

基于贝叶斯知识追踪的网安人才能力 智能化评估方法

张方娇^{1,2}, 赵建军^{1,2}, 刘心宇^{1,2}, 王晓蕾^{1,2}, 刘奇旭^{1,2}, 崔翔^{3,1}

¹中国科学院信息工程研究所 北京 中国 100093

²中国科学院大学网络空间安全学院 北京 中国 100049

³广州大学网络空间先进技术研究院 广州 中国 510006

摘要 近年来,网络空间安全形势日益严峻,导致网络空间安全人才(以下简称网安人才)缺口巨大,国家加快网安人才评估的需求愈加强烈。针对当前网安人才能力评估精准度不足的问题,本文提出了一种改进的贝叶斯知识追踪 CT-BKT(Cybersecurity Talents Bayesian Knowledge Tracing)模型,通过网安人才能力评估时的个性化智能化问答过程,该模型可对网安人才的知识状态进行追踪,从而实现对网安人才能力的动态精准评估。为了验证 CT-BKT 模型的有效性,本文以 Web 安全为例,梳理了 Web 安全的知识技能体系并构建了相应题库,实现了一个面向 Web 安全领域的网安人才技能智能化评估系统 CTIES(Cybersecurity Talents Intelligent Evaluation System)。通过对 22 名网安人员进行 Web 安全的能力评估,本文提出的 CT-BKT 知识追踪模型的对网安人才的知识掌握状态的预测准确率较高,CTIES 系统能细致且直观地展现网安人才 Web 安全的知识掌握程度及相应专业技能水平,验证了本文所提出的网安人才能力评估方法的可行性和有效性。

关键词 贝叶斯网络; 知识追踪模型; 网安人才; 智能化评估; Web 安全

中图分类号 TP391.6 DOI 号 10.19363/J.cnki.cn10-1380/tn.2021.01.06

Cybersecurity Talents Intelligent Evaluation Based on Bayesian Knowledge Tracing Model

ZHANG Fangjiao^{1,2}, ZHAO Jianjun^{1,2}, LIU Xinyu^{1,2}, WANG Xiaolei^{1,2}, LIU Qixu^{1,2}, CUI Xiang^{3,1}

¹ Depart Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

² School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

³ Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China

Abstract In recent years, the situation of cyberspace security is becoming more and more serious, which leads to a huge gap of cybersecurity talents. And our country has an increasingly strong demand for cybersecurity talents. To solve the accuracy in cybersecurity talents evaluation, this paper proposes an improved Bayesian knowledge tracking CT-BKT (Cybersecurity Talents Bayesian Knowledge Tracing) model. By tracking the knowledge status of cybersecurity talents, the individualized questions can be intelligently generated, so that dynamic and accurate evaluation of their capabilities can be achieved according to their answering to selected questions. In order to verify the effectiveness of CT-BKT model, here Web security is taken as an example. We sort out the knowledge and skills of Web security and construct the corresponding question bank, and finally implements a Cybersecurity Talents Intelligent Evaluation system (CTIES) in the Web security field. Through the evaluation of 22 cybersecurity talents, CT-BKT knowledge tracking model proposed in this paper has a high prediction accuracy. Besides, CTIES system can give the more detailed and direct display of cybersecurity talents' knowledge mastery of Web security and corresponding professional skill level. The experiment verifies the feasibility and effectiveness of cybersecurity talents evaluation proposed in this paper.

Key words bayesian network; knowledge tracing model; cybersecurity talents; intelligent evaluation; web security

1 引言

网络空间已成为人类社会生存和发展的新空间,

被视为继“陆、海、空、天”之外的国家“第五疆域”。网络空间的竞争,归根结底是人才的竞争,网络安全人才培养已被美国、欧盟、日本、韩国等多

通讯作者: 赵建军, 硕士, 助理研究员, Email: zhaojianjun@iie.ac.cn。

本课题得到中国科学院网络测评技术重点实验室和网络安全防护技术北京市重点实验室资助。

收稿日期: 2020-09-30; 修改日期: 2020-11-29; 定稿日期: 2020-11-30

个国家纳入国家战略。我国也高度重视网络空间安全和信息化工作,确立了网络强国战略思想,并就网络空间安全人才(以下简称网安人才)发展做出一系列重要部署,推出多项有力措施^[1]。2014年2月27日,中央网络空间安全和信息化领导小组(现更名为中央网络安全和信息化委员会)成立,习近平总书记亲自担任组长并主持召开第一次会议;2015年6月国务院学位委员会增设“网络空间安全”一级学科;2016年6月12日,中央网络安全和信息化、国家发展和改革委员会、教育部等联合发布《关于加强网络安全学科建设和人才培养的意见》;2016年12月27日,经中央网络安全和信息化委员会批准,国家互联网信息办公室发布《国家网络空间安全战略》;《中华人民共和国网络安全法》于2017年6月1日起施行,其提到了网络安全人才培养的概念,这是首次以法律条款的形式对网络空间安全领域的人才问题进行规定^[1]。通过持续的政策措施引导,网安人才队伍建设取得了显著成绩。网络空间安全学院在多所大学落地;网络空间安全职业培训和专业认证快速推进;网络安全竞赛和攻防实战演练蓬勃发展;多地规划建设网络安全人才和创新基地,出台人才培养和引进政策;各行业明确并落实网络安全责任制和人员合规要求,注重安全人员的教育和技能培训;国家深入开展网络空间安全宣传教育,全社会的网络空间安全意识显著提高^[1-2]。

近年来,我国已经加快网安人才的培养步伐,但人才缺口依然巨大,网安人才的数量和质量仍然严重不足,难以满足国家网络空间安全的需求。我国网络安全人才缺口近百万^[3],高校是我国培养网络空间安全人才的主阵地,但目前每年网络空间安全学历人才培养的数量不足1.5万人;截止到2018年底,我国241所高校设置有网络安全相关专业244个^[4],与我国理工科院校总量相比,设置有网络安全相关专业的高校占比较少。2019年7月26日,奇安信行业安全研究中心与智联招聘联合发布《2019网络安全人才市场状况研究报告》^[4]。该报告显示,中国网络安全人才需求规模依然呈现大幅增长态势,2019年6月网络安全人才市场需求的规模达到2016年1月需求的24.6倍,相比2018年7月也增长了3倍。2020年受全球疫情影响,安全人才的需求也大幅下降,但有58%的用人单位认为,网络安全人才需求会在短期内大幅增长^[5]。除了我国面临网安人才需求缺口巨大的问题之外,人才荒已成为国际问题。国际信息系统安全认证协会(ISC)²于2019年11月发布《2019年(ISC)²网络安全人力研究报告》^[6],首次估算

目前的网络安全从业人员为280万,预计目前网络安全人才的缺口407万。数据显示网络安全从业人员数量仍需增加145%。人才培养已成为网络空间安全领域的一个重要研究课题,加强网络空间安全人才培养刻不容缓。

网安人才培养涉及到人才选拔、培训、评估、认证等多个环节,其中,如何对网安人才已达到的技能水平进行精准评估至关重要。然而,现有的人才评估手段并不能有效适用于网安人才,尤其不适用于掌握特殊网安技能的人才^[7],造成这种局面的原因主要有三方面:其一,我国网安教育起步较晚,高校网安实践型人才储备不足,缺乏精通尖端网络安全技术的教师队伍;其二,高校普遍缺乏网络安全实践和演练场景,导致学生重理论而轻实战;其三,现有的以夺旗赛(Capture The Flag, CTF)模式为主的网络安全竞赛及认证模式,虽然在一定程度上能对网安人才进行评价,但却因其模式固定化和题目静态化等原因而广受争议。因此,如何对网安人才能力进行精准评估,满足多行业、多领域人才需求,并协助高校等机构完善网安人才培养模式,考察解决实际问题的能力,为企业事业单位输送实战型攻防兼备人才,有着非常重要的现实意义。

针对上述问题,本文首先是构建网安人才的知识追踪模型,进而在模型基础上设计实现针对网安人才的智能化测评系统,可根据网安人才测评过程中题目作答正确与否的情况动态更新知识追踪模型中网安人才的知识掌握状态,从而实现网安人才知识的追踪及网安人才能力的快速精准评估。

本文的主要贡献如下。

1) 针对网安人才技能水平精准评估不足问题,提出了一种网安人才能力评估贝叶斯知识追踪模型CT-BKT;

2) 提出了基于CT-BKT知识追踪模型的智能化测评与推荐算法,实现网安人才动态精准评估;

3) 基于所提出的网安人才知识追踪模型和测评算法,实现了面向网安人才的技能智能化评估系统—CTIES(Cybersecurity Talents Intelligent Evaluation System);

4) 以Web安全方向为实例验证本文所提出的人才评估方法。梳理了Web安全方向的知识领域模型并构建了相应题库。通过对22名网安人才进行能力测评,结果表明所提出的模型、算法及系统可行、有效。

2 相关工作

传统的笔试和面试等网安人才能力评估方法主

观因素较大, 影响能力评估的准确性和可信性。当前较为主流的网安人才能力评估方法主要有两种: 网络安全竞赛及网络空间安全认证, 本小节就这两种评估方法进行论述。

2.1 网络安全竞赛

安全竞赛作为人才培养和选拔的主要渠道, 一方面弥补了课本理论和动手实践之间的鸿沟; 另一方面, 竞赛种类繁多, 品类各异, 不同的竞赛面向不同的群体—从入门选手到安全极客(Geek), 不同的竞赛侧重不同的能力维度, 从攻击、防御、智能, 不同安全细分领域的从业人员能够在不同的竞赛中得到针对性锻炼。以 CTF 为代表的网络安全竞赛这几年发展得十分火热。CTFTIME 收录的 CTF 赛事资讯统计如下图所示(截止到 2020 年 9 月 23 日)^[8-9], 从图 1 和图 2 中可以看出, 从 2011 年开始, CTF 赛事数量及参赛队伍几乎以线性比例在增加, 其中 2020 年数据不完整。

