2022 届硕士专业学位研究生学位论文

分类号：_____ 学校代码：10269

密　级：_____ 学　　号：71194501214

East China Normal University

硕士专业学位论文

Master's Degree Thesis (Professional)

智能网联汽车安全模型风险评估方法设计及实现

院　　系:	**信息学部软件工程学院**
专业学位类别:	**工 程 硕 士**
专业学位领域:	**软 件 工 程**
指 导 教 师:	**刘 虹　副研究员**
学 位 申 请 人:	**颜　卿**

2022 年 9 月 9 日

Thesis for Master's Degree (Professional) in 2022

University Code: 10269

Student ID: 71194501214

EAST CHINA NORMAL UNIVERSITY

This is English Title

Department:	School of Computer Science and Technology
Category:	Master of Engineering
Field:	Computer Technology
Supervisor:	x x (Professor)
Candidate:	x x

October, 2021

华东师范大学学位论文原创性声明

郑重声明：本人呈交的学位论文《智能网联汽车安全模型风险评估方法设计及实现》，是在华东师范大学攻读硕士/博士（请勾选）学位期间，在导师的指导下进行的研究工作及取得的研究成果。除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确说明并表示谢意。

作者签名:_____ 日期: 年 月 日

华东师范大学学位论文著作权使用声明

《智能网联汽车安全模型风险评估方法设计及实现》是本人在华东师范大学攻读学位期间在导师指导下完成的硕士/博士（请勾选）学位论文，本论文的研究成果归华东师范大学所有。本人同意华东师范大学根据相关规定保留和使用此学位论文，并向主管部门和相关机构如国家图书馆、中信所和“知网”送交学位论文的印刷版和电子版；允许学位论文进入华东师范大学图书馆及数据库被查阅、借阅；同意学校将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于（请勾选）

() 1. 经华东师范大学相关部门审查核定的“内部”或“涉密”学位论文 *，于年月日解密，解密后适用上述授权。

() 2. 不保密，适用上述授权。

导师签名:_____ 本人签名:_____

年 月 日

* “涉密”学位论文应是已经华东师范大学学位评定委员会办公室或保密委员会审定过的学位论文（需附获批的《华东师范大学研究生申请学位论文“涉密”审批表》方为有效），未经上述部门审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权）。

硕士学位论文答辩委员会成员名单

姓名	职称	单位	备注
xxx	xxx	xxx	主席
xxx	xxx	华东师范大学	
xxx	xxx	华东师范大学	

摘　要

随着工业智能、大数据、移动互联网、物联网、云计算等技术的飞速发展，汽车正以一种全新的方式，从传统的封闭系统，转向智能城市，智能交通，智能通信，智能驾驶等新的概念融合的开放系统。现代智能网联汽车拥有许多感应器，其内部的各种线路将电子控制单元和传感器彼此相连、融合，构成了一个包含几百万行代码的汽车互联网络。因而，复杂的网络配线系统、各类电子控制单元、传感器通信等都将面临前所未有的安全威胁和攻击，汽车网络安全问题正变得比以往任何时候都更加突出。正在起草的 SAE J3061 和 ISO/SAE 21434 也表明，汽车网络安全已经被提升到与功能安全同等或更重要的地位。

本文主要有以下三个贡献点：

• 首先对智能网联车辆的体系结构进行了研究，并对其所面临的安全威胁进行了分析，并对其攻击来源和攻击途径进行了分析；

• 不仅利用传统构建攻击树对智能网联汽车系统进行了威胁建模，而且还提出了一种基于微软 STRIDE 的改进后的攻击树威胁建模方案 (称为 SATT);

• 将 SATT 应用在智能网联汽车复杂的网络攻击路径中并构建模型，对构建的攻击树威胁建模，基于 FAHP（模糊层次分析法）计算了攻击概率，并验证了模型的可用性。

本文旨在通过对智能网联汽车威胁建模以及安全风险评估的研究，使得更多学者关注该领域，以此希望对智能网联汽车威胁安全建模和安全风险评估领域的发展起到推动作用。

关于本文章节安排, 首先，介绍了智能网联汽车的安全架构并提出了一种分层的车载网络模型, 并对智能网联汽车网联系统进行了介绍，将其划分为 TSP 云端通信、V2X 通信、车载通信三个部分进行详述，阐述了车内外的通信原理和机制。接

着对智能网联汽车所面临的七大安全威胁进行了分析和整理，然后将攻击入口划分为物理攻击、近距离无线攻击、远距离无线攻击三个方面分布进行了详述，并对智能网联汽车的攻击路径进行了分析。紧接着介绍了安全威胁的主流模型。威胁模型分析有助于汽车网络安全早期概念阶段的开发, 传统的安全威胁分析方法主要有: 微软的 STRIDE 威胁模型, 攻击树威胁模型还有新型的 HEAVENS 以及 EVITAS 等威胁模型。目前主流的威胁模型是: 攻击树威胁模型和 STRIDE 威胁模型。然而，基于传统攻击树的威胁分析存在主观因素多、准确率低的缺点。本文提出了 SATT 新型威胁建模方案。因此，借助微软的 STRIDE 威胁模型，我们识别与资产相对应的威胁，并构建一个更全面的攻击树。最后，对于攻击树的每个威胁攻击序列，基于 FAHP 计算攻击概率。此外，将 FAHP 与层次分析法和传统方法进行了比较。最后对一辆自动驾驶实验车进行了网络攻击的路径分析及建模实验，并对模型进行了基于该威胁模型的安全风险评估，最后对实验评估数据进行了分析，验证了模型的可用性，取得了不错的效果。结果表明，该方法在安全威胁分析中起到了一定的作用。

关键词: 智能网联汽车，风险评估，威胁建模, STRIDE, 攻击树, SATT

ABSTRACT

I

Keywords: *Keywords 1; Keywords 2; Keywords 3; Keywords 4; Keywords 5*

目录

图目录

表目录

第一章 绪 论

1.1 研究背景及意义

近些年，由于移动网络、物联网以及工业智能化等技术的迅速发展，汽车产业链也迎来了大变革，汽车由传统的代步工具发展为集出行、娱乐、智能为一体的行驶在马路上的电脑。汽车的智能和互联性正在推动车载网络系统的复杂性和多样性的增加。智能网联汽车目前正处于渗透率快速提升的阶段，智能网联汽车能够将手机的百万量级的应用融合到汽车中，实现汽车应用的量级突破。智能网联汽车有望继智能手机之后，成为新一代的超级终端。根据中商情报网数据显示 [1]，2016-2020 年我国智能网联汽车产业规模呈现连续上涨趋势，2020 年产业规模增长到了 2556 亿元，同比增长 54.3%。预计，2022 年智能网联汽车产业规模将超 3500 亿元。

汽车的智能和互联性正在推动车载网络系统的复杂性和多样性的增加。信息通信技术 (ICT) 给传统车辆带来了巨大的创新，也给现代车辆带来了重大的安全挑战。原本隔离的车载网络连接到外部，增加了互联和自动化车辆 (CAV) 的攻击面，并带来了新的安全风险。汽车网络安全引起了公众的关注。

Checkoway 等人 [2] 从网络安全的角度描述了现代车辆的安全威胁模型和外部攻击媒介，并研究了如何进入车辆的内部网络。2015 年，查理 · 米勒和克里斯 · 瓦拉塞克 (Chris Valasek) 演示了如何通过攻击车载信息娱乐 (IVI) 系统来入侵一辆吉普车的车载网络，并导致车辆的异常行为，导致 140 万辆汽车被召回。与此同时，自动网络安全开始引起公众的广泛关注 [3]。Koscher 等人 [4] 通过嗅探并向控制器局域网 (CAN) 总线注入恶意代码，通过拒绝服务 (DoS) 攻击阻断电子控制单元 (ECU) 通信，从而控制车辆的多个功能模块。在 [5] 中，针对 CAN 的安全缺陷，提出了广播、无认证、无加密、仲裁优先、接口易访问等五种对 CAN 的攻击方法。除了通过 CAN 攻击车辆，本地互联网络 (LIN) [6]，FlexRay [7] [8] 总线系统和其他外部接口，例如通用串行总线 (USB)，蓝牙，Wi-Fi，蜂窝和车载诊断 (OBD)，也可用于非法访问车载网络 [9]。

