

美国网络空间安全学科认证体系研究

张宁, 李晖

(西安电子科技大学网络与信息安全学院, 陕西 西安 710071)

摘要: 介绍了美国国家安全局和国土安全部联合出台的网络空间安全专业认证体系, 具体介绍了两个认证类别: 一为网络空间防御学科两年制、四年制、研究中心 3 个类别认证的基本情况, 包括认证对象、标准、流程和具体认证操作方法; 二为网络空间操作的学科认证的基本情况和简单的认证需求。归纳分析介绍了这两个类别的培养大纲即所要求的知识单元设置, 简单分析研究了该学科的认证在美国的发展和现状, 以期对我国的网络空间安全学科认证流程、标准和专业培养计划给出借鉴。

关键词: 网络空间安全; 专业认证; 培养计划; 学科

中图分类号: G643.0

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00018

Study on designation of cyber information assurance education in USA

ZHANG Ning, LI Hui

(School of Cyber Engineering, Xidian University, Xi'an 710071, China)

Abstract: National centers of academic excellence-cyber defense and cyber operation programs sponsored by NSA and DHS in USA were introduced and analyzed. The basic criteria and procedure of national centers of academic excellence-cyber defense with three programs, 2 years/4 years education and research center were introduced, as well as the national centers of academic excellence-cyber operation with the basic criteria. The Curriculum i.e. knowledge units were analyzed in detail. The development and current situation of the designations were investigated. Hopefully the study would be helpful to improve the accretion of the discipline of cyber security in our country.

Key words: cyber security, accreditation, curriculum, discipline

1 引言

近年来, 工程教育专业认证作为保证高等工程教育质量、实现工程教育国际相互认可的重要举措而受到了世界各国的重视。在教育部的发起和组织下, 我国于 2006 年正式开展了工程教育专业认证的试点工作。美国是工程教育专业认证最早的国家, 认证制度发展得比较完备和健全。美

国认证制度的建立对提高美国工程教育的质量发挥了极其重要的作用, 同时也对世界高等工程教育的发展产生了深远的影响。美国的工程教育认证是由美国工程与技术鉴定委员会 (ABET, Accreditation Board for Engineering and Technology) 提供的。

网络空间安全已成为国家安全的重要组成部分。我国于 2015 年批准网络空间安全作为一级学

收稿日期: 2016-01-02; 修回日期: 2016-01-08。通信作者: 张宁, zhangningxd@gmail.com

基金项目: 中央网信办网络安全人才培养试点基地建设基金资助项目

Foundation Item: Project of Cyber Security Talent Cultivation Based on Office of Central Leading Group for Cyberspace Affairs

科,目前高校已经纷纷开始设立网络空间安全相关的学科专业。而此专业的认证体系还有待发展与完善。美国特别重视网络安全人才的培养,美国国家安全局(NSA, National Security Agency)和国土安全部(DHS, Department of Homeland Security)针对网络空间安全设立了网络空间防御(CAE-CD, national centers of academic excellence in cyber defense)^[1]和网络空间操作(CAE-CO, national centers of academic excellence in cyber operation)学术优秀计划^[2],即专业认证计划。

CAE-CD项目的目的是通过推进网络空间防御高等教育和研究以及培养更多在网络空间防御方向学有专长的专业人才,降低美国全国信息基础建设的安全隐患。

CAE-CO是美国网络安全教育国家行动(NICE, national initiative for cyber security education)的一部分,目的是建设“数字国家”并且扩大能够支撑国家网络安全的技术人才池,为教育机构提供一个与计算机科学(CS, computer science)、计算机工程(CE, computer engineering)、电子工程(EE, electronic engineering)相关,基于大量的实践和实验操作教育的跨学科专业。CAE-CO项目是CAE-CD项目的有效补充,强调网络空间操作技术(信息搜集、漏洞挖掘、应急响应等),旨在提高国家在网络安全方面的地位。这些技术主要用于美国的情报、军事、执法机构执行特殊的任务。

这两个认证项目规定了从事网络空间防御和操作人才培养所需要具备的基本条件、培养计划的基本知识单元。美国的教育机构符合要求都可以申请认证,由NSA和DHS设置专门的机构进行认证以保证学术机构确实达到了认证的要求,对申请认证的学术机构设定了严格的学术与科研要求,以保障人才培养的质量,专业认证的有效期为2~5年不等。

2 CAE-CD项目简介

2.1 CAE-CD项目背景

CAE-CD项目起源于信息保障学术卓越计划(CAE-IAE, CAE in information assurance education),是于1998年由NSA发起的,DHS于2004

