

# 汽车物理信息安全研究小组简介

王思山<sup>1</sup>

<sup>1</sup> 湖北汽车工业学院  
汽车物理信息安全研究小组

2023





# 目录 I

## 1. 研究小组基本情况

- 研究小组介绍
- 研究小组成员

## 2. 研究目标与内容

- 研究目标
- 研究背景与研究内容

## 3. 研究平台和基础

- 研究平台
- 研究基础

## 4. 团队对外合作

## 5. 团队管理

## 6. 资源参考

# 研究小组介绍

## 名称

“**汽车物理信息安全研究小组**”是湖北汽车工业学院汽车工程师学院为主要成员的研究群体。

## 形象标识



## 联系信息

- 网址: <https://gnuarmfuns.github.io>
- 邮件: [gnuarmfuns@huat.edu.cn](mailto:gnuarmfuns@huat.edu.cn)

# 研究小组介绍

## 资源信息

- 虚拟仿真省级一流课程: <http://selfdriving.huat.edu.cn>
- 代码托管空间: <http://265n8573t2.zicp.fun>
- Jetbrain 全家桶: <https://huat.jetbrains.space>
- 飞书知识库: <https://gnuarmfuns.feishu.cn/wiki>
- 自建课程: <https://10-200-11-127-9090.wvpn.huat.edu.cn/>
- 团队网址: <https://gnuarmfuns.github.io>

## 校内访问

- GPU 服务器地址: 10.202.6.4/5

# 研究小组成员



小组负责人

研究生

本科生



# 个人简介

## 王思山

- |      |  |
|------|--|
| 研究方向 | 汽车物理信息系统安全研究、包括车载网络攻击与防御、汽车嵌入式系统安全和车辆行为监控与识别；  |
| 个人简介 | <ul style="list-style-type: none"><li>• 参与或主持国家级高新科技计划项目 1 项、湖北省省部级科研项目 4 项和多项十堰市市级项目、主持或参与东风等企业的横向课题，课题经费 300 多万元；</li><li>• 发表论文 14 篇，其中 SCIEI 检索论文 4 篇，合作发表 TOP 期刊 2 篇，合作申请专利 15 个。</li></ul> |

# 研究目标



## 目标

团队旨在解决新型汽车电子电气架构（EEA）下汽车的网络安全与数据安全问题。主要研究方法是采用**人工智能技术**和**嵌入式系统开发**为工具的汽车信息分析与数据挖掘。