安全威胁远不止前面提到的那些。因此，有必要在车辆的早期开发阶段进行安全威胁分析，以找出威胁漏洞，实施安全措施，预防安全问题。在汽车领域有许多威胁分析和风险评估 (TARA) 方法。SAE J3061 [10] 作为第一本针对网络物理车辆系统的网络安全指南，提出了 EVITA(电子安全车辆入侵保护应用程序)、HEAVENS (修复漏洞以增强软件安全性)、TVRA(威胁、漏洞和风险分析)、OCTAVE(运营关键威胁、资产和漏洞评估) 以及其他安全分析方法。然而，并不是所有提到的方法都适用于智能网联汽车。TVRA 是为数据和电信网络开发的，不适用于汽车。OCTAVE 适用于企业信息安全的风险评估，但不适用于汽车系统。只有 EVITA 和 HEAVES 更适合智能汽车领域。

因此，以智能网联信息系统为载体的智能网联汽车，其威胁安全的研究意义将是十分重要和深远的。

- 智能网联汽车的信息安全关系到人类的生命和财产的安全，因此，对智能网联车辆的攻击与威胁问题进行深入的研究，可以促进整车厂商对其进行改进，以保障人民的生命和财产的安全。
- 通过及时发现智能网联车辆网络系统的缺陷，并对其进行攻击的路径进行描述，可以将智能网联车辆所面临的安全风险进行全面、明确的展现，帮助安全开发者了解到相关知识，并及时定位风险源，从而为进一步研究更安全的防护措施打下基础。
- 基于攻击树的威胁建模分析可以建立威胁和安全属性之间的直接映射。它支持更好地理解和列出 TOE 的威胁。使评价结果更加具有说服力。

1.2 国内外研究现状

由于智能网联汽车的高度集成及其智能化，其功能越来越丰富，系统复杂度也越来越高，对外暴漏的接口也随之增多。从有线网络到无线网络，再到汽车上的各种插口，汽车与外界联系的手段不断增加，同时网络中将不可避免的存在各式各样的漏洞，例如软件漏洞、代码漏洞、硬件接口漏洞等，因此，对其攻击的手段也将变得越来越多样化，对其攻击路径的分析也变得越发艰难，以下列出一些当

前国内外学者研究的比较典型的漏洞利用。

Checkoway 等人从网络安全的角度描述了现代车辆的安全威胁模型和外部攻击媒介，并研究了如何进入车辆的内部网络。他们试图通过系统分析现代汽车的外部攻击面来解决这个问题。通过广泛的攻击媒介 (包括机械工具、CD 播放器、蓝牙和蜂窝无线电) 进行远程利用是可行的，此外，无线通信信道允许远程车辆控制、位置跟踪、车内音频泄漏和盗窃。CAN 协议是一种广泛应用于车载网络的总线协议。CAN 协议有几个内在漏洞，例如广播传输、无认证、无加密、基于 ID 的优先级方案和可用接口。这些漏洞使车载网络容易受到恶意攻击。Liu 等人总结了以下有效攻击方法: 帧嗅探, 帧伪造, 帧注入, 重放攻击, 拒绝服务攻击等。此外新型的智能网联汽车具有手机 APP 等能操控智能网联汽车本身的外部操控智能设备因此从手机端 APP 等进行攻击也是目前比较流行的一个新颖攻击方法。

已有的这些研究表明，智能网联汽车的发展尚未成熟，仍然存在较多的安全隐患。尤其是针对无线系统的攻击，其隐蔽性强，覆盖范围广，往往会给驾驶者带来严重的安全隐患和灾难性后果。当前对于智能网联汽车的安全意识正在逐步增强，但是并没有形成统一的理论体系和安全标准，智能网联汽车的安全问题不仅仅牵涉到经济问题，还关系驾驶者和其他人的生命安全。因此，研究整个智能网联汽车的信息安全至关重要.

1.3 本文工作和主要贡献

本文贡献点主要有如下三个:

1. 智能网联汽车架构及威胁分析

   分析智能网联汽车的系统架构及其通信机制，并从云平台、APP、T-BOX、IVI、CAN 总线、ECU、车间通信七个方面分析智能网联汽车所面临的安全威胁。

2. 分析了 TARA 中主流的威胁建模方法如 HEAVENS, IEVITAS, STRIDE, 攻击树等。

   研究智能网联汽车的威胁模型，结合 STRIDE 和攻击树模型提出一种创新的名为 SATT 的威胁建模方法，对实际商用的汽车外部复杂网络中的通信和 TSP 部分进行威胁建模，并对两种建模方法进行比较和分析。

3. 风险评估与威胁框架

研究复杂网络环境下智能网联汽车的远程攻击方法，对某知名品牌汽车进行漏洞挖掘和渗透测试，利用硬件拆检、协议分析、算法破解和软件逆向等多种方式分析漏洞，并编写软件，成功获取目标车辆敏感信息，并实现了远程入侵和完全控制，所阐述的一系列攻击方法在智能网联车领域又是一种全新的攻击手段，为智能网联汽车安全研究提供更多的思考空间和方向，为智能网联汽车的安全发展奠定基石。

1.4 论文组织结构

本文主要研究针对智能网联汽车领域的威胁分析与风险评估。是在车联网概念阶段应用的一种分析技术，可帮助识别特征的潜在威胁并评估与已识别威胁相关的风险。具体章节结构如下：

第一章，绪论。主要介绍的是本文章的研究背景以及意义，对当下智能网联汽车（ICV）的信息安全及风险评估领域的研究进行了介绍和总结，并对文章的主要工作和文章的章节进行了介绍。

第二章，相关概念及研究。对本文中的相关理论与技术基础进行了详细介绍，分别对 ICV 的系统架构、TSP 系统的组成、ICV 通信技术以及智能网联汽车常见的七大安全威胁做了介绍。对 ICV 的攻击来源做了分析和整理。对目前现有 TARA 常用方法进行了整理和分类。

第三章研究智能网联汽车的威胁模型，介绍了传统的 STRIDE 威胁建模方法尝建模分析和攻击树模型。

第四章，研究智能网联汽车的威胁模型，结合 STRIDE 和攻击树模型提出一种创新的名为 SATT 的威胁建模方法，对实际商用的汽车外部复杂网络中的通信和 TSP 部分进行威胁建模。

第五章，基于上述提出的威胁建模方法研究复杂网络环境下智能网联汽车的远程攻击方法，对某知名品牌汽车进行漏洞挖掘和渗透测试，利用硬件拆检、协议分析、算法破解和软件逆向等多种方式分析漏洞，并编写软件，成功获取目标车辆敏感信息，并实现了远程入侵和完全控制，更为关键的是，还攻破一系列汽车车主

的账号，从而可以实现大批量控制。

第六章，总结与展望。对本文工作进行总结，分析本文的不足以及尚未解决的问题，同时对下一步工作进行展望。

第二章　相关概念及研究

本章首先介绍了 CAV 的网络系统架构，主要从六个方面介绍，包括 TSP 云服务、V2X 车载通信、车载网络、CAN 总线、IVI、T-BOX，分别分析了它们的系统架构的组成和原理，最后从云平台、APP、T-BOX、IVI、CAN 总线、ECU、车间通信七个方面介绍了智能网联汽车所面临的安全威胁

2.1　智能网联汽车联网系统架构

2.1.1 车载网络架构划分

智能网联汽车是指车联网与智能车的有机联合，是搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与人、路、后台等智能信息交换共享，实现安全、舒适、节能、高效行驶，并最终可替代人来操作的新一代汽车 [11]。车联网在智能辅助驾驶、智能交通规划等领域，都具有不错的应用前景。车载网络架构如图 2.1 所示。这是一个以域为中心的体系结构，具有以太网作为主干，分为五个领域: 动力系统、底盘、车身、信息娱乐和高级驾驶辅助系统 (ADAS)。每个域控制器通过一个中央网关与以太网主干连接。CAN/CAN FD 和 LIN 用作每个域中的通信协议。此外，车载网络可以通过远程信息处理单元和接口 (如 OBD、USB 和 Wi-Fi) 连接到外部网络。这种集中式架构通过域控制器和以太网提供智能网联汽车所需的计算和通信能力。然而，车辆的外部接口也增加了。这些开放的接口给智能网联汽车带来了新的攻击面和安全隐患。为了更好地描述安全威胁，我们提出了基于这种架构的三层车载网络模型。

