身处于风险之中.因此,目前学术界、工业界、政府部门和军方对于受过良好教育和训练的安全人员的需求越来越迫切,而这需要相关高校进行专门投入的信息安全教育才能满足.

传统意义上,很多高校都开设了各种层次和不同形式的信息安全课程,但是这很难满足快速发展的信息安全形势对信息安全人才的需求.文献[1]给出了美国佐治亚州大学系统中所提供的网络安全相关的学位/认证项目情况,包括该州所有大学能提供的网络安全相关的博士、硕士和学士学位,以及第二学位及证书项目等,并调研了毕业生的情况,调查结果表明即使有这么多学位课程项目存在,仍然不能提供足够多的网络安全相关毕业生来满足网络安全方面的工作需求.

本文对本科信息安全教学近些年的研究现状进行了调研和综述,因为本科信息安全教学是整个信息安全教学体系中最重要的一环,它除了能够满足各行各业对安全专业人员以及具备安全技能的人才需求外,也可以为信息安全领域的专业研究提供具有坚实理论和足够技能的人才基础.

1 本科信息安全教学的困难和要解决的问题

信息安全教学是计算机科学教学中最具挑战性的任务,因为需

要成功地将抽象概念和实际应用结合起来[2].信息安全知识的理解和掌握需要很多其他课程甚至学科的理论和实践基础,包括程序设计语言、计算机网络、操作系统、数据库系统、软件工程、计算机体系结构、Web 程序设计等计算机科学和工程方面的知识,以及数学、概论统计等基础[3].此外,因为是由大量动态的因素造成了安全威胁,所以解决安全挑战所需的认知结构需要不断地增强和发展[4].

完成信息安全课程的构建和实施有效的信息安全教学,需要考虑和解决以下问题.

1.1 学习者的定位、教学目标的设定和课程体系的确定

课程的学习者群体不同,教学目标的设定不同,面临的困难也不一样.

计算机科学和信息技术相关专业的信息安全教学对象往往是具有一定技术基础的学生,而教学培养目标是信息安全领域未来的科学家、业界的信息安全专家、具有安全思维的信息系统开发者等,因此课程的构建往往不是一门信息安全课程,而是一个课程体系,甚至是学位课程体系.

面向所有专业的普适信息安全教学,学习者可能来自不同的专业,学习的基础、兴趣和主动性以及学习投入都会相差非常大,教学培养目标是具有信息安全技能和素养的各领域人才,课程的构建往往是一门综合性质的信息安全课程,或者是可以融入其他课程的信息安全教学模块.

1.2 课程教学内容的构建

如前所述,课程教学内容的建设需要结合学习者定位和教学目标来进行,因此不同的学校需要采取不同的策略.

从课程内容来说,需要从众多的信息安全研究主题中选择出符合教学目标的信息安全主题子集,并构建成具有清晰内部逻辑联系的有机整体,这项工作对课程构建者具有较高的要求.此外,现有的一些课程中,由于各方面的限制,课程内容的具体性和实践性可能都不够,例如文献[5]指出,虽然隐私基础知识的重要性在显著增长,但是在此领域的教学研究前期并没有提供具体的内容,因此需要完善、细化和充实具体的主题内容.

当努力构建信息安全课程后,面临的困难还包括课程内容很容易过时的问题.因为新的攻击方法和相应的应对技术在对抗中不断快速向前发展,因此信息安全教学还需要考虑提供好的方法或者工具,来帮助学生在课程学习结束后,能够通过积极主动的努力自学跟上新的网络安全形势.

1.3 教学形式和方法的选择

如果想达到良好的教学效果,需要根据教学培养目标、课程内容和学习者情况采取合适的教学形式,例如是面对面教室教学还是 MOOC 这样的远程教学.

当确定教学方式后,需要根据教学内容选择能尽量帮助学生快速掌握相关内容,同时又具有较高知识保留度的教学方法.教学方法的选择还需要尽可能地考虑到学生个体的不同,让学生主动以研究者角色投入学习.可以考虑根据信息安全教学的特点,结合其他学科的研究结果来选择和构造教学方法.

教学方法对于激发学生的学习动机非常重要[6].在信息安全知识学习中,一方面是现实世界中安全形势对学习者带来的迫切压力,另一方面是信息安全学习对于坚实理论基础的要求和未来实践对于实际技能的掌握要求所形成的困难.对于学习者来说,动机的提升在整个学习中的重要性是无容置疑的.

此外,教学方式和教学方法的选择还与学校、院系和教师个人所能够获得的资源有很大关系.

1.4 课程实验的建设

传统的信息安全课程实验主要目标是使得学生不仅能够理解遇到的信息安全问题背后所蕴含和涉及的理论和技术,还需要具有应用这些理论知识的能力,从而能够进行设计、开发和实现创新解决方案,这种能力可以体现在不同粒度和层次的信息安全问题解决上.课程实验的建设分为两个子问题:实验环境的构建和实验作业的构造.

