

从书本到现实—网络安全人才的提前蝶变

专业学位类别： 电子信息

适用课程： 网络安全

作者姓名： 李晖¹、杨晓明²、李兴华¹、卢列文²、
李红宁¹、李帅²

工作单位： ¹西安电子科技大学

²工业和信息化部电子第五研究所

中国专业学位案例中心

2024 年 8 月 25 日

案例正文

从书本到现实—网络安全人才的提前蝶变

李晖¹ 杨晓明² 李兴华¹ 卢列文² 李红宁¹ 李帅²

摘 要：数字化转型背景下，网络安全人才培养与市场需求之间存在严重脱节。本文以校企合作为背景，从密评开始，确保理论与实践的无缝对接；通过工控漏洞挖掘，强化实战能力，有效识别和应对网络安全威胁；同时，构建防御阵线，培养具备实战经验的网络安全防御人才。本文深度整合优质资源平台，确保学术界和产业界的双重指导。此外，通过揭榜挂帅和深度实践，激发创新精神和实践能力，旨在完成网络安全人才的提前蝶变，培养一批具有创新思维和实战经验的新质生产力。

Abstract: In the context of digital transformation, a significant gap persists between cybersecurity talent training and market demand. Based on the College-Enterprise Cooperation, this paper starts from Commercial Cryptography Application Security Evaluation to ensure the seamless connection between theoretical knowledge and practical skills. By mining industrial control vulnerabilities and enhancing practical capabilities, we can effectively identify and respond to network security threats. At the same time, building a defense front and cultivating cybersecurity defense talents with practical experience. This paper deeply integrates high-quality resources and platforms to ensure dual guidance from academia and industry. In addition, through the unveiling of the list and in-depth practical projects, to stimulate the spirit of innovation and practical ability, aimed at achieving the early transformation and cultivating a group of new quality productive forces with innovative thinking and practical experience for the field of network security.

关键词：数字化转型、密评、网络安全

KeyWords: digital transformation、Commercial Cryptography Application Security Evaluation、cybersecurity

* (1)本案例系教育部学位与研究生教育发展中心 2024 年度工程案例项目成果(项目名称：筑牢国家安全技术底座，培育网络安全教学新质生产力；项目编号：GC-241070105；首席专家：李晖)。

(2)本案例复制权、发表权、信息网络传播权等相关权益由教育部学位与研究生教育发展中心依法享有，如有相关需要，请取得教育部学位与研究生教育发展中心授权。

(3)本案例只供课堂讨论之用，并无意暗示或说明某种行为是否有效。

作者信息：李晖，西安电子科技大学网络与信息安全学院教授，执行院长；杨晓明，工业和信息化部电子第五研究所软件与系统研究院，院长；李兴华，西安电子科技大学网络与信息安全学院教授，副院长；卢列文，工业和信息化部电子第五研究所软件与系统研究院，副院长；李红宁，西安电子科技大学广州研究院，副教授；李帅，工业和信息化部电子第五研究所数据治理服务中心，副主任。

引言

在数字化转型浪潮的推动下，网络空间安全作为国家安全的重要基石，其战略地位已上升至前所未有的高度。网络攻击的频发与复杂化要求我们具备更强的防御能力和技术储备，而核心在于培养具备创新能力与实战经验的高端网络安全人才。为响应国家发展战略，西安电子科技大学携手工信部电子五所，积极探索网络安全卓越工程师的创新培养模式，以期在教育与实践的深度融合中实现人才培养质量的全面提升。

1. 工程项目背景及现状

随着信息技术的飞速发展，网络攻防技术呈现快速迭代的态势，攻击手段日益复杂、隐蔽性增强、影响范围扩大，这使得网络安全已成为社会各界关注的焦点。这无疑加剧了对网络安全专业人才的迫切需求。然而，目前网络安全人才的培养与市场的实际需求之间存在一定的差距，传统教育体系普遍存在“重理论、轻实践”的问题，导致毕业生在实际工作中难以快速适应行业需求。鉴于此，培养具有创新精神和实践能力的网络安全精英，实现卓越工程师教育与实践的完美融合，已成为我们亟待解决的首要任务。

本案例聚焦于网络空间安全领域，以密码学的理论精髓与实践应用为起点，逐步拓展至漏洞挖掘与网络攻防技术的深层探索，形成了系统化的校企合作培养模式。我们致力于通过合理的教育过渡搭建一座桥梁，无缝衔接教育供给与市场需求。在这一培养过程中，我们通过理论与实践的精准结合，以及多方资源的深度整合，深入洞察社会的实际需求，运用前沿的科技力量，旨在全面提升学生的综合能力和职业素养，打造以实战为导向的网络安全工程教育体系，期望达成高校、学生与企业三方的和谐共赢，实现效益的最大化平衡与优化。

