附件6

项目编号：

**大学生创新创业孵化项目**

**申 报 书**

**申请者姓名： 朱佳超**

**所 学 专 业： 计算机科学技术**

**孵化项目名称： 工业控制设备内核漏洞动态分析系统**

**项目所属行业： 工业互联网**

**项目承担单位（公章）： 杭州电子科技大学**

**填报日期： 2020 年 1 月 2 日**

**浙江省大学生科技创新活动计划暨新苗人才计划实施办公室 制**

填写说明

一、凡申报本孵化项目的申请人，须认真阅读本项目有关通知，封面申请者姓名一栏填写项目负责人。

二、格式要求：申报书中各项内容以Word文档格式填写，表格中的字体为小四号仿宋体，1.5倍行距；表格空间不足的，可以扩展或另附纸张；均用A4纸双面打印，于左侧装订成册。

三、申报书由所在学校领导审查、签署意见并加盖公章后，一式1份（原件），报送浙江省大学生科技创新活动计划暨新苗人才计划实施办公室。

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项  目  概  况 | 项目名称 | | | 工业控制设备内核漏洞动态分析系统 | | | | | | | |
| 项目性质 | | | （）基础研究 （🗸）应用研究 | | | | | | | |
| 项目来源 | | | （）自主立题 （🗸）教师指导选题 | | | | | | | |
| 起止时间 | | | 自 2020 年 3 月 至 2021 年 11 月 | | | | | | | |
| 项目状况 | | 1、研发阶段🗸 2、中试阶段 3、批量（规模）生产（选项打√） | | | | | | | | | |
| 申请人 | 姓名 | 朱佳超 | 性别 | | 男 | 出生年月 | 1996.04 | | 入学年份 | 2019.09 | |
| 所在院系 | 计算机学院 | 学号 | | 192050147 | 联系电话 | 15869114920 | | 电子信箱 | 3232283602@qq.com | |
| 项 目 组  主要成员 | | 姓名 | 性别 | | 年龄 | 学院 | 专业 | 学号 | 具体分工 | | |
| 田佳 | 女 | | 24 | 计算机学院 | 计算机技术 | 182050176 | 前台页面展示 | | |
| 袁玮琪 | 男 | | 25 | 计算机学院 | 计算机技术 | 191050039 | 网络爬虫、漏洞库的整合 | | |
| 史文武 | 男 | | 22 | 计算机学院 | 计算机技术 | 191050044 | 系统测试相关工作 | | |
| 史文武 | 男 | | 22 | 计算机学院 | 计算机技术 | 191050044 | 系统测试相关工作 | | |
| 项  目  指  导  教  师 | | 姓名 | | | 徐向华 | 性 别 | 男 | | 出生年月 | | 1965.10 |
| 主要研究方向 | | | 大数据处理、数据挖掘、工业互联网安全、物联网安全、物联网协议、无线传感网络 | | | | | | |
| 近三年获奖成果：国家级\_\_等奖\_\_2\_项，省部级\_\_等奖\_1\_\_项 | | | | | | | | | |
| 近三年科研经费\_\_\_\_\_\_\_\_\_\_\_\_万元，年均\_\_\_\_\_\_\_\_\_\_\_万元 | | | | | | | | | |
| 项  目  主  要  内  容  简  介 | | 随着工业化和信息化的深度融合，工业控制设备内核中存在的漏洞所能引发的风险，会给工业控制系统的安全防护带来巨大挑战。因此对工业控制设备内核漏洞的分析及防护不仅关系着工业生产安全、国际经济与国防安全等诸多关键领域的安全，更具有十分重要的现实意义。  工业控制设备内核漏洞动态分析系统通过提取设备内核固件中的文件系统，搭配上定制的内核，在QEMU模拟处理器上动态的模拟设备的运行，然后通过专业漏洞库去分析测试设备内核中所存在的漏洞。  工业控制设备内核漏洞动态分析系统可用于支撑监管机构及设备运营单位对工控设备等重要设施进行安全检查、风险评估，提高关键设施地网络安全防护能力。 | | | | | | | | | |