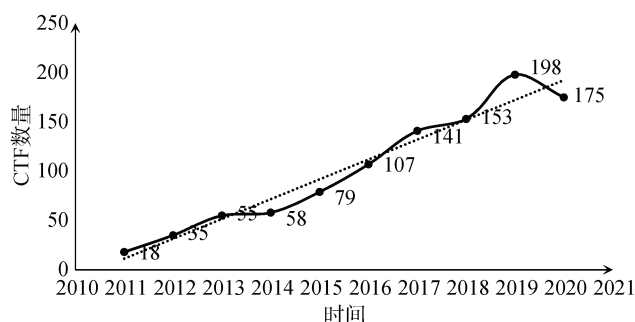


图 1 CTF 比赛数量统计
Figure 1 CTF competitions

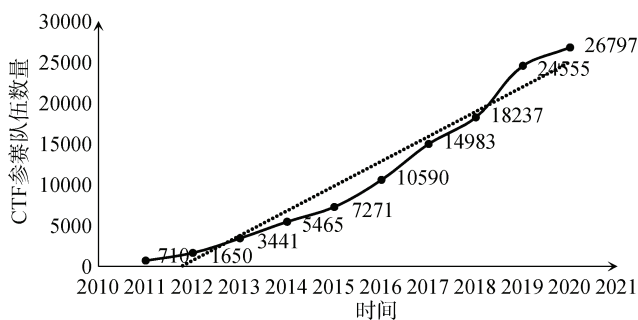


图 2 CTF 参赛队伍数量统计
Figure 2 CTF teams

CTF 起源于 1996 年举办的 DEFCON 全球黑客大会。发展至今已有 21 年的历史。DEFCON CTF 是目前全球最高技术水平和影响力的 CTF 竞赛, 被认为是 CTF 赛场中的“世界杯”。随着网络攻防技术发展, CTF 竞赛形式在全球范围内愈加流行, CTF 比赛的数量与规模发展迅猛, 国内外各类高质量的 CTF

竞赛层出不穷, CTF 已经成为了学习提升信息安全技术, 展现安全能力和水平的重要途径。

CTF 竞赛的解题模式包括逆向分析、Web 应用漏洞分析与利用、二进制漏洞挖掘与利用、密码学、移动安全、取证分析、安全编程等技术挑战类别, 基本上覆盖了网络空间安全的基础知识与技能体系。CTF 竞赛的攻防模式更注重 Web 应用、二进制文件、嵌入式或工业控制系统等类型环境的漏洞挖掘、修补与利用技术, 属于网络空间安全领域的核心对抗能力。CTF 竞赛可以促进团队合作与互助互学, 成为推动网络安全课外实践教学体系建设的关键一环。美国、日本、韩国等国家以及欧洲、我国台湾等地区已经将 CTF 对抗竞技赛用于网络空间安全教育和人才培养, 而相关政府机构也为科研教育机构与民营企业开展相关竞赛活动提供了丰富的资金与资源支持^[10]。随着国内对网络安全行业的日益重视, 2014 年, 国家互联网应急中心、中央网信办、西安、上海等政府部门也相继面向大学生和安全从业人员举办网络安全技术竞赛^[11]。近几年国内高校、知名企业也开始相继举办网络安全技术竞赛。国内高校中最早开展的安全技术竞赛是北京理工大学的信息安全与对抗技术竞赛(Information Security and Countermeasures Contest, ISCC)。从 2010 年开始, 西安电子科技大学、杭州电子科技大学、浙江大学、上海交通大学等高校开始举办面向全国的安全技术竞赛。还有一些高校, 如中国石油大学、天津理工大学等, 相继开展校内范围的安全类学科知识竞赛。从 2013 年起, 奇虎 360、百度、阿里巴巴、奇安信等企业为了招揽人才开始举办安全技术竞赛。

国内外激烈的安全技术竞赛, 吸引了很多的学生和安全从业人员, 培养了许多国内外网安人才。国外比较著名的 CTF 战队有来自美国 CMU 的超级明星战队 PPP 及美国 UCSB 大学的传统强队 Shellphish、来自俄罗斯的 More Smoked Leet Chicken 战队等; 国内比较著名的战队有蓝莲花战队、0ops 战队、NuLL 战队、eee 战队、A*0*E 联合战队等^[4]。

CTF 比赛在国内外开展得如火如荼, 对网安人才的培养和选拔, 无疑具有积极的推动作用。但是, 当前 CTF 竞赛在网安人才的培养和评测过程中存在不足。根据 CTFTIME^[8]提供的国际 CTF 赛事列表, 绝大多数比赛的比赛模式都为解题模式(Jeopardy), 只是涵盖网络空间安全的基础知识与技能, 缺乏核心对抗能力考查, 这与真实的攻防场景还有很大差距。总结 CTF 比赛有多方面的不足: 比赛知识点高度集中, 适合有经验的网安人才参赛训练, 不适合

网安初学者; 比赛环境仅比赛期间可用, 不能用于日常网安人才培养; 题目考点脱离现实场景和业务需求, 实战性不强^[12]; CTF 赛事多数是团队作战, 很难对个人能力进行界定及评估。

2.2 网络空间安全认证

网络空间安全认证用于评判从业人员是否可以从事某种网络空间安全专业技术工作所需要的知识、技术和能力^[13]。网络空间安全认证是网安人才培养和评价体系的重要组成部分, 有利于合理使用专业技术人才, 提高网安人才队伍的专业素养和业务能力标准, 加快网安人才的培养。

美国等发达国家高度重视网络空间安全认证且认证体系相对较完善, 政府制定政策倡导网络空间安全认证; 行业协会设定网络空间安全认证标准, 创立更新认证项目; 高校及科研院所辅助认证体系建设, 开展教育和培训活动; 企业针对内部员工开展非认证职业培训。通过以上举措形成了规模化的认证与培训产业^[13]。

目前, 国际信息系统安全认证联盟(ISC)²、信息系统审计与管控协会(ISACA)、国际电子商务顾问局(EC-Council)和美国计算机行业协会(CompTIA)等协会创立的网络空间安全认证具有较高的权威性和认可度。具有代表性的认证有以下几种:

1) (ISC)²^[14]: CISSP 认证(注册信息系统安全师)、CSSLP 认证(注册软件生命周期安全师)、CCFP 认证(注册网络取证师)、SSCP 认证(系统安全认证从业者)、CCSP 认证(注册云安全师)。

2) ISACA^[15]: CISA 认证(注册信息系统审计师)、CISM 认证(注册信息安全经理)、CGEIT 认证(企业信息科技管治认证)、CRISC 认证(风险及信息系统监控认证)。

3) EC-Council^[16]: CEH 认证(道德黑客)、ECSA 认证(安全分析师)、LPT 认证(授权渗透测试员)、CCISO 认证(首席信息安全官)等。

4) CompTIA^[17]: 职业级的安全职业者 CompTIA A+、CompTIA Network+ 和 CompTIA Security+ 认证等。

经过多年发展, 我国已形成初步的网络空间安全认证体系。主要由中国信息安全测评中心代表国家具体实施信息安全测评认证, 主要包括注册信息安全专业人员(CISP)、注册信息安全员(CISM)、信息安全专业人员-渗透测试工程师(CISP-PTE)及安全编程等专项培训、信息安全意识培训^[18]。

网络空间安全认证可以提升现有网络空间安全从业人员的技术水平和实践能力, 是世界各国网络空间安全人才培养的重要组成部分, 网络空间安全认证与学历教育一同构成了网络空间安全人才输送的两条主要渠道^[13]。虽然网络空间安全认证对网安人才能力评估起到了积极的作用, 加快了网安人才的快速培养, 但是也存在一些问题, 总结如表 1 所示。从表 1 中可以看出: 大部分认证的申请人为信息安全专业人士, 考试题型多为选择题, 解题知识性较强, 脱离现实场景和业务需求, 侧重对知识点的熟悉程度, 为了做题而做题。

目前我国已有的认证项目数量不多, 分级不够精细, 尚未形成层次的、互补的完整认证体系; 认证的知识领域重叠比例较高, 认证针对性不强, 认证和岗位之间的映射粒度大, 不能满足网络空间安全岗位的技能评估需求。综合来看, 目前我国网络空间安全认证体系并不完善, 不能快速弥补我国当前网安人才巨大的缺口, 也难以满足国家关于“加强网络空间安全人才建设”的战略需求。

表 1 网络空间安全认证
Table 1 Cybersecurity profession certifications

类别	Security+	Certified Ethical Hacker (CEH)	Certified Information Security Manager (CISM)	Certified Information Systems Security Professional (CISSP)	CISP	CISP-PTE
认证机构	CompTIA	EC-Council	ISACA	(ISC) ²	中国信息安全测评中心	中国信息安全测评中心
题型	90min, 单选题为主, 多选题, 实操题	4hours, 125 道选择题, 无实际操作	4hours, 200 道选择题	6hours, 250 道选择题	2hours, 100 道单项选择题	2hours, 20 道单选题+实操题
申请要求	无限制, 但建议两年及以上 IT 安全管理经验的人参加	具备至少 2 年的相关安全经验	具备 3~5 年左右信息安全管理经验	具备 2 年或者 2 年以上相关工作经验	至少具备 1 年从事信息安全有关的工作经历	无限制, 专注于培养考核高级应用安全人才