年加入。CAE-IAE研究中心认证项目于2008年开始,旨在鼓励大学和学生们在网络安全方向向博士学位标准的研究努力。2010年,CAE两年制信息保障教育认证计划开始授予两年制的研究中心、技术学校、政府培训机构等。目前,这3项认证项目统称为CAE-CD项目,包含3个项目的认证:四年制学士/硕士教育(CAE-CD)、两年制预科教育(CEA-CD2Y)和研究中心项目(CAE-CER)。

该项目预期显著地促进了网络空间防御知识以及实践的进步与发展。各机构通过CAE申请网站提交申请,申请时间为每年9月中旬到1月中旬,申请一旦接受评估会第一时间通知被评院系,并给出相应反馈。官方的认证结果在6月正式公布。申请不通过的当年不得再次申请。来自NSA、DHS以及其他政府、学术和产业合作者的资深网络空间防御从业人员以及学科专家会对申请进行审核。认证的最后一个步骤是现场评估,评估重点包括课程内容、课程相关性、实验室设施以及教师参与度等。申请认证的新机构将经过至少3次独立审核。再认证的机构将接受至少两次独立审核。不符合要求的机构会在公告日收到审核报告。未通过的申请会立即向机构返回审核报告。

成功申请的机构将会被认证为全国网络空间防御优秀人才教育中心,持续5个学年,届时各机构必须重新申请再认证以保留其专业资质。CAE-CD项目将逐年持续更新并加强衡量标准(包括知识单元和重点领域等)以确保其跟上不断发展的网络空间防御形势。

2.2 CAE CD项目认证标准

2.2.1 CAE-CD项目两年制教育/四年制教育/研究所认证

下面以列表的形式给出CAE-CD项目中两年制教育/四年制教育/研究所认证的目标、开放对象和基本要求。具体内容如表1所示,其中CD(cyber defence)代表网络防御。

2.2.2 认证信息简表

CAE-CD教育项目的认证以打分的形式进行,其中四年制教育项目的认证信息最为全面,两年制是四年制的缩简版,限于篇幅,仅

给出四年制教育的认证信息的简表, 如表 2 所示。

CAE-CD 研究项目的认证是在“有和无”之间评价, 基本要求满足 CAE-CD 四年制教育的认证标准, 重点评价出版物和研究论文的同行评议、毕业学生的人数和质量、基金项目、对学生学习科目要求盲审。

3 CAE-CO 项目背景与简介

CAE-CO 项目于 2012 年正式运行, 是 NICE 框架的一部分, 也是 CAE-CD 项目的补充, CAE-CO 认证面向四年制本科和研究生院校对应专业进行认证, 要求必须是建立在 CS、EE 或 CE 专业的院系, 或拥有同等技术水平的专业的院系, 或在两个或两个以上的专业之间有所协作的院系。认证评估标准和要求也会随着项目的逐步成熟, 技术的进步和网络空间技术的发展情况不断修改, 具体如表 3 所示。表 3 中 CO (cyber operation) 代表网络操作。

表 3 中的 10 项要求均为强制的, 其中第 1

项和第 3 项要求经过 ABET 工程认证, 可以说 CAE-CO 是专业认证之上的专业认证, 对于各项的详细说明参见文献[4]。

申请时间是当年 11 月 15 日到次年 1 月 15 日, 3 月和 4 月是入校评估, 结果公示时间为 5 月 15 日, 正式公布时间为 6 月。该认证每 5 年进行一次, 要求主要提供学科发展的情况, 所有的 CAE-CO 认证机构每年必须完成提交年度报告, 报告中必须明确说明本专业年度的学术活动、亮点和突出成就, 以及任何专业变化 (包括培养大纲修订和教师变动等)。

4 课程设置基本要求

4.1 CAE-CD 课程设置

CAE-CD 项目的核心知识单元和原信息保障计划中的知识单元矩阵吻合, 表 4 列出了不同项目要求的各个知识单元。其中, 课程大纲/先修课程/先修学位/学生作业/课程模式/课程模块/证书 (比如 CCNA) 均可说明覆盖知识单元, 一门课程可以覆盖多个知识单元。

