**2021年四川省科学技术奖励提名项目公示**

**科技进步奖**

1. **项目名称：**

铁路关键信息基础设施安全管控技术及应用

**二、提名单位：**西南交通大学

**提名意见：**该项目围绕铁路关键信息基础设施在海量并发访问、高实时性条件下的高可信、高可靠安全管控，内、外网攻击的安全防御，持续性安全保障等系列重大难题，历经十多年攻关，创建了网络化安全超算的数学模型，形成了“安全威胁唯快不破”的“计算”优势，具备高性能的对抗能力。创新了全面强制访问控制及审计的形式化理论与方法，形成了“以不变应万变”的计算、计划优势，具备主动防御的威胁拦截能力。创建了可软件定义的柔性防御拓扑网络结构，形成了自适应威胁环境的免疫进化优势，具备无感化的风险管控能力。建成了中国铁路系统安全保障系统，抵御了来自海内外的有组织的黑客攻击，形成成套技术和标准。

项目成果应用于中国铁路总公司、铁科院和全国18个铁路局集团公司，覆盖所有铁路客运车站，服务所有铁路旅客，为保障中国铁路系统的安全运营及中国铁路客运的发展与变革发挥了重大且积极的作用，全面提升了铁路系统的安全性，极大地提升了我国铁路客运服务和管理水平，取得巨大的经济效益和社会效益。

提名该项目为四川省科技进步一等奖。

**三、项目简介**

我国运营着全球规模最大的铁路关键信息基础设施：保障列车安全高效运行的列控系统、提供电气列车唯一动力来源的牵引供电系统、超千亿级访问交易量的铁路客票系统、十万余座轨旁布设基站的移动通信系统，以及覆盖全国18个铁路局的多活数据中心，均处于网络攻防对抗的主战场，一旦遭到破坏、丧失功能或者数据泄露，可致车毁人亡，直接影响铁路运输质量和安全。铁路关键信息基础设施安全防护难题主要包括：

1、防御计算力不从心：铁路运行的提速增效，要求铁路关键信息基础设施同构匹配高可靠低时延零干扰的安全性能。然而，攻防对抗属性下有限算力的瓶颈，难以保持安全能力，迫使逆向选择折衷防护；

2、防御模式亡羊补牢：铁路的高严苛安全性，不允许铁路关键信息基础设施存在安全的试错机会。然而，技术命门的不受控，使得基于先验知识的封堵查杀只能设防已知攻击，难以抵御跨越信息物理边界的未知威胁；

3、防御架构松散僵化：铁路属于复杂巨系统，内嵌其中的铁路关键信息基础设施呈现出堆叠式安全和不对称防守的消极特性。然而，处于相似结构下的静态防御难以有效应对动态复合的网络攻击。

为彻底解决上述难题，项目团队在国家科技部、国铁集团、工信部、国家发改委的长期持续支持下潜心研究20余年，形成了网络空间中敢打仗、能打仗、打胜仗的铁路关键信息基础设施安全管控系统理论体系、技术体系和成套装备：

1、针对防御计算力不从心的问题，研究存算传一体化融合的超算技术，基于多目标群决策的模型原理，构建“感知—决策—适配”架构下的网络资源“无人驾驶”机制，实现存储、计算与传输能力间的动态转换和组合应用，显著提升网络化计算的韧性力量；

2、针对防御模式亡羊补牢的问题，研究紧耦合应用、强相关场景的基线安全技术，基于网络栈表征式的强制访问控制理论和方法，构建了基础设备的“白操作”、实时通信的“白环境”、业务应用的“白行为”，实现了不依赖于漏洞/后门/攻击等先验特征知识的创新型主动防御机制；

3、针对防御架构松散僵化的问题，研究软件可定义、功能可重构、规模可伸缩的柔性防御技术，基于可编程网络原理与多代理权变结构，构建风险激励下的挂图作战智能管控体系，实现防护部件的集约控制、按需协同和敏捷响应，支持最高四级等保的多疆域、多等级、多目标的安全防御。

项目成果已在国铁集团、所属18个路局、4000多个站段等实施应用，广泛涵盖了大数据、混合云、物联网、工控网和移动网等信息新基建形态，有效提升了行车安全和铁路运输秩序。以列控系统为例，解决了功能安全与信息安全融合场景下的安全防护难题，年均完成威胁识别分析和SIL等级验证1156次以上；以铁路客票安全为例，实现最高峰每小时拦截亿万次扫描或攻击。项目获发明专利24项，标准4项,论文100余篇，其他知识产权150多项，近3年服务旅客超百亿人次。成果累计销售额逾35亿元，经济和社会效益显著，院士专家组评价为：“整体技术处于国际领先水平”。

