2022 届硕士专业学位研究生学位论文

分类号：

密 级：

学校代码： 10269

学 号： 71194501214



East China Normal University

硕士专业学位论文

**Master’s** **Degree** **Thesis** **(Professional)**

智能网联汽车威胁模型设计与外部入 侵检测研究

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

Thesis for Master’s Degree (Professional) in 2022

University Code: 10269 Student ID:

EAST CHINA NORMAL UNIVERSITY

**Design** **of** **Intelligent** **Networked** **Vehicle**

**Threat** **Model** **and** **Research** **on** **External**

**Intrusion** **Detection**

Department: Software Engineering Institute

Category: Master of Engineering

Field: Software Engineering

Supervisor: Prof.Hong Liu

Candidate: Qing Yan

华东师范大学学位论文原创性声明

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

《智能网联汽车威胁模型设计与外部入侵检测研究》

导师签名: 本人签名:

年 月 日

硕士学位论文答辩委员会成员名单

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名 | 职称 | 单位 | 备注 |
|  |  |  | 主席 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

摘 要

随着工业智能、大数据、物联网和云计算等技术的快速进步， 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。因此现代智能网联汽车将面临前所未有的安全威胁和 攻击， 黑客或攻击者可以通过蓝牙、 Wi-Fi 和蜂窝等外部接口非法访问和控制车辆。 汽车网络安全问题正变得比以往任何时候都更加突出。越来越多的国际安全标准 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：

• 对车载 **IVI** 系统进行了全面的系统安全分析， 并利用传统的 **STRIDE** 模型对 其进行了威胁建模，最后对几个典型的数据流进行了威胁评级。

• 提出了一种基于 **STRIDE**模型的改进后的攻击树威胁建模方案 **(**称为 **SATT)**， 将 **SATT**应用在实际智能网联汽车网络， 建立了威胁分析模型， 并利用 **FAHP** (模糊层次分析法) 对攻击概率进行了计算， 进行了风险评估， 最后验证了模 型的可用性。

• 通过知名安全软件 **Isograph** **AttackTree** **+** 进行了仿真建模实验。研究智能网 联汽车的远程攻击方法， 对汽车进行漏洞挖掘和渗透测试， 通过蓝牙劫持信 号、数据篡改抓包和车联 **APP** 破解等多种方式攻击车载系统， 成功获取目标 车辆敏感信息和实时位置，并实现了远程入侵和完全控制。

本文目的是通过对智能网联汽车威胁建模以及安全风险评估的研究， 以期为

更多学者对其在智能网联汽车威胁模型的应用提供有益的借鉴和帮助。

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。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。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， 将其与传统方法进行了比较。结果表明， 该方法在安 全威胁分析中起到了一定的作用。最后， 针对汽车， 黑客可以使用多种方法进行攻 击， 比如利用蓝牙劫持信号、数据篡改抓包以及反向编译破解车联 APP 等方式。这 些攻击可以导致汽车被远程控制，从而对车辆安全和驾驶者的生命安全造成威胁。 关键词: 智能网联汽车，风险评估，威胁建模， STRIDE ，攻击树， SATT

**ABSTRACT**

With the rapid development of industrial intelligence, big data, mobile Internet, Internet of Things, cloud computing and other technologies, In a brand-new way, the automobile is changing from a traditional closed system to an open system which integrates new con- cepts such as smart city, intelligent transportation, intelligent communication and intelli-

gent driving. Modern intelligent networked cars have many sensors, and various internal circuits connect and fuse electronic control units and sensors, thus forming an automobile internet network containing millions of lines of codes. Therefore, the complex network wiring system, various electronic control units, sensor communication, etc. will all face unprecedented security threats and attacks, The problem of automobile network security is becoming more prominent than ever before. SAE J3061 [[1](#_bookmark3)] and ISO/SAE 21434 [[2](#_bookmark4)], which are being drafted, also show that automobile network security has been raised. Rise to the same or more important position as functional safety. This paper has the following three main contributions:

• Firstly, the architecture of intelligent networked vehicles is studied, and the security threats it faces are analyzed, and the attack sources and attack paths are analyzed.

• Not only the traditional attack tree is used to model the threat of intelligent net- worked automobile system, but also an improved attack tree threat modeling scheme based on Microsoft STRIDE (called SATT) is proposed. ;

• SATT is applied to the complex network attack path of intelligent networked vehi- cles, and the model is built. The threat of the attack tree is modeled, and the attack

probability is calculated based on FAHP (Fuzzy Analytic Hierarchy Process), and the usability of the model is verified.。

This paper aims to make more scholars pay attention to this field through the research of intelligent networked vehicle threat modeling and safety risk assessment, so as to promote the development of intelligent networked vehicle threat safety modeling and safety risk

assessment. Traditional threat analysis based on attack tree has many subjective factors and low accuracy. This paper presents a new threat modeling scheme of SATT. With the help of Microsoft’s STRIDE threat model, we identify threats corresponding to assets and build a more comprehensive attack tree. most Then, for each threat attack sequence in the attack tree, the attack probability is calculated based on FAHP. In addition, FAHP is com-

bined with analytic hierarchy process and The traditional methods are compared. Finally, a self-driving experimental vehicle was attacked by network. Path analysis and modeling experiments are carried out, and the security risk assessment of the model based on the threat model is carried out. Finally, the experiment The evaluation data are analyzed, the usability of the model is verified, and good results are achieved. The results show that this method plays a certain role in security threat analysis.

**Keywords:***ICV;* *TARA;* *STRIDE;* *ATTACK* *TREE;* *SATT*

目录

[摘要](#_bookmark1) i

[Abstract](#_bookmark2) iii

[图目录](#_bookmark6) ix

[表目录](#_bookmark7) ix

第一章 [绪 论](#_bookmark8) [1](#_bookmark9)

1.1 [研究背景及意义](#_bookmark10) [1](#_bookmark11)

1.2 [国内外研究现状](#_bookmark12) [2](#_bookmark13)

[1.2.1 智能网联汽车威胁面的研究](#_bookmark14) [2](#_bookmark15)

[1.2.2 智能网联汽车威胁建模的研究](#_bookmark16) [4](#_bookmark17)

1.3 [本文工作和主要贡献](#_bookmark18) [4](#_bookmark19)

1.4 [论文组织结构](#_bookmark20) [5](#_bookmark21)

第二章 [相关概念及研究](#_bookmark22) [7](#_bookmark23)

2.1 [智能网联汽车联网系统架构](#_bookmark24) [7](#_bookmark25)

[2.1.1 车载网络架构划分](#_bookmark26) [7](#_bookmark27)

[2.1.2 TSP 云端通信技术](#_bookmark28) [9](#_bookmark5)

[2.1.3 V2X 车载通信技术](#_bookmark29) [11](#_bookmark30)

2.2 [智能网联汽车主要攻击手段](#_bookmark31) [12](#_bookmark32)

2.3 [智能网联汽车面临的安全威胁](#_bookmark33) [13](#_bookmark34)

[2.3.1 ICV 中的潜在威胁](#_bookmark35) [13](#_bookmark36)

[2.3.2 近距离车外通信的潜在威胁](#_bookmark37) [14](#_bookmark38)

[2.3.3 车辆内部网络的潜在威胁](#_bookmark39) [15](#_bookmark40)

2.4 [STRIDE 威胁建模分析](#_bookmark41) [15](#_bookmark42)

[2.4.1 四类元素和六大威胁](#_bookmark43) [16](#_bookmark44)

[2.4.2 STRIDE 四类元素与六类威胁的对应关系](#_bookmark45) [17](#_bookmark46)

[2.4.3 STRIDE 威胁建模流程](#_bookmark47) [17](#_bookmark48)

2.5 [本章小结](#_bookmark49) [20](#_bookmark50)

第三章 [基于 STRIDE 对车载 IVI 系统的威胁建模](#_bookmark51) [21](#_bookmark52)

3.1 [IVI 系统基本功能架构](#_bookmark53) [21](#_bookmark54)

3.2 [IVI 系统的安全风险分析](#_bookmark55) [23](#_bookmark56)

[3.2.1 外部通信实体安全风险](#_bookmark57) [23](#_bookmark58)

[3.2.2 无线通信网络安全风险](#_bookmark59) [24](#_bookmark60)

[3.2.3 IVI 操作系统安全风险](#_bookmark61) [24](#_bookmark62)

[3.2.4 IVI 应用数据安全风险](#_bookmark63) [26](#_bookmark64)

[3.2.5 车载物理设备安全风险](#_bookmark65) [26](#_bookmark66)

3.3 [基于 STRIDE 的 IVI 威胁建模实例](#_bookmark67) [27](#_bookmark68)

[3.3.1 车载 IIVI 系统的 STRIDE 威胁模型](#_bookmark69) [27](#_bookmark70)