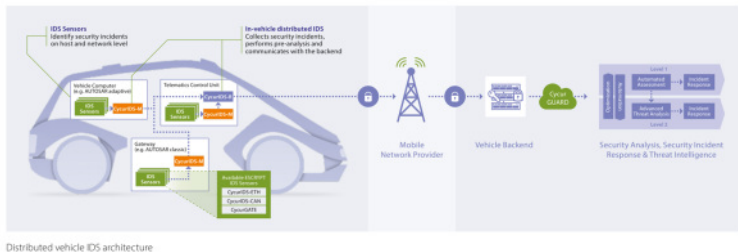


图 1: 汽车防护系统全景图

# 研究背景

## 智能汽车攻击面的扩展

随着汽车智能化的发展,智能汽车攻击面急速扩展,带来未知和不可预测的攻击点。



图 2: 智能汽车攻击面



# 研究背景



## 汽车 EEA 架构的演变

汽车的智能化和信息化使得 EEA 架构从专用封闭网络向开发通用网络演变,降低了攻击的门槛。

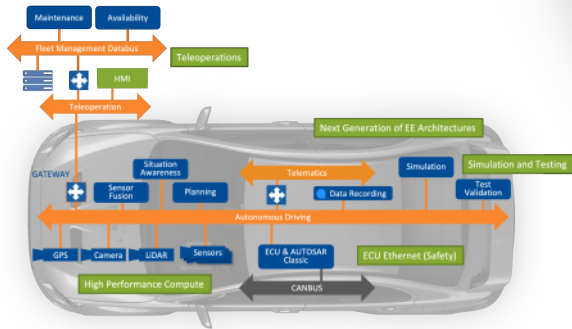


图 3: 下一代 EEA 架构

<sup>1</sup><https://www.rti.com/products/dds-standard>

# 研究内容

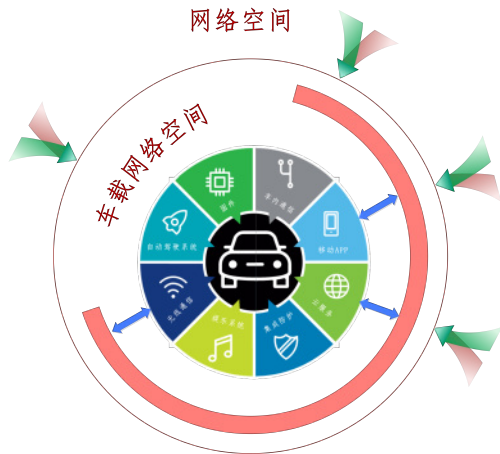


图 4: 汽车网络空间与网络空间

# 研究内容

## 潜在的解决方案

- Cryptography
  - AUTOSAR 软件包中添加的信息安全组件 SecOC;
  - TLS 技术在汽车以太网中的应用;
  - Hardware Security Modules (HSMs) 和 Hardware Security Engine(HSE);
  - 安全启动, 固件安全。
- Anomaly/Intrusion Detection (IDS) and Prevention (IPS) systems
  - 基于签名技术的通信;
  - 基于异常检测, 如基于上下文的分析技术;
  - 数据驱动的大数据分析, 数据挖掘。
- 行业规范
  - ISO/SAE 21434 –standard for cyber security in automotive;
  - 汽车软件升级通用技术要求

# 研究内容



## 汽车入侵检测防御系统 (IDPS)

基于嵌入式多核 MCU 硬件，设计面向嵌入式 TCP/IP 协议栈的动态可配置的入侵检测与防御系统。

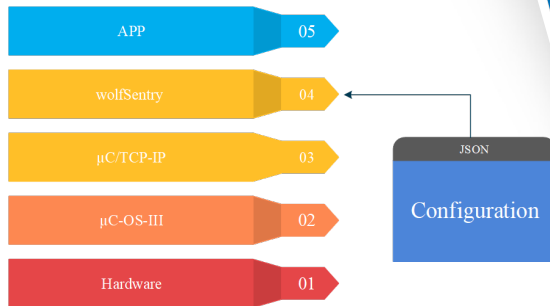


图 5: 基于嵌入式 RTOS 和 TCP 协议栈的 IDPS

<sup>1</sup><https://www.wolfssl.com/products/wolfssentry>

# 研究内容



## 基于大数据和机器学习的入侵检测

基于机器学习的恶意代码检测具有较高的准确率，此技术可对未知的恶意代码实现自动化的分析。

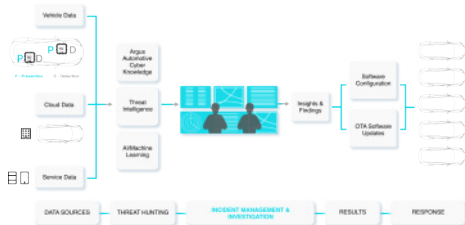


图 6: Vehicle Security Operations Center (VSOC)

<sup>1</sup> <https://ieee-dataport.org/documents/tow-ids-automotive-ethernet-intrusion-dataset>

<sup>2</sup> <https://ieee-dataport.org/open-access/automotive-ethernet-intrusion-dataset>