表 1 CAE-CD 项目两年制教育/四年制教育/研究所认证基本情况

	开放对象	项目目标	基本要求
CAE-CD 两年制教育认证	地区认可的两年制社区学院、技术院校、州政府或联邦政府支持的网络安全培训中心或美国政府网络安全培训中心	1) 为社区、技术院校和政府培训机构的信息保障和 CD 教育项目以及提供认证 2) 在 CD 领域提供创新型、全方位和多学科的教育和培训标准。不断提高该领域的项目、课程、教师、学生和其他机构的质量 3) 在社区和技术学院以及政府培训中心, 以学位和证书项目形式提供 CD 教育和培训, 加强网络安全教育工作力度, 为国家提供一个培养合格技术人才的渠道 4) 在中小学建立一个有效的教育网络, 鼓励学生及早进入 CD 领域学习	1) CAE-CD 教育机构的建立和维护, 网络空间防御学科建设, 两年 CAE 课程实施, 学生培养, 相关教师的工作和培训进修 2) 课程设置能覆盖 CAE-CD 项目两年制教育的核心知识单元
CAE-CD 四年制教育认证	地区认可的四年制学校、研究生大学以及国防学校	1) 建立在本科以及研究生水平以上致力于 CD 尖端领域的教育项目 2) 为国家提供合格的学生, 要求学生具备成为网络空间防御专业人士的能力 3) 不断地改进 CD 项目的质量、优化课程、提高师资水平、完善学生以及其他制度体系, 鼓励教师参与 CD 方面科研项目、提高学术水平、职业以及教学能力发展 4) 培养并鼓励美国各教育机构进一步开展以 CD 为重点的教育以及深入研究	1) CAE-CD 教育机构的建立和维护, 网络空间防御学科建设, 四年制 CAE 课程实施, 学生培养, 相关教师的工作和培训进修 2) 课程设置能覆盖 CAE-CD 项目两年制教育、四年制教育的核心知识单元, 以及至少 5 种可选的知识单元
CAE-CD 研究所认证	国防院校、拥有博士点的部队院校或地方院校, 四年制研究性大学/由卡耐基基金会分级系统确定的博士/研究性大学/其他独立组织/官方承认的重要 CD 研究机构	1) 该项目鼓励各学校和教育研究机构将 CD 学科研究项目纳入课堂并成为课堂的一部分 2) 鼓励为国家安全局、国土安全部等联邦机构提供学术 CD 方案 (使其能够洞悉行业动态), 从而支持先进的学术、研究和开发能力 3) 鼓励推动政府与学术之间的研究和交流 4) 为 CAE-CD 研究机构提供机会与保障, 使其在保护关键信息系统和网络方面便于开展深入研究	1) 在满足 CAE-CD 四年制教育的认证标准之上 2) 积极开展网络空间防御方向的科学研究 (教职人员及学生)、论文、研究成果以及研究基金项目

表 2

CAE-CD 四年项目认证信息

	标准	标准描述	强制/总分
00 提交意向书			
01 实体“中心” 10/10	网络空间中心	实际场地，官方说明，包含在意向书中	5/5
	中心网站	提供超链接	5/5
02 课程计划 17/20	教学计划	培养方案，课程大纲，覆盖全部必修知识单元，5 个选修知识单元	10/10
	电子书库	电子资源的获取和利用	2/5
	学生参与教学计划	3 年内登记在册和毕业的学生信息和数量	5/5
03 学生科研 12/25	学生科研要求	论文发表等：5~10 篇学生撰写的论文、学位论文等，每篇 1 分	5/10
	实体/虚拟实验室	实验室、实验资源说明、实验课程大纲等	2/5
	研究实验课目录	研究性课程与实验性课程，每课程 1 分	5/10
04 教师和课程量 9/20	教学主管	教学主管的简历和其他资料	5/5
	全职教师	每教师 2 分，需提交所有教师的有关信息	4/10
	兼职教师和助教	每人员 1 分，简历以及授课信息	0/5
05 教职员工科研 9/41	论文发表	近三年内每篇 2 分	4/10
	书籍出版	每书 5 分，每章 1 分	0/10
	讲座会议	每次 1 分	2/6
	学术组织	每评审人资格或组织成员 2 分	2/6
	基金项目	每项资助 2 分	0/6
	参与或组织竞赛	每活动 1 分	1/3
06 跨学科建设 7/15	为其他专业开课	每节课 2 分，需提供课程名称和教学大纲	4/10
	在其他专业课上加入 CD 内容	提供 5~10 个 3 年内有关 CD 的论文或项目链接，每项 1 分	3/5
07 信息系统安全策略 16/20	安全负责人	个人信息，职位描述	5/5
	安全策略和计划	信息系统安全方案	5/5
	实践实施	包括培训、标语、教程等	6/10
08 外延 15/30	共享课	与其他院校的共享课以及教师交流	3/5
	学分互认	证明与其他教育机构的学分互认	3/5
	社会比赛	过去 3 年内参与比赛赞助与网络安全演习	0/5
	CAE 协作	与其他 CAE 机构的合作	0/5
	行业合作	与网络安全行业公司以及雇主单位的合作	0/5
	社区活动	包括社区学校科普等活动	2/5
合计			95/181