文献[7]给出了网络安全实验室的理想构造指南,具体的建议包括:1)实验室计算机必须连接到因特网从而可以下载所需的工具和访问在线信息;2)实验室计算机必须和校园网隔离;3)实验室网络环境应该尽可能符合实际,从而能够开展绝大多数流行和已知的信息安全练习;4)实验室必须以方便进行管理、分配以及从复杂性不一的不同作业进行扩展的方式来建设;5)实验室应该有足够的 IT 教师和技术人员来提供维护和解决问题;6)实验室应该能够使得本地和远程学生都方便使用.

对于专业教学来说,因为有足够的软硬件资源、经费和教师的支持,因此构建这样的实验室环境是

一个建设目标.但是对于非专业教学来说,资源不足以构建这样高要求的环境,因此需要结合教学目标和教学内容,构建安全程度足够同时又有助于学生动手实践的教学环境.

实验作业需要结合每个教学主题精心构造,应该包括指南资料、作业和评估方法等,作业设计应该考虑让绝大多数学生都可以动手实践但是又具有一定的挑战性,同时需要防止作弊.实验作业的构建需要耗费教师非常多的精力,因此在后续的内容中可以看到有一些结合实际情况有效利用现有资源的构造方法.

1.5 教师的角色和作用

信息安全教学对教师的要求也很高,除了克服课程构建中的重重困难外,在教学过程中,教师还需要能够在不同的教学阶段承担不同的任务,例如文献[3]所提到的很好的示范:

1)在课程准备阶段,教师设计和修改教学方案和课件;

2)在课程讲授阶段,教师以引人入胜的方式讲解必备的理论知识,演示传授相关的安全技能;

3)在课程实践执行阶段,教师扮演教练和引导者的角色,为学生提供指导建议和技术支持;

4)教师也扮演研究者角色,观察、记录每个学生的行为和贡献,同时使用量化指标来评估每个学生的学习效果和产出,并及时反馈以改进学生的学习路径.

2 信息安全重要性与信息安全教育地位的不足

尽管信息安全的重要性在世界各国政府的最新政策中都能清晰无误地体现,但是在各个学校的实际教学体系中并没有得到与之相称的地位,这是因为信息安全在信息系统服务于社会的整个生命周期中往往是作为反思存在的.

Zatko[8]重新思考了信息安全在本科教育中的地位和角色.一门科目是如何被教学的,将影响学生如何进行思考,尽管信息安全已经被纳入几乎所有的计算机科学课程体系,但是现阶段信息安全教学中体现的仍然是“安全也是一种反思”.因此程序员在设计和开发过程中不会一开始就将安全纳入考虑,最终会导致具有脆弱性的系统;运维人员和用户也是在发生安全问题的时候才会想到应用信息安全知识和技能.Zatko[8]为了分析信息安全教学在美国各大学计算机学科教学中的地位,通过邮件调查的方式,希望通过由系主任们打分来判断信息安全在计算机科学所有课程中的地位、信息安全课程到底是理论性的还是应用性的,以及目前的教学形式是独立课程进行还是集成到其他课程中进行.根据最终收到的33个不同大学的系主任们的回复,Zatko[8]得出的结论是:在系主任们的认知中,信息安全的重要性与绝大多数计算机科学课程相比排名处于比较低的位置,如图1所示(每个系主任选出自己认为最重要的5门课程,33人中只有6人选择了信息安全).同时,和其他科目相比,系主任们认为信息安全是理论性最强的科目之一,当然,算法和数据结构理论性更强一些.但是信息安全是对理论投入实践的要求其实非常高,否则是不能满足学生们未来职业生涯中保障信息安全的实践能力需求的.此外,还有一个问题是,并不是所有的计算机科学教授都能理解他们领域的安全问题.

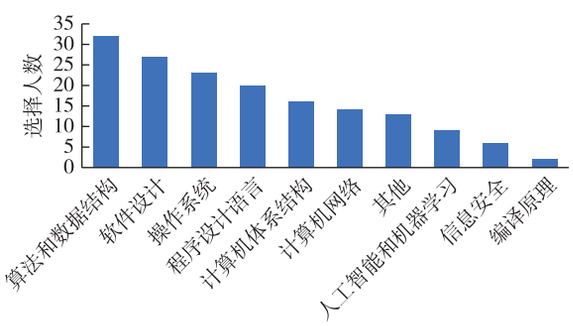

图1 计算机系主任心目中最重要的科目排名

Fig. 1 Importance ranking of the 10 computer science subjects by department heads[8]

这样的情况显然是不能与目前严峻的信息安全形势和整个社会对信息安全专业人士的需求相匹配的.Zatko[8]希望可以通过立法来促使教育领域将信息安全纳入计算机科学各个领域的教学.

在现代信息社会中,人们几乎在任何时刻任何地点以不同的方式在使用着信息技术.在导致信息安全问题的因素中,最主要的是没有能够对使用信息系统的人进行正确和足够的信息安全教育.因此,信息安全教育不仅仅是信息技术相关专业需要进行,其他所有专业都应该给予足够的重视.和计算思维教育的推进一样,信息安全教育的目标应该是让学习者最终形成“安全思维”[4].这包括深入的技术思考能力、识别复杂和紧急行为并做出反应的能力、掌握使用抽象和原则的能力、评估风险和掌控不确

定性的能力、问题求解和推理能力以及反向思考的能力.