综上可得, 传统的笔试、面试等评估方法和当前主流的网络安全竞赛和认证的网安人才评估方法存

在一些不足, 无法满足不同层次网安人才的需求; 缺乏实战应用, 无法贴合现实场景; 无法满足各类

网安岗位人才的需求,无法全面高效精准评估网安人才的专业能力。

为了实现网安人才能力的精准评估,本文利用改进后的贝叶斯知识追踪模型实现网安人才知识状态的追踪。当前利用贝叶斯网络进行人才能力评估的文献很少,已有的方法为利用贝叶斯网络对简历进行分析处理辅助 HR 进行人才评估,但该评估方法未包含人才的行为,不能对人才个人真实专业能力进行评估。以 Web 安全方向为例,在 Web 安全方向知识领域模型基础上,本文提出了基于知识追踪模型的动态测评与推荐算法,并设计实现了 Web 安全方向的网安人才技能智能化测评系统,以达到对网安人才知识状态更精准评估的目的。

3 CT-BKT 知识追踪模型

人工智能技术推动教育信息化快速发展,通过人工智能技术在教育领域的运用实现其辅助甚至替代作用。在人工智能技术辅助教学过程中,智适应学习系统是其中一个重要环节。智适应学习系统驱动个性化教育,可以精确地对学习者的知识状态进行评测,能检测出学习者的薄弱知识点,并针对薄弱知识点推荐学习资源辅导学习者学习和练习^[23]。本文借鉴智适应学习系统中的知识追踪方法对网安人才的知识掌握状态进行追踪,最终实现网安人才能力的评估。

知识追踪模型能够将学生在解决问题中的行为表现解释为学生知识的掌握情况,是一种学生学习效果评估与学习状态预测模型,其有利于实现学生的个性化评价,在智适应学习系统中发挥着重要的作用^[19]。而贝叶斯知识追踪模型(Bayesian Knowledge Tracing, BKT)在 20 世纪 90 年代由卡耐基梅隆大学教授 Corbett 和 Anderson 提出^[20],由于其简捷、预测准确且易解释的特点被广泛采用,在智适应学习系统对学生的知识水平进行评估和预测,取得了较好的效果。贝叶斯知识追踪模型通过将学生的知识状态假设为一组二元变量来对学生知识点的变化进行追踪^[19],即掌握或者没有掌握知识点。通过学生连续回答一系列考察知识点的问题判断学生是否掌握该知识点。该模型是隐马尔可夫模型的典型应用^[21],将学生知识状态作为一种潜在变量,学生回答问题对错的情况等可观测变量来对其进行更新。

本文利用改进后的贝叶斯知识追踪模型对网安人才掌握的知识状态进行评估。改进后的模型 CT-BKT(Cybersecurity Talents Bayesian Knowledge Tracing Model)考虑网安人才对知识点的初始化掌握

程度以及测试题目难度对测试人员的影响,以提高模型知识追踪的准确率。改进的模型如图 3 所示。

3.1 CT-BKT 模型结构

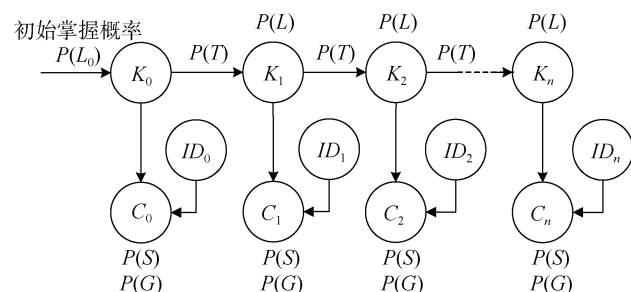


图 3 CT-BKT 模型结构图

Figure 3 CT-BKT model structure

CT-BKT 为每个知识点使用一个隐马尔可夫模型进行知识点的知识状态进行建模,图 3 体现了一个知识点的建模情况。CT-BKT 模型中变量的定义如下所示:

K_i : 隐藏变量,表示做第 i 道题目之前网安人才该知识点的知识状态, $0 \leq i \leq n$, $n+1$ 为测评的题目数量。 K_i 具有离散的两种状态: 未掌握(0 状态)和已掌握(1 状态)。当 $i > 0$ 时, K_i 反映了在前一次做题结束后,被测评的网安人才对该知识点的掌握情况。

C_i : 观测变量,表示第 i 道题目网安人才的答题状态, $0 \leq i \leq n$ 。 C_i 具有离散的两种状态: 正确(1 状态)和错误(0 状态)。将已知的网安人才答题表现作为输入,预测其对知识点的掌握情况以及未来再次遇到该知识点时的表现。

ID_i : 题目难度(Item Difficulty)变量,表示第 i 道题目的难度状态, $0 \leq i \leq n$ 。在传统 BKT 模型的基础上,本文提出的 CT-BKT 模型考虑到了题目难度对网安人才答题状态的影响。题目难度大,答对题目的概率比较小;题目难度小,答对题目的概率比较大。

$P(L)$: 知识点掌握概率, $P(L_0)$ 为初始掌握概率,表示答题之前网安人才已经掌握该知识点的概率。本文的初始概率由网安人才在自身专业领域的知识积累决定,可以从多个维度进行刻画,如公式(1)所示。本文从 m 个维度刻画网安人才知识点的初始掌握概率,每个维度所占的比重为 $e(j)$,该值为固定值。每个维度的权重系数为 θ_j ,该值和网安人才个人相关。如果网安人才在该维度方面专业领域能力较强,则该系数的取值较大。

$$P(L_0) = \sum_{j=1}^m \theta_j \times e(j) \quad (1)$$

$P(T)$: 知识转移概率, 即经过测评后, 网安人才对于该知识点由未掌握状态到掌握状态的转移概率。

$P(G)$: 猜对概率。网安人才即使未掌握知识点仍能正确回答问题的概率。本文设计的测试题目类型主要包括理论题(非CTF类型)和实操题(CTF类型)两种类型。本文在文章后面的论述中以CTF题目来统称实操题。对于CTF题目而言, 题目难度 ID 无论大小, 因其输出空间一般不可枚举, 所以被测人员猜对(或者说成功暴力枚举)的概率极小。这里我们直接假设, CTF题猜对的概率为0。

$P(S)$: 失误概率。网安人才尽管掌握该知识点, 但仍回答错误的概率。

CT-BKT模型使用了贝叶斯算法, 每一个知识状态节点都是通过一个条件概率表CPT(Conditional Probability Table)来量化父节点对自身节点的影响, 即前一道题目的答题表现状态对当前题目知识状态及表现状态可能的影响。由上述参数的定义, 我们得到知识状态节点与表现节点的CPT如表2所示, CPT由初始知识状态概率矩阵、知识状态转移概率矩阵和答题状态概率矩阵组成。

表2 条件概率表CPT
Table 2 Conditional probability table

初始知识状态概率矩阵		知识状态转移概率矩阵			答题状态概率矩阵		
做题目前知识状态	概率	前一道题目知识状态	当前题目知识状态	概率	当前题目知识状态	当前答题表现状态	概率
已掌握知识点	$P(L_0)$	已掌握知识点	未掌握知识点	0	已掌握知识点	答题正确	$1 - P(S)$
		已掌握知识点	已掌握知识点	1	已掌握知识点	答题错误	$P(S)$
未掌握知识点	$1 - P(L_0)$	未掌握知识点	未掌握知识点	$1 - P(T)$	未掌握知识点	答题正确	$P(G)$
		未掌握知识点	已掌握知识点	$P(T)$	未掌握知识点	答题错误	$1 - P(G)$

3.2 CT-BKT模型应用

根据条件概率表CPT, 我们可以看出, 网安人才知识状态由未掌握状态转移到掌握状态的概率为 $P(T)$, 仍然为未掌握状态的概率为 $1 - P(T)$ 。当网安人才答题时, 若已经掌握相应知识点, 却答题错误的概率为 $P(S)$, 相应地答题正确的概率为 $1 - P(S)$; 在不掌握某个知识点的情况下, 答题正确的概率为 $P(G)$, 答题错误的概率为 $1 - P(G)$ 。上述为一个知识点的掌握状态追踪过程, 针对网安人才的能力测评需要对专业知识领域的多个知识点进行考核而且不同知识点的难度是不同的, 因此对应着上述模型的各个参数都会有所不同, 需要对不同的知识点分别训练对应的四个参数, 可以基于EM算法的鲍姆-韦尔奇算法实现对CT-BKT模型相关参数的估计^[25]。

根据对CT-BKT模型的分析, 我们能得到网安人才答题正确与否及其知识掌握情况概率。具体说明如下:

1) 正确回答第 $m-1$ 道题目的情况下, 网安人才对于知识点的掌握概率 $P(L_m | Correct_{m-1})$ 如公式(2)所示, 这里 $1 \leq m \leq n$ 。网安人才题目回答正确的概率包括掌握知识点的情况下没有失误的概率和没有掌握知识点的情况下猜对的概率。

$$P(L_m | Correct_{m-1}) = \frac{P(L_{m-1}) \times (1 - P(S))}{P(L_{m-1}) \times (1 - P(S)) + (1 - P(L_{m-1})) \times P(G)} \quad (2)$$