[3.3.2 DF 数据流威胁描述](#_bookmark71) [28](#_bookmark72)

[3.3.3 威胁评级](#_bookmark73) [28](#_bookmark74)

3.4 [本章小结](#_bookmark75) [29](#_bookmark76)

第四章 [基于 STRIDE 攻击树和 FAHP 的威胁建模方法](#_bookmark77) [30](#_bookmark78)

4.1 [三层车载网络模型](#_bookmark79) [30](#_bookmark80)

4.2 [SATT 安全威胁建模步骤概述](#_bookmark81) [30](#_bookmark82)

[4.2.1 系统资产分析](#_bookmark83) [30](#_bookmark84)

[4.2.2 基于 STRIDE 的攻击树建模](#_bookmark85) [32](#_bookmark86)

[4.2.3 攻击序列的量化](#_bookmark87) [33](#_bookmark88)

[4.2.4 基于 FAHP 的安全属性权重的确定](#_bookmark89) [34](#_bookmark90)

[4.2.5 计算攻击序列的概率并进行风险评估](#_bookmark91) [36](#_bookmark92)

4.3 [应用场景: 分析车载网络系统的安全威胁](#_bookmark93) [36](#_bookmark94)

[4.3.1 车载网络的安全威胁分析](#_bookmark95) [36](#_bookmark96)

[4.3.2 有效性比较](#_bookmark97) [39](#_bookmark98)

[4.3.3 SATT 威胁建模与其他威胁建模对比评估](#_bookmark99) [43](#_bookmark100)

4.4 [本章小结](#_bookmark101) [43](#_bookmark102)

第五章 [仿真实验风险评估和远程入侵渗透测试](#_bookmark103) [44](#_bookmark104)

5.1 [实验环境](#_bookmark105) [44](#_bookmark106)

[5.1.1 实验对象](#_bookmark107) [44](#_bookmark108)

[5.1.2 车辆内部架构](#_bookmark109) [44](#_bookmark110)

[5.1.3 实验工具](#_bookmark111) [44](#_bookmark112)

5.2 [实验过程](#_bookmark113) [45](#_bookmark114)

[5.2.1 攻击路径分析](#_bookmark115) [45](#_bookmark116)

[5.2.2 构建攻击树](#_bookmark117) [47](#_bookmark118)

5.3 [实验结果分析](#_bookmark119) [47](#_bookmark120)

5.4 [远程渗透及攻击测试](#_bookmark121) [48](#_bookmark122)

[5.4.1 蓝牙近距离通信漏洞利用](#_bookmark123) [49](#_bookmark124)

[5.4.2 逆向工程 APP 和破解请求加密](#_bookmark125) [52](#_bookmark126)

[5.4.3 流量抓包和远程登录](#_bookmark127) [58](#_bookmark128)

5.5 [防御措施](#_bookmark129) [60](#_bookmark130)

5.6 [本章小结](#_bookmark131) [61](#_bookmark132)

第六章 [总结与展望](#_bookmark133) [62](#_bookmark134)

6.1 [工作总结](#_bookmark135) [62](#_bookmark136)

6.2 [未来展望](#_bookmark137) [62](#_bookmark138)

[参考文献](#_bookmark137) [63](#_bookmark139)

[致谢](#_bookmark140) [68](#_bookmark141)

图目录

[图 2.1 车联网网络架构图](#_bookmark142) [8](#_bookmark143)

[图 2.2 TSP 系统组成](#_bookmark144) [10](#_bookmark145)

[图 2.3 v2x 应用场景](#_bookmark146) [12](#_bookmark32)

[图 2.4 四类元素和六类威胁对应关系](#_bookmark147) [17](#_bookmark148)

[图 2.5 常用 web 场景数据流图](#_bookmark149) [18](#_bookmark150)

[图 3.1 IVI 系统基础模块结构](#_bookmark151) [22](#_bookmark152)

[图 3.2 车载娱乐 IVI 系统安全威胁建模图](#_bookmark153) [27](#_bookmark154)

[图 4.1 三层车载网络模型图](#_bookmark155) [31](#_bookmark156)

[图 4.2 SATT 安全威胁建模步骤流程图](#_bookmark157) [31](#_bookmark158)

[图 4.3 SATT 攻击树](#_bookmark159) [32](#_bookmark160)

[图 4.4 实例节点定义图](#_bookmark161) [37](#_bookmark162)

[图 5.1 测试车辆](#_bookmark163) [45](#_bookmark164)

[图 5.2 软件建模流程图](#_bookmark165) [46](#_bookmark166)

[图 5.3 attack tree 仿真实验结果图](#_bookmark167) [47](#_bookmark168)

[图 5.4 漏洞挖掘和攻击步骤图](#_bookmark169) [48](#_bookmark170)

[图 5.5 蓝牙握手协议示意图](#_bookmark171) [50](#_bookmark172)

[图 5.6 蓝牙传输数据打印文件图](#_bookmark173) [52](#_bookmark174)

[图 5.7 蓝牙对应操作数据字段图](#_bookmark175) [52](#_bookmark176)

[图 5.8 反编译命令执行行图](#_bookmark177) [53](#_bookmark178)

[图 5.9 apk 开发文件列表图](#_bookmark179) [54](#_bookmark180)

[图 5.10 目标 APK 加固分析](#_bookmark181) [55](#_bookmark182)

[图 5.11 HTTP 请求返回验证 Cookie 示意图](#_bookmark183) [59](#_bookmark184)

[图 5.12 Fiddler 抓取 HTTP 请求车辆状态信息接口图](#_bookmark185) [60](#_bookmark186)

表目录

[表 2.1 元素 STRIDE 威胁分析](#_bookmark187) [19](#_bookmark188)

[表 2.2 威胁列表](#_bookmark189) [19](#_bookmark190)

[表 2.3 威胁评级](#_bookmark191) [20](#_bookmark192)

[表 3.1 常用汽车厂商的 IVI 系统](#_bookmark193) [21](#_bookmark54)

[表 3.2 GPS 威胁列表](#_bookmark194) [29](#_bookmark195)

[表 4.1 评分标准表](#_bookmark196) [34](#_bookmark197)

[表 4.2 权重判断表](#_bookmark198) [35](#_bookmark199)

[表 4.3 攻击树节点定义表](#_bookmark200) [37](#_bookmark201)

[表 4.4 攻击序列评分表](#_bookmark202) [38](#_bookmark203)

[表 4.5 基于 FAHP 的攻击序列可能性表](#_bookmark204) [39](#_bookmark205)

[表 4.6 重要性比例标度标准](#_bookmark206) [40](#_bookmark207)

[表 4.7 随机一致性指标表](#_bookmark208) [42](#_bookmark209)

第一章 绪 论

**1.1** 研究背景及意义

随着移动互联网、物联网、工业智能化等技术的快速发展， 本世纪以来汽车产 业也发生了翻天覆地的变化， 汽车由传统的交通工具向出行、娱乐、智能等方向发 展。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 [[3](#_bookmark210)]，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， 2023 年智能网联汽车产业规模将超 3500 亿元， 根据国家 发改委预测 [[4](#_bookmark211)] ，2025 年中国智能汽车数量将达 2800 万辆， 渗透率 82% ，2030 年 将达到约 3800 万辆，渗透率达到 95%。

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 ICV (Intelligent Connected Vehicle，智能 网联汽车) 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 [[5](#_bookmark212)] 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 拉塞克演示了如何通过攻击 IVI(In-Vehicle Infotainment, 车载娱乐信息系统) 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 [[6](#_bookmark213)] 。Koscher 等人 [[7](#_bookmark214)] 通过嗅探 并向 CAN(ControllerArea Network, 控制器局域网络) 总线注入恶意代码， 通过 Dos (Denial of Service, 拒绝服务) 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 Liu 的研究 [[8](#_bookmark215)] 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) [[9](#_bookmark216)] ，FlexRay [[10](#_bookmark217)] [[11](#_bookmark218)] 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 OBD (On-Board Diagnostics，车 载诊断系统)，也可用于非法访问车载网络 [[12](#_bookmark219)]。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。

因此， 以智能网联信息系统为载体的智能网联汽车， 其威胁建模的研究意义 将是十分重要和深远的, 主要体现在以下几点：

• 智能网联汽车的信息安全对车载驾驶人身安全和财产安全至关重要， 因此， 对智能网联汽车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汽车网络系统的缺陷， 可以将智能网联汽车所面临的 安全风险进行全面、明确的展现， 为安全开发人员提供必要的信息， 并能及 时发现危险来源，为更安全的保护工作做好准备。。

• 针对智能网联汽车提出的新的威胁建模方法, 并成功地实现了一款商用 SUV 的远程入侵实验， 证明了在智能网联汽车中仍有很多安全隐患， 弥补了车联 网研究领域的短板。