表 3

CAE-CO 项目认证标准

编号	标准	标准描述
1	培养计划（包括必修和选修）	必修全选/选修 18 选 10（课程设置见 4.2 节）
2	CO 方面的学位、证书、或研究领域	学生必须明确地以 CO 为专门的研究领域
3	专业认证及培养计划审核	考虑计算机科学、电子工程、计算机工程的专业认证，需要进行大纲审核
4	CO 是一门跨学科专业	CO 必须被有效纳入基础培训课程中
5	CO 专业的持续性和动态性	证据表明专业教育要坚持进行（每 18 个月）
6	教师参与 CO 方面科研工作	包括教师项目、论文发表、参加相关会议
7	学生参与 CO 方面科研工作	包括参与科研项目、论文发表、参加相关会议
8	学生参与基于网络服务的学习活动	包括参加地方/区域/国家进行网络操练，延伸至社区大学以及中学等
9	承诺支持 CAE-CO 项目	申请：宣布承诺。补充：在 5 年的认证窗口中，有至少 8 名学生和 3 名老师
10	参与 CO 教育科研工作的教师人数	至少两位专门从事 CO 课程的老师（非计算机/电子/CE 核心课程）

表 4

CAE-CD 知识单元

核心知识单元 (2 年项目) 11 个知识单元			
01 基本数据分析	04 网络威胁	07 密码学	10 政策法规道德义务
02 脚本或语言简介	05 安全设计原理	08 信息系统组成	11 系统管理
03 网络防御	06 信息安全基础	09 网络原理	
核心知识单元 (4 年项目+2 年项目核心知识单元) 6 个知识单元			
01 数据库	03 网络技术与协议	05 概率论与统计	06 编程语言
02 网络防御	04 操作系统概念		
可选知识单元 51 个知识单元			
01 密码学进展	13 入侵检测	27 信息安全标准	39 安全编程管理
02 网络技术与协议进展	14 数字取证	28 生命周期安全	40 安全风险评估
03 算法	15 设备取证	29 低级编程语言	41 软件安全
04 模拟通信	16 主机取证	30 移动通信技术	42 软件逆向工程
05 云计算	17 媒体取证	31 网络安全管理	43 软件安全分析
06 网络安全规划与管理	18 网络取证	32 操作系统加固	44 供应链安全
07 数据管理	19 嵌入式系统	33 操作系统原理	45 系统编程
08 数据结构	20 法证审计	34 网络安全操作概论	46 系统认证与授权
09 数据库	21 形式化方法	35 渗透测试	47 系统安全工程
10 电子通信	22 欺诈防范与管理	36 质量评估与功能测试	48 虚拟化技术
11 工业控制系统	23 硬件逆向安全	37 射频原理	49 漏洞分析
12 计算原理	24 硬件安全	38 安全编程实践	50 无线传感器网络
	25 信息安全基础设施		51 自主学习和研究
	26 信息安全义务		

表 5

CAE-CD 研究中心重点研究领域

01 网络调查	06 工业控制系统安全	10 安全嵌入式系统	14 安全事件分析和应对
02 数据管理系统安全	07 网络安全管理	11 安全移动技术	15 安全政策发展和合规
03 数据安全性分析	08 网络安全工程	12 安全软件开发	16 系统安全管理
04 数字取证	09 安全云计算	13 安全通信	17 系统安全工程
05 医疗安全			

对于以上这些课程, NSA 和 DHS 都给出了详细的大纲, 说明了学生学习后应该具备的能力, 并说明了需要的作业的形式(包括项目, 实践等)。详见文献[4]。关于这些课程与原 NICE 计划中规定的课程的对应也有详细的矩阵说明, 详见文献[4]。CAE-CDR 项目规定了网络防御重点研究领域, 如表 5 所示。

4.2 CAE-CO 课程设置

CAE-CO 项目规定了 10 门必修课程、18 门选修课程, 其中必选课程 10 门以上, 课程大致说明如表 6 所示。

5 现阶段美国高校的 CAE-CD 项目和 CAE-CO 项目的认证情况

5.1 CAE-CD 项目

截至目前(2016 年 1 月)共计 160 个高校和研究机构列入 CAE-CD 项目, 其中 CAE-R 61 个, CAE-CD 105 个, CAE-2Y 26 个, 部分知名院校