3 课程建设和教学内容研究

信息安全课程的建设需要由各个学校根据自己对学生的培养目标、现有的课程体系和社会对学校的需求综合指定,所以可以是一个完整的学位课程体系,也可以是若干门课程构成的课程群,以及一门概论性质的独立课程,或者以模块化的方式融入计算机科学教学体系的其他课程中.下面分类介绍近期主要的一些代表性的工作及其教学研究思路.

3.1 信息安全学位课程体系的建设

德国吕贝克大学建立了一个新的信息技术安全学位程序[9].这个学位程序依托大学和研究所的信息安全研究领域的力量,可以满足德国国内和国际上对安全专家培养的需求.该学位程序的信息安全教学目标包括:使学生获得相关的专业技能,从而能够使用合适的工具分析和解决 security、safety 和可靠性方面的问题.学生要具备深厚的信息安全专业知识,能够理解安全威胁,并可以在信息系统的不同层次上对抗和消除安全威胁,并使得学生能够在系统设计中就考虑和集成安全.学生还应该具备足够的基础理论知识,从而可以理解和处理未来的安全挑战.

这是一个根植于计算机科学的学士学位课程体系,学分分配上大约 40%的课程学分是核心计算机科学课程,16%是数学课程,37%是安全相关课程,7%是自由选择课程.计算机科学与数学课程的教学目标是让学生具备足够的抽象分析、结构化和形式化刻画问题的能力.同时坚实的软件开发技能在保证系统安全可靠方面和理论知识一样重要.

3.2 数门课程构建的信息安全课程群

斯洛文尼亚马里博尔大学电子工程和计算机科学的教师们在其博洛尼亚学习程序中构建了由几门信息安全相关的课程组成的课程群[10].在博洛尼亚程序第一层次,构建的课程是“信息和通信技术安全”,对学生介绍网络安全的概貌以及对于信息技术的重要性.在博洛尼亚程序第二层次,以模块化的方式构建“信息系统安全和安全管理”课程系列,包括“高级信息安全”、“数据保护”和“信息系统的可靠性和测试”三门课程.

3.3 单独一门课程的信息安全概论课程建设

印度加尔各答的贾达沃普尔大学给出了有关建设“信息安全”课程的工作[11].该课程的受众是本科生和一年级研究生,课程提供了对于进一步学习信息安全以及在此领域内进行研究所需的基本知识的细节化概述.主要的模块包括:1)信息安全的定义和概念;2)安全策略和保障;3)安全访问控制;4)信息安全缺口和漏洞分析;5)信息安全最佳实践(各种安全标准);6)信息安全度量;7)信息安全风险管理;8)密码学原理;9)信息安全技术.

3.4 将信息安全模块化融入计算机科学课程教学体系

美国德州农机大学的工作将信息安全内容按照网络安全概念和方法构造成独立的模块化的方式,可以被使用在不同级别的课程中,包括大学本科的各个年级、社区学院的联合学位,甚至高中课程中[12].每个模块都可以被独立使用,包括模块描述和解释、幻灯片、实验室练习、实验室解答以及评估练习.这使得外部的教师可以不需要额外准备就在自己的课程中使用这些模块.

该课程内容建设的主要目标包括:1)为 8 门计算机科学课程开发信息安全模块的课程大纲和教学材料模块,从计算机科学的第一门课程开始,直到高级水平的课程;2)开发相应的能实际动手操作的代码模块系列,从最简单的概念开始,直到高级概念,保证学生能够通过实际编码实现对信息安全概念的理解、测试代码以及回答练习问题来获得对概念的深入理解.

最终 41 个不同的信息安全主题模块在该项目中被开发出来,这种新型的跨越课程大纲的信息安全教学方法可以满足美国对于受过教育的网络安全专业人士的培养需求.

3.5 结合 MOOC 的大规模信息安全教育工作

美国北卡罗莱纳州立大学的研究者进行了一个校园版本的信息安全课程的 MOOC 化建设实践,从以下课程元素进行了两者的对比:面对面讲座、在线视频讲座、其他在线内容、具有自动反馈的在线测验、小组项目、动手作业和练习、作业互评、面对面讨论和问题回答、在线讨论和问题回答、学生自我控制.进而通过比较学习者统计信息、学习动机以及学生学习产出等因素,最终目标是实现面向大规模教育的软件安全课程构建[13].

3.6 结合信息安全认证的课程体系建设

美国 La Salle 大学的研究者觉得工作市场对于

信息安全证书看得很重,因此证书需要紧密地和信息安全课程绑定在一起,该工作为本科生设计了一个新的信息安全课程[14].首先,该课程以安全视野将覆盖的话题组织起来并实现理论和实践之间的平衡;其次,引入一些内嵌的模块来主动保持所覆盖的话题能够跟上最新的发展;然后,开发了同等重要的强调攻击和防御技能的一组实验,从而可以提升学生的兴趣并激励学生关键性的思考,同时解决相关的法律和道德问题;最后,将信息安全等级认证中关键的知识集加入课程中从而帮助学生获得安全证书.