1.1 密码学：理论到实践的桥梁

密码学技术不仅是网络空间安全的基石，更是其核心支撑。在当前地缘政治紧张局势加剧和意识形态对立不断升级的国际背景下，国际安全形势的不稳定性

日益凸显，治理风险随之上升。密码学技术在维护国家机密、军事战略、经济政策、外交活动等敏感信息的安全方面扮演着至关重要的角色，是信息安全防护体系中至关重要的一环。当前，以5G、大数据、云计算和物联网为代表的新兴技术加速发展，推动社会进入全面数字化转型阶段，但与此同时也带来了空前复杂的网络安全挑战。而密码学技术为这些系统和新技术提供了坚实的安全保障，其应用已成为应对数字时代安全威胁的核心手段。然而，在密码学教育过程中，往往存在重理论、轻实践的倾向，导致学生对密码技术在现实场景中的应用理解不足，实践经验匮乏，难以在解决实际问题时充分发挥专业能力。理论研究的深度与广度无疑为密码学技术奠定了坚实基础，但仅停留于理论层面的学习无法满足实际需求，只有将这些理论通过实践检验并应用于实际场景，才能真正发挥其价值，解决现实世界中的安全问题。实践不仅是检验理论的试金石，更是推动理论创新与技术发展的重要驱动力。通过实践，我们可以加深对理论知识的认识，在掌握技术细节的同时提升问题解决能力，让学生深刻体会学以致用道理，并且能够发现理论的不足，进一步优化和完善，形成理论与实践相互促进的良性循环。为此，构建以实践为导向的密码学教学模式势在必行。在教育过程中，需通过引入真实案例和模拟实验环境，帮助学生将理论与应用场景有效结合。只有在理论与实践的深度融合中，才能培养出适应复杂安全形势、具备创新能力和实战技能的网络空间安全专业人才，为应对未来挑战提供强有力的技术保障与人才支撑。

1.2 工控与物联网漏洞挖掘：实战技术的提升

数字化时代的快速发展伴随着工业控制设备（工控）和物联网设备数量的爆发式增长。这些设备在数据处理与传输、精确控制任务执行等方面承担了重要角色，其安全性直接关系到关键基础设施的稳定运行和社会经济的可持续发展。设备数量的激增意味着潜在的安全漏洞和攻击面也随之扩大，使得网络安全威胁日益复杂化、多样化。工控设备和物联网设备通常运行于高度复杂的网络环境中，面临着来自多方面的安全挑战，攻击手段的隐蔽性和多样性不断提高，从传统的漏洞利用到高级持续性威胁（APT）攻击，威胁的演变速度对现有安全防护体系提出了严峻考验。这种动态且复杂的安全环境要求我们必须持续优化安全防护措施，通过技术手段的创新应对不断升级的威胁。随着技术的发展，工控和物联网设备正逐步向智能化和自动化方向演进，它们需要处理的数据量和种类也在不断增加，从而进一步增加了安全管理的复杂性。在此背景下漏洞挖掘技术已成为提升设备安全性的关键途径。通过漏洞挖掘，能够有效识别系统中潜在的安全缺陷，并及时采取修复措施，不仅可以显著增强系统的整体安全性，还能够预防恶意攻击，减少由安全事件导致的经济和社会损失。此外，漏洞修复的及时性和有效性

对于节约运营成本、保护关键基础设施、维护数据完整性以及确保业务连续性具有重要意义。在智能化设备不断普及的趋势下，漏洞挖掘技术的应用还能够提升用户体验，增强信任感和满意度，为构建更加稳健的网络安全生态提供保障。因此，在工控与物联网领域，加强漏洞挖掘能力的培养与研究具有重要的战略意义。通过构建系统化的漏洞分析和修复机制，并结合先进的防护技术，我们可以更高效地应对复杂多变的安全威胁，为数字化时代的安全发展奠定坚实基础。 ，

1.3 网络安全：防御阵线的构筑与加固

随着万物互联的愿景逐步成为现实，网络安全的复杂性也随之增加。攻防对抗的动态性和激烈程度也与日俱增，每天都有新的攻击手段和防御技术涌现，攻防双方的博弈在全球范围内持续演变。 ，无论是在国际还是国内舞台上，针对关键基础设施的网络攻击事件屡见不鲜，这些攻击可能导致电力中断、航运停摆、交通瘫痪，甚至导致系统全面崩溃和功能丧失，严重威胁国家安全与社会秩序。事实上，网络战已经从理论研究阶段进入实质性对抗层面，成为现代战争的重要组成部分。权威统计数据揭示了一个严峻的现实：高校、科研院所、政府机构以及军事部门等关键行业领域正面临着日益密集的网络攻击，这些攻击威胁到了数据安全、关键信息基础设施的稳固以及人工智能的安全性。在这种复杂且高度动态的网络安全新局面下，迫切需要培养一批具备实战能力和创新精神的高水平网络安全技术人才。他们将作为“数字化堡垒”的守护者，为国家和社会构筑起坚不可摧的安全屏障。因此，加速网络安全实战型防御人才的实践教学创新与改革变得尤为迫切。

为有效应对前述挑战，高等教育机构与产业界的紧密合作至关重要。西安电子科技大学作为国内网络空间安全专业人才培养的领军者，凭借卓越工程师教育经验，率先探索校企深度融合的人才培养模式。工信部电子五所，作为国家首批商用密码应用安全性测评机构之一，在网络安全评估领域积累了丰富经验，已在全国范围内对多个省的政府机关、事业单位、电力企业等进行了商用密码应用安全性评估。基于双方的优势资源，西安电子科技大学与工信部电子五所携手共建网络安全人才培养基地，提出了“教育供给侧改革”与“产业需求侧引导”相结合的培养理念。通过实施双导师制度，项目驱动教学，双方以产业需求为核心导向，面向密码技术测评、工控与物联网安全、网络攻防等前沿领域展开实践教学创新。

这一合作模式以高校的研究能力为理论支撑，以企业的应用场景为实践平台，力求在解决实际问题的过程中挖掘技术潜力，为学生提供全方位的培养路径。学生不仅能够参与真实项目，学习先进技术，还能从高校导师与企业导师的双重指

导中获得多维度的成长。最终，这一模式将为社会输送一批兼具理论深度与实践能力、创新意识与实战经验的高素质网络安全专业人才，为国家的数字化转型与网络安全战略提供重要支撑。