2) 错误回答第 $m-1$ 道题目的情况下, 网安人才对于知识点的掌握概率 $P(L_m | Incorrect_{m-1})$ 如公式(3)所示, 这里 $1 \leq m \leq n$ 。网安人才题目回答错误的概率包括掌握知识点的情况下失误的概率和没有掌握知识点的情况下且没有猜对的概率。

$$P(L_m | Incorrect_{m-1}) = \frac{P(L_{m-1}) \times P(S)}{P(L_{m-1}) \times P(S) + (1 - P(L_{m-1})) \times (1 - P(G))} \quad (3)$$

3) 网安人才回答第 m 道题目时对于知识点掌握程度的概率 $P(L_m)$ 如公式(4)所示, 这里 $1 \leq m \leq n$ 。该概率由两部分组成, 包括网安人才回答完第 $m-1$ 道题目时对于题目涉及知识点的掌握概率和回答第 m 道题目时知识状态由未掌握状态转移为掌握状态的概率之和。

$$P(L_m) = P(L_{m-1} | Evidence_{m-1}) + (1 - P(L_{m-1} | Evidence_{m-1})) \times P(T) \quad (4)$$

其中, $P(L_{m-1} | Evidence_{m-1})$ 表示根据网安人才的第 $m-1$ 道题目的回答情况对相关知识点更新后该知识点的掌握概率。

4) 网安人才回答第 m 道题目时回答正确的概率 $P(Correct_m)$ 如公式(5)所示, 这里 $1 \leq m \leq n$ 。该概率

也由两部分组成, 包括网安人才掌握该知识点而且回答题目时没有发生失误的概率和网安人才没有掌握该知识点但却猜对题目的概率。

$$P(\text{Correct}_m) = P(L_m) * (1 - P(S)) + (1 - P(L_m)) * P(T) \quad (5)$$

每当网安人才完成一道题目的测试时, CT-BKT 模型基于网安人才回答题目的正确与错误的序列实时迭代更新网安人才对于知识点的掌握情况信息, 并能预测网安人才再次遇到该知识点时的未来答题表现。

4 系统设计与实现

围绕针对网安人才的 CT-BKT 知识追踪模型, 本文设计实现了一种面向网安人才技能智能化评估系统—CTIES 系统。系统以网安人才自身专业积累及回答题目正确与否的动态信息为输入, 以网安人才的知识掌握程度为输出。在详细介绍 CTIES 系统之前, 本章我们首先讨论网络空间安全领域的知识领域模型, 知识领域模型是 CTIES 系统的基础。

4.1 知识领域模型

在智适应学习系统里, 知识领域模型主要描述所学习的知识结构, 建立详细的专业领域内的知识点结构图谱并把细分后的知识点智能化表达出来^[22-23]。本文的知识领域模型主要是指网络空间安全领域的专业知识结构。知识领域模型构建是 CTIES 系统的关键基础, 直接决定了被测试的网安人才对知识点的定位是否精准, 其构建方式及内容与 CTIES 系统的评测效果密切相关。知识领域模型一

般需要具有丰富教研经验的优质教师对领域知识内容进行把握和细分。为方便阐述论文的核心思想, 本文以 Web 安全技能精准评估为例, 讨论 Web 安全方向的知识领域模型及相应的 CTIES 系统。显然, 所设计的模型、系统和方法, 也可以扩展到二进制、密码学、移动安全、取证分析等技能评估。

借鉴 Web 应用开发采用的前端和后端的分工方式, 我们从攻防角度出发基于前端浏览器安全和后端服务器安全两个维度构建 Web 安全方向的知识领域模型并使用思维导图的树状图形式描述 Web 安全方向的知识间的层级关系, 使得知识领域模型更好理解。我们引用中国网络空间安全人才教育联盟发布的《网络空间安全工程技术人员培养体系指南》^[24](以下简称人才培养体系指南)中 Web 安全知识技能体系, 将其作为 Web 安全方向的知识领域模型, 并在其基础上进行少许改动。主要区别包括:

1) 将人才培养体系指南中“劫持攻击”知识点修改为“客户端劫持攻击”, 并将该知识点下的子知识点“DNS 劫持”删除。

2) 在人才培养体系指南中添加新的知识点——“Web 服务器运维”。“Web 服务器运维”是针对承载着 Web 应用的服务器进行安全配置和检查, 能提前检测并发现 Web 服务器中存在的安全问题进行及时处置, 防止发生数据泄露等重大安全事件。该知识点偏向安全防御, 在日常信息系统安全运维中非常重要, 这里我们将其列入到 Web 安全方向的知识领域模型里。“Web 服务器运维”知识点涉及的技术主要包括 Web 服务器配置、日志审计、代码审计、WAF 配置、杀软配置、系统加固及其他类型 Web 服务器运维。

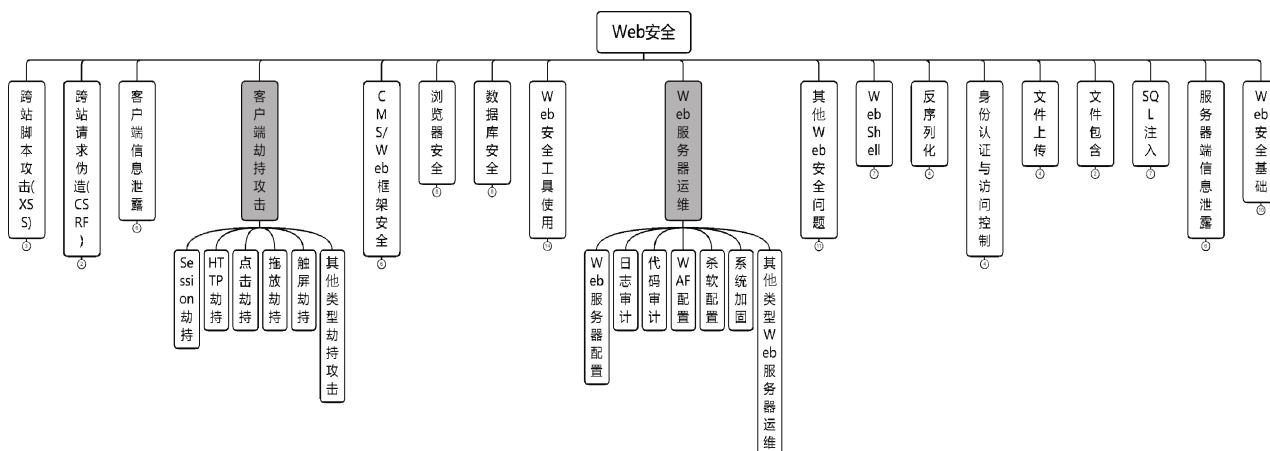


图 4 Web 安全方向的知识领域模型

Figure 4 Web security knowledge model

Web 安全方向的知识领域模型如图 4 所示, 总共 3 层, 第一层为 Web 安全方向, 第二层为 Web 安全方向下的所有知识点, 第三层为单个知识点下的子知识点, 第三层是第二层知识点更细化的内容。因篇幅有限, 第三层子知识点未全部展开描述。从图 4 可以看出, Web 安全方向共包含 18 个知识点, 具体包括跨站脚本攻击(XSS)、跨站请求伪造(CSRF)、客户端信息泄露、客户端劫持攻击、CMS/Web 框架安全、浏览器安全、数据库安全、Web 安全工具使用、Web 服务器运维、其他 Web 安全问题、Webshell、反序

列化、身份认证与访问控制、文件上传、文件包含、SQL 注入、服务器端信息泄露、Web 安全基础。图 4 中知识点下圆圈中数字即为该知识点包含的子知识点的数量。Web 安全方向的知识点之间及子知识点之间划分原则为: 尽量独立无关联。

CTIES 系统将根据 Web 安全知识领域模型中知识点及子知识点的内容进行题目设计, 同时, 根据网安人才的知识状态情况推荐相关题目给网安人才进行测评, 从而实现 Web 安全方向的网安人才能力评估。

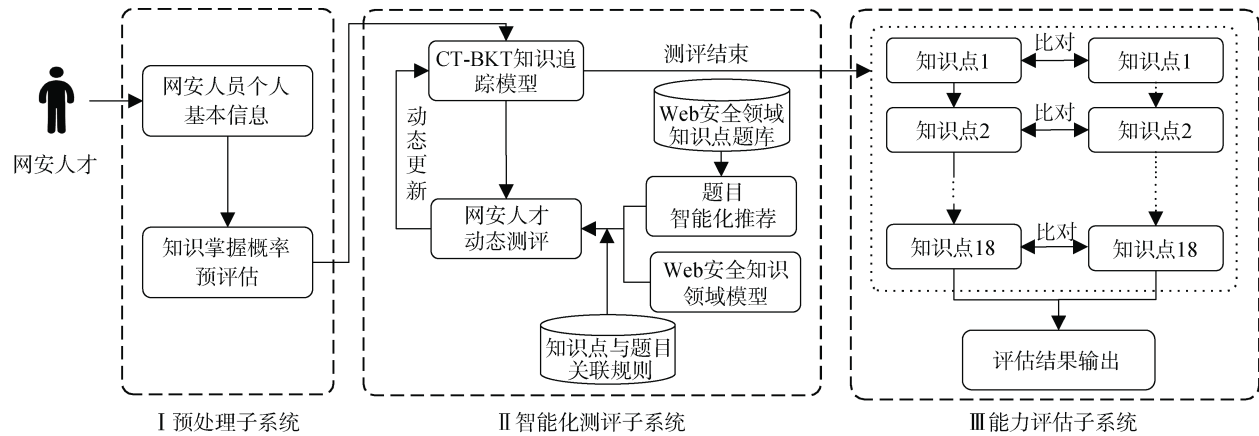


图 5 CTIES 系统架构图
Figure 5 CTIES System architecture

4.2 系统实现

CTIES 系统由预处理子系统、智能化测评子系统和能力评估子系统组成, 系统架构图如图 5 所示。其中, 预处理子系统的任务是根据网安人才个人基本信息进行知识掌握情况的预评估; 智能化测评子系统的任务是根据网安人才能力测评过程中答题情况进行智能化动态出题, 并实时更新网安人才知识掌握状态; 能力评估子系统的任务是通过对比网安人才的答题情况进行对比分析, 判断网安人才的知识掌握情况, 并输出最终的能力评估结果。