3.7 信息安全独立子方向的课程建设

美国加州大学伯克利分校的研究者为了对公众进行在线隐私问题教育花费2年时间构建了隐私教学项目课程[5].课程目标是使得学生具有足够的信息来指导他们做出有关在线隐私的明智选择.

美国Howard大学的研究者发现很少有人强调对网络安全事件的学习和分析过程中所涉及的行为问题,引入了一门高年级本科生课程来弥补这方面的不足,称为"行为化网络安全"[15].该课程的目标在于:为了应对诚实用户的粗心行为,以及黑客的聪明但是恶意的行为,网络安全专家和学生必须对动机、人格、行为以及其他主要在心理学或行为科学中研究的理论进行一些了解和掌握.

3.8 数据科学融入信息安全教学

近年以来,越来越多的研究者应用数据科学技术来解决安全领域的挑战,包括使用机器学习、统计学习、数据挖掘和自然语言处理技术来应对入侵检测、恶意代码检测、钓鱼和拒绝服务攻击等复杂的安全挑战.美国德州休斯敦大学的研究者总结了安全领域对数据科学技术的迫切需求,突出了适合于安全领域的关键的数据科学方法及其应用,开设了"安全分析学"课程[16].

该课程以模块形式组织,具有4个模块:安全基础、用于安全的非监督学习技术、用于安全的监督学习技术,以及用于安全的自然语言处理.

1)安全基础模块介绍安全的目标和机制、恶意软件、入侵检测、Web安全、密码安全、邮件安全、移动安全以及系统管理基础.目标是覆盖基本的安全概念,还包括数据预处理和可视化等内容.

2)非监督学习模块,将学习关联规则挖掘和聚类在信息安全事件中的分析应用.

3)监督学习模块,由安全领域的独特需求驱动,将强调异常检测技术、单类别学习、半监督学习、代价敏感学习、在线学习以及这些技术如何用来应对安全挑战.

4)自然语言处理模块中,强调提升鲁棒性的技术,以及非静态的HMMs.

文献[16]也向学生介绍对抗性机器学习,尽管该技术仍然处于幼儿期.每个模块都设置一个课前测试、课后测试、小测验以及作业.学生必须完成一个项目,在项目中需要应用和调整至少两种数据科学技术来解决信息安全问题.

4 教学方法研究

4.1 基于主动式体验学习的信息安全教学方法

日本九州大学等单位在物联网安全教育中采用了基于主动式体验学习的信息安全教学方法[17].课程基于ADDIE(分析、设计、开发、实现、评估)模型进行设计.

体验式学习组的教学设计研究接受了学习金字塔理论,图2给出了这个理论的基本思想,说明每种教学方法在课程结束以后学生的知识保留率,被动式学习方法中讲座只有5%,阅读资料方式为10%,使用音频视频资料进行学习为20%,通过演示进行教学则达到30%,参与式主动学习方法中分组讨论可以达到50%,实践练习达到75%,而通过教会其他人的方式则能够达到90%,因此参与式主动学习方法更加有效[17].九州大学在教学中采用了分组讨论和实践练习等主动参与式学习方法,通过设置每次课程的前置测试和课后的后置测试,以及每次课程结束后1个月左右的延迟测试,表明主动参与式学习方法在知识保留率上确实是高于对照组的传统被动式学习教学方法的.因此对于信息安全教学来说,主动式学习方法是一个好的选择.不过这种方法对于需要投入的教学资源要求也比较高,九州大学的这个教学研究工作因为只有1个教师和1个助教,因此限制学生人数为10人左右.

4.2 基于竞赛和对抗的教学方法

希腊空军学院的研究工作使用基于竞赛的学习方案来进行信息安全基本概念的教学[3].通过将学生分成A(攻击方)和B(防御方)两组,每隔一个星期,以两组角色互换的方式进行基于竞赛的教学.课程结束后学生都报告觉得实验很有趣并且很有挑战性.基于信息安全本质上就是攻防对抗的科学,因此在信息安全教学中引入竞赛和对抗的方法是很自然

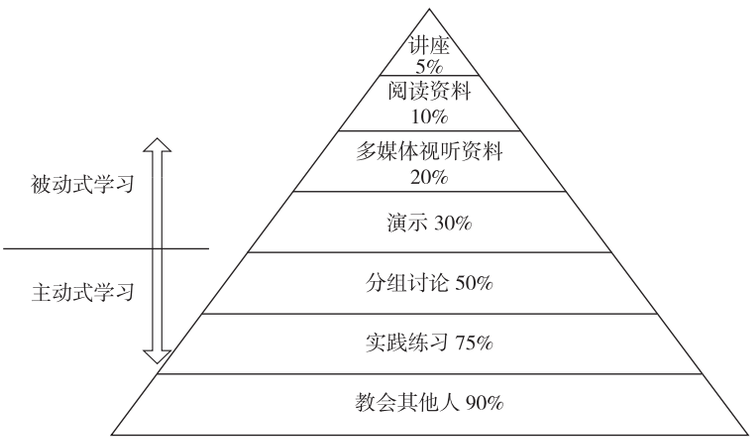

图 2　学习金字塔理论

Fig. 2　Learning pyramid theory by NTL

的选择,很多教学工作也采取了这种方式[9,18].