包括普林斯顿大学、卡耐基梅隆大学、马里兰大学、约翰·霍普金斯大学、加州大学戴维斯分校、普度大学、华盛顿大学、南加州大学、宾夕法尼亚大学等。基本年限为 5 年, 从 2014 年至 2021 年。详见文献[5]。

5.2 CAE-CO 项目

CAE-CO 项目的认证学校共计 14 个, 在这 14 个学校中, 空军技术研究所、海军研究所、西点军校均为军事院校, 其他大学均为百强大学, 其中卡耐基梅隆大学是 NSA 网络安全专业合作高校, 详见文献[6]。

6 结束语

本文简单总结了美国 NSA 和 DHS 给出的两个大项 CAE-CD 项目和 CAE-CO 项目的认证体系, 值得一提的是, 美国的工程教育专业认证是由 ABET 组织主持进行的, 但网络空间安全学科的认证是由国家机构 NSA 和 DHS 联合主持的。

表 6

CAE-CO 知识单元

	课程	备注
必修 10 门	低级编程语言	C 语言和汇编语言, 必须有实验
	软件逆向工程	用工具进行动、静态分析, 实验
	操作系统理论	CPU、文件系统、并发同步等
	网络	计算机通信网、网络结构、网络安全流量分析等
	移动蜂窝网技术	智能手机系统, Android, iOS, 移动加密认证技术 LTE 802.11/b/g/n
	离散数学和算法	算法复杂度、正则表示、数学基础、信息论、熵原理等
	网络攻防概论	包括密码学、云、虚拟化等
	安全基础理论	安全原则、机制、策略等
	漏洞	溢出, 远程操控
	法律	国际法、法律现状等
选修 18 选 10	可编程逻辑语言	硬件编程
	FPGA 设计	在可编程逻辑设备上仿真
	无线网络安全	2G/3G/4G/Wi-Fi/Bluetooth/Rfid
	虚拟化	工作站、服务器、公用基础设施等
	大规模分布式系统	云结构
	信息系统风险管理	威胁分析和响应
	计算机结构	数字逻辑电路
	单片机设计	按照性能和功能要求设计
	软件安全分析	源码分析、二进制代码分析等
	安全软件设计	设计方法、项目管理、代码管理等
	嵌入式系统	资源受限设备上的功能实现
	取证与媒体应急管理	网络取证、媒体取证、操作系统取证、设备取证等
	系统编程	内核模块、GPU 等
	现代密码学	密码学原理与应用
	数据采集与监视控制系统	分布式节点控制与漏洞分析
	人机交互与实用安全	接口安全与可用性
	网络攻防行为构成与分析	行为阶段分析
	硬件逆向工程	硬件渗透、探测、篡改等

在我国网络空间安全学科刚被设立为一级学科的形势下, 各个高校和教育机构争相开设了网络空间安全专业, 专业认证势在必行, 如何有效进行认证, 有效通过认证推进我国的网络安全学科发展是一项亟需推进的工作, 希望本文对美国网络安全专业认证情况的研究能对我国的网络安全专业认证给出一些思路。

参考文献:

- [1] National centers of academic excellence-cyber defense[EB/OL]. (2015-07-06). <https://www.nsa.gov/academia/nae-cd/index.shtml>.
- [2] National centers of academic excellence-cyber defense[EB/OL]. (2012-06-10). https://www.nsa.gov/academia/nat_cae_cyber_ops/index.shtml.
- [3] Criteria for measurement for CAS/cyber operations[EB/OL]. (2012-06-10). https://www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_criteria.shtml.
- [4] CAE requirements and resources[EB/OL]. <https://www.iad.gov/NIETP/CAERequirements.cfm>.

- [5] NSA/DHS national CAS in cyber defense designated institutions[EB/OL]. https://www.iad.gov/nietp/reports/cae_designated_institutions.cfm.
- [6] List of centers of academic excellence in cyber operations[EB/OL]. (2012-06-08). https://www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_centers.shtml.

作者简介:



张宁 (1979-), 女, 陕西宝鸡人, 博士, 西安电子科技大学副教授, 主要研究方向为公钥密码学、应用密码学、无线物理层安全、信息安全法。

李晖 (1968-), 男, 河南灵宝人, 博士, 西安电子科技大学教授、博士生导师, 主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。