2.工程的实施过程

本案例紧密结合当前研究生培养目标与企业实际需求，在实施过程中注重实现课堂教学与实践训练的深度融合，确保理论学习与实战能力的同步提升。通过将课堂与实践无缝对接、将实习与科研有效并行、推动论文成果与项目进展相辅相成，逐步构建起西安电子科技大学与工信部电子五所之间的深度校企合作人才培养体系。案例以密码应用安全评估为起点，逐步延伸至漏洞挖掘及防御体系的构建，形成了一条从基础理论到实际应用的系统性实践路径。这一培养模式不仅涵盖了密码技术应用的核心知识，还将网络攻防实战能力的培养纳入整个教学体系，为学生提供了从技术细节到系统设计的全面学习体验。具体实施流程如图1所示。

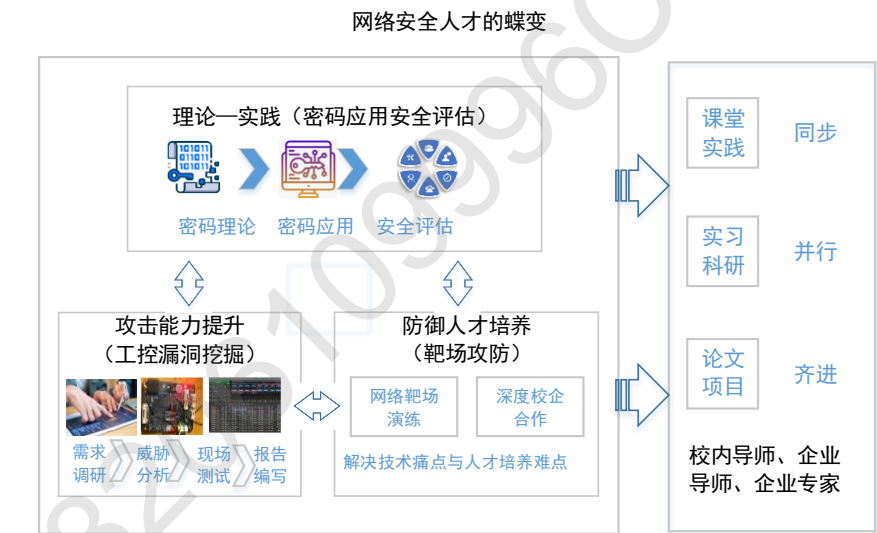


图1 网络安全新质生产力培养

整个实施过程分为多个阶段，包括案例选择、课程设计与优化、任务揭榜挂帅、企业实习实践以及总结反馈与评估等环节。通过多阶段、系统化的实施路径，本案例实现了从理论到实践、从课堂到企业、从个人成长到团队协作的全方位提升，为网络安全领域的高端人才培养探索出了一条行之有效的创新模式。

案例选择：首先，工信部电子五所作为国内商用密码应用安全性评估的领军机构，不仅自主研发了包括IPSec、SSL、SSH协议分析器在内的一系列分析工具，还配备了全面的检测设备，致力于解决密码应用评估中的实际挑战。其次，电子

五所在网络安全领域承担了多项重要研究项目，建立了漏洞挖掘与反制平台，具备针对工控设备、物联网设备、基础软件的漏洞挖掘基础，并自主研制出基于GAN的未知协议fuzz工具、大规模软件并行fuzz工具和BinEmu固件仿真调试框架等漏洞挖掘工具。此外，电子五所定制开发的网络安全实训靶场、网络安全攻防演练靶场，可为培育具备解决问题能力的创新型实战人才提供良好的平台保障。基于此，我们从卓越工程师培养开始，逐步实现理论与实践的过度，提升实战能力和加固防御力量的培养，选择对云上应用仿真系统的密评、IoT类目标漏洞挖掘、防御型人才培养为典型，进行深度融合的人才培养。

课程设计与优化：校内讲师与企业导师通力合作，共同制定课程大纲与框架，将实际案例贯穿于课程的各个教学环节，确保案例教学与理论讲解无缝衔接、相辅相成。通过将企业需求和学术前沿相结合，使课程内容既具有理论深度又具备实战导向。此外，根据课堂反馈与效果检测，采用以学生为中心的教学优化机制，鼓励学生以“主人公”的身份深度参与课程内容和教学方法的改进，不断迭代优化课程设计，从而提升学习效果和各方满意度。

揭榜挂帅：针对企业实际需求，汇集形成系统化的需求文档，并在课堂上发布任务清单。参与学生与指导教师通过案例分析、需求评估等环节明确任务目标，鼓励学生主动揭榜挂帅，激发学习兴趣与竞争意识。在这一过程中，校内导师与企业导师全程参与指导与把控，通过阶段性评估与专家反馈进一步完善任务目标，确保任务执行的科学性与达成度。该环节不仅强化了学生的独立研究能力，还培养了其在团队协作中解决复杂问题的意识与能力。

实习实践：在课堂学习的基础上，通过导师引导，将案例教学与实习实践有机结合。学生根据自身兴趣和专业基础，与电子五所进行双向选择后参与企业实践。在真实的工作环境中，学生能够将课堂所学的理论知识和技能应用到实际任务中，通过完成企业实际需求中的关键任务，显著提升实践能力、问题解决能力和职业素养。企业实践为学生提供了深度接触行业应用的宝贵机会，同时也为企业贡献了新的技术视角和解决方案。