4.3　游戏化教学方法

在信息安全的教学中,游戏化方法是一个增进学生学习动力的好方法.游戏化的目的是提高学生的学习兴趣、增加学生的课程参与度,因此需要让学生能够玩得起来,这就需要考虑对于参与者的信息安全水平和经验不能有太多限制,游戏开动的时间、地点也不能限制得太死,还需要能够不断“升级”,以将最新的脆弱性、攻击模式和解决方案等信息更新到游戏中,从而可以让游戏玩家能够跟上信息安全形势的发展.

挪威的研究者开发了一个单人塔防游戏,塔防游戏的概念如防御、基地和敌人等可以与信息安全中的防御、资产和攻击等直接类比.这个游戏是由数据驱动的,可以周期性地自动从在线安全相关来源提取数据,游戏设计成客户机-服务器模式,服务器端每 24 小时更新资产、攻击模式和防御模式等信息[18].

文献[6]给出了研究如何使用游戏化方法改进网络安全管理教学的经验.课程游戏化教学是通过每天给学生通过邮件发送技术问题,然后根据得分排名来实现的.排名是在线公开的,学生可以查看自己的排位.学生觉得很享受这种方式,觉得每天答题可以帮助他们测试自己对知识的掌握程度,复习并更深入地思考学到的内容.他们期待每天收到问题,通过挑战的刺激来增强学习的动力,帮助他们更有计划地学习,而不会将任务留到学期结束,因此可以更有效率地组织学习时间.课后调查表明绝大多数同学认为这可以改进他们的学习习惯.

日本的研究者尝试使用 KIPS(卡巴斯基工业保护模拟)来给大学生进行运营安全教育[19].KIPS 是一个基于游戏化理论的安全训练游戏,用于在短时间内以快乐的方式帮助学习重要基础设施中的网络安全基础.该工作的结果表明,通过使用像 KIPS 这样基于场景的教学材料,个性化教学指南变得容易了,并且对安全教学材料的改进也比较有效率.

4.4　可视化教学手段的使用

美国密歇根理工大学等三所大学的合作研究给出了 RBACvisual[20] 和 UNIXvisual[21] 这样的可视化工具演示访问控制过程中每一步是如何决策的,帮助信息安全教学.通过可视化工具的帮助,学生无需花费时间学习一门安全规格说明语言就可以实践安全策略设计,指导教师也可以使用该工具在上课时讨论复杂的案例并很容易地演示策略修改后的效果.

4.5　利用学生可以接触的设备和服务改进信息安全教学

美国佛罗里达农机大学的研究者给出了将移动设备集成到信息安全教学中的方法[22],鼓励学生关注智能手机恶意代码和安全话题相关的报刊新闻或技术新闻,并让学生完成下述类型的作业:1)你为何选择移动设备的话题? 2)你选择的文章中讨论的话题是如何与基本的移动安全目标相关的——机密性、完整性、可用性? 3)文章中讨论的话题对于全球或社会的影响是怎样的? 课程实践证明大多数学生都乐于完成这些作业.

美国海军学院等单位在新生的一门必修网络安全引论课程中使用校园网中学生经常接触的消息留

言板作为工具来教授网络安全中的一些重要概念[23],例如:验证和 cookies、跨站脚本攻击和注入攻击、公钥加密中的中间人攻击、密码选择和密码文件管理等.这个工作有点类似于网络安全教学中常使用的夺旗练习,从学生学习角度看这个工具效果很好.

4.6 基于案例研究的教学方法

美国威斯康星大学使用一个跨越整个学期的纵向案例研究[24],这样可以保持整个学习环境的稳定,而不用每周切换.同时,学生能够看到并理解一个安全的系统中,信息安全是如何由网络安全、物理安全和事件反应以及其他一些内容构成的.该案例研究可以使用在 3 学分的信息安全课程,用于高级别的计算机科学和管理信息系统专业本科生和研究生,以及 2 学分的 MBA 课程,甚至 1 学分的欧洲的国际暑期学校短课程.

上海第二工业大学的研究者将 2 种无证书签名模式的安全分析作为教学案例,展示了如何进行安全分析,从而在不需要签名者私钥的情况下伪造一个合法的无证书签名,进而作为改进,给出了一些克服现有问题的简单思路[25].通过案例教学,教师可以更加清晰地解释无证书签名模式的概念,学生也可以更快和更容易地掌握相关内容.

