附件1

上海市2021年网络安全产业创新攻关目录

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **序号** | **攻关方向** | **内容简述** |
| 基础技术创新 | 1 | 零信任网络访问 | 针对可扩展的混合IT环境下平台、业务、用户、终端所呈现的多样化趋势和安全需求，构建零信任网络安全访问架构，包括（但不限于）支持持续认证、细粒度的上下文访问控制、信令分离等防御理念的软件定义边界（SDP）；业务场景动态适变、具备灵活智能策略体系的身份与访问管理系统；云原生微隔离、API对接微隔离、主机代理微隔离等微隔离技术。实现业务系统动态访问控制和授权，有效实现可持续的零信任安全防护体系。 |
| 2 | 隐私计算 | 针对数据资产作为生产要素带来的隐私计算和安全保障需求，构建体系化的隐私计算及安全保障架构，包括（但不限于）隐私计算模型框架、隐私保护场景适应的密码体系应用、隐私控制与抗大数据分析的隐私保护技术、数据敏感性量化、恶意收集数据行为检测和准确溯源、基于信息隐藏的隐私保护技术以及支持高并发的隐私保护服务架构、场景动态适应的隐私动态度量与隐私保护效果评估技术等。有效解决数字化转型下数据安全问题。 |
| 3 | 新一代数字身份认证 | 针对万物智能互联时代数字身份管理需求，构建新一代数字身份认证技术，包括（但不限于）器件级硬件指纹技术、低功耗密码技术及应用、多场景适用的物联网安全通信协议、云和边缘计算多维适配的可信身份安全计算环境，面向万物智能互联的数字身份安全体系和数字信任体系等。有效应对万物智能互联时代数字身份管理存在的设备数量巨大、智能硬件算力参差不齐、基础计算架构碎片化、身份仿冒和伪造泛滥等安全挑战。 |
| 4 | 人工智能安全 | 针对人工智能应用的新型网络攻击检测和防护需求，构建基于人工智能的安全评估与防御技术能力，包括（但不限于）动态可扩展的网络安全大脑、网络攻击的智能检测与效果研判、漏洞智能化挖掘、基于人工智能模型的脆弱性分析。有效应对人工智能时代网络攻击趋于智能化、大规模网络攻击频繁、网络攻击隐蔽性提高等问题。 |
| 应用技术创新 | 5 | 数据流通安全 | 面向互联网、政务、金融、大数据等重点行业数据流通需求，构建安全合规的数据流通体系，包括（但不限于）安全多方计算、区块链、联邦学习、可信执行环境、开源代码供应链安全等技术。实现海量数据在开放流通环境下的安全和隐私，有效支撑数据要素市场的构建。 |
| 6 | 智能工控安全 | 针对各类工业企业数字化、网络化和智能化发展需求，构建“5G+AI+工业互联网”下的智能工控安全技术能力，包括（但不限于）工业云平台可信安全环境、安全工业通信协议、工业控制系统漏洞发现与态势感知、CPS供应链安全体系等。有效保障传统产业数字化转型安全。 |
| 7 | 智能汽车安全 | 针对智能网联汽车发展的安全需求，构建融合终端安全、通讯安全、数据安全的专业化和轻量级的安全技术体系，包括（但不限于）传感器异常数据识别技术、CAN总线认证加密技术、车载IDPS技术、V2X通信安全防护技术、车联网移动APP安全防护与检测技术等。全面护航智能网联汽车产业的创新发展。 |
| 8 | 金融科技安全 | 针对金融科技发展中的各类安全风险，构建促进金融业务创新发展、满足合规监管需要的安全技术体系，包括（但不限于）区块链安全技术、数字货币安全技术、数字反欺诈技术、数据取证技术、金融创新监管沙箱技术等。 |
| 服务业态创新 | 9 | 网络安全保险 | 面向各类组织对冲网络安全残余风险所需的保险工具和服务需求，推动网络安全技术产品的高质量和广覆盖，包括针对不同业态的网络安全保险解决方案，以及面向网络安全保险业态的新型网络安全产品服务。 |
| 10 | 网络安全监管与合规智能化 | 面向国内外网络安全合规监管需求，以智能化技术平台赋能网络安全领域的监管、合规和治理，推动全行业网络安全能力的提升。包括网络安全和数据安全的检测和评估工具、网络安全等保合规工具/平台、个人信息保护自评估服务平台、跨境数据审查和合规服务、网络安全合规情报服务等。 |