- 终端节点层: 这一层包含车辆中各个域的 ECU 节点、传感器和执行器。这是模型的中心部分。如果受到攻击，它会直接影响车辆的安全。
- 网络通信层: 该层由各种车载网络通信协议组成，如以太网、CAN/CAN FD、LIN 等。这一层的主要目的是传输数据并与之交互。
- 接口设备层: 这一层包括各种可以与外部环境交互的通信设备接口，如 OBD、USB 等。

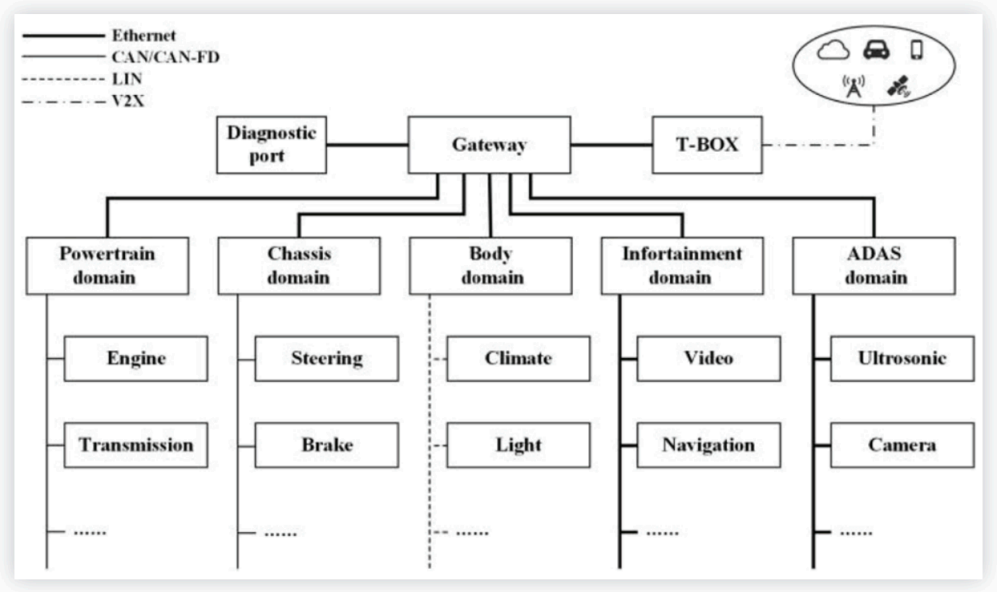

图 2.1　车联网网络架构图

目前的汽车结构中，车辆内部网络主要由 CAN 总线和 ECU 组成。ECU 是嵌入式设备，包括各种智能系统，如无钥匙控制单元（KCU，key control unit）、防抱死制动系统（ABS，antilock brake system）、BCM 和紧急制动辅助（EBA，electronic brake assist）等，通常被用于监控车辆状态、控制车辆行为。CAN 总线是 ECU 之间通信的桥梁，负责将汽车内部各 ECU 连接起来，使它们能够进行高效的信息通信。

CAN 总线与大量嵌入式设备的多功能连接在为用户提供便利服务的同时，也带来了一些易入侵的接口。恶意攻击者能够利用车载信息娱乐（IVI，in-vehicle infotainment）系统的 USB 接口和 Wi-Fi 接口恶意窃取用户隐私信息，甚至能够利用 IVI 系统入侵 CAN 达到控制车辆的目的。车载诊断（OBD-II，on-board diagnostics-II）接口是美国工程师协会在 20 世纪 90 年代制定 CAN 总线规范时规定开放的车载诊断接口，通常被用来检测汽车故障并监测汽车尾气排放。然而，OBD-II 接口也很容易成为恶意攻击者非法窃取汽车 CAN 总线数据的入口。此外，T-BOX、胎压侦测系统（TPMS，tire pressure monitoring system）、RKE、ABS 等大量嵌入式设备都存在可被利用的攻击面。这里简单的介绍上述英文名词的定义。

- CAN 控制器局域网 (Controller Area Network，简称 CAN 或者 CAN bus) 是一种功能丰富的车用总线标准。被设计用于在不需要主机（Host）的情况下，允

许网络上的单片机和仪器相互通信。它基于消息传递协议，设计之初在车辆上采用复用通信线缆，以降低铜线使用量，后来也被其他行业所使用。

- ADAS 可帮助驾驶员进行驾驶和停车功能。通过安全的人机界面，ADAS 提高了汽车和道路的安全性。ADAS 使用传感器和摄像头等自动化技术来检测附近的障碍物或驾驶员错误，并做出相应的反应。ADAS 可以实现不同级别的自动驾驶，具体取决于车内安装的功能。
- OBD 是英文 On-Board Diagnostics 的缩写，中文翻译为“车载自动诊断系统”。这个系统将从发动机的运行状况随时监控汽车是否尾气超标，一旦超标，会马上发出警示。当系统出现故障时，故障 (MIL) 灯或检查发动机 (Check Engine) 警告灯亮，同时动力总成控制模块 (PCM) 将故障信息存入存储器，通过一定的程序可以将故障码从 PCM 中读出。根据故障码的提示，维修人员能迅速准确地确定故障的性质和部位。
- ECU（Electronic Control Unit）电子控制器单元，又称为汽车的“行车电脑”，它们的用途就是控制汽车的行驶状态以及实现其各种功能。主要是利用各种传感器、总线的数据采集与交换，来判断车辆状态以及司机的意图并通过执行器来操控汽车。
- T-BOX 作为无线网关，通过 4G 远程无线通讯、GPS 卫星定位、加速度传感和 CAN 通讯等功能，为整车提供远程通讯接口，提供包括行车数据采集、行驶轨迹记录、车辆故障监控、车辆远程查询和控制（开闭锁、空调控制、车窗控制、发送机扭矩限制、发动机启停）、驾驶行为分析、4G 无线热点分享等服务。

TSP 云端通信技术

（Telematics Service Provider）汽车远程服务提供商，在 Telematics 产业链居于核心地位，上接汽车、车载设备制造商、网络运营商，下接内容提供商。Telematics 服务集合了位置服务、Gis 服务和通信服务等现代计算机技术，为车主和个人提供强大的服务（导航、娱乐、资讯、安防、SNS、远程保养）。

通常所说的 Telematics 就是指应用无线通信技术的车载电脑系统。随着电脑和网络

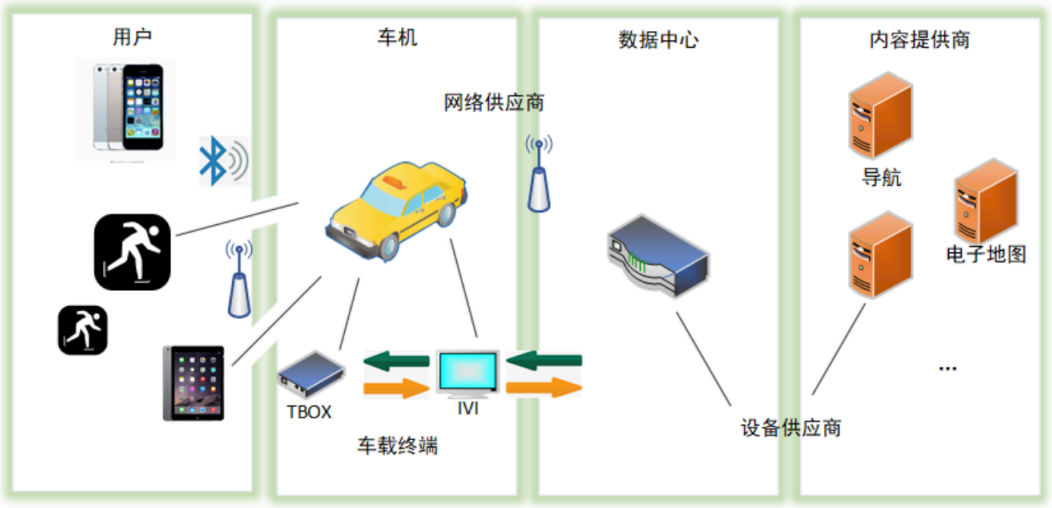

图 2.2　TSP 系统组成

技术应用到汽车上，正在形成称之为 Telematics 的新的电脑市场。Telematics 是无线通信技术、卫星导航系统、网络通信技术和车载电脑的综合产物，被认为是未来的汽车技术之星。汽车行驶当中出现故障时，通过无线通信连接服务中心，进行远程车辆诊断，内置在发动机上的计算机记录汽车主要部件的状态，并随时为维修人员提供准确的故障位置和原因。通过终端机接收信息并查看交通地图、路况介绍、交通信息、安全与治安服务以及娱乐信息服务等，在后座还可以玩电子游戏、网络应用（包括金融、新闻、E-mail 等）。通过 Telematics 提供的服务，用户不仅可以了解交通信息、临近停车场的车位状况，确认当前位置，还可以与家中的网络服务器连接, 及时了解家中的电器运转情况、安全情况以及客人来访情况。也就是说：综合上述所有功能的车载计算机系统叫 Telematics。Telematics 系统运作模式就目前发展的模式观察，基本上可将其分为汽车定位系统（GPS）与资讯存取（Access）两部分。功能特色：卫星定位、道路救援、汽车防窃、自动防撞系统、车况掌握、个人化资讯接收、多媒体娱乐资讯接收。