**二、项目的研究目的及意义**

|  |
| --- |
| 1、申请项目的必要性、目的及意义  信息技术和网络技术的迅猛发展，国家安全边界已经超过地理空间限制，延伸到信息网络，网络空间成为继陆、海、空、天的第五大国家主权空间。作为网络空间安全的重要组成部分，工业控制设备的网络安全涉及国家关键基础设施和经济社会稳定，辐射范围广泛，国家十分重视。在工业控制设备的网络安全中处于首要地位的，是工业控制设备的内核安全，工业控制设备内核中存在的漏洞如果不检测防护，其涉及的不仅仅是信息泄露、信息系统无法使用等“小”问题，而是会对现实世界造成直接的、实质性的影响。因此对工业控制设备内核系统的漏洞分析不仅关系着工业生产安全、国际经济与国防安全等诸多关键领域的安全，更具有十分重要的现实意义。  该系统用于分析检测工业控制设备内核系统中的漏洞信息，在QEMU模拟处理器上动态的模拟内核系统的运行，然后专业漏洞库去分析内核中所存在的漏洞，并根据分析结果输出安全预警和分析报告，满足监管机构及设备运营单位对工控系统及安防监控等重要设施进行安全检查、风险评估。 |
| 1. 项目的背景、主要内容、技术水平及应用范围   **项目背景：**  随着“中国制造2025”和“智慧城市”建设的推荐，网络安全问题随之产生，工业控制网络安全形式日趋严峻。近年来，世界各国发生了众多工业基础设施已经成为国家间攻防对抗以及恐怖主义威胁的新形势和新手段，看不见的硝烟战争已经打响，安全形势相当严峻。工业控制系统广泛应用于各个领域，包括基础设施（金融、能源、通信、电力、交通）、民生（水、电、燃气、医院、智慧城市、智能汽车）、工业生产（冶金、电力、石油化工、核能等）和军工等。超过80%的涉及国计民生的关键基础设施依靠工业控制设备来实现自动化作业。网络信息安全防护理念正在发生深刻演变，以工业控制设备为中枢神经的国家关键基础设施安全和关键信息基础设施安全面临更为严峻的全新挑战。  国内工业控制设备主要面临如下威胁：设备存在大量的高危漏洞，越来越普遍的设备后门实施，高级持续性威胁，无线技术的广泛应用给工业控制系统的安全防护带来巨大的挑战。积极应对网络安全威胁，有效防范网络安全风险，是网络时代维护国家安全、社会稳定、公众利益的重要使命。因此，开发一个对工业控制设备进行漏洞检测的系统是极其必要的。  **主要内容：**  本项目搭建工业控制设备内核漏洞动态分析系统，通过提取工控设备的内核系统，对其进行动态仿真，并在动态仿真的过程中对系统进行漏洞检测，主要包括网页信息泄露检测、snmp协议的安全性评估以及利用metasploit框架的攻击检测。  总体来说，该系统由三大部分组成，包含前端页面展示，服务端数据实现和前台页面的业务交互逻辑。系统的功能包含5个模块，分别为工控设备固件的提取与预处理、设备内核系统的动态仿真、漏洞库、漏洞的检测、用户登录模块。漏洞库模块集成了国家信息安全漏洞平台等数据，自动化更新漏洞库数据，用户可以通过漏洞库模块浏览、检索最新的工控信息。用户登录模块包含用户登录、登出以及用户权限控制相关内容。漏洞的检测是对待测工控设备的内核进行动态的分析。工控设备固件的提取与预处理就是从设备固件中提取内核与文件系统，然后进行处理，以便能够部署在QEMU上进行动态仿真。设备内核系统的动态仿真就是通过QEMU来模拟设备的运作。详细的整体流程内容如图1所示。    图1 整体流程内容  **技术水平：**  （1）Linux系统内核的二进制分析  （2）使用unicom来模拟CPU执行，相对于AFL，不需要编译、插装，在无源码状态下，同样也可以进行测试。相对于KAFL，不需要使用intel的 Intel Processor Trace技术，能够模拟arm、powerpc在内的多个指令集。  **应用范围**：  工业控制设备中所有基于Linux的嵌入式系统 |
| 1. 实施该项目所具备的基础、优势和风险   **基础：**  安全技术研发方面，项目团队成员有开发编码经验，掌握网络威胁检测、数据收集、数据预处理、数据挖掘、工控协议分析、工控安全、网络爬虫、平台搭建等相关技术，能够应用这些技术到本项目中。  指导老师方面，本项目指导老师现任浙江省数据存储传输技术重点实验室主任，杭州电子科技大学智能与软件技术研究所副所长，工业互联网研究中心副主任，他主持国家973项目课题1项，国家科学基金面上项目2项，浙江省重大科技专项和杭州市科技计划项目6项以及横向课题多项，作为主要成员参与国家科技支撑计划项目、国家自然基金、浙江省重大科技专项等项目10多项，涉及研究方向包括工控安全、网络安全、物联网安全、数据挖掘等多个方面，具有丰富的项目经验。  工程能力方面，本团队对工控领域项目已有两年的研究基础，针对工业控制设备内核动态分析系统方面，已经深入研究目前的AFL内容，详细流程见图2所示。    图2 AFL详细流程图  **优势：**  项目团队成员本硕均是计算机专业，具有扎实的编程能力，能够胜任本系统项目的开发工作；项目团队成员参与过多项项目，使用过网络爬虫、数据挖掘、机器学习、工控协议分析、工控安全、数据可视化等技术，熟悉主流数据库，对数据的动态交互与展示有实践经验，能够承担本项目所需要的技术研发工作。本项目指导老师具有丰富的项目指导经验，能够帮助解决项目研发过程中遇到的技术和实施难题，保障项目顺利完成。  **风险：**  本项目实施过程中存在一些技术风险，具体如下：  （1）本项目的老师和同学都来自计算机专业，对于工业控制方面的了解尚有不足，对工控网络安全得知识还需扩展。  （2）工控系统相关设备、工业控制协议颇多，需要更全面地深入研究。 |
| 4、项目计划目标  项目计划实现以下目标：   1. 集成工控设备内核专业漏洞库。 2. 实现对于工控设备内核的文件系统的提取和预处理操作。 3. 实现工控设备的动态仿真，在仿真模拟过程中挖掘工控设备的漏洞信息。 4. 将各种数据动态展现到主界面，可视化各种信息，达到快速、简单、直观、易说明问题的程序。 5. 对系统进行各种测试，并修改bug，最后通过各种测试。 |