总结反馈：通过贯穿全程的案例学习、揭榜挂帅和实习实践，综合分析每位学生与讲师的教学参与表现，为其建立全面的能力画像。基于画像结果，对案例课程设计和教学效果进行评估，并将反馈融入到课程优化和环节改进中，为后续教学提供科学依据。最终，这一闭环式改进流程不仅确保了教学质量的持续提升，也为培养具有创新能力和实战经验的研究生奠定了坚实基础。

通过上述环节的全面实施，不仅激发了学生的创新思维和解决问题的能力，还进一步加强了学术研究与企业实践之间的紧密结合，有效推动了知识的转化和

实际应用。为学生提供了宝贵的实践机会，提升了其就业竞争力，同时也为企业解决了实际问题，形成了校企合作、互利共赢的良性循环。

3.工程方案分析论证

3.1 密码应用安全评估

在熟悉掌握密码基本理论的前提下，学生通过云上应用仿真系统（如图2所示）开展密码应用安全评估实践。典型密评场景涵盖检测工具和方法的应用、网络通信协议分析、配置检查、数字签名验证等关键环节，系统学习云上应用中密码安全性评估的知识要点。通过这一过程，学生不仅能够熟悉常见云上应用的密码检测与评估方法，还能培养解决密码应用实际问题的思维能力与动手实践能力。基于人工智能的计算方法优势，探索机器学习、深度学习等技术在密码算法、协议分析，以及密评实践、密码安全攻防中的应用。例如，通过利用AI技术提升密码算法和协议分析的效率与精度，有助于优化密码安全评估流程。同时，在实践中引入基于AI的分组密码算法结构识别，培养学生对密码算法的分析能力，增强其在密码攻防场景中的技术优势。这一整合人工智能与密码学的教学方法，不仅丰富了教学内容，还提升了学生的实践操作水平和创新能力。

在密评案例实施时，首先，在**测评准备阶段和方案确定阶段**，通过课堂介绍密码应用安全性评估的实施流程、被测系统密码应用情况、检测工具、测评对象等，引导学生根据已经了解到的系统情况，分析被测系统以及相关的密码应用，利用智慧教室实施分组研讨，确定本次测评的测评对象和检测工具接入点，形成可行的测评方案。利用工业和信息化部电子第五研究的信息编码算法应用公共服务平台，搭建各类密评案例的模拟仿真环境，利用商用密码设备搭建实验环境验证解决方案和支撑现场数据分析。

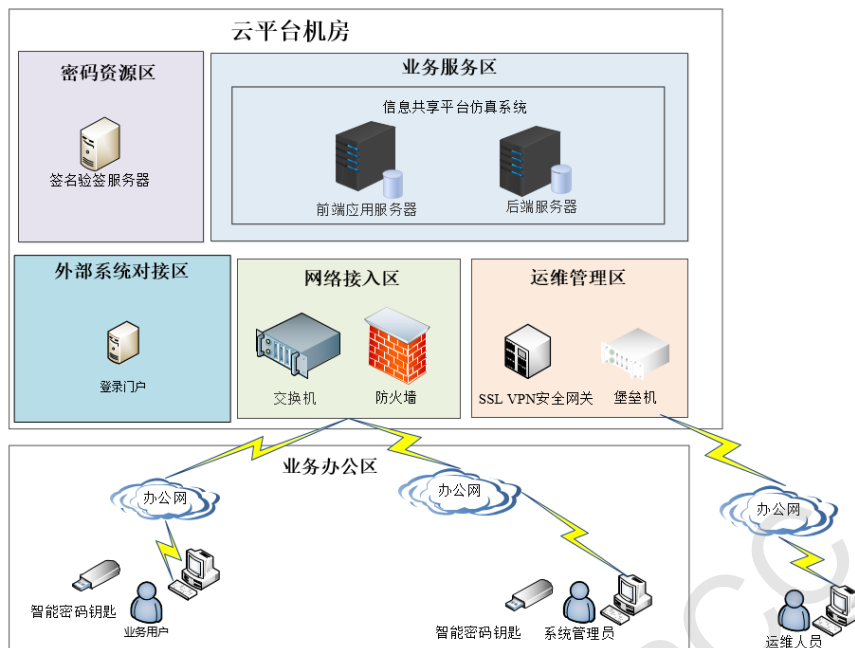


图2 云上应用仿真系统

然后，进入到**现场测评阶段**：

1) 指导学生分析系统和设备涉及的网络通信信道的通信协议使用的密码技术。常见的使用密码技术的通信协议包括TLS协议、IPSec协议、SSH协议等，这些协议可以基于RSA2048等公钥密码算法实现通信实体的身份鉴别，使用AES、chacha20-poly1305等对称密码算法实现通信过程中数据的机密性保护，使用HMAC技术或者chacha20-poly1305算法、GCM模式的AES算法等可鉴别的加密机制等技术实现通信过程中数据的完整性保护。学生需要查找数字证书、密码学套件等，从而判断建立网络通道时完成身份鉴别、网络通信数据的机密性、完整性保护所使用的密码技术。

在分析网络通道时，需要使用协议分析工具捕获并解析流量包。面对TLSv1.3协议中加密的数字证书，协议分析工具无法解析的问题，需要通过合适的方法和途径，如小组讨论、资料查询等，解决如何从浏览器或服务器导出并检查证书的签名算法和有效期，以确保其符合安全标准。

在分析运维登录VPN的网络通道时，使用协议分析工具抓取流量包后进行解析，难点是TLCP协议中握手阶段没有传递数字证书的过程，学生通过课堂相关知识利用，在老师指导下发现传递证书可能在紧跟着Server Hello后的OpenVPN协议中，将OpenVPN协议的P_CTRL_V1消息中的"OpenVPN Protocol"的内容导出为二进制文件，并在二进制文件中寻找并导出数字证书。