**1.2** 国内外研究现状

关于智能网联汽车威胁建模及安全风险评估的问题， 其国内外的相关研究现 状如下：

**1.2.1** 智能网联汽车威胁面的研究

智能网联汽车由于具有高度的集成化和智能化， 使其具有更多的功能接口和 更复杂的系统复杂性。随着时间的推移和黑客的研究深入， 暴露在外界的威胁也会 越来越多。从有线、无线、到汽车各种接口， 使汽车与外部世界的接触方式日益增 多， 同时也必然会出现各方面的网络安全问题、各种漏洞， 例如软件漏洞、代码漏 洞、硬件接口漏洞等。而且， 它的攻击方式也会越来越复杂， 想要破解它的攻击方 式也会越来越困难。目前国内外学者对一些较为典型的漏洞使用进行了研究如下。

智能网联汽车的威胁面主要包括以下几个方面：

数据隐私和安全问题： 智能网联汽车会收集和传输大量的车辆和驾驶员数据， 包括车速、位置、加速度、刹车、转向等信息， 这些数据可能会被黑客窃取或篡改， 对车主的隐私和安全造成威胁。

远程攻击和控制问题： 智能网联汽车可以通过互联网远程控制， 包括启动、停 止、加速、刹车等操作， 如果被黑客攻击， 将可能导致车辆失控、事故等严重后果。

车内网络攻击问题： 智能网联汽车中包括了各种车载系统， 如娱乐系统、导航 系统、气候控制系统等， 这些系统可能存在漏洞或被攻击， 会对车辆的稳定性和安 全性产生影响。

车辆网络安全问题： 智能网联汽车中的各个模块和传感器通过网络进行通信， 网络安全问题可能导致信息泄露、攻击等安全威胁。

Checkoway[[5](#_bookmark212)] 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。

Gosman[[13](#_bookmark220)] 等人综述了智能网联汽车中的数据聚合和隐私保护问题， 并介绍 了当前的解决方法和技术。

Alomar[[14](#_bookmark221)] 等人介绍了智能网联汽车中的通信安全问题， 并提出了一些解决 方案和技术，如认证和加密技术、安全路由协议等。

Deng [[15](#_bookmark222)] 等人综述了车辆自组网中的安全和隐私问题， 并提出了一些解决方 案和技术，如密钥管理、入侵检测、安全路由等。

Peter [[16](#_bookmark223)] 等人对现代汽车远程无钥匙进入系统进行了实验评估， 并发现了一 些系统的漏洞和安全问题，提出了一些安全建议和改进方案。

Liu[[8](#_bookmark215)] 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。

**1.2.2** 智能网联汽车威胁建模的研究

微软公司提出了 STRIDE 威胁模型 [[17](#_bookmark224)] 用于识别计算机安全威胁。用于帮助 推理和发现对系统的威胁。它与可以并行构建的目标系统模型结合使用。这包括 对流程、数据存储、数据流和信任边界的全面分解。

Mats Olsson[[18](#_bookmark225)] 等人提出了HEAVENS威胁安全模型，针对车辆电子电气(E/E) 系统的信息安全威胁分析和风险评估的方法、流程及工具支持， 可结构化和系统 化的方法发现潜在威胁。

Mohsin 等人 [[19](#_bookmark226)] 介绍了一种基于概率模型检测的形式化风险分析框架。他们 的框架能够生成系统威胁模型，用于正式计算攻击的可能性和成本。

Agadakos[[20](#_bookmark227)] 等人介绍了一种使用 Alloy 为物联网中的网络物理攻击路径建模 的方法。他们的方法最终也会产生潜在的威胁。还提出了支持物联网威胁分析方 面的非形式化方法。

UcedaVelez 等人提出了 [[21](#_bookmark228)] 攻击模拟和威胁分析 (PASTA) 威胁建模方法的过 程。它介绍了各种类型的应用程序威胁建模， 并介绍了一种以风险为中心的方法， 旨在应用与定义的威胁模型、漏洞、弱点和攻击模式可能产生的影响相称的安全对 策。

VAST[[22](#_bookmark229)] 框架旨在简化威胁建模和风险分析的过程。它通过使用可视化技术 和敏捷方法来帮助安全团队更快地建模威胁和分析风险。 VAST 框架还提供了一组 工具和技术来辅助威胁建模和风险分析。

Trike 框架 [[23](#_bookmark230)] 是专门针对嵌入式系统进行威胁建模和风险分析的框架。它通 过使用攻击树、数据流分析和形式化方法来建模威胁和分析风险。 Trike 框架还提 供了一组工具和技术来辅助威胁建模和风险分析。

**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 CAN 、IVI、车内网络通信几个方面分析智能网联汽车所面临的安全威

胁。对车载 IVI 系统进行了全面的系统安全分析， 并利用传统的 STRIDE 模 型对其进行了威胁建模，最后对几个典型的数据流进行了威胁评级。

2. 分析了主流的威胁建模方法如 HEAVENS, EVITAS, 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， 对实际商用的汽车的网络架构进行了威胁建模并威 胁分析模型， 利用 FAHP (模糊层次分析法) 对攻击概率进行了计算， 进行 了风险评估， 最后验证了模型的可用性。并和传统的 STRIDE 和攻击树建模 做比较分析。

3. 仿真实验和远程实例攻击通过知名安全软件 Isograph AttackTree + 进行了仿 真建模实验。研究智能网联汽车的远程攻击方法， 对汽车进行漏洞挖掘和渗 透测试， 通过蓝牙劫持信号、数据篡改抓包和车联 APP 破解等多种方式攻击 车载系统， 成功获取目标车辆敏感信息和实时位置， 并实现了远程入侵和完 全控制。

**1.4** 论文组织结构

第一章是绪论， 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)的研究现状进行了介绍和总结，最后说明了本文章节的安排。

第二章是相关理论和基础技术介绍， 分别对智能网联汽车的系统架构、 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。对目前现有威胁建模常用方法进行了整理和分类、并 介绍了模糊层次分析法为后续的威胁模型提出做了前置理论基础准备。

第三章我们首先介绍了对车载 IVI 系统进行了全面的系统安全分析， 并利用 传统的 STRIDE 模型对其进行了威胁建模， 最后对几个典型的数据流进行了威胁 评级。

第四章我们结合 STRIDE 和攻击树模型提出一种创新的名为 SATT 的威胁建 模方法， 对汽车网络架构进行威胁建模进行了威胁分析、并和传统的 STRIDE 建模 进行了比较分析。

第五章， 基于上述提出的威胁建模方法， 先进行了仿真实验后对汽车通过蓝

牙劫持信号、数据篡改抓包和车联 APP 逆向编译等方法进行实际攻击实验。

第六章， 总结与展望。最后， 对全文进行了总结， 并对存在的问题和存在的问 题进行了分析，并提出了今后的研究方向。

第二章 相关概念及研究

本章首先介绍了智能网联汽车的网络系统架构， 包括 TSP 云服务、 V2X 车载 通信等分别分析了它们的系统架构的组成和原理， 其次还介绍了目前主要的攻击 手段和智能网联汽车面临的主要威胁。对目前主流威胁建模方法进行了介绍。

**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

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。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， 如紧急制动辅助(EBA，electronic brake assist)、防抱死制动系统(ABS， antilock brake system) 等。 CAN 总线是 ECU 间的接口能把汽车里的 ECU 连接在一 起的通讯桥，使它们能够进行高效的信息通信。

在使用 CAN 总线时， 由于其与大量的内嵌式设备之间的广泛联系， 给使用者 带来了极大的便利， 但是也带来了一定的安全威胁。黑客能够利用车载信息娱乐 (IVI ，in-vehicle infotainment)系统暴露出来的外部接口如 USB 等恶意进入系统内 部获取隐私信息。

车载诊断界面主要用于车辆故障的检测和废气监测， 而 OBD-II 接口则一般 是非法侵入车辆 CAN 总线数据的通道。另外， T-BOX ，胎压。许多嵌入式设备如 TPMS 、RKE 、ABS 等都有大量可利用的攻击面。