Telematics 系统的应用领域：基本上可分为前座系统、后座系统与引擎机械系统三大子系统。前座系统主要以安全、车辆保全、驾驶简易性与舒适性为主要考量。后座系统则以多媒体娱乐为主，包括互动式游戏、高传真音响视听系统、随选视讯、数位广播与数位电视等。引擎机械系统，主要是根据车用电脑所收集的车况资讯，进行车况诊断、行车效率最佳化、远距引擎调整或零件预定等。

Telematics 目前主要应用在车载系统上，根据使用目的不同，Telematics 可分为三种基本类型，即交通信息与导航服务、安全驾驶与车辆保护及故障诊断的车辆维护服务、娱乐及通信服务。提供全球定位系统技术、地理信息系统、智能型交通系统技术。值得一题的是 Telematics 逐渐演变为综合了 GPS 的跟踪装置和无线通信等技术的车载系统。

TSP 一词狭义的在互联汽车行业中被用作对服务提供者进行分类的广义术语以安全车到云为核心的汽车价值链数据管理。然而，目前 TSP 扮演的传统角色在价值链中不断进化。TSP 一词已被 IT 公司，系统集成商，甚至一级企业等采用。网络运营商正在将其 M2M/IOT 服务扩展到汽车行业，意图将数据连接“去商品化”。越来越多的汽车制造商通过 TSP 创造和集成更多的车载部件。

2.1.3 V2X 车载通信技术

Vehicle to Everything (V2X) 是一种车载通信系统，支持将信息从车辆传输到可能影响车辆的交通系统的移动部件。V2X 技术的主要目的是提高道路安全、节能和道路交通效率。

车联网的工作原理: 在 V2X 通信系统中，信息通过高带宽、高可靠性的链路从车辆传感器和其他来源传播，使其能够与其他汽车、停车位和交通信号灯等基础设施以及使用智能手机的行人进行通信。通过与车辆周围的其他实体共享速度等信息，该技术提高了驾驶员对潜在危险的认识，并有助于降低伤害、道路事故死亡和与其他车辆碰撞的严重程度。该技术还通过警告驾驶员即将到来的交通、建议替代路线以避免交通和识别可用停车位来提高交通效率。

V2X 技术的组成部分: V2X 技术的关键组成部分包括 V2V（车对车）和 V2I（车对基础设施）。V2V 允许车辆与道路上的其他车辆进行通信，而 V2I 允许车辆与外部实体进行通信，例如交通信号灯、停车位、骑自行车的人和行人。这些技术有助于改善道路安全、减少燃料消耗并增强驾驶员与其他道路使用者（例如骑自行车者和行人）之间的体验。

当 V2X 系统集成到传统车辆中时，驾驶员可以接收有关天气模式、附近事故、道路状况、道路工程警告、紧急车辆接近以及使用同一条道路的其他驾驶员活动的

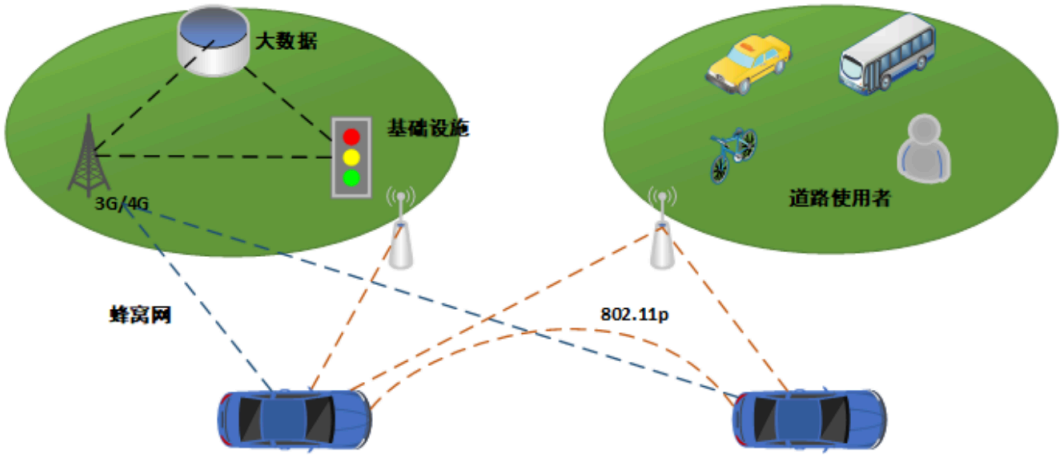

图 2.3　v2x 应用场景

重要信息。

配备 V2X 系统的自动驾驶汽车可以为车辆现有的导航系统提供更多信息。该系统还使自动驾驶汽车能够扫描周围环境并根据收到的信息立即做出决定。

如图 2.3 所示，是基于 V2X 简单的一个应用场景。智能网联汽车不仅可以借助蜂窝网络，使得汽车与基站、云平台、路边单元等基础设备相连接实现 V2I，而且还可以通过基站，与周围的车辆进行连接，从而实现 V2V。智能网联汽车在与其他基础设备、非机动车、车辆、行人等进行通信的时候，使用诸如 802.11p 等协议。

车载内部网络通信技术

现代车载通信系统中有五种最广泛使用的车载网络：LIN（本地互连网络）、CAN（控制器局域网）、FlexRay、以太网和 MOST（面向媒体的系统传输）。各有优势和劣势。根据实际观察，LIN 经常用于通常不需要严格时序性能的低速通信。CAN 广泛部署在动力总成和车身控制领域，也是从车辆中检索 OBD（车载诊断）数据的标准接口。FlexRay 具有高确定性和容错性，这通常在高级底盘控制和通信主干等应用中需要。有线以太网在量产汽车中仍然相对较新，可能仅用于 ECU 闪烁和有限的网络主干连接等应用。然而，它在延迟和抖动非常有限的高速数据传输方面具有巨大潜力。因此，以太网在未来可能会获得更多车载网络的份额。

- LIN 是一种低成本、低速且易于实现的车载网络，主要用于简单且时间要求

不高的应用，例如传统的中央门锁激活、车窗升降器控制、后视镜调节，方向盘按钮模块，以及许多低刷新率传感器。LIN 最突出的优势是它的成本比其他主要网络低得多 [18]. 这种优势来自多个方面。首先，LIN 控制器相对便宜。LIN 模块使用 UART（通用异步接收器/发送器）端口来发送和接收串行数据。

- CAN 网络长期以来一直用于传输大部分车载通信信号。尽管后来针对 CAN 无法满足的一些要求开发了各种不同的网络，但 CAN 在汽车网络中仍然保持着普及，特别是在动力总成系统和上半身电子设备中。车辆中的 CAN 芯片估计数量已接近 5 亿个。最近的一项预测甚至预计 CAN 网络将在未来十年内继续在车载通信系统中蓬勃发展。
- 出于解决不确定性、增加带宽和增强 LIN 和 CAN 等网络的抗故障能力的目标，FlexRay 由 FlexRay 联盟发起。目前，它已越来越多地应用于车辆动力学领域和域间通信。FlexRay 网络比 LIN 和 CAN 具有更快的传输速度和更高的容错性。它的成本也明显更高，尽管 FlexRay 系统的实际成本可能存在争议。FlexRay 的传输能力有三个最突出的特性：1) 它可以在同一周期内传输确定性和动态数据；2）它比 LIN 和 CAN（包括 TTCAN 和 CANFD）具有更大的有效载荷；3）在网络拓扑方面非常灵活。
- 随着在新型车辆中越来越多地实施 ADAS 和多媒体功能，强烈要求更宽的车辆网络带宽。以太网是超越 CAN 和 FlexRay 的下一代车载网络的一个非常有前途的候选者。近年来，它越来越受到汽车行业的关注。到 2023 年，以太网在新车中的渗透率将高达 40%。