4.2.1 预处理子系统

预处理子系统以网安人才的个人基本信息为输入, 输出其对 Web 安全方向的知识初始掌握情况, 该输出即为智能化测评子系统的输入。预处理子系统主要完成网安人才能力的预评估。

为了更准确地对网安人才进行初始评估, 在个人基本信息方面, 我们从多个维度对网安人才的个人信息进行收集, 尽可能设置了体现网安人才自身专业领域知识积累的多个内容项, 主要包括五大类: 网安人才的专业或者研究方向、工作岗位名称(如已经参加工作)、Web 安全认证证书获得情况、参加 CTF

比赛及是否获奖情况、参加网络安全攻防演练大赛及是否获奖情况。我们假设如果网安人才的专业、研究方向或工作岗位为 Web 安全、信息安全、网络空间安全相关的专业, 则 Web 安全的知识掌握概率应该更高; 如果网安人才拥有 Web 安全相关的认证证书、参加过 CTF 比赛或者网络安全攻防演练大赛, 其 Web 安全的知识掌握概率应该更高, 而且参加大赛获奖的名次越好, Web 安全知识掌握的概率越大。

表 3 个人基本信息部分项说明
Table 3 Basic personal information

个人基本信息部分项	说明
专业/研究方向	设置四个层次: Web 安全/信息安全/网络空间安全等 计算机相关专业 其他
工作岗位	设置三个层次: 渗透测试工程师 安全运营工程师/高级威胁分析工程师/信息安全专家(红队方向) 其他
Web 安全认证证书	设置两个层次: 信息安全专业人员-渗透测试工程师(CISP-PTE)、CEH(道德黑客) 其他或者无
CTF 比赛	设置四个层次: 特等奖、一等奖、二等奖、三等奖
网络安全攻防演练大赛	设置四个层次: 特等奖、一等奖、二等奖、三等奖

我们为不同的个人基本信息项及每项信息项的不同层次设置不同的权重值, 最终根据公式(1)计算网安人才的 Web 安全知识初始掌握概率 $P(L_0)$, 表示答题之前网安人才已经掌握该知识点的概率。如果网安人才在 Web 安全领域有着较为丰富的经历, 则其初始掌握概率较大。本文我们将该值统一设定为网安人才针对 18 个知识点及相关子知识点的初始掌握概率值, 不再做区分处理。

4.2.2 智能化测评子系统

智能化测评子系统以预处理子系统计算出的网安人才的初始知识掌握概率为输入, 并将其作为 CT-BKT 知识追踪模型参数 $P(L)$ 的初始值 $P(L_0)$ 。随后 CTIES 系统根据网安人才的答题情况动态出题进行测评, 直到测评结束。该子系统具体包括三项功能: 第一, 构建 Web 安全方向相关的知识点题库; 第二, 设计题库中题目与 Web 安全知识点的关联规则; 第三, 对网安人才进行智能化测评。

1) Web 安全方向相关知识点题库构建。根据 Web 安全方向的知识领域模型的子知识点进行题目设计, 具体地, 针对知识领域模型中第三层子知识点进行题目设计。本文我们共对 Web 安全方向下的 99 个第三层子知识点进行出题, 题目类型包括理论题(单选题)和 CTF 题。这里的子知识点不包括含“其他……”字样的子知识点。理论题目的考核内容针对单个子知识点进行题目设置, 针对 Web 安全方向下的每个知识点设置若干道与该知识点下的每个子知识点内容相关的题目。CTF 题考核的内容一般不仅仅涉及单个子知识点, 更多地是涉及多个子知识点。CTIES 的系统设置若干道 CTF 题目, CTF 题的考核内容的设置需要覆盖 Web 安全方向的所有子知识点。

2) 题目与 Web 安全知识点的关联规则设计。在构建好 Web 安全方向的知识领域模型并构建完 Web 安全方向相关子知识点的题库后, 需要对子知识点及包含该子知识点的题目进行关联解析。当网安人才通过 CTIES 系统进行能力测评时, 系统能即时从题库中挑选出相关考核子知识点的题目推荐给网安人才进行作答。

3) 智能化测评与推荐。为了对网安人才的知识状态进行追踪, CTIES 系统需要基于要考核的不同的知识点进行题目的推送, 并根据网安人才的答题情况进行推测, 动态更新网安人才的知识掌握概率。网安人才每完成一道习题后都需要立刻更新 CT-BKT 模型中网安人才对于相关子知识点的掌握情况信息, 具体如图 6 所示。这里需要注意的是, CT-BKT 模型中网安人才的 Web 安全方向各个子知识的初始掌握

概率由预处理子系统给出。

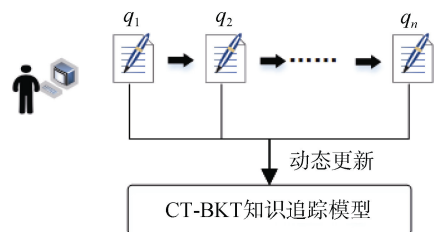


图 6 实时反馈的网安人才测评交互过程

Figure 6 Cybersecurity talents interaction with real-time feedback

如何利用较少的题目有效获得对 Web 安全方向知识领域模型中全部知识点及子知识点的合理评估是智能化测评与推荐算法要重点解决的问题。在该算法与网安人才测评答题互动的过程中, 网安人才每测评完成一道题目, 都只有正确、错误两个选项, 这意味着网安人才是否掌握题目相关子知识点及知识点的概率。Web 安全方向知识领域模型中各个知识点及子知识点之间相对独立, 所以当网安人才完成题目回答时, 只需要更新题目相关子知识点的掌握概率即可, 而不需要更新与该子知识点或知识点相关的其他知识点的掌握概率信息。

CTIES 系统测评的题目主要有两种类型: 理论题和 CTF 题。CTIES 系统先对网安人才进行理论题的测评, 待理论题测评结束后, 系统继续进行 CTF 题的测评。理论题和 CTF 题的测评规则说明如下:

a) **理论题:** 系统随机选择要测评的知识点, 然后顺序测评该知识点包含的子知识点, 直到 Web 安全方向的知识点全部测评结束。关于子知识点的测评, 系统会随机选择正在测评的知识点下的子知识点进行测评, 并依据题目与 Web 安全知识点的关联规则选取题库中相关子知识点的题目进行推荐测评。当子知识点的掌握概率大于某个阈值时, 则停止该子知识点的测评并继续下一个子知识点的测评。阈值用于判断网安人才是否真正掌握了相应 Web 安全方向的子知识点。当网安人才连续答错系统推荐的三道题目时, 我们认为其没有掌握该子知识点, 不再继续出题测评该子知识点。当子知识点测评结束后, 进入下一个知识点的测评; 如果 Web 安全方向所有的知识点都已测评结束, 则系统进入到 CTF 题目测评的阶段。

b) **CTF 题:** 系统随机选择覆盖要考核知识点的 CTF 题目推荐给网安人才进行测评。当正确解答出 CTF 题目时, 网安人才对于 CTF 题目关联的知识点的知识掌握概率提高; 否则, 网安人才对于 CTF 题

目关联的知识点的知识掌握概率降低。当网安人才结束当前的 CTF 题目测评时, 系统会根据网安人才的答题正确与否的情况自动更新 CT-BKT 知识追踪模型中相关知识点的掌握概率。同时, 系统会进入到下一道 CTF 题目的测评, 直到系统推荐的所有的 CTF 题目测评结束。

当 CTIES 系统对网安人才完成上述理论题和 CTF 题的推荐测评时, 系统得到了网安人才所有 Web 安全方向的知识点的掌握概率测评值。根据上述对 CTIES 系统智能化测评与推荐过程的讲述, 算法 1 给出了这部分功能的伪代码描述。

算法 1. 基于 CT-BKT 知识追踪模型和 Web 安全方向知识领域模型的智能化测评与推荐算法。

输入: CT-BKT 知识追踪模型、Web 安全方向知识领域模型、Web 安全方向知识点题库、题目与 Web 安全知识点的关联规则

输出: 所有 Web 安全方向知识点及子知识点的掌握概率测评值、CTIES 系统推荐的理论题和 CTF 题

```

1: CT-BKT 知识追踪模型中知识点的初始掌握
   概率赋值
2: FOR 知识点 IN Web 安全知识领域模型
   DO
3:   FOR 子知识点 IN 知识点 DO
4:     FOR 理论题 IN 理论题库 DO
5:       随机选择子知识点相关理论题进行测
   评
6:       动态更新 CT-BKT 知识追踪模型
7:       IF 连续回答错误次数  $\geq 3$  THEN
8:         BREAK
9:       ELSE IF 子知识点概率  $\geq$  阈值
   THEN
10:        BREAK
11:      END IF
12:    END IF
13:  END FOR
14: END FOR
15: END FOR
16: RETURN 所有 Web 安全方向知识点及子
   知识点的掌握概率测评值和 CTIES 系统推荐给网安
   人才测评的理论题
17:
18: FOR CTF 题 IN CTF 题库
19:   随机选择 CTF 题进行测评
20:   动态更新 CT-BKT 知识追踪模型
21: END FOR