在分析远程管理Linux操作系统服务器的网络通道时，解析SSH协议时遇到

的难点是协议分析工具解析出SSH协议，但加密算法使用RC4等高风险密码算法，而且不包含实现通信数据完整性保护的MAC算法，学生通过交流，并在老师指导下学会查看堡垒机支持的密码学算法，并在Linux操作系统的服务器的配置文件中修改加密算法并添加无高风险密码算法的MAC配置，然后重启SSH服务使修改生效，再次抓包解析后，解析的SSH协议使用无高风险的加密算法，而且包含添加的MAC算法。

在分析远程管理Window操作系统服务器的网络通道时，学生在Window操作系统的服务器使用协议分析工具抓取流量包后进行解析，解析RDP协议时遇到的难点是RDP协议中使用RC4等高风险密码算法，学生通过讨论、思考，掌握Windows2012及以上版本的Windows服务器支持RDP协议基于TLSv1.1及以上版本实现，并在老师指导下学会给Windows RDP协议配置基于TLS协议实现。

在分析各种通信协议中的分组密码算法时，除了工具测试和配置检查，引导学生基于人工智能技术进行分组密码算法识别，从捕获的加密流量中获取密文进行特征提取与模型训练测试，通过对密文数据集的训练和测试后，辅助分析通信协议使用的分组密码算法，助力密码算法分析的智能化发展。

2)验证使用智能密码钥匙登录系统是否采用符合标准的基于数字签名的“挑战-应答”机制。实体鉴别机制包括单向鉴别和相互鉴别，使用智能密码钥匙登录系统一般是单向鉴别，单向鉴别又分为一次传递鉴别和两次传递鉴别，为了防止重放攻击，一次传递鉴别需要双方保持时间同步，或者鉴别方验证序列号没有重复，这在一些情况下难以实现，采用“挑战-应答”机制可以有效克服这种困难。实体鉴别机制的被鉴别方可以使用对称加密、密码校验算法、数字签名来计算自己的身份鉴别信息，其中使用数字签名机制通过合规CA机构颁发的数字证书可以较好实现身份鉴别信息和唯一实体做绑定。

首先，根据已有知识思考如何导出智能密码钥匙中的数字证书，查看证书的颁发机构、有效期、签名算法等是否符合要求。然后，分组讨论形式查阅资料，掌握浏览器中的开发者工具的使用，在网络选项选择保留日志，然后使用智能密码钥匙登录系统，在网络选项下查找前端收到的随机数和发送的签名值。其中技术难点包括：在浏览器中的开发者工具的网络选项下未查找到前端收到的随机数，通过思考和指导发现可以在登录代码中找到涉及随机数的部分，打断点，然后使用智能密码钥匙登录系统后查找随机数；前端仍未查找到后端发送的随机数，查看登录代码，通过修改登录代码，使登录时由后端生成随机数发送到前端后再计算数字签名。最后，学生根据签名原文、数字证书、签名值，在老师指导下使用验签工具验证数字签名是否有效。

最后，在**分析结果阶段**，学生需基于测评证据，对被测系统和设备的安全状况进行全面评估。具体包括对网络通道中通信协议的分析、对智能密码钥匙登录系统时应用的密码技术的合规性、正确性及有效性的全面审查。学生通过查阅资料 and 小组讨论，结合所学密码学理论与实践知识，对被测系统的密码应用存在的不足进行深入剖析，评估其潜在风险和对系统整体安全性的可能影响。在此过程中，学生需要特别关注密码技术在实际应用中的具体表现，例如密钥管理机制是否完善、通信过程中密码算法的选择是否符合规范，以及密码实施过程中是否存在配置缺陷或操作漏洞。通过多角度分析，学生不仅可以识别现有问题，还能预测潜在的攻击路径和安全隐患，从而为系统优化提出建设性建议。最终，学生将对本次密评案例的实施过程进行总结，形成一份结构化的系统测评报告。

3.2 漏洞挖掘

漏洞挖掘的实施过程中，主要难点在于：对IoT类目标对象的资产梳理与攻击路径识别、根据实际情况选择合适的漏洞挖掘方法与工具。这些难点既对技术能力提出了严苛要求，也考验了实践过程中的分析与应变能力。

案例中包含漏洞挖掘工程实施过程中的难点和解决思路，从理论到实践为学生提供全面指导。从漏洞定义与类型介绍、漏洞挖掘方法体系、固件提取、工控协议安全、模糊测试、静态审计、源码审计、逆向分析、漏洞挖掘案例等关键技术方法，对工控系统及IoT设备的漏洞挖掘知识要点进行系统全面的展示，为学生教授常见工控系统与IoT设备漏洞挖掘技术方法，通过理论讲解与实践操作的结合，学生不仅能够系统学习工控系统与IoT设备漏洞挖掘的核心方法，还能在实际问题解决过程中培养创新思维与实战能力，案例学习过程中部分硬件如图3所示。