这里简单的介绍上述英文名词的定义。

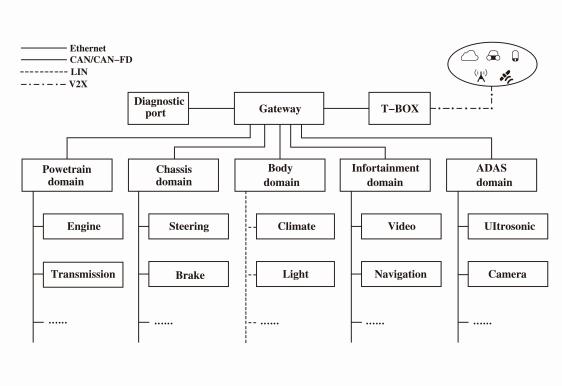


图 2.1 车联网网络架构图

• CAN 控制器局域网 (Controller Area Network，简称 CAN 或者 CAN bus) CAN 总线是一种基于消息的协议， 旨在允许当今汽车以及其他设备中的电子控制 单元 (ECU) 以可靠的、优先级驱动的方式相互通信。网络中的所有设备都可 以接收消息或“帧”，这不需要主机。 CAN 受到 ISO- 11898 下的一组丰富的国 际标准的支持。

• 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， 是智能网联汽车内部的计算机系 统， 用于跟踪和调节汽车的性能。该车载计算机系统从车辆内部的传感器网 络收集信息， 然后系统可以使用这些信息来调节汽车系统或提醒用户注意问 题。技术人员可以简单地插入 OBD 系统以收集车辆数据并诊断问题。 OBD 系统在帮助用户更好地了解车辆诊断方面提供了很大帮助。

• ECU (Electronic Control Unit) 电子控制器单元， 又称为汽车的“行车电脑”，是 车辆内部的一种小型设备， 用于控制该车辆中的一个或多个电气系统。它告 诉电气系统该做什么以及如何操作。 ECU 的核心是一个微控制器， 由嵌入式 软件控制。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。它主 要是利用各种传感器和总线进行数据的收集和交换， 从而判断出驾驶员的驾 驶意图和驾驶意图，并由执行器控制汽车。

• T-BOX 作为无线网关，是远程信息处理控制单元(TCU)，由 GPS 单元、通 信外部接口、电子处理单元、微控制器、移动通信单元和内存组成， 实现车 内终端信息的交互、云和路边单元(RSU )。一般具有故障诊断、低功耗设计、 休眠唤醒、 SD 卡扩展、输出电源、 RS232/485 、USB 和 IO 接口等新功能。

**2.1.2** **TSP** 云端通信技术

(Telematics Service Provider) 汽车远程服务提供商， 其主要提供基于互联网和 移动通信技术的远程车辆监控、远程控制、车辆数据分析和诊断等服务。这些服务 可以使车主通过智能手机或其他互联网设备， 实现远程控制车辆的功能， 例如开 启或关闭车门、启动或停止发动机、调整车内温度、锁定或解锁车辆等， 同时还能 够通过实时监测车辆的状态、行驶路线、油耗、故障码等数据， 提供更为精准的车 辆管理和维护服务， 从而提高车主的使用体验和安全性能。汽车远程服务提供商 的出现， 为汽车行业注入了新的活力和创新动力， 推动了汽车行业的数字化转型 和服务升级。

远程信息处理系统通常具有以下组件：

• 车队通信软件系统

• GPS 跟踪设备

• 引擎接口

• 输入/输出接口

• SIM 卡

• 加速度计

• 蜂鸣器

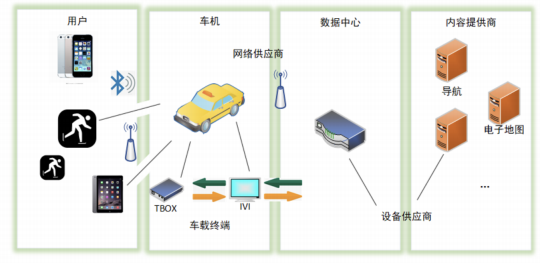


图 2.2 TSP 系统组成

根据其业务模式和服务内容的不同， 可以将汽车远程服务提供商分为以下几 种类型：

1. 汽车制造商自营型远程服务提供商： 由汽车制造商自己开发和提供远程服 务平台， 向车主提供车辆远程监控、控制、故障诊断和维护等服务。例如， 福特的 “福特 Pass”和特斯拉的“特斯拉网络”等。

2. 第三方平台型远程服务提供商： 由独立的第三方公司开发和提供远程服务 平台，向多个汽车制造商和车主提供服务。例如， OnStar 和 UVO 等。

3. 车载通信设备厂商型远程服务提供商： 提供车载通信设备和相关服务， 以 支持车辆远程监控、控制和数据传输等功能。例如，华为、高通等。

4. 车联网解决方案提供商型远程服务提供商： 提供车联网解决方案和服务， 以 支持车辆远程监控、控制、故障诊断和维护等功能。例如， 百度车联网、车易通等。

以上是一些常见的汽车远程服务提供商类型， 随着技术和市场的不断发展， 还 可能出现新的类型。

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 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。

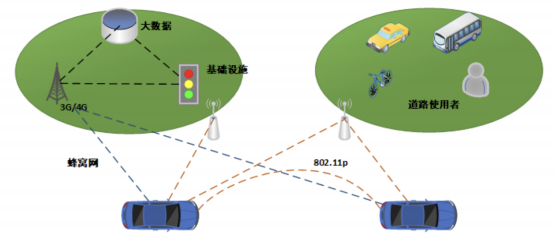


图 2.3 v2x 应用场景

**2.2** 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 [[24](#_bookmark231)]。 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 [[25](#_bookmark232)]。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 [[24](#_bookmark231)]。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 [[26](#_bookmark233)]. 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 [[27](#_bookmark234)]. 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。

**2.3** 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。

**2.3.1** **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体可以分成四类： 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) 蜂窝网络蜂窝网解决了 ICV 的远程通讯问题， 但也存在着一些新的安全问 题。比如， 利用无线通讯通道进行汽车定位追踪及通讯监视。破解汽车固件， 可实 现了车辆的遥控(如方向盘等)。

(2) Wi-Fi 黑客通过 Wi-Fi 连接可以进行很多恶意攻击。如利用 Wi-Fi 远程访问 车内网络； 入侵 IVI 系统安装木马； 监控汽车通信管道和访问流量。在文献 [[28](#_bookmark235)] 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。它还能实现特斯拉电动汽车的天窗和车门的遥控启动， 以及在驾驶过程中 制动利用安全漏洞， 远程入侵了特斯拉车的网络。并且可以对特斯拉进行任意的 车身和驾驶控制。

(3) GPS GPS 是汽车导航中最重要部分。在无人驾驶中， GPS 导航作为汽车的 “大脑”，能够为汽车提供最优的行车路径， 从而确保 GPS 系统的安全性。这是一个 在自动驾驶方面很有意义的工作。文献 [[29](#_bookmark236)] 显示了使用便携 GPS 诱骗装置对汽车 GPS 进行了篡改，造成严重的破坏。

**2.3.2** 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主要为蓝牙攻击和高频无 线电攻击两类。

1. 身份识别攻击：利用近距离通信技术(如 NFC 、蓝牙、 Wi-Fi Direct 等)在 车辆周围进行身份识别攻击， 从而欺骗车辆或者远程服务器， 获取敏感信息或者 非法控制车辆。

2. 入侵车载系统攻击： 在车辆附近或车内， 通过近距离通信技术进行入侵车 载系统， 从而获取车辆信息或非法控制车辆。例如， 通过蓝牙连接入侵车载系统， 获取车辆的行驶记录、地理位置等敏感信息。

3. 物理攻击： 通过直接接触车载设备进行攻击， 例如通过物理接触、拆卸等方 式攻击车辆 ECU (发动机控制单元)等。

4. 数据篡改： 对车辆的数据进行篡改， 例如篡改车辆传感器的数据、车辆位置 信息等，以影响车辆的正常运行。

以上是近距离通信的潜在威胁， 网络安全公司和汽车制造商需要采取相应的 安全措施， 以保护智能网联汽车的安全性能。例如， 通过加密和认证技术， 确保车 辆和服务器之间的通信安全； 通过网络安全防护技术， 确保车辆内部系统的安全 性能等。

**2.3.3** 车辆内部网络的潜在威胁

1. 内部攻击： 利用车载系统内部的漏洞或者恶意软件， 攻击车辆内部网络或者 其他车载系统， 获取敏感信息或者非法控制车辆。例如， 通过攻击车辆的 CAN 总 线， 控制车辆的刹车或者加速器等关键系统。文献 [[7](#_bookmark214)] 利用侧信道攻击， 通过 CAN 总线采集数据通信来窃听驾驶人员的个人隐私， 证实 ICV 中存在用户的个人隐私 信息有被泄漏的危险。