由于现代车载通信系统几乎总是由运行不同通信协议的各种子网组合而成，因此作为不同子网之间接口的汽车网关对于整个车载通信网络至关重要，不容忽视。

通信系统中的汽车网关通常具有三种可能的功能。首先，它可以作为一个协议桥来促进跨不同子网的数据传输。这也是网关最正统的作用。其次，它可以用来“扩展”网络带宽，网关连接到相同协议的其他子网，以避免一个网段过载。第三，网关可以作为防火墙工作，在其中它起到保护作用，以抵御未经授权的外部访问尝试并最大程度地减少不希望的干扰。

网关有两种分类。如果基于路由机制，网关可以分为消息路由或信号路由。如果根据 ECU 的整体功能，网关可以分为独立的或集成的。

消息路由网关通常根据路由表将入口消息路由到指定的子网，有时甚至不改变传入消息的 ID 或传输周期（例如，路由到相同协议但具有不同协议的网络）波特率）。参考 OSI 模型，只需要到网络层的功能来完成消息路由。相反，信号路由网关需要解包入口消息，重构新消息，并将它们发送到指定的子网。通常，信号路由网关比消息路由网关的计算要求更高，并且可能需要在 OSI 模型方面实现高于网络层的软件。不同协议之间的网关（例如 CAN 和 FlexRay 之间，

另一方面，独立网关是仅用于路由而没有任何其他应用功能（通常除了网络管理和诊断）的网关。集成网关不仅可以路由消息，还可以部分作为具有其他功能的普通 ECU，例如车身控制或插图面板控制。

在车载网络设计中，独立网关和集成网关之间的选择主要取决于 ECU 的成本和计算能力。集成网关更便宜，但需要更多的计算能力，因为它们还需要同时完成非路由任务。独立网关可能会带来额外的硬件成本，例如新的 ECU 和电线，但可以在系统设计、组件测试、维护甚至封装方面带来极大的灵活性和便利性。

在为实际应用设计汽车网络网关时，过程变得更加复杂，并且可能因情况而异。在高度分布式的车载网络中，如何应对网络复杂性不断提高、域间通信量大、时序要求严格、带宽需求增加等挑战，已成为当今汽车网关研究的热门话题。此外，网关的软件架构也非常关键。由于网关在汽车中非常灵活，因此其软件也应该非常易于实施，并满足未来开发的可靠性、可维护性、可重用性和可移植性等质量要求。

第三章　智能网联安全与威胁建模

3.1　智能网联汽车面临的安全威胁

安全性是智能网联汽车面临的迅速出现的重大挑战。在车载网络的背景下，安全问题通常是指通信数据可能被恶意攻击者窃听、欺骗、丢弃、修改、泛滥、窃取等危险情况。在车辆向自动驾驶和协作驾驶发展的时代，安全性在车载网络的设计中变得越来越重要。

3.1.1　智能网联汽车主要攻击手段

发明车载网络协议时，安全问题并不是主要问题。因此，许多安全功能天生就缺失了。例如，CAN 缺乏必要的保护来确保信号的可用性、机密性和真实性 [12]。FlexRay 虽然能够在出现错误的情况下保持正确操作，但无法抵御格式良好的恶意错误消息 [13]。尽管如此，这些缺点在过去并未构成迫在眉睫的安全威胁，因为车辆很少与外界连接，而老式的安全攻击通常需要对车载网络进行物理访问。

然而，现代车辆正在通过各种方式迅速变得更加互联，用于许多高级应用。例如，车辆可以通过 DSRC（专用短程通信）连接以实现 VANET（车载自组织网络）功能，通过 Wi-Fi/蓝牙实现车载娱乐，并通过蜂窝网络实现远程信息处理服务。尽管这些连接使车辆更加智能和舒适，但它们也将车载网络大量暴露给外部对手。例如，CAN 通信可能会被智能手机恶意软件通过蜂窝网络远程篡改 [12]。软件病毒可能通过受感染的娱乐媒体（如 CD（光盘）或蓝牙播放器）传播到车载组件。此外，还可以通过攻击 OEM 存储中心的 ECU 密钥管理不善来侵入车载网络。

此外，直接访问的威胁仍然存在，因为攻击者也可能物理侵入通信线路，直接针对网络组件的弱点发起攻击。这种典型的攻击可能包括反汇编可执行代码和将恶意代码注入运行时环境。

车载网络的安全漏洞不仅可能对车辆用户造成严重后果，还会对其他道路交通参与者造成严重后果。例如，安全漏洞可能导致车辆用户的隐私泄露。目标私人数据可能包括车辆诊断流、机柜对话、摄像记录、驾驶模式和车辆位置 [14]. 这种

典型的攻击是通过未经授权的窃听进行的。其次，安全漏洞可能导致车主或原始设备制造商的直接金钱损失。在此类攻击中，攻击者经常故意修改或重放所需的车载数据以实现非法收益，例如车辆盗窃或里程表欺诈。第三级安全漏洞可能会对车辆使用者造成安全威胁。这种攻击通常涉及对安全关键车载数据的恶意修改或伪造，例如轮胎压力、车速、发动机扭矩请求和制动命令. 这可能导致非自愿驾驶机动甚至交通事故。考虑到自动驾驶的出现，这种危险至关重要，值得研究界更多关注。第四，车载网络安全漏洞会对其他道路参与者造成安全威胁，甚至瘫痪整个交通系统。由于车辆将在大型网络中互连，例如 VANET，因此信号可信度对于协调交通系统中的所有车辆都极为重要 [15]. 但是，如果车载网络安全受到损害，这种可信度可能会被破坏。例如，被篡改的车载网络可能会产生虚假数据，如果虚假数据已经传播到车辆外部并被其他人认为是“值得信赖的”，则可能对其他车辆造成极大的危险。综合上述研究现状，将攻击手段分为以下类型:

- 远距离通信攻击: 如利用蜂窝网络、Wi-Fi 等进行伪装拦截通信信号等从而达到攻击的目的。
- 近距离车外通信: 利用蓝牙攻击和高频无线电攻击。如通过蓝牙连接车载娱乐系统，伪装发送信号给车载娱乐系统从而达到攻击的目的。
- 车辆内部网络: 如通过车辆内部 USB 攻击 IVI 系统等。

3.1.2 ICV 中的潜在威胁

在远距离通信中，恶意攻击者入侵汽车的方式大致可分为 4 种: 蜂窝网络、Wi-Fi、车载单元（OBU，on board unit）/路侧单元（RSU，road side unit）和全球定位系统（GPS，global positioning system）。

1) 蜂窝网络蜂窝网络解决了 ICV 远程通信的难题，也造成了一些安全隐患。如通过破解了汽车固件，实现了对汽车设备（方向盘等）的远程控制。通过无线通信信道实现了对车辆的远程控制、位置跟踪和通信监控。

2) Wi-Fi 入侵者利用 Wi-Fi 连接可以进行很多恶意操作。如利用 Wi-Fi 远程访问车内网络；在信息娱乐控制台植入恶意软件；对汽车 Wi-Fi 的网络流量进行监控。在文献 [16] 中，腾讯科恩安全实验室研究员远程入侵了特斯拉汽车的网关、BCM 和

自动驾驶系统。并可以实现远程开启特斯拉电动车的天窗、车门以及在行驶中启动刹车。通过安全漏洞，无物理接触远程成功攻入特斯拉车电网络，并实现对特斯拉进行任意的车身和行车控制。

3) OBU/RSU OBU 和 RSU 是利用专用短程通信技术建立微波通信链路来实现车辆识别和电子支付功能的设备。然而，它们在为用户出行带来方便的同时，也产生了一些安全隐患，文献 [17] 揭露了针对新兴互联车辆的交通信号控制的拥塞攻击。