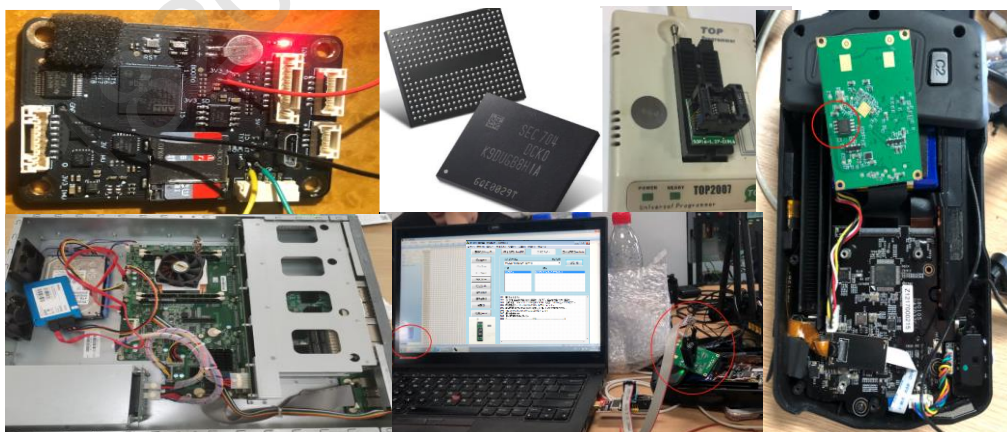


图3 部分硬件展示

1) 对IoT类目标对象的资产梳理与攻击路径识别过程中, 首先确定目标对象的版本型号、芯片型号、处理器架构、硬件接口类型、相关芯片手册和用户手册等信息, 同时需要梳理其配套调试、升级、应用和组态等上位软件, 了解对象在整个系统中的位置、作用以及基本功能的使用, 再依据对象特点和工程经验识别出攻击路径并制定测试方案。

带领学生了解路由器、摄像头、PLC等典型IoT和工控设备对象的软硬件架构组成和常用的Mavlink、SBUS、Modbus、S7、Profinet等通信协议, 总结并演示包含官网下载、在线升级分析、RT809H编程器读取、adb调试口提取等固件提取方式, 梳理固件未加固可篡改、硬编码敏感数据(如API密钥、密码口令、URL、私钥证书等)等常见缺陷和漏洞, 指导使用binwalk、IDA pro等工具对其他潜在漏洞进行分析, 引导学生形成漏洞挖掘基本思路, 此外通过布置课后练习, 要求学生针对具体对象梳理其信息并列出攻击思路, 以提高学生们的信息搜集和整理能力, 最终使学生(1)了解工控系统以及IoT设备的整体框架;(2)形成清晰明确的漏洞挖掘方法和思路流程。

2) 在选择合适漏洞挖掘方法与工具方面, 作为注重实操和应用的环节, 课程中搭建仿真环境, 结合流量分析、逆向分析和模糊测试等技术方法, 介绍常用的分析工具的使用场景和基本使用方法, 并深入讲解高效且实用性强的模糊测试方法的原理实现和使用技巧。

对于逆向分析、仿真运行、动态调试等漏洞挖掘方法及工具的使用上, 要求学生完成CVE-2021-29302路由器缓冲区溢出漏洞的漏洞复现。学生首先需要在官网下载包含漏洞的路由器固件, 使用qemu封装的仿真工具FAP进行仿真运行, 再结合gdb和IDA pro调试分析工具找到漏洞位置并分析漏洞成因, 最终编写python脚本完成漏洞利用。对于流量分析、模糊测试等漏洞挖掘方法及工具的使用上, 要求学生使用boofuzz和AFL分别对Modbus网络协议和二进制程序进行模糊测试。(1)学生通过wireshark捕获仿真程序的网络数据并依据Modbus协议规范分析报文中各字段的含义和作用, 利用boofuzz提供的API编写测试脚本对Modbus仿真程序开展测试;(2)系统介绍AFL二进制模糊测试工具的整体架构、路径覆盖率反馈原理、forkserver机制、变异策略和基本使用等, 并指导学生完成Fuzzing101项目的所有练习。最终使学生(1)掌握模糊测试技术, 能够对工控系统及IoT设备中协议、软件等进行漏洞挖掘;(2)掌握静态分析技术和动态调试技术, 能够对对工控系统及IoT设备中协议、软件等进行漏洞复现和漏洞挖掘。

此外在课程案例中会引入TARA分析等工程分析方法, 使学生了解掌握资产识别、威胁场景分析、影响等级评估、攻击路径分析、攻击可行性等级评估、风

险值确定、风险处置决策等一系列威胁分析流程，通过这一系列威胁分析流程，学生能够深入识别目标对象潜在的威胁和安全漏洞，再综合考虑攻击可行性和影响等级等因素，确定系统可能存在的风险及其风险等级。这一过程不仅帮助学生构建全面的威胁评估视角，也为其在后续安全防护设计中做出更科学、合理的决策奠定基础。

通过将以上理论与实践的结合，不仅显著提高了漏洞挖掘的效率，还使学生更深入地理解工控系统和物联网（IoT）设备面临的系统性安全挑战。通过分析实际场景中复杂的安全问题，学生能够学会权衡不同因素对系统风险的影响，从而在设计和实施安全防护策略时具备更强的专业判断能力。

同时在漏洞挖掘的教学实践中，引导学生使用污点分析、人工智能等技术辅助人工分析，提高漏洞发现的效率和准确性。污点分析技术通过追踪数据流向和输入源，帮助学生识别潜在的漏洞传播路径，尤其是在复杂系统中，这种方法可以显著弥补人工分析可能存在的覆盖不足问题。学生通过使用污点分析，能够更直观地了解数据在系统中的流转方式及其潜在的安全隐患。

此外，人工智能技术的引入为漏洞挖掘提供了更加智能化的支持。通过对大量样本数据的学习，AI模型能够自动识别异常模式和潜在漏洞，为学生提供高效且精准的分析工具。例如，在海量的系统日志或代码中，人工智能可以快速筛选出高风险区域，大幅度减少人工分析的工作量并提升分析的精准度。通过这些技术的实践应用，学生不仅能掌握漏洞挖掘的先进方法，还能够在此过程中激发对前沿技术的兴趣，培养其分析和解决复杂问题的能力。