```

22: RETURN 所有 Web 安全方向知识点及子知识点的掌握概率测评值和 CTIES 系统推荐给网安人才测评的 CTF 题

智能化测评子系统通过构建 Web 安全知识点题库, 并结合 Web 安全方向的知识领域模型, 建立 Web 安全知识点及子知识点与题目之间的关联, 并根据网安人员测评情况动态推荐题目, 最终完成对网安人才的能力测评, 获得网安人才 Web 安全方向所有知识点的掌握概率测评值, 即利用 CT-BKT 知识追踪模型进行追踪后的测评结果。通过对这些掌握概率测评值进行分析就能推断网安人才对 Web 安全方向的知识点的具体掌握情况, 实现对网安人才进行能力评估并选拔所需要的网安人才。

4.2.3 能力评估子系统

能力评估子系统以智能化测评子系统测评过程中产生的数据为输入, 包括 Web 安全方向知识点题库、网安人才的答题记录和网安人才所有 Web 安全方向知识点的掌握概率测评值, 通过对上述数据进行分析, 最终输出网安人才的 Web 安全方向的能力评估情况。该子系统的主要的功能是对网安人才能力进行评估及结果可视化, 具体包括测评数据采集及存储、测评行为数据分析和测评数据可视化。

测评数据采集及存储主要是收集记录网安人才测评过程中 CTIES 系统推荐的测评题目、网安人才解答题目正确与否情况以及 CT-BKT 模型追踪的网安人才知识的掌握概率, 并完成数据的汇总、存储、备份及安全等基本功能。

测评行为数据分析主要是读取存储的网安人才的测评数据, 并对这些数据进行进一步的数据挖掘, 计算和验证相关的统计规律, 最终能够追踪和评价每位测评的网安人才在 Web 安全方向的知识掌握程度, 实现网安人才的能力评估和预测。同时, 通过对不同网安人才的历史测评记录进行分析, 可验证测评系统 CTIES 的有效性并能及时调整题目推荐策略及推荐题库, 以便系统能更好地对网安人才进行能力评估。

测评数据可视化主要是处理测评行为数据分析产生的分析结果, 以可视化的方式展示网安人才的知识追踪过程以及能力评估结果。我们将 Web 安全方向的知识领域模型中的 18 个知识点归纳总结为六种专业技能以便更直观了解网安人才的能力水平, 六种专业技能分别为基础知识、前端安全、组件安全、后端安全、运维安全。各专业技能包含的 Web 安全知识点的情况如表 4 所示。

表 4 专业技能说明
Table 4 Professional skills

专业技能	Web 安全知识领域模型
基础知识	Web 安全基础、Web 安全工具使用
前端安全	跨站脚本攻击(XSS)、浏览器安全、客户端信息泄露、客户端劫持攻击
组件安全	CMS/Web 框架安全、数据库安全、反序列化
后端安全	Webshell、文件上传、文件包含、SQL 注入、跨站请求伪造(CSRF)
运维安全	Web 服务器运维、身份认证与访问控制、数据库安全、服务器端信息泄露

5 实验与分析

本章对 22 名网安人才进行了能力测评, 验证了本文提出的贝叶斯知识追踪模型 CT-BKT、基于 CT-BKT 知识追踪模型的智能化测评与推荐算法及网安人才技能智能化评估系统—CTIES 系统的可行

性和有效性。此外, 本章还讨论了 CTIES 系统存在的缺陷并提出下一步的改进方向。

5.1 实验设计

5.1.1 实验对象及数据集

本次实验共邀请 22 名网安人才使用 CTIES 系统答题, 通过网安人才对 CTIES 系统中设置的题目作答评估其 Web 安全方向的专业技能水平。实验收集系统记录的每名网安人才的答题情况作为要分析的数据集, 该数据集信息包括网安人才 ID、题目信息、题目类型、回答正确与错误情况、题目关联的知识点及子知识点等内容。具体的数据集结构如图 7 所示。其中, k 值为网安人才测评过程中针对某一子知识点进行作答的题目数量。CTIES 系统规定: 针对理论题, k 的取值为 $3 \leq k \leq 5$, 即每名网安人才每个子知识点的答题数量最多 5 道, 最少 3 道, 其中 1 道题目用于测试来验证 CT-BKT 知识追踪模型预测网安人才答题情况, 其他题目作为训练集。

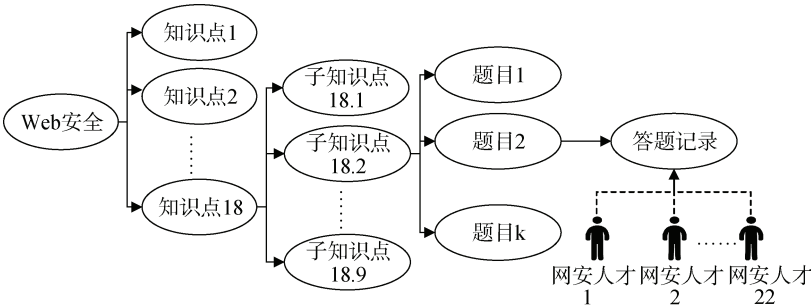


图 7 数据集结构图
Figure 7 Structure diagram of data set

5.1.2 题目设置

Web 安全方向的知识领域模型涉及的子知识点较多, 如果为每个子知识点设置 5 道理论题目, 题目数量较多; 且要设计出覆盖 Web 安全方向的所有知识点及子知识点的 CTF 题目, 需耗费大量的时间和精力。综合考虑测评时长、题目设置等多种因素, 为了验证本文提出的模型及算法, CTIES 系统的题目设置只针对部分子知识点详细设置题目。本次实验共设置 140 道题目, 题目设置情况说明如下:

1) 理论题: 针对第 18 个知识点“Web 安全基础”下的子知识点^[24], 我们对每个子知识点设置了 5 道题目; 其余 17 个知识点的子知识点各设置 1 道理论题。这里的子知识点不包括含“其他……”字样的子知识点。“Web 安全基础”下的子知识点情况详见表 5 所示。本次实验设置共计 135 道理论题。5.2 小节测评结果分析中主要针对“Web 安全基础”知识点及其子知识点进行分析。

表 5 Web 安全基础

Table 5 Knowledge base of Web security

序号	知识点	子知识点
1	Web 安全基础	HTTP/HTTPS 协议
2		Cookie/Session
3		同源策略
4		Web 编解码
5		Web 加解密
6		Web 编程基础
7		操作系统基础
8		数据库基础
9		社会工程学

2) CTF 题: 针对部分子知识点设置 CTF 题目, 每道 CTF 题目包含 1 个或者至多 3 个子知识点。本次实验共设置 5 道 CTF 题。CTF 题目设置情况如表 5 所示。

表 6 CTF 题目设置
Table 6 CTF items

序号	题目文本	涉及知识点(知识点: 子知识点)
1	who are you?	Web 安全工具使用: Burpsuite 使用 Web 安全基础: Cookie/Session
2	Hello World	Web 安全基础: Web 编解码 服务器端信息泄露: Git 信息泄露
3	SQL 注入 2	SQL 注入: 联合查询注入 服务器端信息泄露: 源码泄露
4	文件包含	文件包含: 本地文件包含 Web 安全基础: Web 编解码
5	COOKIE	Web 安全基础: Cookie/Session

5.2 测评结果分析

本小节通过对评估系统收集的网安人才答题情况的数据集进行分析, 从知识追踪模型结果比较、网安人才知识掌握情况及网安人才能力评估等方面对本文提出的模型、算法及系统进行分析与效果验证。

5.2.1 知识追踪模型结果比较

我们将本文提出的 CT-BKT 知识追踪模型与标准贝叶斯知识追踪模型 BKT 进行模型结果比较。CTIES 系统以网安人才理论题停止答题后的 1 道理论题目的答题情况作为测试, 其余题目的答题情况用作训练知识追踪模型。根据训练好的知识追踪模型计算出网安人才测试题目做对的概率, 然后进行二值映射, 将预测值与真实数据进行对比验证模型的有效性。实验选取准确率、AUC(Area Under Curve)、F1-Score 这三个常用的模型评价指标对模型进行对比分析。

1) 准确率: 准确率是指数据集中正确预测的样本数与总样本数之比, 准确率取值范围为 0-1。准确率的值越高, 表明模型的效果越好。“Web 安全基础”知识点下的 9 个子知识点的两种模型的准确率情况如图 8 所示。

从图 8 可以看出, 本文提出的 CT-BKT 知识追踪模型的各个子知识点的准确率不低于 BKT 的准确率, 第 2、3、5 个子知识点的准确率有了较高的提升, 总体上来说, CT-BKT 模型的效果更优。因此, 我们可以使用贝叶斯知识追踪来评估网安人才的知识掌握水平, 而且本文在标准 BKT 模型基础上提出的 CT-BKT 模型效果更佳。

2) AUC: AUC 用于直观地评价模型中分类器的效果, 在 CT-BKT 模型中体现在对于用户答题情况的预测效果。AUC 是 ROC 曲线(横坐标为伪阳性率 FPR、纵坐标为真阳性率 TPR)下与坐标轴围成的面积大小。AUC 的取值范围为 0.5 和 1 之间, 当 AUC 值为 0.5 时, 说明模型的分类效果与随机分类器的效