美国密西根理工大学给出了一个使用新颖的自上而下案例驱动的教学模型来重组网络安全教学的方法[26].教学设计中,从现实世界的网络安全攻击事件开始,通过向学生从开始到结束完整的分析整个事件,从而以事件驱动的方式让学生理解这些攻击是如何进行的.在案例分析的过程中,这些攻击事件涉及的不同的网络安全方面的信息安全话题被以自上而下的方式组织起来,通过教师指导下的班级内讨论、精心选择的阅读材料和动手实践的实验作业,从而达到良好的学习效果.这种新的模型可以使用实际生活中的案例吸引学生的注意力和兴趣,而兴趣是最好的老师.也可以帮助教师从广泛的范围内选择重要而时新的安全话题,进而改进学生的学习产出,特别在于能够帮助学生获得网络安全的整体系统视图.

4.7 基于反转课堂的教学方法

解放军陆军工程大学的研究者认为信息安全教学面对的学生的基础水平相差巨大,大多数学生刚离开高中,仅仅具有一些使用简单的操作系统、Office 软件和常用工具的能力,而另一些学生掌握了编程、数据结构、数据库等计算机知识.由于基础不同,学生的学习兴趣也不一致.而反转课堂可以应用于信息系统安全教育,通过将教为中心转换为学为中心,追求形式和内容之间的交互,以及重构评估方法,学生将从被动的接受者转为积极的研究者[27].

4.8 学习风格自适应性在远程信息安全教学中的应用

英国伯明翰大学等单位的研究者开发了一个能够提供更多个性化和自适应学习的远程学习系统[2],可以根据学习者个体的学习风格产生个性化顺序的学习材料.

学习风格被定义为“作为相当稳定的指示器来说明学习者如何理解学习环境、与学习环境交互以及进行响应的特征识别、影响以及心理行为”.基于信息理解风格的自适应方法可以为感觉型学生和直觉型学生生成不同的学习路径.感觉型学生首先学习具体的学习目标,然后和抽象的学习目标交互,也就是例子和实践活动应该首先给出,然后才是概念和数学模型.而直觉型学生是从抽象到具体.如图 3 所示[2].

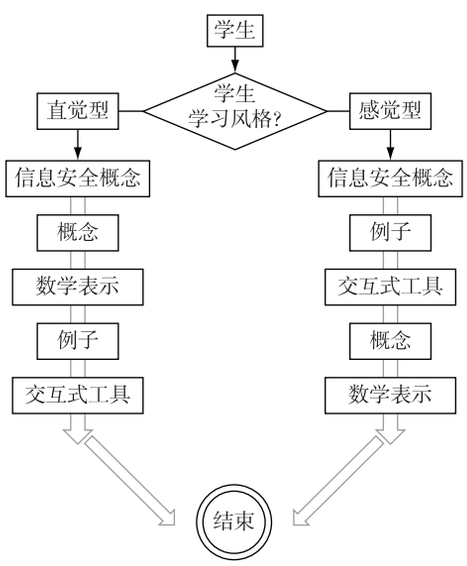

图 3 根据学生的学习风格生成不同的学习路径

Fig. 3 Generation of learning paths according to students' learning styles

4.9 神经认知研究在信息安全教学中的应用

文献[4]的工作表明神经认知研究在网络安全教育领域也很有应用研究机会.研究心理表达和学习产出之间的关系将会是很有价值的贡献.另一个有趣的方向是模糊性/歧义、神经活动以及创造性之间的交叉.大脑不喜欢不确定性,但是不成熟的决定

和不确定性会导致天真和不完全的解决方案.创造性地纳入模糊性可以为网络安全思维做出有价值的贡献.

5 课程实验建设

在信息安全的教学中,由于未来工作中对实际安全技能的要求非常高,而信息安全理论只有很好地应用才能发挥实际作用,因此几乎所有的信息安全课程都需要精心地构建课程实验让学生动手实践,并且这些课程实验作业一方面要求尽量符合最新的实际信息安全形势要求,另一方面又需要让学生能够顺利开展.

5.1 利用计算机专业学生毕业设计项目进行的信息安全课程实验建设

文献[28]给出了一个持续多年的计算机专业本科生毕业设计项目,可以为高中和非计算机专业的大学学生提供信息安全课程的动手实践实验作业,包括的实验模块有跨站脚本、SQL 注入、远程文件包含等.由本科生通过毕业项目构建的包含脆弱性的 Web 服务器应用,将指导性材料和预装的虚拟机打包起来,已经被集成到美国军事学院的一门中级通用教育信息技术课程的多个信息安全模块中.

脆弱性 Web 服务器系统由高年级本科生利用他们毕业设计时间不断迭代进行设计和构造.学生通常由 3~6 人组成一个小组,并且尽可能地让不同专业领域的学生构成一个小组.每个项目至少具有一个教师作为导师,学生还可以根据需要来寻找不同领域的导师进行指导.虽然这是多年持续的项目开发,但对于每一届学生来说并不是重复项目,而是不断地扩展和改进项目.这样的构建方式既能够使得每一届学生都能够有很好的毕业设计项目可以进行,也使得学生们毕业设计的成果具有实际应用价值,同时还能够让信息安全教学具有不断跟上时代发展的实验作业环境和内容.

