

冯皓楠

电话: 18811796269 | 邮箱: fenghaonan@bupt.cn | 政治面貌: 党员
GitHub: <https://github.com/fy222fy> | 博客: https://me.csdn.net/qz_29024667



教育经历

北京邮电大学 网络空间安全学院 计算机技术 工程硕士
北京邮电大学 网络空间安全学院 信息安全专业 本科

2018 年 9 月 - 2021 年 6 月
2014 年 9 月 - 2018 年 6 月

荣誉奖项

- 专利**: 一种利用移动终端实时安全解锁计算机的方法 (专利申请号: 201910918214.X) 2019 年 9 月
- 论文**: [NDSS 2021][一作] A Formal Analysis of the FIDO UAF Protocol.
[TDSC 2023][一作] FIDO Gets Verified: A Formal Analysis of the Universal Authentication Framework.
- 竞赛获奖**: 第四届全国密码技术竞赛特等奖 (2018), 北京邮电大学大学生创新创业实践成果一等奖 (2017)
- 学业**: 国家奖学金(2019)、一等奖学金 (2018 - 2019)、北京邮电大学优秀毕业论文 (2018)
- 漏洞**: 中国移动和包支付 Android 客户端指纹支付安全漏洞 (等级: 中危 编号: CNNVD-202005-1219) 2020 年 5 月

工作经历

- 【实习】蚂蚁集团 OceanBase 部门 - 研发** 2020 年 6 月 - 2020 年 9 月
设计分布式数据库 (OceanBase) 大对象数据类型 (LOB) 的存储方案, 并用 C++ 语言编写一个完整的数据库 Demo 进行验证。
- 【正式】蚂蚁集团 基础安全部 - 安全工程师** 2021 年 9 月 - 2023 年 3 月
基于 MPC 协议 + 可信执行环境 (TEE) 实现可信密态计算系统 (TECC), 获取信通院评测证书, 并完成产品化落地。
① 实现基于 ABY3 协议的基础算子 (C++) ② 完成 ABY3 协议在恶意模型下的安全证明
③ 完成服务端部分产品功能的研发 (JAVA), 适配 TEE 环境 ④ 实现基于 K8S 的产品私有云、公有云部署和运维
- 【正式】蚂蚁集团 隐私计算部 - 安全工程师** 2023 年 3 月 - 至今
实现 TECC 融入隐语 (SecretFlow), 参与隐语中开源产品 (SecretPad) 的研发, 完成隐语联邦学习算法攻防框架的设计与实现。
① 隐语开源产品的研发工作 (JAVA) ② 隐语下联邦学习算法支持、业务支持 (Python)
③ 开源社区技术支持 (Python) ④ 实现联邦学习下算法的自动攻防框架, 自动寻找最优攻击方式

项目实践

- 一种支持手机安全协作的 Windows 系统登录系统 (第四届全国密码技术竞赛)** 2018 年 11 月
该系统借助蓝牙, 利用手机安全地实现了“人来解锁, 人走锁定”的 Windows 辅助登录系统。项目在 2018 年杭州举办的第四届全国密码技术竞赛总决赛中获得特等奖, 并成功申请专利。本人负责密码算法集成、服务端功能、协议形式化验证、主讲等工作。
- 跨平台的密码管理系统 Keyper (北京邮电大学大学生创新创业实践活动)** 2016 年 10 月 - 2017 年 5 月
用户可以在该系统上分等级并且安全地保存自己在各网站或应用上的密码, 不仅可以跨平台使用, 而且结合 U 盾, 实现了指纹验证功能。该项目在大创中获得一等奖, 并参与了第十届全国大学生信息安全竞赛获得了二等奖。
- 人脸识别图书管理系统:** 2019 年 3 月
使用 Python Flask Web + MySQL 框架, 实现了人脸识别图书管理网站。并用 HTML + CSS + JavaScript 进行了简单的前端开发。
- 加密网盘, 加密的实时通讯系统, 支持多用户多策略的云备份系统等 (本科课程设计)** 2014 年 9 月 - 2018 年 6 月
通过多线程实现网盘的并发连接, 通过心跳线判断连接状态, 防止突然断网, 实现文件秒传功能、断点续传等功能 (C#)。
- FIDO 协议的形式化分析 (研究生实验室项目-论文主要的工作)** 2018 年 9 月 - 2020 年 3 月
利用形式化语言 (Applied pi-calculus) 对 FIDO UAF 认证协议进行建模与描述, 并使用 ProVerif 形式化分析工具进行分析, 提出了一套完整的验证结论和漏洞处理方案, 并实践了两种攻击方案。
① 发表 1 篇论文 (NDSS) 和 1 篇期刊 (TDSC) ② 在京东金融和移动和包上复现漏洞, 并申报 CNNVD 漏洞
③ 发现了 ProVerif 工具的漏洞, 并完成贡献和修复 ④ 实现自动寻找最大/最小安全假设的形式化分析工具并开源

技能/其他

- 编程语言**: Python (熟练), Java (熟练), C/C++ (熟悉)
- 专业知识**: 熟悉常用的数据结构、数据库、密码学、隐私计算原理, 了解操作系统、计算机网络等计算机科学技术。
- 其他**: 熟练掌握 ProVerif 形式化分析工具以及 LaTeX; PR、AE 制作视频; 英语 CET6 449。
- 兴趣爱好**: 热爱各种运动, 曾任校短跑队、院篮球队、校足球队队员。

组织经历

- 本科担任班长, 开设学习交流会, 带领班级参与评优获得“北京市优秀班集体”称号, 并连续三年被评为“优秀班干部”;
- 在大创、课程小组中多次担任负责人, 带领团队完成项目, 并上台进行展示; 担任“星火志愿者”, 参加支教等志愿者活动。
- 参与科技部、体育部, 为院内大型活动制作视频, 并协助组织举办校内院内体育文艺活动;