果相同, 也就是说, 模型是没有意义的; 当 AUC 的值越接近 1 时, 说明模型的分类效果越优。两种模型的 AUC 值情况如图 9 所示。

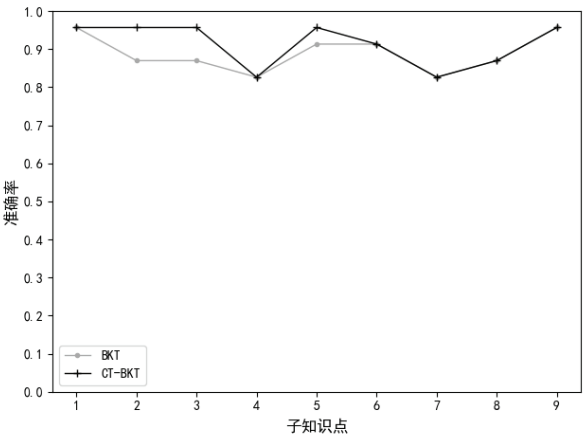


图 8 两种模型预测准确率比较图

Figure 8 Accuracy comparison chart of two models

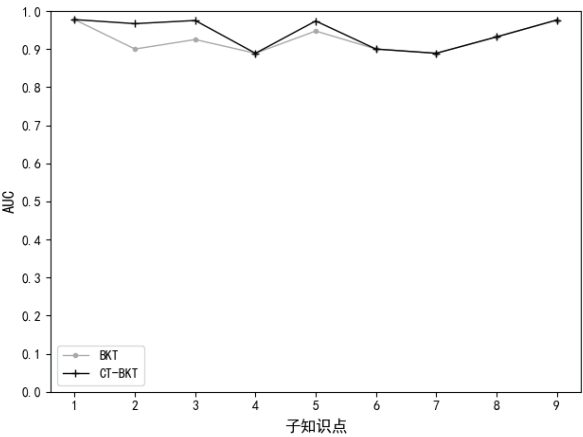


图 9 两种模型 AUC 比较图

Figure 9 AUC comparison chart of two models

从图 9 可以看出, CT-BKT 模型和 BKT 模型在训练过程中, CS-BKT 模型的 AUC 值总体高于标准贝叶斯追踪模型的值, 因此, 本文提出的 CT-BKT 模型的预测能力更好, 效果更优。

3) F1-Score: F1-Score 综合考虑了模型的精确率(查准率)和召回率(查全率), 通过对两者加权调和平均, 在尽可能的提高两者取值的同时, 也使得两者之间的差异尽可能小。F1-Score 的值越大说明模型质量更高。两种模型的 F1-Score 情况如图 10 所示。

由图 10 可以看出, CT-BKT 模型和 BKT 模型在训练过程中, CS-BKT 模型的 F1-Score 值总体高于 BKT 模型, 因此 CS-BKT 模型的拟合程度更优, 模型训练效果更好。

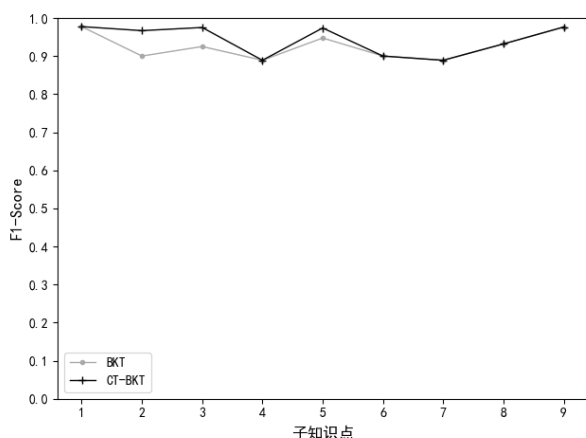


图 10 两种模型 F1-Score 比较图

Figure 10 F1-Score comparison chart of two models

5.2.2 网安人才技能评估

通过使用 CT-BKT 知识追踪模型, CTIES 系统可以根据网安人才的题目作答情况来追踪网安人才 Web 安全方向的知识点的掌握情况。本小节通过选取其中一名网安人才的测评结果进行分析, 一方面用于阐述本文的核心思想及 CTIES 系统的测评过程, 另外一方面展现该系统的人才能力评估效果, 包括

网安人才的知识掌握情况以及人才技能评估情况。选取的该名网安人才的初始知识掌握概率 $P(L_0)$ 为 0.0731707, 其本人专业方向为 Web 安全, 没有获得信息安全相关证书、也未参加过 CTF 竞赛和网络安全攻防演练, 该名网安人才的专业领域的知识积累较少, 所以初始知识掌握概率较低。完成 CTIES 系统测评后, 我们可以看到该名网安人才针对“Web 安全基础”知识点理论题的答题情况如表 7 所示。表 7 中测试题为理论题停止答题后的 1 道理论题。

从表 7 可以看到, 该名网安人才共答题 33 道, 其中子知识点“HTTP/HTTPS 协议”、“Web 编解码”“数据库基础”分别答题 3 道, 当该名网安人才这 3 个子知识点的掌握概率较高时, 系统认为该名网安人才已掌握相关的子知识点, 系统便停止出题(这里, 我们设置知识掌握概率的阈值为 0.7); 而其他子知识点答题 4 道。我们可以看到, 针对该名网安人才当前题目的答题情况, CTIES 系统可进行智能化动态出题, 而且系统可以以较少的题目更精准评估网安人才的知识掌握水平, 实现网安人才技能的智能化评估。关于测试题目, 系统共预测该名网安人才答对题目 7 道(共 9 道), 准确率较高。

表 7 某名网安人才“Web 安全基础”答题情况

Table 7 Cybersecurity talent's performance of knowledge base of Web security

序号	知识点	子知识点	题目作答数量(不包含测试题)	测试题的预测情况	测试题的真实答题情况
1	Web 安全基础	HTTP/HTTPS 协议	3	1	1
2		Cookie/Session	4	1	1
3		同源策略	4	1	1
4		Web 编解码	3	1	0
5		Web 加解密	4	1	1
6		Web 编程基础	4	1	1
7		操作系统基础	4	0	1
8		数据库基础	3	1	1
9		社会工程学	4	1	1

同时, 我们可以更直观地了解到该名网安人才“Web 安全基础”方向的知识点的掌握概率情况, 如图 11 所示。

从图 11 可以看出, 除了子知识点 7“操作系统基础”外, 该名网安人才的其他“Web 安全基础”子知识点的掌握概率较高, 特别是“同源策略”、“社会工程学”两个子知识点的掌握良好; 而在“操作系统基础”方面的知识掌握水平一般。具体地, 我们将网安人才的知识掌握情况按照基础知识、前端安全、

组件安全、后端安全、运维安全六种专业技能(4.2.3 章节提及)来进行归类展现, 以更直观地了解网安人才的技能水平。具体如图 12 所示。

从图 12 可以看出, 该名网安人才在 Web 安全基础知识方面技能较好, 也就是说在 Web 安全基础和 Web 安全工具的使用两个方面的知识掌握程度较好。其他知识点的效果展现不是很好。除第 18 个知识点“Web 安全基础”外, 其余知识点的设置题目较少。本文将一道题的答题正确与否来代表子知识点的掌

握程度,效果显然是不好的。

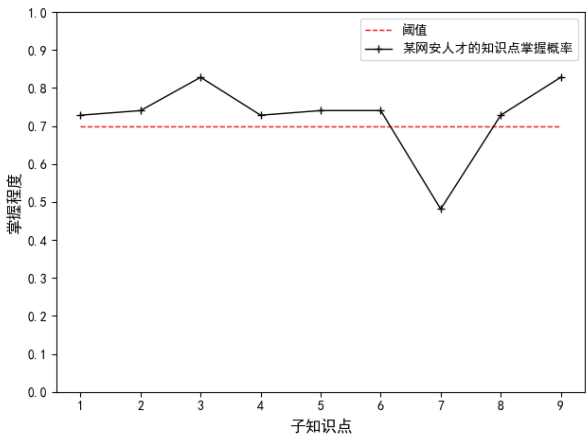


图 11 网安人才的知识点掌握概率情况图

Figure 11 Cybersecurity talent’s knowledge mastery probability chart

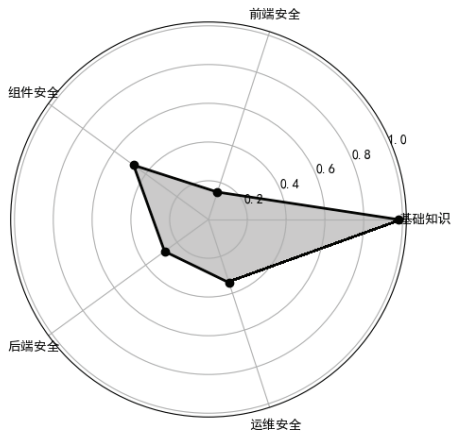


图 12 网安人才专业技能图

Figure 12 Cybersecurity talent’s skills chart

通过网安人才能力智能化评估系统 CTIES 系统,可以更加细致地了解网安人才的 Web 安全方向的知识掌握情况,为网安人才的培养和选拔提供依据。

5.3 缺陷分析

本文研究探讨了基于贝叶斯知识追踪的网安人才能力智能化评估方法,构建了可实现网安人才知识状态追踪的 CT-BKT 知识追踪模型,并在此基础上实现了网安人才技能智能化评估系统—CTIES 系统。虽然本文实验验证了模型的有效性,但是本文的工作仍然有较大的改进空间,具体体现在:题目设置方面,CTF 题目的设置未全部覆盖“Web 安全基础”知识点的子知识点,不能充分训练模型并完全体现网安人才“Web 安全基础”的知识掌握状态;系统设置涉及多个知识点的 CTF 题目,CTF 题目的答题情况将同步更新所有子知识点的掌