5.2 独立进行的信息安全课程实验建设

美国波士顿大学的研究者给出了一个非常简单但是扩展性很好的信息安全实验建设配置[29],将学生放到对手的位置思考,强调穿透性测试中的攻击性技术,构建了可以用于波士顿大学一个学期的网络安全课程教学的结构化的实验作业集.课程实验介绍基础性的、流行的穿透性工具,对这些工具的实际使用,以及如何减轻和对抗由这些工具所发起的攻击,具体内容包括:法律和道德、有关虚拟机、操作系统和工具的介绍、搜索引擎入侵和社会工程学、网络工具和脚本、网络攻击、Metasploit 开源漏洞检测工具、口令破解、入侵检测.虽然该课程面向的学习者是各个不同专业的学生,学生们的背景差别比较大,但是教师通过清晰的选择练习和设置指导使得绝大多数学生都能够进行实践,课后调查显示大多数学生觉得作业具有挑战性.

密歇根理工大学等两所大学的合作工作也设计了覆盖广泛的信息安全原理、思想和技术的信息安全实验作业,配合使用一些成熟的开源工具,经过虚拟环境的测试并在他们的信息安全课程中使用[30].

德国达姆施塔特工业大学给出了一个交互的数字化学习平台 SecLab[31],学生能够在沙箱 Web 环境中学习和理解在不同场景下安全脆弱性是如何被利用的,该系统具有 110 个新颖的交互式安全和隐私任务.

5.3 基于云计算构建信息安全课程实验

美国卡耐基梅隆大学等三所大学的研究者合作的工作[7]提出云可以为教师和学生(无论本地还是远程)提供按需的、可伸缩的、专注的、隔离的、虚拟无限的和易于配置的虚拟机,因此,部署基于云的实验室相比传统实验室具有明显的优点,能够克服传统实验室在面临学生数量增加时难以扩展的缺点.该工作推动实现了基于云的网络安全实验室,包括了能够在云环境中应用的常用的安全工具、包和软件.

5.4 基于 IP 暗区数据进行信息安全实验构建

奥地利维也纳工业大学和美国加州大学圣地亚戈分校的研究者使用来源于加州大学圣地亚戈分校运行的一个大型 IP 暗区监控所捕获的数据构建网络交通异常检测方法的网络安全实验项目[32].在给出的实验中,学生学习面对网络安全挑战,搜索和分析可疑的异常网络交通情况,教师鼓励学生不断探索来发现数据中的新现象,并且进行表达和解释他们的发现.学生将不仅能够获得安全相关的技能,还能获得统计数据分析和数据挖掘技术的知识.

6 结语

本文从信息安全教育的迫切需求切入,围绕信息安全教学的学科地位、课程建设、教学方式和教学方法选择、课程实验构建等几个方面,对近年来最新的信息安全教学研究成果进行了介绍.信息安全是一个不断在发展的领域,新的技术在不断浮现,为了

满足信息化时代整个社会对于信息安全的迫切需求,大学必须承担起本科信息安全教育的重担,为社会各界源源不断地培养理论与技能并重的信息安全专业人才和具有安全思维和技能的各领域人才,因此对于信息安全教学方法的研究将继续发展,未来的研究方向包括将最新的技术领域例如区块链技术纳入教学内容体系,同时构造更加适合信息安全的教学方法.

参考文献

References

[1] Peltsverger S.A survey of university system of Georgia cyber security programs[C]//Proceedings of the 2015 Information Security Curriculum Development Conference, 2015.DOI:10.1145/2885990.2886004

[2] Alshammari M, Anane R, Hendley R J. The impact of learning style adaptivity in teaching computer security [C]//The 20th Annual ACM Conference on Innovation and Technology in Computer Science Education, 2015: 135-140

[3] Andreatos A S. Designing educational scenarios to teach network security [C] // IEEE Global Engineering Education Conference (EDUCON), 2017: 1606-1610

[4] Dark M. Thinking about cybersecurity[J]. IEEE Security & Privacy, 2015, 13(1): 61-65

[5] Egelman S, Bernd J, Friedland G, et al. The teaching privacy curriculum [C] // Proceedings of the 47th ACM Technical Symposium on Computing Science Education, 2016: 591-596

[6] Martin S, Diaz G, Castro M, et al. Increasing engagement in a network security management course through gamification[C]//IEEE Global Engineering Education Conference (EDUCON), 2019: 1380-1383

[7] Salah K, Hammoud M, Zeadally S. Teaching cybersecurity using the cloud[J]. IEEE Transactions on Learning Technologies, 2015, 8(4): 383-392

[8] Zatko S. Rethinking the role of security in undergraduate education[J]. IEEE Security & Privacy, 2016, 14(2): 73-78

[9] Stelzner M, Eisenbarth T. IT security in Lübeck: the design of a modern and future-proof security curriculum [C] // 2018 12th European Workshop on Microelectronics Education (EWME), 2018: 79-82