2. 外部攻击： 利用外部设备或者无线信号， 攻击车载系统或者车辆内部网络。 例如， 通过无线电波攻击车载系统， 篡改车辆传感器的数据或者获取车辆敏感信 息。

3. 物理攻击： 通过直接接触车载设备进行攻击， 例如通过物理接触、拆卸等方 式攻击车辆 ECU (发动机控制单元)等。

4. 软件漏洞： 车辆内部系统中可能存在软件漏洞， 黑客可以利用这些漏洞进 行攻击，从而获取车辆敏感信息或者非法控制车辆。

为了保护车辆内部网络的安全性能， 汽车制造商和网络安全公司需要采取相 应的安全措施。例如， 通过加密和认证技术， 确保车辆内部系统之间的通信安全； 通过网络安全防护技术， 防止恶意软件入侵车辆内部系统等。此外， 汽车制造商需 要在车辆生产过程中， 注重软件安全性能的检测和修复， 以降低车辆内部系统被 攻击的风险。

**2.4** **STRIDE** 威胁建模分析

STRIDE 是一个信息安全威胁建模框架， 它被用于识别和评估软件系统中的安 全威胁。

**2.4.1** 四类元素和六大威胁

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)、Information Disclosure (信息泄露)、Denial of service(拒绝服务) 和 Elevation of privilege (权限提升)。每种威胁都代表着一种攻 击者可以利用的不同技术或策略， 攻击者可以利用这些技术或策略来利用系统的 漏洞和缺陷， 从而获得不当的访问权限或控制权。 STRIDE 框架的目的是帮助软件 开发人员、安全工程师和系统管理员在设计、实施和维护软件系统时识别和处理安 全威胁。通过识别系统中存在的安全威胁， 可以更好地保护软件系统免受未经授 权的访问、数据泄露、服务中断等安全威胁的影响。

建立 STRIDE 的威胁模型， 首先要画出数据流， 数据流是由四大要素构成， 分 别是：【外部实体】、【处理过程】、【数据存储】和【数据流】。STRIDE 威胁模型的 关键在于利用四种不同类型的要素来绘制数据流图， 并根据不同的威胁类型， 对 不同类型的威胁进行相应的消除。

四类元素的介绍如下：

1. 外部实体

用户、软件系统或系统不受系统控制的装置。一种系统或一种产物的输入或输 出。将外部实体以一个长方形的形式表示在数据流图中。

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

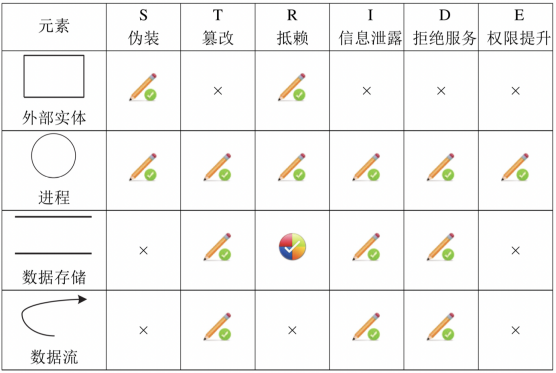


图 2.4 四类元素和六类威胁对应关系

线隔离出信任边界。

**2.4.2** **STRIDE** 四类元素与六类威胁的对应关系

具体的对应关系 2.4示例， 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。

**2.4.3** **STRIDE** 威胁建模流程

(1) 分解业务场景， 绘制数据流图表(DFD )， 以特定的场景为目标， 因此， 应 当按照实际的应用情况， 如电商业务中采购、登记等进行分类。如果有有多少种 情况， 或者如何划分， 取决于用户所用的系统和企业。淘宝， 京与电商平台如拼多 多、 AmazonEC2、腾讯等国产平台。不同的系统会产生不同的商业场景。每个服务

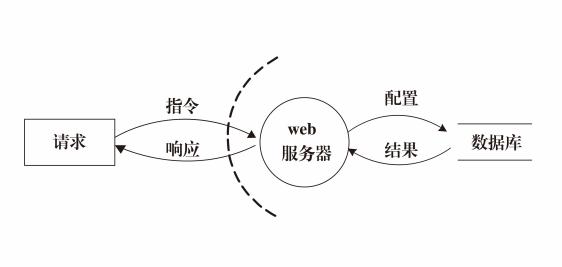


图 2.5 常用 web 场景数据流图

与每个场景 STRIDE 威胁建模是独立的， 不会互相干扰， 所以每个已分解的业务场 景都要进行深入的研究， 对不同的 STRIDE 威胁进行建模。接下来， 就是要画出一 个数据流图表。数据流图四个单元： 数据流(箭头)、数据存储单元(双横线)、进 程(圆形) 以及外部实体/交互方(正方素数的标准符号。在图 2.5 中可以看到。除 以上四大核心部件之外， 在实践中， 还可以添加一个叫做“信任边界”的元素， 我们 用虚线标出的该元素。当数据流通过不同的信任界限时， 就必须使用用线条来区 别信任边界。因为在接下来的威胁模型中， 信任边界是不会被划分所以， 大部分的 核心要素都包含： 四大元素： 进程， 数据存储， 数据流， 以及交互方/外部实体这 里没有所谓的“信任边界”。在增加了信任边界之后， 每个节点和每个数据流都必须 执行分析对其在 6 个维度的安全威胁进行分析和判定。

(2 ) 列出节点元素的安全威胁， 逐个具体分析。绘制完数据流图之后， 需要列 出数据流中的每个节点元素可能面临的安全威胁，并逐个分析。如表 2.1 所示。

表中列出了每种元素可能面临的安全威胁， 下面对表进行简单分析数据流需 要分析“篡改(替换)、外部实体可能面临“伪装”和“抵赖”两种威胁、“信息丢失或泄 露”和“拒绝服务”三种威胁。

(3 ) 输出威胁列表： 分析完数据流图中所有元素的潜在安全威胁后， 如表 2.2 是一个输出威胁列表： 包括消减方案和威胁评级。威胁列表可以帮助生成我们对 威胁进行深入分析和改进的模型。威胁等级， 基于所产生的后果来评估和评分。这

表 2.1 元素 STRIDE 威胁分析

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 元素类型 | 伪装 | 篡改 | 抵赖 | 信息泄露 | 拒绝服务 | 权限提升 |
| 外部实体 | X | X | X | X | X | X |
| 进程 | X | X | X | X | X | X |
| 数据存储 | X | X | X | X | X | X |
| 数据流 | X | X | X | X | X | X |

表 2.2 威胁列表

|  |  |
| --- | --- |
| 组件(威胁的目标) | GPS 自动导航进程 |
| 威胁描述 | 黑客通过劫持 GPS 信号误导用户自动导航 |
| 威胁类别 | I |
| 攻击方法 | 利用网络监控劫持信号通道 |
| 消减方案(对策) | 提供加密和验证通道 |
| 危险评级 | 待定 |

样就能对威胁进行归类， 首先要处理的是最大的威胁， 其次才是较小的。学术上 目前有很多种不同的威胁等级。以安全缺陷等级为例， 它包括 DREAD 和 CVSS (Common Vulnerability Scoring System) 两种常见评级方法。不同的评估方式在维 度和计算上存在细微差不同， 但从本质上讲， 危险等级 = 发生的几率 × 所造成的 损失。具体要根据实际用途使用。

DREAD 是一个常用的安全风险评估框架，它由五个因素组成，分别是：Damage (损害)、 Reproducibility (再现性)、 Exploitability (利用难度)、 Affected Users (受 影响的用户)和 Discoverability (可发现性)。

每个因素都有一个分值(通常是 0 到 10 )，分值越高表示该因素对系统安全的 威胁越大。安全评估人员可以通过对每个因素进行分析和评估， 计算出系统的总 体安全风险分值。 DREAD 框架的目的是帮助安全评估人员、开发人员和系统管理 员更好地了解系统中存在的安全威胁，并采取相应的措施来降低风险。

最终的威胁评级由这 6 个指标加权平均计算得出，公式如下：

(Dam + Rep + Exp +Aff + Dis )

Rank[0 : 10] =

2

表 2.3 威胁评级

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 等级 | 极高 (4) | 高 (3) | 中 (2) | 低 (1) |
| 潜在的损失 D | 获取最高权限 | 泄露关键信息 | 泄露敏感信息 | 泄露其他信息 |
| 重现性 R | 可随时攻击 | 易重复攻击 | 可重复攻击 | 难重复攻击 |
| 可利用性 E | 非常容易利用 | 较为容易攻击 | 高级黑客可利用 | 攻击条件苛刻 |
| 受影响用户 A | 所有用户 | 管理员 | 一般用户 | 其他用户 |
| 可发现性 D | 漏洞过于明显 | 需要漏洞挖掘 | 限定范围可发现 | 隐藏性极高 |

Rank 代表着威胁等级， 从 0 到 10 ，代表着从零到高的危险。这一公式并非统 一不变的标准， 只是为了让该评级方式的威胁值与 CVSS 范围保持相同。每个指标 的得分为 0 至 4 ，表明了威胁的严重性。