# 研究内容

## HSE 与可信固件

通过硬件加密引擎（HSE）实现固件的加密与签名验证。

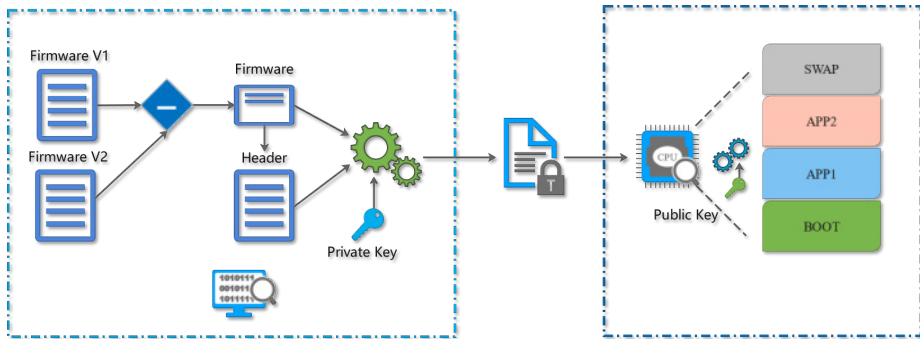


图 7: 固件更新流程

<sup>1</sup><https://www.wolfssl.com/products/wolfboot>

# 研究内容



## CAN 和 CAN FD 故障注入

设计基于 FPGA 的 CAN 和 CAN FD 硬件解析器，可以用于对总线的攻击与安全性测试。

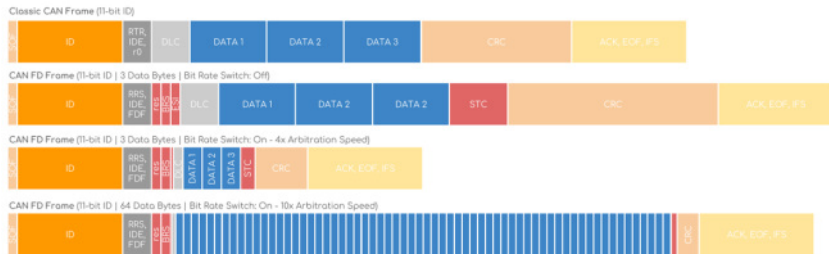


图 8: CAN 和 CAN FD 信息格式

<sup>1</sup>[https://gitlab.fel.cvut.cz/canbus/ctucanfd\\_ip\\_core](https://gitlab.fel.cvut.cz/canbus/ctucanfd_ip_core)

# 研究内容



## 基于机器学习的驾驶行为分析

基于机器学习方法和驾驶行为分析的车辆加速度预测模型。首先对驾驶行为数据进行预处理，选取目标车辆的相对距离、相对速度和加速度作为特征变量来描述驾驶行为，驾驶员画像。