[10] Holbl M, Welzer T. Experience with teaching cybersecurity [C] // 2017 27th EAEEIE Annual Conference (EAEEIE), 2017: 1-4

[11] Neogy S. Information security [C] // Proceedings of the 1st International Conference on Internet of Things and Machine Learning, 2017: 1-8

[12] Lodgher A, Yang J, Bulut U. An innovative modular approach of teaching cyber security across computing curricula [C] // IEEE Frontiers in Education Conference (FIE), 2018: 1-5

[13] Theisen C, Williams L, Oliver K, et al. Software security education at scale[C]//Proceedings of the 38th International Conference on Software Engineering Companion, 2016: 346-355

[14] Wang Y, McCoey M, Zou H. Developing an undergraduate course curriculum on information security[C]//Proceedings of the 19th Annual SIG Conference on Information Technology Education, 2018: 66-71

[15] Patterson W, Winston C, Fleming L. Behavioral cybersecurity: human factors in the cybersecurity curriculum[M] // Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2016: 253-266

[16] Verma R. Security analytics: adapting data science for security challenges[C]//Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, 2018: 40-41

[17] Ban Y, Okamura K, Kaneko K. Effectiveness of experiential learning for keeping knowledge retention in IoT security education[C]//2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), 2017: 699-704

[18] Lovgren D E H, Li J Y, Oyetoyan T D. A data-driven security game to facilitate information security education [C]//2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings, 2019: 256-257

[19] Yonemura K, Yajima K, Komura R, et al. Practical security education on operational technology using gamification method[C]//2017 7th IEEE International Conference on Control System, Computing and Engineering (ICCSCE), 2017: 284-288

[20] Wang M, Mayo J, Shene C K, et al. RBACvisual: a visualization tool for teaching access control using role-based access control[C]//Proceedings of the 2015 ACM Conference on Innovation and Technology in Computer Science Education, 2015: 141-146

[21] Wang M, Mayo J, Shene C K, et al. UNIXvisual: a visualization tool for teaching the UNIX permission model[C] // Proceedings of the 2016 ACM Conference on Innovation and Technology in Computer Science Education, 2016: 356-356

[22] Chi H M. Integrate mobile devices into CS security education[C]//Proceedings of the 2015 Information Security Curriculum Development Conference, 2015: 1-4

[23] Greenlaw R, Brown C, Dannelly Z, et al. Using a message board as a teaching tool in an introductory cyber-security course[C]//Proceedings of the 46th ACM Technical Symposium on Computer Science Education, 2015: 308-313

[24] Lincke S J, Hawk S R. The development of a longitudinal security case study[C]//Proceedings of the 16th Annual Conference on Information Technology Education, 2015: 49-54

[25] Hu X M, Jiang W R, Ma C, et al. Security and design analysis of certificateless signature schemes as teaching cases of cryptography and security course education[C] // 2018 9th International Conference on Information Technology in Medicine and Education (ITME), 2018: 601-605

[26] Cai Y,Arney T.Cybersecurity should be taught top-down and case-driven[C]//Proceedings of the 18th Annual Conference on Information Technology Education,2017:103-108
[27] Zhao M,Chen P,Wang J S,et al.The practice of the flipped classroom mode in the information system security curriculum[C]//2018 9th International Conference on Information Technology in Medicine and Education (ITME),2018:669-672
[28] Estes T,Finocchiaro J,Blair J,et al.A capstone design project for teaching cybersecurity to non-technical users[C]//Proceedings of the 17th Annual Conference on Information Technology Education,2016:142-147
[29] Timchenko M,Starobinski D.A simple laboratory environment for real-world offensive security education[C]//Proceedings of the 46th ACM Technical Symposium on Computer Science Education,2015:657-662
[30] Wang X L,Bai Y,Hembroff G C.Hands-on exercises for IT security education[C]//Proceedings of the 16th Annual Conference on Information Technology Education,2015:161-166
[31] Ghiglieri M,Stopczynski M.SecLab:an innovative approach to learn and understand current security and privacy issues[C]//Proceedings of the 17th Annual Conference on Information Technology Education,2016:67-72
[32] Zseby T,Iglesias Vazquez F,King A,et al.Teaching network security with IP darkspace data[J].IEEE Transactions on Education,2016,59(1):1-7

A survey of recent progress on undergraduate information security teaching

HUANG Daming[1] ZHONG Sheng[1]
1 Department of Computer Science and Technology,Nanjing University,Nanjing 210023

Abstract With the rapid development of techniques such as cloud computing,mobile application and IoT,information technology nowadays has been fully integrated into our daily life.The need for security professionals and experts is growing due to the emerging security related issues.Information security education is the key to solve these problems.This paper gives a systematic description of the recent progress on research of information security teaching,which includes the difficulties faced by information security teaching,the issues to resolve,course curriculum design and course construction,teaching method research and practical experimental construction.Finally,future direction for information security teaching is given.

Key words information security teaching;course curriculum;course design;teaching method