**四、主要知识产权和标准规范等目录（不超过10件）**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 知识产权（标准）类别 | 知识产权（标准）具体名称 | 国家（地区） | 授权号（标准编号） | 授权（标准发布）日期 | 证书编号（标准批准发布部门） | 权利人（标准起草单位） | 发明人（标准起草人） | 发明专利（标准）有效状态 |
| 发明专利 | 基于可设定信息安全目标的获得性安全保障方法及系统 | 中国 | ZL200810065382.0 | 2010年6月2日 | 第629630号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;刘智;邹跃军;徐国前;宋晶;郑伟范;伍立华;彭华; | 有效 |
| 发明专利 | SOA安全保障系统及方法 | 中国 | ZL200910107186.X | 2011年11月23日 | 第867620号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;唐威;伍立华;曾旭东;邹跃军; | 有效 |
| 发明专利 | 一种防火墙系统、安全服务平台及防火墙系统的管理方法 | 中国 | ZL200910157311.8 | 2011年12月7日 | 第874569号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;陈飞;伍立华;任海广;张知之; | 有效 |
| 发明专利 | 一种可用性风险扩散评估方法 | 中国 | ZL200910157522.1 | 2012年8月1日 | 第1016488号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;伍立华;刘云;曾干;曾旭东; | 有效 |
| 发明专利 | 一种业务工作流的流程识别方法 | 中国 | ZL200910157312.2 | 2012年5月9日 | 第943039号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;周文柱;曾干;刘喜雨;施珉; | 有效 |
| 发明专利 | 一种支持动态交互的实时信息安全服务方法及系统 | 中国 | ZL201010617827.9 | 2013年9月11日 | 第1263687号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;郑伟范; | 有效 |
| 发明专利 | 一种日志事件关联分析系统与方法 | 中国 | ZL200910157310.3 | 2011年8月24日 | 第830337号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;曾旭东;唐娟;刘云;马诗真; | 有效 |
| 发明专利 | 安全终端系统及终端安全方法 | 中国 | ZL200910106166.0 | 2011年8月24日 | 第828198号，中华人民共和国知识产权局 | 深圳市永达电子有限公司 | 戚建淮;邹跃军;唐威; | 有效 |
| 发明专利 | 一种电子文件的授权下载方法及系统 | 中国 | ZL201010236332.1 | 2012年5月23日 | 第955973号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;唐威;曾广良;陈健;田佳;李勇新; | 有效 |
| 发明专利 | 一种应用在身份鉴别中的安全输入法 | 中国 | ZL201010236336.X | 2012年9月12日 | 第1043909号，中华人民共和国知识产权局 | 深圳市永达电子股份有限公司 | 戚建淮;唐威;曾广良;陈健;田佳;李勇新; | 有效 |

**五、论文专著目录**（不超过5篇/部，非必填）

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 论文（专著） | 年卷页码 | 发表时间 | 通讯作者 | 第一作者 | 国内作者 | 他引总次数 | 检索数据库 | 论文署名单位是否包含国外单位 |
| 1 | 普通高等教育“十一五”国家级规划教材：《现代密码学》，人民邮电出版社出版 | **ISBN** 978-7-115-21157-6 |  2009-09 | 何大可 | 何大可 | 何大可，彭代渊，唐小虎，何明星，梅其祥 | 113 | 中国知网 | 否 |
| 2 | 基于贝叶斯网络的半监督聚类集成模型/软件学报 | 2010年第21卷第11期 | 2010-11-15 | 戚建淮 | [王红军](https://nxgp.cnki.net/kcms/author/detail?v=cGwEW1TFPBTmRT_zJ5UVi9S8aja3nFY5JGHUOMS77sMuF-Wgkya08CtvYAFsuXWGb8x2XHfYPBi97edt2FsP1VpDMwhuOYrNsUqBAqCa3vrEACUyDjeQAg==&uniplatform=NZKPT" \t "https://nxgp.cnki.net/kcms/_blank) | 王红军，李志蜀，戚建淮，成飏，周鹏，周维 | 43 | 中国知网 | 否 |
| 3 | 支持可信计算的软件保护模型/西南交通大学学报 | 第63-67+96页 |  2006-02-28 | 何大可 | 郑宇 | 郑宇，何大可，梅其祥 | 25 | 中国知网 | 否 |
| 合 计 | 181 |  |  |

**六、主要完成人：**戚建淮、宋晶、郑伟范、何大可、姚倩、胡显荃、唐娟、周杰、汪暘、谢栋平

**七、主要完成单位：**西南交通大学、深圳市永达电子信息股份有限公司、中国铁路成都局集团有限公司、成都卫士通信息产业股份有限公司、成都市以太节点科技有限公司