**三、预期成果、知识产权形成及经济、社会效益分析**

|  |
| --- |
| 1. 项目的预期成果及知识产权归属情况   工业控制设备内核动态分析系统：  申请发明专利2项；  软件著作权1项；  本项目产生的知识产权归项目团队成员和指导老师共同拥有。 |
| 1. 项目的市场前景分析   现在市场上存在很多的工控设备，但大多只注重于其功能的实现，在安全防护方面的关注较少，而本系统的存在可以提高对工控设备的安全检测与防护，并且本系统具有成本低、实用性强、可靠性高、可扩展等特点，所以市场前景乐观。 |
| 1. 项目的盈利能力分析及财务预算   系统研发成功后，因系统具有的成本低、实用性强、可靠性高、可扩展等特点，可以向监管机构及工控设备运营单位进行推广使用，进而产生经济效益。  本项目财务预算一共1万元，支出详细如下表：   |  |  |  | | --- | --- | --- | | 支出项 | 依据和理由 | 金额（万元） | | 设备材料费 | 购置工控设备、内存条等配件 | 0.3 | | 差旅会议费 | 去本地或外地企业、高校进行学术调研和会议交流 | 0.4 | | 知识产权费 | 用于发表论文、申请专利和软件著作权 | 0.3 | | 总计 |  | 1 | |
| 1. 项目的社会效益分析   本项目的社会效益主要表现在以下两个方面：   1. 对于国家，通过工业控制设备内核漏洞动态分析系统对国家关键基础设施进行安全检查、风险评估，保证国家的战略安全，减少工控设备的安全事件的发生，维护国家安全。 2. 对于社会，系统提高对工控系统和网络设备的安全检测与防护，促进了社会稳定，避免工业控制的安全威胁人类生活，稳定社会利益。 |

**四、项目实施进度方案**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 本项目进度安排如下表所示：   |  |  | | --- | --- | | 起止年月 | 进度目标 | | 2020.02~2020.03 | 项目需求调研，关键技术研究 | | 2020.04~2020.06 | 总体方案设计 | | 2020.7~2021.01 | 系统模块开发、集成、测试 | | 2021.04 | 项目中期检查 | | 2021.04~2021.05 | 系统改进 | | 2021.06~2021.09 | 项目验收 | |

**五、项目组承诺**

|  |
| --- |
| **承 诺 书**  以上所填内容真实可靠，本项目组承诺：该项目立项后，将严格遵守有关规定、遵守本申报书和预算表中规定的条款和内容，保证按计划进度完成项目任务。  项目组全体成员（签章）：    年　　月　　日 |

**六、学校审核意见：**

|  |
| --- |
| 负责单位（公章）  年 月 日 |

**七、专家组审核意见**

|  |
| --- |
| 专家组组长签章：  年 月 日 |

**八、实施办公室审核意见**

|  |
| --- |
| 公章：  年 月 日 |