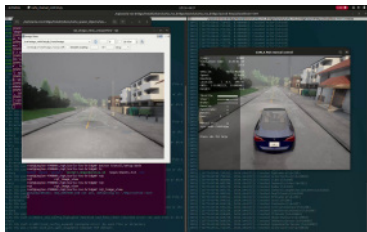


图 9: 基于虚拟仿真环境的数据训练平台

<sup>1</sup><https://arxiv.org/abs/1607.03611>



# 研究内容

## 联邦学习在隐私保护中的应用

联邦迁移学习将联邦学习的思想和迁移学习的相结合，对数据降维和保护各方的数据隐私。



图 10: 联邦学习基本原理

<sup>1</sup> <https://www.ndss-symposium.org/ndss-program/autosec-2021/>

# 研究内容



## 传感器与自动驾驶系统攻击

在自动驾驶系统和传感器信息处理软件中，一般采用人工智能技术，但是人工智能技术的泛化性不足，甚至会出现弱点，因此传感器及数据的攻击可能给车辆带来致命打击。



图 11: 虚假障碍物

<sup>1</sup> <https://www.ndss-symposium.org/ndss-program/autosec-2021>

# 研究平台



图 12: 教学用实验室



图 13: 学生办公场地

# 研究平台



图 14: MPC5748G-GW-RDB



图 15: MPC574XG-MB

# 研究平台

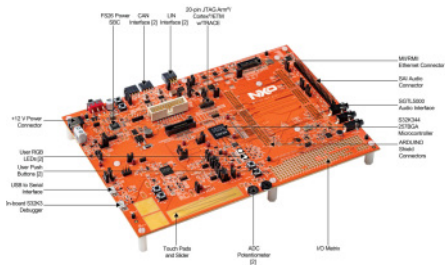


图 16: S32K3X4EVB-Q257

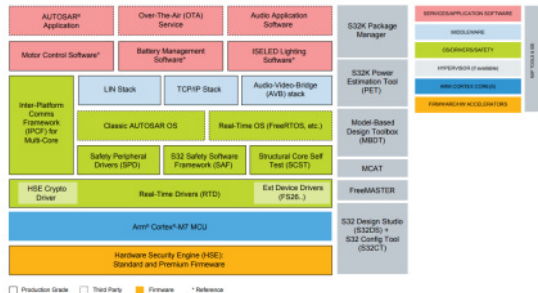


图 17: S32K 软件架构

# 研究平台



图 18: 四轮驱动底盘



图 19: 四足机器人

# 研究平台

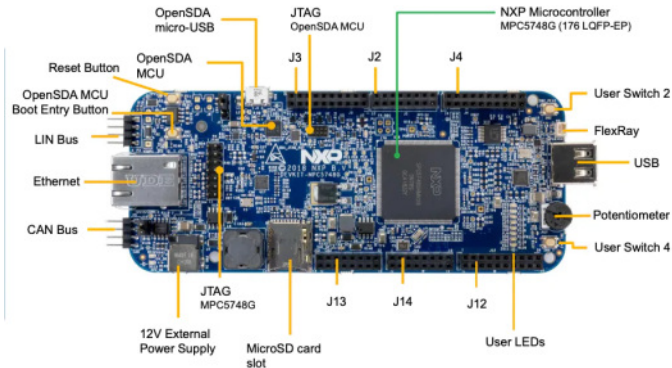


图 20: DEVKIT-MPC5748G

<sup>1</sup> <https://www.nxp.com/document/guide/get-started-with-the-devkit-mpc5748g:NGS-DEVKIT-MPC5748G>

# 研究平台

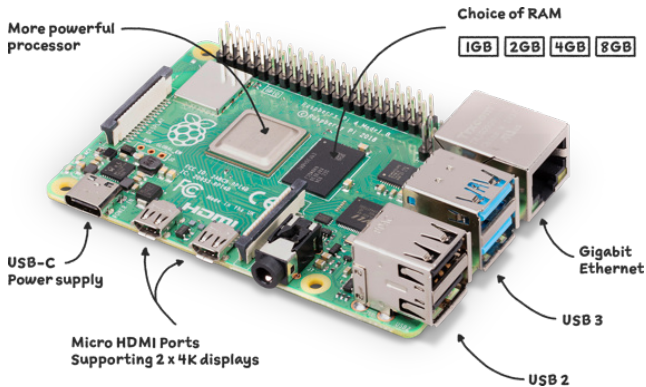


图 21: Raspberry Pi

<sup>1</sup><https://www.raspberrypi.com/products/raspberry-pi-4-model-b>



# 研究平台



图 22: CAN 总线测试平台

# 研究平台



图 23: 半实物仿真平台

## 基于 $\mu\text{C}/\text{OS-III}$ 的 $\mu\text{C}/\text{TCP-IP}$ 协议栈

A compact, reliable, high-performance TCP/IP protocol stack designed for embedded applications, featuring dual IPv4 and IPv6 support.