4) GPS GPS 是汽车导航中不可缺少的一部分。在无人驾驶中，GPS 导航作为汽车的“大脑”，能够为汽车提供最佳的行驶路线，因此，保证 GPS 的安全是无人驾驶领域的一项重要工作。文献 [18] 展示了使用便携式 GPS 欺骗器篡改车辆的 GPS 路线，严重威胁 GPS 的安全。

3.1.3 近距离车外通信的潜在威胁

在近距离车外通信中，恶意攻击者入侵汽车的方式可分为蓝牙攻击和高频无线电攻击两类。

1) 蓝牙攻击蓝牙作为一种近距离数据交换的通信方式，也是恶意攻击者关注的一个攻击面。攻击者能够利用蓝牙接口在汽车的信息娱乐单元上执行恶意代码，从而实现对车辆内部网络的渗透和攻击。文献 [19] 利用蓝牙漏洞，开发出一款名为“BlueBorn”的攻击向量，实现了对 IVI 系统的控制。

2) 高频无线电攻击随着高频无线电在 RKE、无钥匙点火等电子元件中的应用，很多攻击者开始关注利用高频无线电实现欺骗攻击的方法。通过软件无线电欺骗实现了对 RKE 系统的攻击，文献 [20] 则使用软件无线电欺骗实现了对汽车 TPMS 系统的攻击。

3.1.4 车辆内部网络的潜在威胁

车辆内部网络的攻击面大致可分为 USB 接口和 CAN 接口两部分。

1) USB 接口在 ICV 中，USB 接口可以直接与 IVI 连接，实现自动播放音频和视频文件的功能。因此，攻击者可以在网约车、出租车等平台以播放音乐为借口，悄悄向车内植入木马病毒从而实现对汽车的控制。2015 年，黑客曾利用 USB 攻击造成

马自达汽车 IVI 系统瘫痪。

2) CAN 接口 CAN 总线是 ECU 之间信息传输的通道，ECU 和 CAN 总线协同工作可以监控车辆状态和车辆行为，然而，CAN 总线具有一定的脆弱性。目前，许多汽车都安装有辅助设备（如保险狗、Mobileye、ELM327 等），它们具有为用户提供车道偏离警告、前方碰撞警告和车速预警等功能。攻击者可以利用这些辅助设备的脆弱性，通过 Wi-Fi 发送控制指令，这些设备能够将指令传输到 CAN 总线，从而使攻击者实现对车辆状态的远程控制。文献 [4] 利用侧信道攻击，通过收集 CAN 总线的数据流量窃取驾驶员的隐私信息，验证了 ICV 中的用户隐私信息存在被泄露的风险。

3.2 威胁建模方法论

威胁建模被定义为根据业务和技术利益相关者的输入，主动识别和解决对组织系统的潜在威胁的过程。通常在设计产品或新功能时完成，以避免将来出现安全漏洞的成本。

威胁建模是分析系统的各种业务和技术要求、识别潜在威胁并记录这些威胁对系统的脆弱程度的过程。威胁是指未经授权的一方访问组织的敏感信息、应用程序或网络的任何情况。威胁建模过程的目的是清楚地了解组织的各种资产、对这些资产的可能威胁，以及如何以及何时可以减轻这些威胁。威胁建模的最终产品是一个强大的安全系统。2020 年 4 月，视频通讯应用 Zoom 的股价从 159.56 美元跌至 111.41 美元。一旦用户群增加，Zoom 的许多安全漏洞就会暴露出来——其中大部分是 Zoom 没有预料到的。2020 年 7 月，Twitter 以一组具有内部系统访问权限的员工为目标而遭到黑客攻击，导致当时通过比特币汇款的用户损失了 117,000 美元。有了这样的安全攻击，品牌就会失去资本和信任。恶意软件攻击事件不会很快停止。Cybersecurity Ventures 预测 [21]，到 2021 年，网络犯罪损失每年将给全世界造成约 6 万亿美元的损失。这正是威胁建模过程可以在很大程度上减轻这些风险的地方。

举例来说, 在智能网联汽车中手机 APP 存储用户信息的过时加密算法是威胁建模的一个应用。

- 漏洞是 MD5 等过时的加密算法。
- 威胁是使用暴力破解散列密码。
- 攻击者是试图在线出售个人信息的黑客。
- 缓解策略是将加密算法更改为更现代和更强大的东西。

威胁建模可以通过三种不同的方式进行：

以资产为中心：盘点各种资产，分析每个资产的脆弱性。

以攻击者为中心：考虑可能的攻击者、每个人想要攻击的资产以及如何攻击。

以软件为中心：关注系统设计、数据如何在各个层之间流动以及如何配置

3.2.1 威胁建模步骤

要进行有效的威胁建模，需要以下利益相关者的意见：

- 提供应用程序的业务影响的业务利益相关者。
- 架构师提供应用生态系统的概述。
- 用于特定代码输入的程序员，例如使用的框架、编码指南等。
- DevOps 提供服务器和网络配置的详细信息。
- 专家学者在关键参数上的影响因子

3.2.2 设定目标

设定目标时要牢记您的应用程序必须具有：保护数据免受未经授权的披露的机密性防止未经授权的信息更改的完整性即使系统受到攻击也能提供所需的服务在可用性和性能方面记下您承诺的 SLA。您需要保护哪些商业秘密和知识产权? 也许在这个阶段最重要的问题是你想在威胁建模上花费多少时间和金钱?

3.2.3 可视化

这是记录组成系统的不同组件的步骤。对整个应用程序的清晰记录的概述将大大简化流程。这包括记下用例、数据流、数据模式和部署图。您可以构建两种类型的可视化。数据流图：它描述了数据是如何设计为在您的系统中移动的。它显示了操作级别，并清楚地显示了数据进入和退出每个组件的位置、数据存储、流程、

交互和信任边界。流程图：它描述了用户如何在各种用例中交互和移动。它处于应用程序级别。DFD 专注于系统内部的工作方式，而 PFD 则专注于用户和第三方与系统的交互。您可以选择其中之一或同时使用两者。现在您已经确定了应用程序中最重要的参与者和资产，是时候进行威胁评估了。

3.2.4 识别威胁

在上一步中，您构建了图表以了解您的系统。在此步骤中，您将需要分析这些图表以了解实际威胁。在这个阶段，您需要弄清楚您的资产可能被破坏的各种方式以及潜在的攻击者是谁。有很多方法可以做到这一点。我们将在下一节介绍六种最突出的威胁评估建模方法。

3.2.5 缓解

识别完威胁后，您将获得与每个资产及其操作相关的威胁的主列表或库以及可能的攻击者配置文件列表。现在您需要弄清楚您的应用程序容易受到哪些威胁。让我们考虑一下本文第一部分中的前一个示例。您将观察到“使用暴力破解密码”是威胁，而“使用 MD5 算法存储密码”是系统漏洞。确定漏洞后，您需要分析与每个漏洞相关的风险。基于此风险分析，您可以通过以下方式处理漏洞：
不要做任何事情（风险太低或太难造成相关威胁）删除与其关联的功能关闭功能或减少功能引入代码、基础设施或设计修复
您还将创建漏洞日志，以便在未来的迭代中随后解决。

3.2.6 验证

在验证期间，您检查是否所有漏洞都已得到解决。所有的威胁都被缓解了吗？是否清楚地记录了剩余风险？完成此操作后，您需要决定管理已识别威胁的后续步骤，并决定下一次威胁建模迭代的时间。请记住，威胁建模不是一次性活动。它需要在预定的时间间隔或在应用程序开发的特定里程碑期间重复。

3.3 STRIDE 建模方法

常见的威胁建模方法有：基于攻击树模型的威胁建模和 STRIDE 威胁建模。攻击树模型是 Schneier Bruce 在上世纪末提出的一种威胁建模方法 [47]，其年代久远，理论也日益完善。此方法使用树形结构搭建攻击模型，让建模人员从面临黑客攻击的角度考虑问题，树形结构的每一个节点，都必须被慎重考虑和布局，因为每个节点的配置稍有不慎，都有可能被黑客攻击。攻击树模型的优点是可以利用简单的网络模型构建复杂的威胁类型和攻击方式，其扩展性强。这样的结构，还可以从深度优先和广度优先不同的策略来考虑问题。当整个攻击树模型足够完整时，就可以很好的预防威胁，抵御非法攻击。不过，其劣势也非常明显，由于攻击树模型完全是从黑客的角度来思考问题的，因而，建模者必须要具备很强的技术能力，并且有较好的攻击经验，所以难易大规模实施基于攻击树模型的威胁建模。因此，实际中，我们更多的使用的是微软提出的 STRIDE 威胁建模方法。