**2.5** 本章小结

本章主要介绍了智能网联汽车的系统架构， 首先从整体上给出其车联网系统 的架构介绍， 然后对 TSP云服务、 V2X, 车载网络通信进行了详细分析， 解释了车 载网络通信各个协议之前的区别和优劣。接着对三种不同的威胁进行了描述。本 文重点对 STRIDE 系统进行了威胁模型的分析。为后续的智能互联汽车威胁模型 的提出提供了前置理论来源。

第三章 基于 **STRIDE** 对车载 **IVI** 系统的威胁建模

本章首先介绍了基于 STRIDE 的威胁建模过程并说明车载 IVI 系统所面临的 潜在风险和安全威胁, 最后基于 STRIDE 威胁模型对一个车载系统进行实例威胁分 析和威胁评级。

**3.1** **IVI** 系统基本功能架构

IVI 系统是一种嵌入式系统， 一般由硬件和软件两部分组成。开发 IVI 系统需 要进行需求分析、系统架构设计、硬件设计、软件开发、测试和调试等多个环节。 其中， 需求分析和系统架构设计是 IVI 系统开发的重要基础， 硬件设计和软件开 发是 IVI 系统开发的核心步骤， 测试和调试是确保 IVI 系统质量的关键环节。整个 IVI 系统的开发需要团队协作， 综合考虑到硬件和软件两方面， 以提供高性能、稳 定性和易用性的 IVI 系统。一些著名的汽车 IVI 系统的具体情况如表 3.1 所示 为了

|  |  |  |
| --- | --- | --- |
| 厂商 | 系统名称 | 车型 |
| 丰田 | Entune | 多款车型 |
| 本田 | HondaLink | 多款车型 |
| 日产 | NissanConnect | 多款车型 |
| 福特 | SYNC | 多款车型 |
| 雪佛兰 | Chevy MyLink | 多款车型 |
| 捷豹路虎 | InControl | 多款车型 |
| 宝马 | iDrive | 多款车型 |
| 奥迪 | MMI | 多款车型 |
| 梅赛德斯-奔驰 | COMAND | 多款车型 |

表 3.1 常用汽车厂商的 IVI 系统

有目的地进行 IVI 系统的网络安全性风险的研究， 本文从基础的角度， 结合各种车 辆的 IVI 系统的基础设施和功能， 从理论上总结出 IVI 的基本功能架构。 IVI 的基 础功能体系结构包括应用、通讯、控制、控制等模块。

通讯模组因车辆配置 IVI 的内容及模式而异， 在车辆网络中， 一般包含 4 G/5 G、蓝牙、 WiFi 、DSRC 等通讯手段， 也有一些车辆连接 GPS 、G-Sensor、V-Sensor

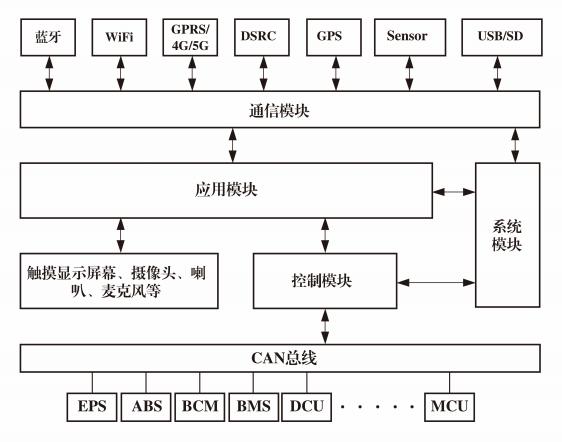


图 3. 1 IVI 系统基础模块结构

等位置及局部感应装置， 另外， 通讯模组还设有 USB 、SD 等外接装置， 也可通过 T-BOX 与外界终端进行通讯。 IVI 系统通过通信模块所实现的有线无线通信方式， 与诸如 TSP、智能终端、智能网联车辆等的车辆外设备进行通信， 包括数据、短信、 语音等。如图 3.1 所示我们给出了 IVI 系统的基本功能结构。 IVI 系统的基本功能 架构由多个部分组成，下面详细说明：

主机部分： 主机是 ivi 系统的核心部分， 包括处理器、内存、存储器、接口等。 处理器用于处理 ivi 系统的各种计算任务， 内存用于存储 ivi 系统的运行数据， 存 储器用于存储 ivi 系统的程序和数据，接口用于连接其他设备和传输数据。

显示器部分： 显示器用于显示 ivi 系统的图形用户界面和相关信息。 ivi 系统的 显示器一般采用触摸屏或非触摸屏两种形式， 可以显示多媒体内容、导航地图、车 辆状态等信息。

输入设备部分： 输入设备用于用户输入信息， 可以是触摸屏、物理按键、语音

识别等。通过输入设备，用户可以控制 ivi 系统的各种功能， 例如切换音乐、调整

空调等。

音频系统部分：音频系统用于处理 ivi 系统的音频信息， 包括音频解码器、放 大器、扬声器、麦克风等。通过音频系统， 用户可以听取音乐、电话、导航语音等 信息。

网络连接部分： 网络连接用于连接 ivi 系统和外部网络， 包括蓝牙、 Wi-Fi、GPS 等。通过网络连接， ivi 系统可以与外部设备进行数据交换和通信， 例如手机、互 联网、车载系统等。

应用程序部分：应用程序是 ivi 系统的具体功能和服务， 包括导航、娱乐、通 讯等。应用程序可以通过显示器和输入设备进行交互，提供各种功能和服务。

总的来说， ivi 系统的基本功能架构需要考虑到硬件和软件两方面， 以确保系 统的性能和稳定性。主机和显示器是 ivi 系统的核心部分， 输入设备和音频系统是 提供良好用户体验的重要组成部分， 网络连接和应用程序则是 ivi 系统与外部世界 进行交互和提供具体服务的关键。

**3.2** **IVI** 系统的安全风险分析

通过对 IVI 系统外部网络环境、内部网络结构、应用运行平台、业务功能服务 等方面的分析， 认为 IVI 网络的安全性因素主要有： 外部通信实体、无线通信网络、 车载物理设备、 IVI 操作系统、 IVI 应用服务、 IVI 应用数据、车载总线网络等。

**3.2.1** 外部通信实体安全风险

IVI 系统的外部通信主体包括用户、外部设备、车辆总线、云服务和第三方应 用程序。作为最终使用者， 用户通过触摸屏、物理按键、语音控制等方式与 IVI 系 统进行交互， 从而实现对车载娱乐、导航、通讯等功能的使用。外部设备是 IVI 系 统的扩展， 通过蓝牙、 USB 等通信协议与 IVI 系统连接， 实现多媒体、导航等功能 的互通。车辆总线是连接车内各个电子设备的数据总线， IVI 系统需要与车辆总线 进行通信， 才能获取车辆的状态信息， 以及控制车内其他电子设备。通过互联网连 接云服务， IVI 系统可以获取实时的天气、路况、交通状况等信息， 以及进行远程

控制车辆、升级系统等操作。另外， IVI 系统可以支持第三方应用程序， 这些应用 程序通过与 IVI 系统进行交互，实现在车内使用的功能。

**3.2.2** 无线通信网络安全风险

IVI 系统作为一个复杂的系统， 集成了多个功能模块， 包括 GPS 导航、蓝牙 连接和 Wi-Fi 接入等。这些模块都存在着潜在的漏洞和安全隐患， 可能会被黑客利 用。例如， 黑客可能会通过蓝牙连接获取用户的个人信息， 或者通过 Wi-Fi 接入控 制车辆的功能等。如果黑客成功攻击了 IVI 系统， 他们可能会窃取车主的个人信 息， 例如登录名、密码、信用卡信息等。这不仅会损害车主的个人隐私， 也可能导 致身份盗窃和金融欺诈等问题。如果黑客能够远程控制 IVI 系统， 他们可能会控制 车辆的功能， 例如加速、刹车、转向等， 从而导致车辆失控， 可能会引发交通事故。 无线通信可能使得 IVI 系统感染病毒。例如， 黑客可以通过无线网络向 IVI 系统传 输病毒， 导致系统崩溃或者失去控制。 IVI 系统中的蓝牙连接可能受到攻击， 例如 蓝牙拦截、蓝牙干扰等。黑客可以通过这些攻击方式获取用户的信息、窃取车辆的 控制权或者干扰系统的正常工作。 IVI 系统中的 Wi-Fi 连接也可能受到攻击。例如， 黑客可以利用恶意 Wi-Fi 网络欺骗用户连接假的 Wi-Fi 热点， 并获取用户的敏感信 息。

**3.2.3** **IVI** 操作系统安全风险

常用的 IVI 系统操作系统包括 Android Auto 、Apple CarPlay 、QNX 、Linux 和 Windows Embedded Automotive，这些操作系统旨在提供更好的用户体验、高度安 全、可靠和灵活的车载娱乐和信息娱乐解决方案。不同的车辆制造商可能会使用 不同的操作系统，或者选择自己开发或基于其他操作系统进行修改。