3.3 防御力量培养

在防守力量培养模块中，融入全面系统的理论知识讲解与实战技能训练，确保学生能够全面掌握网络安全防守中“恶意行为发现与分析”方向的痛难点问题。通过模块化的教学设计，学生能够在理论学习中理解恶意行为的特性和演化规律，并在实践中掌握应对复杂网络攻击的有效策略。在电子五所组织的攻防演练中，课程将防守实践细化为事件监测、事件分析、事件处置、事件上报等多个环节通过真实演练场景的还原，学生得以全方位参与防护事件的完整流程。在这一过程中，企业导师与学生组成的防守小组紧密协作，针对“恶意行为发现与分析”方向的关键难题逐一攻克。通过导师的专业指导和阶段性突破，学生不仅能够识别复杂攻击行为，还能从分析中发现潜在安全漏洞并制定有效的防护策略。

事件监测。为解决“流量分析”这一技术难点，采取理论与实际相结合的教学策略，对学生进行全面且深入的安全事件监测指导。一方面通过模拟真实网络流

量，训练学生使用流量分析工具，如Wireshark等，进行实时流量监控和异常检测；另一方面结合流量分析设备平台、安全监测设备平台、其他厂商监测平台、失陷检测平台等进行7*24小时安全事件监测。

事件分析。为解决“恶意文件检测与分析”这一技术难点，引入恶意文件分析工具和沙箱环境，教授学生如何检测、分析和处理恶意文件；带领学生通过IDA Pro、Ghidra、OllyDbg等逆向工程工具分析恶意文件的源代码和行为；进一步引导学生通过行为特征识别恶意文件。在教学过程中，定期收集学生反馈，评估教学效果，及时调整教学方法和内容，确保学生能够掌握必要的技能。

事件处置、事件上报。为解决“网络安全事件响应流程完善”这一技术难点，组织学生为电子五所组织的护盾攻防演练一靶标单位模拟网络安全事件，在模拟环境中实践应急响应流程（如图4所示），掌握事前、事中和事后的处理方法，并将防火墙、网络设备阻断、WAF控制、主机排查、应用排查、加固与整改等技能应用于电子五所组织的护盾攻防演练中。



图4 应急响应流程

结合攻防演练过程，引导学生探索AI大模型技术在攻防演练中的应用。通过“课下调研与课上开放式研讨”的教学模式，鼓励学生从理论到实践全面掌握AI在威胁检测、安全事件响应和攻击模拟等方面的作用，深刻理解AI在网络安全领域的实际应用，并依据所学解决企业现存的难题，进一步增强学生解决复杂网络安全问题的能力。

防守情况总结报告。指导学生撰写详细的防守情况总结报告，包括演练过程、观察到的问题、成功和失败的策略、改进建议等。

4.实施效果

在对密码应用安全评估、漏洞挖掘与防守力量的培养过程中，我们对案例实施过程中的相关课程进行了详细的数据分析。通过对110名选课学生的学术表现进行细致统计，我们得出的综合评定结果如图5所示。随着案例实践的深度和难度的逐步提升，优秀率有了显著增长，从22%上升至39%，这一积极变化主要归功于大部分学生在良好阶段通过案例学习显著增强了自身的实践技能。同时，我们也注意到低分区间的扩大，这进一步揭示了学生个体在适应案例学习和展示专业能力方面的差异性。

表1展示了案例相关的额外数据（时间截至2024年7月，包括2024年案例相关论文选题人数，数据来源于调查问卷）。随着案例的持续实施，参与人数和成果数量均呈现出稳步增长的趋势，学生中的论文选题与专业理论及企业需求之间的契合度也在不断提高。特别是在网络安全专业的学生群体中，绝大多数学生对未来职业的定位倾向于选择与其所学专业领域相关的岗位。