握概率,这与真实情况存在一定偏差,网安人才可能掌握部分子知识点,但因未掌握部分子知识点导致 CTF 题目回答错误;实操题目前主要是 CTF 的解题模式题目,在培养和选拔实战型网安人才方面有一定局限性;题目设置的数量和质量对模型的效果有一定的影响。针对上述缺陷,本文未来将对提出的 CT-BKT 模型、智能化评测与推荐算法及相应的 CTIES 系统做进一步的优化完善,提高评估方法对网安人才能力评估的准确性。

6 结束语

网络空间安全形势日趋严峻,网安人才缺口大,而网安人才评价手段有限,如何对网安人才能力进行评估实现网安人才的培养和选拔,以满足当前网安人才的迫切需求成为当务之急。本文对网安人才能力的评估方法进行了深入研究,借鉴智适应学习系统中的知识追踪方法对网安人才的知识掌握状态进行追踪,对较为流行的贝叶斯知识追踪模型进行改进,构建了面向网安人才的 CT-BKT 知识追踪模型用来对网安人才的知识掌握状态进行追踪。同时,本文提出了智能化测评与推荐算法,以期用更少的题目考核获得网安人才知识的掌握情况。基于所提出的知识追踪模型和测评算法,本文实现了面向网安人才的技能智能化评估系统—CTIES 系统。本文梳理了 Web 安全方向的知识领域模型并构建了相应题库,并邀请 22 名网安人才进行答题测评。结果表明,改进后的 CT-BKT 知识追踪模型能较好地体现网安人才在 Web 安全方向的知识掌握状态,而且相比较于标准贝叶斯知识追踪模型,本文提出的 CT-BKT 模型效果更优。同时,我们选取一名网安人才的评测结果进行具体分析,可以看出 CTIES 系统能实现网安人才的智能化评估,而且能直观地展现网安人才 Web 安全方向各知识点的知识掌握及专业技能情况。实验部分验证了本文所提出的网安人才能力评估方法的可行性和有效性。

本文提出了一种网安人才能力评估方法,为网安人才的培养和选拔提供了一种评价手段。虽然本文只是针对 Web 安全方向的网安人才能力进行评估,但所设计的模型、系统和方法,也可以扩展到二进制、密码学、移动安全、取证分析等技能评估。

通过本文提出的网安人才能力评估方法,可以更加细致地了解网安人才的知识掌握情况,为网安人才的培养和选拔提供参考,该方法可以用于多个场景:

- 1) 网安人才日常培养:网安人才可以通过该方

法了解到自身的学科专业的知识掌握情况, 从而及时查缺补漏, 提高学习效率; 教师可以更好地掌握学生的知识学习状态, 及时根据学生的知识掌握情况调整教学内容, 并对没有达到学习要求的学生进行针对性地指导。

2) 网安人才选拔: 该方法可用于 Web 安全或其他技能的专业认证, 也可用于企事业单位考核选拔适合相关岗位的网安人才。根据不同的技能及岗位需求考察的侧重点不同, 构建相应的知识领域模型, 在此基础上设置相关专业知识的题库, 更好地完成相关专业方向认证或岗位网安人才选拔, 弥补已有网安人才能力评估方法的不足。

参考文献

- [1] 中国信息安全从业人员现状调研报告(2018-2019 年度). 中国信息安全测评中心. <http://www.itsec.gov.cn/zxxw/201909/P020190906557330247920.pdf>. 2019.9.6.
- [2] Yan Y Y, Yang X D, Ma Z Y, et al. The Thinking on building Talent Team of Cybersecurity[J]. *China Management Informationization*, 2019, 22(15): 183-184.
(闫育芸, 杨向东, 马卓元, 等. 网络安全视域下我国人才队伍建设的思考[J]. *中国管理信息化*, 2019, 22(15): 183-184.)
- [3] 奇安信, 智联招聘. 2019 网络安全人才市场状况研究报告. <https://cloud.tencent.com/developer/news/430267>. 2019.7.
- [4] Qi B J, Tan L. The Cultivation Mechanism and Enlightenment of Cybersecurity Talents in the World's Network Power[J]. *Civil-Military Integration on Cyberspace*, 2019(12): 58-60.
(齐保军, 谭磊. 世界网络强国网安人才培养机制及启示[J]. *网信军民融合*, 2019(12): 58-60.)
- [5] 奇安信, 智联招聘. 2020 网络安全人才市场状况研究报告. <https://shs3.b.qianxin.com/qax/98892b1e0524f24851a7f1dd623e93d5.pdf>. 2020.8.16
- [6] (ISC)². Strategies for Building and Growing Strong Cybersecurity Teams. <https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482>.
- [7] Wei H. The Considerations on the Status of Cybersecurity Team Construction in China[J]. *China Information Security*, 2018(2): 80-82.
(位华. 我国网络安全人才队伍建设现状及思考[J]. *中国信息安全*, 2018(2): 80-82.)
- [8] CTFtime.org / All about CTF (Capture The Flag). <https://ctftime.org/event/list>.
- [9] CTFtime.org / All about CTF (Capture The Flag). <https://ctftime.org/stats/>.
- [10] Zhuge Jianwei. The current situation of Cyberspace Security Skills Competitions in China[J]. *Communications of the China Computer Federation*. 2016(6).
(诸葛建伟. 我国网络空间安全技能竞赛现状漫谈[J]. *中国计算机学会通讯*. 2016(6).)
- [11] Congfei Jia. The Research on Cyberspace Security & Countermeasures Simulation Methods [D]. Beijing Institute of Technology, 2016.
- [12] 崔翔, 方滨兴, 林建宝等. 一种泛 ctf 网络安全人才培养系统以及基于此系统的出题方法和做题方法. CN108898903A. <https://patentimages.storage.googleapis.com/2f/cf/c9/f1c3eddf0d63f/CN108898903A.pdf>.
- [13] Zhang H L, Yu H N, Fang B X, et al. Research on the Architecture of Cyberspace Security Professional Certification in China[J]. *中国工程科学*, 2016, 18(6): 44-48.
(张宏莉, 于海宁, 方滨兴, 等. 我国网络空间安全职业资格认证体系研究[J]. *中国工程科学*, 2016, 18(6): 44-48.)
- [14] (ISC)². <https://www.isc2.org/>.
- [15] ISACA. <https://www.isaca.org/Pages/default.aspx>.
- [16] EC-Council. <https://www.eccouncil.org/>.
- [17] CompTIA. <http://www.comptia.org/>.
- [18] 中国信息安全测评中心. <http://www.itsec.gov.cn/ryzc/>.
- [19] Liu H Y, Zhang T C, Wu P W, et al. A Review of Knowledge Tracking[J]. *Journal of East China Normal University (Natural Science)*, 2019(5): 1-15.
(刘恒宇, 张天成, 武培文, 等. 知识追踪综述[J]. *华东师范大学学报(自然科学版)*, 2019(5): 1-15.)
- [20] Corbett A T, Anderson J R. Knowledge Tracing: Modeling the Acquisition of Procedural Knowledge[J]. *User Modelling and User-Adapted Interaction*, 1995, 4(4): 253-278.
- [21] Yudelson M V, Koedinger K R, Gordon G J. Individualized Bayesian Knowledge Tracing Models[M]. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013: 171-180.
- [22] Deloitte and Chinese Association of Automation Wisdom Education Committee. <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-global-development-of-ai-based-education-zh-191108.pdf>. Nov, 2019.
- [23] Ling chen. The Design and Implementation of Intelligent Adaptive Learning System Based on Knowledge Tracking [D]. Dalian University of Technology, 2019.
- [24] 中国网络空间安全人才教育联盟. 网络空间安全工程技术人才培养体系指南. <https://www.cncstea.cn/announces/4173.html>. 2019.1.11.
- [25] Zhang Mingxin. Improvement and Application of Bayesian Knowledge Tracing Model Based on Cognitive Diagnosis—Taking

Primary School Mathematics as an Example[D]. East China Normal University, 2019.



张方娇 于2014年在北京邮电大学计算机与科学技术专业获得硕士学位。现任中国科学院信息工程研究所助理研究员。主要研究方向为网络攻防技术、网安人才能力评估。Email: zhangfangjiao@iie.ac.cn



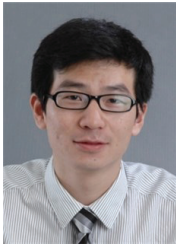
赵建军 于2016年在兰州理工大学通信与信息系统专业获得硕士学位。现在中国科学院大学网络空间安全专业攻读博士学位。研究领域为 Web 安全和口令安全。Email: zhaojianjun@iie.ac.cn



刘心宇 于2019年在安徽大学信息安全专业获得学士学位。现在中国科学院大学网络空间安全专业攻读博士学位。研究领域为 Web 安全。Email: liuxinyu@iie.ac.cn



王晓蕾 于2019年在西安电子科技大学信息安全专业获得学士学位。现在中国科学院大学网络空间安全专业攻读硕士学位。研究领域为 Web 安全。Email: wangxiaolei@iie.ac.cn



刘奇旭 于2011年在中国科学院研究生院信息安全专业获得博士学位。现任中国科学院信息工程研究所副研究员、中国科学院大学网络空间安全学院副教授。主要研究方向为网络攻防技术、网络安全评测。Email: liuqixu@iie.ac.cn



崔翔 于2012年在中国科学院计算技术研究所信息安全专业获得博士学位。现任广州大学网络空间先进技术研究院研究员。研究领域为网络攻防技术。Email: cuixiang@iie.ac.cn