1 系统越狱风险

汽车 IVI 系统越狱是指通过修改或绕过汽车娱乐信息系统的限制， 获取超出 正常用户权限的访问权限，以获取更多功能或控制汽车操作系统的行为。

(a ) 系统稳定性降低。系统的越狱会对系统的稳定产生一定的干扰， 从而提高 系统死机、应用程序闪退、程序故障等问题。

(b) 安全机制失效。越狱可能会导致车载 IVI 系统的操作系统或应用程序被篡 改， 从而使原本的安全机制失效。例如， 黑客可以通过越狱后安装的恶意软件来窃 取车主的个人信息， 这些软件可以绕过原有的数据加密和访问控制机制， 直接获 取数据。

(c ) 系统固件升级问题。越狱后的系统可能会失去原有的安全保护机制， 这使 得黑客可以更轻松地利用系统漏洞进行攻击。而固件升级时， 可能需要下载并安 装未知来源的软件，这可能会增加系统受到攻击的风险。

2 IVI 应用服务安全风险

IVI 软件的安全性是指在 IVI 基础上， 在 IVI 基础上的所有应用软件的安全。 随着汽车网络的服务能力的发展， 汽车上的各种应用软件都具备了网络的能力。这 类软件是针对智能联网车辆进行远程打击的主要手段。

( 1)应用程序漏洞风险

应用程序可能存在输入验证不充分的漏洞， 这种漏洞可能会被黑客利用， 通过 输入恶意数据或代码来攻击 ivi 系统。 SQL 注入攻击、跨站点脚本攻击等类型的攻 击都可以利用应用程序中的输入验证漏洞。身份验证不安全也是应用程序常见的 漏洞之一， 比如密码弱或明文存储等， 这会使黑客轻易地获取用户的身份认证信 息，并获得对 ivi 系统的访问权限。另外， 应用程序可能存在缓冲区溢出漏洞， 这种 漏洞可能会被黑客利用， 将恶意代码插入到应用程序的缓冲区中， 从而实施攻击。 最后，应用程序在 ivi 系统中可能会存储敏感信息，如用户的登录凭据、个人资料 等，如果这些数据没有得到妥善加密或保护，黑客就可以轻易地窃取这些信息。

(2)软件篡改风险

篡改安卓应用程序可能会带来多种安全风险。其中最常见的是恶意代码注入。 黑客可能会将恶意代码注入被篡改的应用程序中， 导致应用程序在用户设备上执 行恶意操作。例如， 恶意代码可能会窃取用户的敏感信息， 如个人身份信息、银行 账户信息等， 然后将这些信息发送到黑客的服务器上， 从而导致用户的隐私泄露。 此外， 恶意代码还可能会感染用户设备病毒， 导致设备功能异常、数据丢失等问 题。另一个安全风险是数据窃取。被篡改的应用程序可能会收集用户的敏感信息， 然后将这些信息发送到黑客的服务器上， 从而导致用户的隐私泄露。例如， 黑客可

能会窃取用户的个人身份信息、银行账户信息等， 从而实施欺诈或其他形式的攻 击。篡改的应用程序还可能包含病毒。当用户安装这些应用程序时， 病毒会感染用 户的设备， 导致设备功能异常、数据丢失等问题。此外， 黑客还可能利用篡改的应 用程序作为入口攻击用户设备或其他系统，进而造成更大的安全威胁。

**3.2.4** **IVI** 应用数据安全风险

IVI 系统一般包括车身控制， 辅助驾驶， 故障检测， 导航定位， 交通信息， 移 动办公， 无线通讯， 在线娱乐和 TSP 等应用程序， 其中包括汽车运行数据、汽车车 主信息、汽车定位信息、车载应用系统数据等。 IVI 系统漏洞， 应用程序漏洞， 病 毒和黑客入侵都会导致 IVI 系统应用程序的资料遭到篡改、破坏、删除等行为， 一 些不经许可的应用程序和使用者可以存取一些机密资料， 从而导致机密资料泄露。 IVI 系统的数据处理存在如下的安全性问题。(a ) 外部安全威胁。而在 IVI 系统中， 黑客则通过 IVI 系统漏洞、 IVI 软件漏洞以及自身的安全漏洞来对 IVI 系统数据、 业务数据或数据库进行攻击。在系统的外部安全性方面， 有未授权的应用， 未授权 的用户， 未授权的数据访问， 数据库通信协议的漏洞， 系统平台的漏洞， 认证的漏 洞。(b) 内部安全威胁。如果使用者不小心存取机密资料， 或不小心更改或移除资 讯或使用者为未经许可之备份， 则可能造成安全性危险。(c ) 共享数据。 IVI 操作 系统、核心应用程序、通用应用程序共享的数据存贮器、共享共享、共享共享等多 种形式的文件， 导致了对系统和核心重要信息的恶意入侵； 系统数据和隐私数据 的明文保存也存在着数据泄漏的安全性问题。(d) 非授权数据访问： 应用程序可能 会允许未经授权的用户访问应用程序数据，导致数据泄露和安全威胁。

**3.2.5** 车载物理设备安全风险

IVI 系统连接到互联网， 因此黑客可以通过网络入侵车辆， 从而控制车辆的物 理设备， 如发动机、转向和制动系统。这可能导致意外事故或车辆失控。 IVI 系统 可能被病毒感染， 这可能会导致 IVI 系统崩溃或停止工作。这可能会影响车辆的其 他系统， 如车载电子控制模块(ECM )，从而导致车辆失控。 IVI 系统可能受到物理 攻击，如破坏或意外碰撞。这可能导致 IVI 系统停止工作或影响车辆的其他系统。

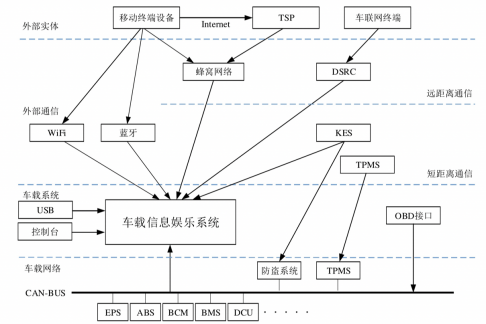


图 3.2 车载娱乐 IVI 系统安全威胁建模图

**3.3** 基于 **STRIDE** 的 **IVI** 威胁建模实例

由于在第四章提出的威胁建模风险评估模型是基于传统的 STRIDE 模型来的, 因此本节将通过传统的 STRIDE 模型对智能网联汽车车载娱乐系统 IVI 进行威胁 建模， 并以此为例对此进行风险评估为后续的新型风险评估模型进行前置理论基 础。

我们从内部环境和外部环境视角， 对 IVI 系统的攻击面和安全威胁进行了全 面分析。在此基础上， 建立了 IVI 系统的安全威胁建模模型如图 3.2。在 IVI 安全 威胁方框模型中， 以虚线为代表， 上层为框图。其中， 最小的是外部实体， 最小的 是在方框图模型的底部。在进行通讯时， 通过的信任边界数目越多， 其所面临的安 全性风险也就越大。

**3.3.1** 车载 **IIVI** 系统的 **STRIDE** 威胁模型

威胁识别是对信息系统划分的各个数据流构建 STRIDE 威胁建模， 分析每个 数据流及其关联的资产是否容易受到 S 、T 、R、I 、D 以及 E 类威胁的攻击， 识别 并记录这些威胁。该 IVI 系统数据流的 STRIDE 威胁模型如图 3.2 所示。

**3.3.2** **DF** 数据流威胁描述

这里我们对三个外部元素： WIFI, USB, GPS 进行威胁评级描述分析并把它们 的数据流分别称为: DF1, DF2, DF3。

( 1 ) DF1 WIFI 与智能网联汽车 IVI 车载娱乐系统交互该数据流可能面临的威 胁有：攻击者通过劫持路由器伪装 Wi-Fi 信号, 窃听用户传输信息 [[30](#_bookmark237)]

(2 ) DF2 USB 与智能网联汽车 IVI 车载娱乐系统交互该数据流可能面临的威 胁有： 通过 USB 设备的固件进行重新编程， 来执行恶意行为， 比如恶意文件下载、 数据泄露等 [[31](#_bookmark238)]。

(3 ) DF2 GPS 与智能网联汽车 IVI 车载娱乐系统交互该数据流可能面临的威胁 有： 通过对搭载 GPS 传感器的车载信号接收器发送虚假信号, 从而误导汽车导航定 位等 [[32](#_bookmark239)]。

