梅本山

mbs2021@163.com · (+86) 188-0018-4976 · mbs0221

教育背景

中国科学院大学, 北京 2019 – 至今
在读博士生 网络空间安全, 预计 2024 年 12 月毕业

中国农业大学, 北京 2017 – 2019
硕士 计算机科学与技术

北京工业大学, 北京 2013 – 2017
学士 计算机科学与技术

研究助理

安全芯片技术 2022 09 – 2022 12
安全芯片技术 2021 09 – 2021 12
概率论与数理统计 2018 09 – 2018 12

本科毕业设计

可信软件基核心模块原型开发

- 可信软件基中的内存分配、协程调度、文本数据解析与无阻塞通道模块的设计与实现

硕士毕业论文

多任务支持向量机的研究与应用

- 多任务学习理论在支持向量机中的研究与应用，包括多任务模型设计和快速求解算法等研究

实习经历

北京恒爱高科有限公司北京 2017 年 1 月 – 2017 年 8 月
实习 软件开发工程师

- 基于 Angular JS 框架实现了酒店预订系统前端
- 采用 C# 的 WPF 框架实现了一个后台应用，用于对接预订系统后端与来电显示盒
- 重构了一个 Android 应用的交互逻辑
- 实现了一个基于蓝牙 BLE 的 Android 心电数据采集应用

北京切尔思云计算科技有限公司北京 2016 年 7 月 – 2016 年 8 月
实习 助理开发工程师

- 学习 JavaScript 上的 MVVM 框架，C# 上的 Entity Framework 与 Git 团队开发
- 基于 MVVM 框架修改 Azure 租户端与管理员端的 WAP 站点主题
- 自定义 Windows Azure Pack (WAP) 工程，开发 RP-Charge 云虚拟机用量展示模块

期刊/会议论文

Cabin: Confining Untrusted Programs within Confidential VM [1] August. 2024
在 AMD SEV-SNP 机密虚拟机内最低特权级中隔离不受信任的应用程序

- 实现了完整的隔离执行框架，可以将 Linux 线程调度到较低虚拟机特权级（VMPL）的用户态

The Road to Trust: Building Enclaves within Confidential VMs [2] August. 2024

在 AMD SEV-SNP 机密虚拟机内最高特权级实现 Enclave 抽象

- 这个工作类似在 ARM TrustZone 上提供 Enclave 编程模型
- 相关技术支持（AMD SEN-SNP 和 linux-svsm）
- 底层技术方案讨论和论文撰写

SVSM-KMS: Safeguarding Keys for Cloud Services with Encrypted Virtualization [3] August. 2024

基于安全虚拟机服务框架（SVSM）的密钥管理系统（KMS）

- 一个在虚拟机内最高特权级部署的 KMS，类似基于 ARM TrustZone 的 keymaster
- 提供 RESTful API，为 HDFS 等云上应用提供密钥管理服务

Safe sample screening for regularized multi-task learning [4] July. 2020

针对多任务学习算法的安全样本筛选

- 研究了安全筛选规则（SSR）在多任务支持向量机上的加速效果

Multi-task ν-twin support vector machines [5] November. 2019

一种新型多任务分类学习算法

- 提出了一种新型的多任务二分类学习算法，分析了模型的数学性质

Multi-task least squares twin support vector machine for classification [6] December. 2018

一种新型多任务分类学习算法 [6]

- 提出了一种新型的多任务二分类学习算法，并给出了对应的优化求解算法

♡ 获奖情况

科技创新奖，北京工业大学 校级	2016 年 12 月
铜奖，第二届鼎新杯北京工业大学学生创新创业大赛	2016 年 11 月
三等奖，全国大学生信息安全竞赛 作品赛	2016 年 08 月
学习优秀奖，北京工业大学 校级	2014 年 12 月

项目经历

国家级大学生创新创业训练计划 立项资助并结题 技术负责人	2016 年
北京工业大学第十六届星火基金 立项资助并结题 项目负责人	2015 年

IT 技能

- 编程语言：C/C++/C#/Java/JavaScript/Python/Rust/Matlab
- 硬件描述语言：Verilog/Chisel
- 平台: Windows, Linux, Android
- 数据库：MySQL, SQLite, SQL Server
- 开发: Linux 内核, Android 应用, Web 前后端

♡ 其他

- 语言: 英语 - 熟练 (六级 465)

References

[1] B. Mei, S. Xia, W. Wang, and D. Lin, "Cabin: Confining untrusted programs within confidential vm," *The 2024 International Conference on Information and Communications Security*, 2024.

[2] W. Wang, L. Song, B. Mei, S. Liu, S. Zhao, S. Yan, X. Wang, D. Meng, and R. Hou, "The road to trust: Building enclaves within confidential vms," *arXiv preprint arXiv:2402.11438*, 2024.

[3] B. Mei, W. Wang, and D. Lin, "Svsm-kms: Safeguarding keys for cloud services with encrypted virtualization," *The 6th International Conference on Science of Cyber Security*, 2024.

[4] B. Mei and Y. Xu, "Safe sample screening for regularized multi-task learning," *Knowledge-Based Systems*, vol. 204, p. 106248, 2020.

[5] B. Mei and Y. Xu, "Multi-task ν-twin support vector machines," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11329–11342, 2020.

[6] B. Mei and Y. Xu, "Multi-task least squares twin support vector machine for classification," *Neurocomputing*, vol. 338, pp. 26–33, 2019.