STRIDE 是微软开发的用于威胁建模的方法和工具。

STRIDE 威胁建模的总体流程：

3.3.1 六类威胁

STRIDE 是从攻击者的角度，把威胁划分成 6 个类别，分别是 Spooling（仿冒）、Tampering(篡改)、Repudiation（抵赖）、InformationDisclosure（信息泄露）、Dos(拒绝服务) 和 Elevation of privilege (权限提升)。

3.3.2 四类元素

我们在来了解下四类元素，STRIDE 威胁建模的第一步就是绘制数据流图，数据流图是由【外部实体】、【处理过程】、【数据存储】、【数据流】这四类元素组成。STRIDE 威胁建模的核心就是使用这四类元素绘制数据流图，然后分析每个元素可能面临的上述六类威胁，针对这些威胁制定消减方法。

四类元素的介绍如下：

1. 外部实体

系统控制范围之外的用户、软件系统或者设备。作为一个系统或产品的输入或输出。在数据流图中用矩形表示外部实体。

2. 处理过程

表示一个任务、一个执行过程，一定有数据流入和流出。在数据流图中用圆形表示。

3. 数据存储

存储数据的内部实体，如数据库、消息队列、文件等。用中间带标签的两条平行线表示。

4. 数据流

外部实体与进程、进程与进程或者进程与数据存储之间的交互，表示数据的流转。在数据流图中用箭头表示。

使用以上四个元素绘制完数据流图后，还需要引入信任边界，安全的本质就是信任问题，信任边界往往就是攻击发起的地方。在数据流图中可以用红色的虚线隔离出信任边界。

如下是一个比较简单的数据流图演示:

3.3.3 STRIDE 四类元素与六类威胁的对应关系

具体的对应关系如下图所示，并不是每个元素都会面临 6 个威胁，比如外部实体只有仿冒和抵赖两类威胁，我们不用关心外部实体会不会被篡改、会不会发生信息泄露、以及拒绝服务等，因为外部实体本来就是我们控制范围之外的。

其中进程（处理过程）会面临全部的 6 个威胁，数据存储中 Repudiation（抵赖）是红色，表示只有存储的数据是审计类日志才会有抵赖的风险，存储其他数据的时候无抵赖。

3.3.4 威胁建模的整体流程

第四章　威胁建模设计方法 NEW

4.1　NEW 威胁建模概述

随着云、容器和 API（Application Programming Interface，应用程序编程接口）技术的快速发展，软件设计方法不断更替，敏捷的自动化工具、第三方库和各种框架百花齐放。接口和应用程序面临的威胁在时刻变化中，传统的一些威胁已经烟消云散，一些传统的建模方法应用在一些新兴领域，例如车联网，可能就变得较为复杂和困难。在此基础上，我们设计了一种新的建模方法，针对传统攻击树主观性强、叶节点概率难以确定等缺点，提出了一种改进方法基于 STRIDE 和 FAHP。STRIDE 模型可以建立威胁和安全属性之间的直接映射。它支持更好地理解和列出 TOE 的威胁，而不是考虑与资产相关的攻击的无限可能性。FAHP 可以计算出影响攻击成功概率的不同因素的权重。该方法如图 4 所示。

4.2　系统资产分析

系统资产分析是安全威胁分析的第一步，主要是对 TOE 的资产进行识别和分类。资产是需要保护的目标。参考汽车行业的 EVITA 项目，车载网络的系统资产由车载设备、车载设备上运行的应用以及各种 ECU 之间的通信链路组成 [12]。

4.3　基于 STRIDE 的攻击树建模

如图 5 所示，我们根据 STRIDE 关键字修改了攻击树。值得注意的是，这里的攻击资产目标包含两种情况: 一种是高层次、抽象的资产目标，如我们提出的网络模型的三个层次，另一种是具体的资产目标实体，如 CAN、ECU 等。确定系统的资产目标后，根据 STRIDE 关键字定义的六类威胁进行威胁识别。我们并不试图重现 STRIDE 威胁建模的过程，而是使用其关键字来指导我们构建更全面的攻击树，因此数据流图 (DFD) 在这里没有使用。通过这种方式，我们可以执行完整的攻击树建模，并且不能忽略关键的安全威胁。

在图 5 中，攻击树中的根节点用 G 表示，子节点可以分为两种: 攻击资产目标节点和威胁节点。它们可以分别用 Ai(i = 1，2，…，n) 和 Ti(i = 1，2，…，n) 来表示。叶子节点代表的攻击事件或方法称为原子攻击，标记为 Ei(i = 1，2，…，n)。实现根节点攻击目标的一系列原子攻击的组合被定义为攻击序列 Pi (i = 1，2，…，n) 。例如，图 5 中有三个攻击序列:P1E1，P2E2，E3，P3E4。

4.4 攻击序列的量化

攻击树模型的结果受叶节点概率的影响，因此叶节点的概率值直接影响威胁分析的准确性。由于攻击序列是代表完整攻击的一系列攻击叶节点的组合，因此这里对攻击序列进行了量化。计算攻击序列的概率。攻击的可能性受多种因素影响。最近关于安全指标的可靠性的工作 [21，22] 表明，缺乏准确清晰的安全指标定义会导致指标的主观性和偏差。攻击序列概率的安全度量不能任意确定。因此，我们使用 HEAVENS 中定义的安全指标，这是相对客观的。在这里，安全指标也称为安全属性。这个属性在决策域，不在安全域。我们为每个攻击序列分配四个安全属性: 专业技能、TOE 知识、机会窗口和设备。采用多属性效用理论将前面讨论的属性转化为效用值，以实现攻击目标。这计算攻击序列概率的等式如 (1) 所示。

P W i x U W x k U W k w U W w e Ue i i i i

其中 I 表示任何攻击序列。Pi 代表攻击序列出现的概率。xi 是专家。ki 代表关于脚趾的知识。wi 是机会之窗，ei 代表装备。Wf 代表攻击难度的权重。Wx 是专业知识的权重，Wk 是关于 TOE 的知识的权重，Ww 是机会之窗的权重，We 是设备的权重。这四个权重之和为 1。Uxi 代表提出了专业知识的效用价值。Uki 是公用事业关于 TOE 的知识值，Uwi 代表机会窗口的效用值和 Uei 代表展示设备的实用价值。值得关注权重向量 W 是针对每个攻击序列的 11 12 1n 而不是整个系统，因为攻击行为不同的攻击序列所代表的效果也不同论安全属性权重。我们不能把重量向量作为 TOE 的常数。此外，我们可以分析 xi、ki、wi 和 ei 与 Uxi、Uki、Uwi 和 Uei 成反比。因此，对于计算的方便性，它们之间的关系取为 U(x) = 1/x。这里，当计算攻击序列的概率时，涉及到四个安全属性，因此这是必要的制定相应的评分标准对其进行评估。采用的评分标准如表 2 所示。

对于一个每个参数的详细解释，请参考 [19]。表 2 与 HEAVeNS 中定义的表 4-4 有些不同。我们的方法涉及到反比例，每个参数的值都不能为零，所以每个值都比原值加 1。

4.5 基于 FAHP 的安全属性权重的确定

对于不同的攻击序列，专家意见的权重、关于 TOE 的知识、机会窗口和设备。FAHP 是对定性问题进行定量分析的一种简单而直观的方法。表 3 所示的 0.1-0.9 标度标准用于定量描述每个属性的相对重要性。在 FAHP 中，应该基于特定的标度准则，通过两两比较元素来构造模糊判断矩阵。如果模糊判断矩阵不一致，则应将其转换为模糊一致判断矩阵。最后，利用模糊一致判断矩阵计算各元素相对重要性的权重。根据表 3 可以得到模糊判断矩阵 R

模糊判断矩阵的一致性应按以下性质进行检验

如果矩阵 R 满足三个条件，则该矩阵是模糊一致判断矩阵。如果不是，为了确保两个元素的相对重要性的一致性，使用基于等式 4 的算术平均来调整矩阵的各个元素。公式如下:

r 是调整后的模糊一致判断矩阵 Ru 的元素。然后，n 是矩阵的阶。每个安全属性的权重向量 Wi 可以通过最小二乘法对矩阵 Ru 进行归一化来计算。方程式如下 [24]:

4.6 计算攻击序列的概率并进行风险评估

攻击序列代表一组攻击行为。它出现的概率表示在每个攻击场景中攻击目标的可能性。当攻击序列所代表的攻击行为实现时，一个攻击事件就完成了。我们可以根据等式 1 计算攻击序列的概率，进行 TARA 来发现安全关键系统中的威胁和漏洞，然后部署相应的安全防御机制。

基于提出的三层车载网络模型，可以先确定三个高级的资产对象类别，然后根据 EVITA 的资产定义导出具体的攻击资产。在 STRIDE 关键字的帮助下识别安全威胁全面攻击树。由于车载网络的整个攻击树很难追踪，我们以网络通信层的 CAN/CAN FD 攻击为例来演示所提出的方法。枚举西 W，西, ,W T 情商。(8) 所

有相关的攻击都是复杂和不必要的。只有一些 1 2 3 n 这里显示了基于物理访问攻击的常见场景，以说明所提出的方法的有效性如图 6 所示。表 4 显示了攻击树中每个节点的含义。我们使用表 3 中的标度标准对每个攻击序列的安全属性进行评分。为了证明该方法的有效性和避免个人评价的主观性，我们进行了问卷调查，并邀请了十位专家，包括相关研究领域的医生和大学教师。参与者的经验越多在塔拉，结果就越准确可靠。最后，取其结果的平均值并取整。评分结果如表 5 所示。图 6 显示了五个攻击序列可以攻击 CAN/ CAN FD。然后，用 FAHP 来判断和比较每个攻击序列的安全属性权重，得到它们的模糊判断矩阵如下

第五章　TSP 渗透测试与远程入侵

5.1　攻击模型

实验环境包括某知名品牌汽车一台，装有远程控制 App 的手机一部，无线路由器一个以及一台装有无线网卡的电脑。软件环境：手机环境为安卓 5.1.1，App 版本 1.1.8（发布日期：2017.8.21）。由于前期通过购买传感器、ECU、单片机和 IVI 等设备，手动搭建了智能网联汽车的安全攻防演练平台，因而对车内网络和环境有了更加深刻的理解，并且对各个部分的通信机制和原理有了更加全面的认识。这样，后期购买的实际的汽车，在不用拆车的情况下，就可以掌握其内部工作机理。购买的汽车如图 5.1 所示，是 2017 款的 SUV，已经具有网联远控的功能，在第四章对其进行威胁建模的基础上，对其进行实际攻击测试，证明当前的 ICV 领域确实还存在很多不容忽视的安全问题。、

整体的流程如图 5.2 所示。大致分为环境搭建、数据分析、漏洞利用和逆向工程几个步骤，与后文的章节基本上是相互对应的。实验用车经过多次测试，已经确定存在相关漏洞；首先需要分析 TSP 与 App 之间的交互数据，主要是为了确定普通用户登陆过程存在的问题已经登陆的格式，并且在漏洞利用部分，编写相应的代码进行测试，判断能否找到账号，其中还要考虑不要触发服务器的入侵检测系统；在逆向工程部分，对 App 进行初级反编译，找出可能存在的加固方式，然后使用动态方式 Dump 内存中的 DEX 文件，再进行反汇编和动态调试，从汇编代码中找到指令以及服务器的认证格式；最后用相应的代码进行验证。

5.2　流量分析和漏洞利用

通过无线信道抓取流量进行分析，我们有两种方法搭载热点：a. 使用一个普通的无线路由器作为无线热点；b. 使用无线网卡连接笔记本电脑，配置一个无线热点。对于这两种搭建无线局域网的方式，我们使用不同的方法进行抓包分析。

5.2.1 数据包抓取与分析

5.3 title 1

5.4 title 2

5.5 title 3

5.6 本章小结

第六章　实验及结果分析

6.1　实验数据集

6.2　实验结果对比

6.3　消融实验研究

6.4　本章小结

第七章　总结与展望

7.1　工作总结

7.2　未来展望

参考文献

[1] ANON. 中国智能网联汽车行业市场前景及投资机会研究报告 [C/OL] // 中国智能网联汽车行业市场前景及投资机会研究报告. .

[2] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive experimental analyses of automotive attack surfaces[C] // 20th USENIX security symposium (USENIX Security 11). 2011.

[3] MILLER C, VALASEK C. Remote exploitation of an unaltered passenger vehicle[J]. Black Hat USA, 2015, 2015(S 91).

[4] KOSCHER K, CZESKIS A, ROESNER F, et al. Experimental security analysis of a modern automobile[C] // 2010 IEEE symposium on security and privacy. 2010 : 447 – 462.

[5] LIU J, ZHANG S, SUN W, et al. In-vehicle network attacks and countermeasures: Challenges and future directions[J]. IEEE Network, 2017, 31(5) : 50 – 58.

[6] DENG J, YU L, FU Y, et al. Security and data privacy of modern automobiles[G] // Data Analytics for Intelligent Transportation Systems. [S.l.] : Elsevier, 2017 : 131 – 163.

[7] TAKAHASHI J, ARAGANE Y, MIYAZAWA T, et al. Automotive attacks and countermeasures on lin-bus[J]. Journal of Information Processing, 2017, 25 : 220 – 228.

[8] GU Z, HAN G, ZENG H, et al. Security-aware mapping and scheduling with hardware co-processors for flexray-based distributed embedded systems[J]. IEEE Transactions on parallel and distributed systems, 2016, 27(10) : 3044 – 3057.

[9] MOUSA A R, NOURELDEEN P, AZER M, et al. Lightweight authentication protocol deployment over FlexRay[C] // Proceedings of the 10th International Conference on Informatics and Systems. 2016 : 233 – 239.

[10] COMMITTEE S J V C S E, OTHERS. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems[J]. SAE International, 2016.

[11] ANON. 我国智能网联汽车产业蓄势待发 [J], 2022.

[12] WOO S, JO H J, LEE D H. A practical wireless attack on the connected car and security protocol for in-vehicle CAN[J]. IEEE Transactions on intelligent transportation systems, 2014, 16(2): 993–1006.

[13] KLEBERGER P, OLOVSSON T, JONSSON E. Security aspects of the in-vehicle network in the connected car[C] // 2011 IEEE Intelligent Vehicles Symposium (IV). 2011: 528–533.

[14] AMOOZADEH M, RAGHURAMU A, CHUAH C-N, et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving[J]. IEEE Communications Magazine, 2015, 53(6): 126–132.

[15] HARDING J, POWELL G, YOON R, et al. Vehicle-to-vehicle communications: readiness of V2V technology for application.[R]. [S.l.]: United States. National Highway Traffic Safety Administration, 2014.

[16] ANON. 腾讯黑客全球首次攻破了特斯拉的安全系统，能够实现远程刹车 [R]. 2016.

[17] ANON. 针对新兴互联车辆的交通信号控制的拥塞攻击 [R]. 2009.

[18] ANON. 使用便携式 GPS 欺骗器篡改车辆的 GPS 路线 [R]. 2020.

[19] ANON. 安天基于蓝牙协议漏洞的 BlueBorne 攻击综合分析报告 [R]. 2018.

[20] ANON. 使用软件无线电欺骗实现了对汽车 TPMS 系统的攻击 [R]. 2019.

[21] ANON. Apache Log4j 漏洞引“炸锅”，谁来保护网络安全？[C/OL] // 中国智能网联汽车行业市场前景及投资机会研究报告. 2021.

致　　谢

千千

二零二一年十月于理科大楼

攻读硕士学位期间发表论文和科研情况

■ 已公开发表的论文

- Zhao, Q., Tao, S., Zhou, J., Wang, L., Lin, X., & He, L. (2020, December). ECNU-SenseMaker at SemEval-2020 Task 4: Leveraging Heterogeneous Knowledge Resources for Commonsense Validation and Explanation. In Proceedings of the Fourteenth Workshop on Semantic Evaluation (pp. 401-410).
- 论文 2
- 论文 3

■ 已发表的专利

- 专利 1
- 专利 2
- 专利 3

■ 参加的比赛

- 比赛 1
- 比赛 2
- 比赛 3