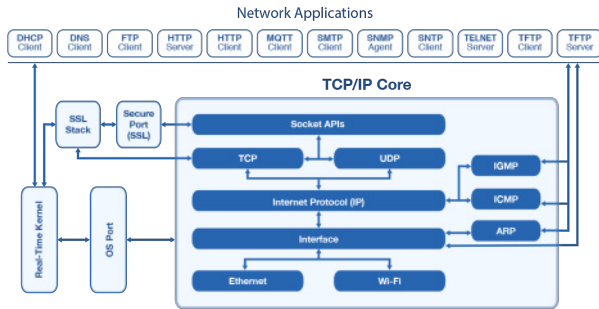


图 24: 网络协议栈  $\mu\text{C}/\text{TCP-IP}$

<sup>1</sup><https://github.com/weston-embedded>

# 研究基础



## Xpediton Enterprise

企业级硬件设计工具套件。

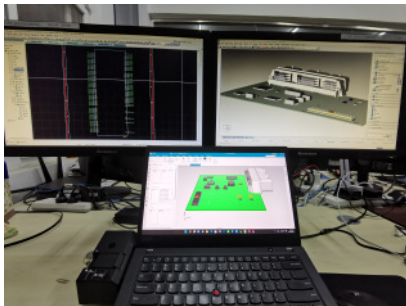


图 25: Xpediton Enterprise

# 研究基础

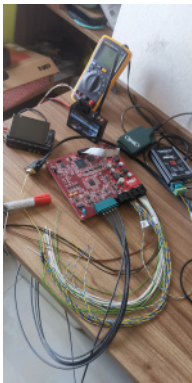


图 26: Automotive Ethernet



图 27: Xavier 控制器

# 研究基础



## 自动驾驶开发

面向 L4 的智能底盘控制器设计和 ADAS 功能开发。



图 28: 东风智能底盘

# 研究基础



## 高校合作

- 中山大学网络安全安全学院
- 南京邮电大学网络安全安全学院

## 企业合作

- 岚图汽车-架构与座舱
- 恒润科技-信息安全部门
- 工信部电子标准化研究院
- 禾骋科技
- 格陆博科技
- 环宇智行

# 教师责任与学生要求

## 教师责任

- 导师是学生的第一责任人;
- 导师为学生提供必要的科研环境、设备、资金和问题的解决;
- 导师主要负责学生的学业, 同时给与学生必要的人为关怀;

## 学生的基本要求

- 自律;
- 注重效率;
- 时间的投入;
- 具有足够的主动性;
- 具有批判性思维。



# 团队管理



## 团队日常运行管理

- 学生应遵守实验室管理的基本准则，确保实验室运行安全；
- 在使用设备前要熟悉设备的操作手册，确保实验室装置和设备安全；
- 学生应每周对自己的工位进行整理，并协同实验室学生整理和打扫实验室；
- 实验室至少每两周开一次例会，例会主要内容是工作汇报、下一步工作计划和需要解决的问题；
- 工作汇报在开会前通过飞书向团队呈现，在实验室大屏上现场汇报；
- 在实验室不允许做与学习和研究不相关的事务；
- 学生在实验室要和睦相处，有问题直接当面解决；
- 实验室办公空间原则上不接待其他同学。

# 学生培养路径

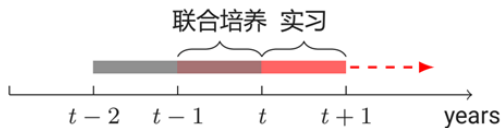


图 29: 本科生培养过程

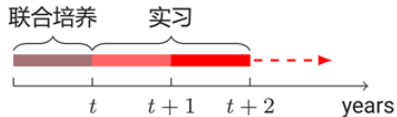


图 30: 研究生培养过程

# 学生培养路径

## 研究生专业与毕业条件

- 通过个人背景和发展方向确定研究生专业方向;
- 研究生第一年为基础培养, 有以下目标:
  - 通过四六级考试;
  - 非计算机本科专业, 通过三级计算机等级考试 (建议信息安全方向);
  - 根据以上提供的开发系统, 熟练掌握一门语言和一个系统的使用与开发;
  - 组队打汽车信息安全相关的比赛;
- 研究生第二年为专业素质培养, 有以下目标:
  - 下厂实习 6-12 个月;
  - 确定自己的研究方向, 开题前完成一篇符合毕业条件论文;
  - 根据个人情况发表 SCI 论文和申请发明专利;
  - 如有条件到中山大学或者南京邮电交流一个月以上;
- 满足学校的专业毕业条件, 根据个人情况至少完成一个发明专利申请和一篇 SCI 论文。

# 资源参考

## 网址

- 中国大学 MOOC – <https://www.icourse163.org/>
- Coursera – <https://www.coursera.org/>
- 中文数学 Wiki – <https://math.fandom.com/zh/wiki/>
- JetBrains 全家桶 – <https://www.jetbrains.com/>
- Latex – <https://www.overleaf.com/>
- Tutorialspoint – <https://www.tutorialspoint.com>
- 3blue1brown – <https://www.3blue1brown.com/>
- OfficePlus – <https://www.officeplus.cn/>
- 专利检索 – <https://pss-system.cponline.cnipa.gov.cn/conventionalSearch>
- Sci-Hub – <https://sci-hub.se/>
- 科研者之家 – <https://www.home-for-researchers.com/>

# Thanks

Doubts and Suggestions

[gnuarmfuncs@huat.edu.cn](mailto:gnuarmfuncs@huat.edu.cn)

湖北汽车工业学院  
HUBEI UNIVERSITY OF AUTOMOTIVE TECHNOLOGY