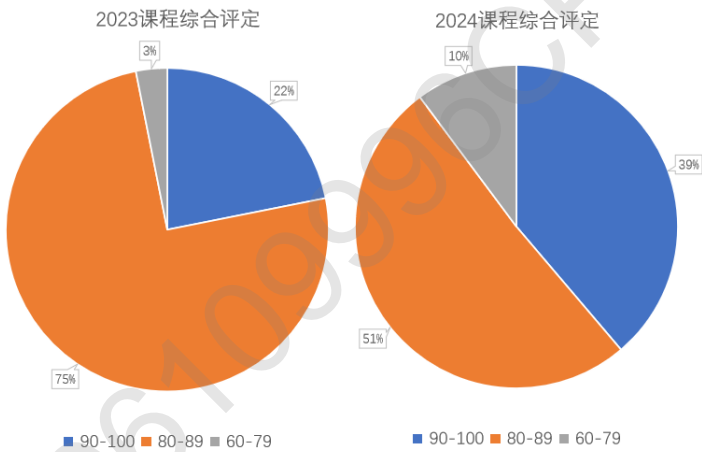


图5 案例综合评定对比

表1 案例相关数据

	案例参与人数	案例相关知识 产权数	案例相关论文 选题人数	安全岗位意向统计
2023年	50	11	17	25
2024年	60	15	20	32

具体而言，案例的深入实施进一步解决了人才培养过程中的以下关键问题：

4.1 促进了理论向实践的提前蝶变

通过密评、漏洞挖掘和安全防御等实践活动，学生能够将校内掌握的理论知

识应用于实际场景，实现从理论到实践的全面转化，真正做到“学以致用”，从而激发其对未来探索的积极性和主动性。部分课堂迁移到企业，充分利用电子五所大型设备、高新科技产品等先进设备和优势资源，让学生近距离接触实际设备和实验平台，仿真与实验相结合，不仅提高了学生的学习兴趣，也可充分验证仿真方案的准确性，从而提高教学效果。通过基于案例的课程内容设计，与企业导师的深度协作逐步增强，参与相关项目的学生人数稳步增长，学生参与安全领域实习实践的比例也逐年提高。在企业的实习实践中，学生将所学理论知识延伸至企业当前的实际需求，直接参与课题研究与项目实践。这不仅为企业注入了新鲜技术力量，也为其培养了具有潜力的未来员工。与此同时，学生在实践中提前锻炼了解决实际问题的能力，为职业发展奠定了坚实基础。这一教学与实践相结合的模式，不仅提升了学生的专业素养和就业竞争力，还推动了高校与企业之间的深度合作。通过理论与实践的双向赋能，逐步实现了学术与产业需求的高效衔接，为网络安全领域培养具有实战能力和创新意识的高素质人才提供了有力支持。

4.2 激发了创新思维，解决现实痛点

基于案例实际问题，通过问题分析与现有条件的考虑，结合先进前沿技术，激发利用学科交叉的创新思维。融合人工智能技术、网络安全技术、通信技术等，漏洞挖掘模块相关学生产生了以下成果：（1）设计了高精度安卓污点分析器，提供用户通讯录敏感信息泄露漏洞检测服务，能够自动化静态分析检测Android APK文件中的敏感信息泄露漏洞，提升了代码覆盖率和精度的同时减少了资源开销。（2）针对模糊测试工具痛点问题：模糊测试器不能针对某个程序块进行定向测试、定向模糊测试器生成的图信息不够全面以及定向模糊测试器在进行变异时没有考虑启动程序命令不同的情况，设计了一款包含静态分析阶段和动态调试阶段双阶段架构的自动化模糊测试器。目前该模糊测试器已被应用在实际的IoT设备漏洞挖掘当中，并发现某路由器设备5个拒绝服务漏洞和1个命令注入漏洞。（3）相关学生完成课程内容学习后参加了电子五所的实习工作，主要负责研究基于QEMU的虚拟设备定制化开发技术，解决固件仿真过程中遇到的部分软硬件依赖缺失问题，以提高仿真适配和成功率，完成了3款路由器固件的仿真运行环境适配任务。

4.3 增强了学术科研与企业实习内容的联系

通过案例问题的全生命周期分析，结合已有的理论根基，针对企业需求，通过调研、实践等环节，对问题现状进行进一步的了解，辅助学生立足实际问题，研究前沿技术，并结合企业工程现状，形成开题报告等，参与项目的同时完成论文写作。2023年12月，参与案例课程的同学中，约34%的论文选题与案例相关课

题实践有关。此外，部分学生参加了电子五所等企业的实习，实习内容为基于案例的相关知识扩展。学生利用电子五所的信息编码算法应用公共服务平台，在各类仿真环境中完成实操，增进了对各种密码技术的理解，培养了密码学实践能力，为将来的密码学理论研究或技术研发奠定了基础。以上进一步增强了研究生培养过程中的工程实践、企业实习与学术科研之间的关系，通过实习实践，加深了对问题的认识，通过企业导师和校内导师的双重指导，为高质量科研成果提供坚实的保障。

通过本案例的实施，西安电子科技大学的师生与工信部电子五所建立了密切的合作关系，为后续企业课题的“揭榜挂帅”奠定了坚实基础。学生在校期间参与企业课题，不仅能够提高自身的实践能力，也可以通过课题研究，获得相应的政策支持，为个人职业发展创造更多机会。企业专家通过案例交流与合作，能够提前接触并选拔优秀的学生人才。这种深度互动不仅为企业实习人员的储备提供了丰富渠道，也为未来的人才招聘奠定了基础，构建了高校与企业之间人才输送的高效桥梁。案例的实施实现了高校教育、企业需求和学生成长的有机结合，为推动校企协同育人和人才培养模式创新提供了典范。

5. 结语部分

本案例从密码学理论出发，延伸至网络攻防实践，对参与单位和企业的相关领域的研究和应用起到了显著的推动作用，同时为网络安全人才培养提供了无缝衔接的培养路径。案例的实施突破了传统学校在密码学与网络安全理论教育中的局限，扩展了专业教育的深度与广度。通过案例实践，不仅提升了学生对密码学理论的理解，还显著增强了其密码应用的实践能力以及网络攻防技术的掌握能力，从而使人才培养更贴近产业实际需求。案例的成功实施充分体现了学生、学校与企业三方需求的高度契合，达到了多方满意的效果。

国际形势对密码与网络安全的需求日益增强，为应对这一日益严峻的挑战，亟需进一步加大在相关研究与应用领域的投入力度，推动密码学与网络安全技术的持续创新和突破。未来可以通过加强与密码设备制造商和开发商的合作，为学生提供更多参与密码应用开发的实践项目。这将有助于学生深入理解密码技术的实际应用场景，并全面提升其密码应用开发能力，为行业输送具备前沿技术能力的高素质人才。网络安全事关国家安全，其核心领域的大型贵重设备及系统的漏洞挖掘，不仅需要先进的智能技术支持，还需要完整的实验环境和配套设施的保障。因此，未来应深化校企合作，进一步加强在深层理论研究、高难度技术攻关和精密技术实践中的协同创新。通过校企资源的全面整合与优势互补，构建高效

协作的科研与教育生态体系，全面实现理论、技术与实践的深度融合，为国家网络安全战略提供坚实支撑。

18206109996CPCC