**3.3.3** 威胁评级

我们通过 STRIDE 的五个属性即第二章提到的威胁评级给这实体威胁进行评 分: Wi-Fi 信号， 潜在损失 D ，可获得很多信息， 所以评分为 3 ；重现性 R ，Wi-Fi 可重现性较强， 评分为 3 ；可利用性， 路由器的设置也极为简单， 评分为 4；受影 响用户 A 影响的一般是普通用户， 评分为 2；可发现性， 较为容易发现， 评分为 2。 再根据评级公式， 可得出威胁评级 Rank = (3 + 2 + 4 + 2 + 2) ÷ 2 = 6.5 。USB ，潜在 损失 D，可获得很多信息， 所以评分为 3；重现性 R，可重现性较强， 评分为 3；可 利用性， 由于要进入车体连接 USB 较难实现， 可利用性低评分为 1 ；受影响用户 A 影响的一般是普通用户， 评分为 2 ；可发现性， 较为容易发现， 评分为 2。再根 据评级公式， 可得出威胁评级 Rank = (3 + 2 + 4 + 1 + 2) ÷ 2 = 6。GPS，潜在损失 D， 可获得很多信息， 所以评分为 3 ；重现性 R ，可重现性较低， 评分为 1 ；可利用性， 由于要通过伪造信号基站成本较高， 可利用性低评分为 1；受影响用户 A 影响的一 般是普通用户， 评分为 2 ；可发现性， 较难发现， 评分为 3。再根据评级公式， 可 得出威胁评级 Rank = (3 + 1 + 1 + 2 + 3) ÷ 2 = 5。如表 3.2我们给出了 GPS 的威胁列 表

表 3.2 GPS 威胁列表

|  |  |
| --- | --- |
| 威胁编号 | A2 |
| 元素实例 | GPS |
| 威胁类别 | Spoofing |
| 威胁描述 | 伪装假 GPS信号影响用户 GPS 功能 |
| 威胁评级 | 5 |
| 消减威胁 | 升级 GPS 固件加固 GPS信号和其他辅助导航软件 |

**3.4** 本章小结

通过研究智能网联汽车 IVI 系统中的安全问题， 本文分析了 IVI 系统在车联网 环境下可能遇到的各种安全隐患。结合 IVI 系统的实际应用情况及未来发展趋势， 对 IVI 系统的安全风险因素进行了全面分析。对 IVI 系统进行网络安全风险分析与 评价， 为 IVI 系统的网络安全问题的深入研究和探讨。最后本文通过对 IVI 系统的 功能结构的分析和总结， 提出了基于 STRIDE 的 IVI威胁建模， 最后给出了典型数 据流的威胁评级。

第四章 基于 **STRIDE** 攻击树和 **FAHP** 的威胁建模方法

本文提出了一种基于 STRIDE 和攻击树的安全威胁分析方法。首先介绍了三层 车载网络模型， 并介绍了该方法的定义和相关步骤， 最后详细的介绍了通过 FAHP 进行安全属性的权重确定和攻击序列的概率确定。

**4.1** 三层车载网络模型

为了更直观的描述车载安全威胁， 我们提出了三层车载网络模型， 如图 4.1 所 示。基于该模型， 可以分析车载网络的资产目标， 有利于攻击树构建过程中威胁的 描述。每一层的含义如下:

• 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。

**4.2** **SATT** 安全威胁建模步骤概述

我们已经从前面的章节知道 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。综合上述两 个方法的优势和特点我们提出了 SATT 安全威胁分析方法， 该方法具体步骤如图 4.2 所示。

**4.2.1** 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

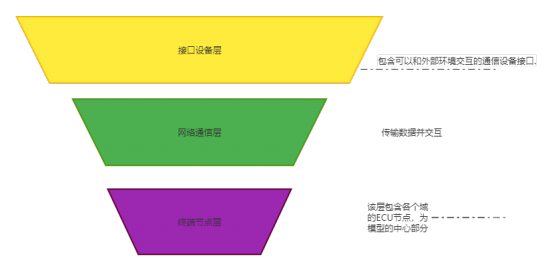


图 4.1 三层车载网络模型图

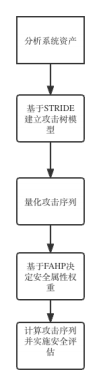


图 4.2 SATT 安全威胁建模步骤流程图

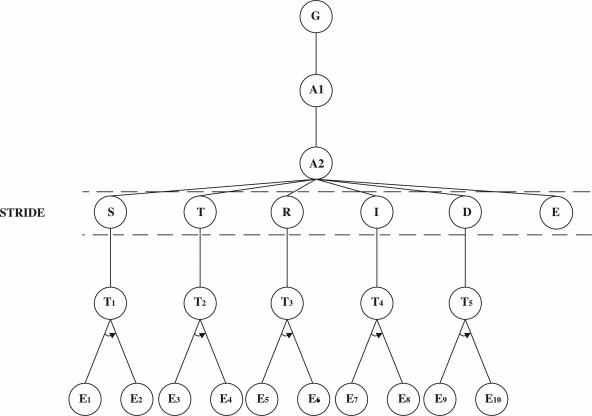


图 4.3 SATT 攻击树

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 [[33](#_bookmark240)]。

**4.2.2** 基于 **STRIDE** 的攻击树建模

如图 4.3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 4.3 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)。

**4.2.3** 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 [[34](#_bookmark241)] 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。

Pi = Wx × Uxi + Wk × Uki + Ww × Uwi + We × Uei

(4. 1)

这里解释下多属性效用理论 [[35](#_bookmark242)]: 多属性决策又称为有限多目标多指标决策， 是一 种综合多属性的多属性决策问题， 并对其进行优选(效率) 或对其进行分类。其理 论与方法已被广泛地运用于工程、技术、经济、管理、军事等各个方面。

关于等式的定义: 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 TOE 的知识。 Wi 是攻击窗口， 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 是攻击窗口的 权重， We 是设备的权重。这四个权重之和为 1。Ux i 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 Ux i 、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

表 4.1 评分标准表

|  |  |  |  |
| --- | --- | --- | --- |
| 专业知识 | 价值 | 关于 TOE | 价值 |
| 外行 | 1 | 公众 | 1 |
| 精通 | 2 | 受限 | 2 |
| 专家 | 3 | 敏感 | 3 |
| 多个专家 | 4 | 临界的 | 4 |
| 攻击窗口 | 价值 | 设备 | 价值 |
| 临界 | 1 | 标准 | 1 |
| 高 | 2 | 专门 | 2 |
| 中 | 3 | 定制的 | 3 |
| 低 | 4 | 多个定制 | 4 |

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 4.1 所示。

**4.2.4** 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[[36](#_bookmark243)] [[37](#_bookmark244)] 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

l r11 r12 · · · r1n 」

r21 r22 · · · r2n

R =

· · · · · · · · · · · ·

「 rn1 rn2 · · · rnn 

模糊判断矩阵的一致性应按以下性质进行检验

rii = 0.5, i = 1, 2, . . . , n (4.2)

表 4.2 权重判断表

|  |  |  |
| --- | --- | --- |
| 比例 | 定义 | 描述 |
| 0.5 | 同等重要 | 这两个因素同等重要 |
| 0.6 | 稍微重要 | 其中一个元素比另一个 稍微重要一些 |
| 0.7 | 明显重要 | 其中一个元素显然比另 一个更重要 |
| 0.8 | 更重要的 | 一个元素比另一个更重 要 |
| 0.9 | 极重要的 | 一个元素比另一个元素 极其重要 |
| 0. 1,0.2,0.3,0.4 | 相反比较 | 如果将元素 ai 与元素 aj 进行比较，则得到判断 rij 。那么，如果 aj 与 αi 比较，则判断为  rji = 1 − rij |

rij = 1 − rji , i, j = 1, 2, . . . , n (4.3)

rij = rik − rjk + 0.5, i, j, k = 1, 2, . . . , n (4.4)

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:

rj =   (rik − rjk + 0.5)

(4.5)

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:

Wi =  −  +  rk

(4.6)

其中 a 是重量差异的影响因子，以及此处需补充:

Wi =   Tk −  (4.7)

根据先前的方法，最后我们可以计算每个攻击序列的安全属性权重向量 W。

W = (W1 , W2 , W3 , . . . , Wn )T (4.8)

**4.2.5** 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 4.1 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。

**4.3** 应用场景**:** 分析车载网络系统的安全威胁

本节通过实例应用 SATT 安全威胁分析方法。

**4.3.1** 车载网络的安全威胁分析

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[[38](#_bookmark245)] 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[[39](#_bookmark246)] [[40](#_bookmark247)] 攻击为例来演示所提出的方法。图 4.3 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。表 4.4 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， 主要面 向了 TARA 相关领域的专家学者等。参与者的 TARA 经验越多。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 4.4 所示。图 4.3 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

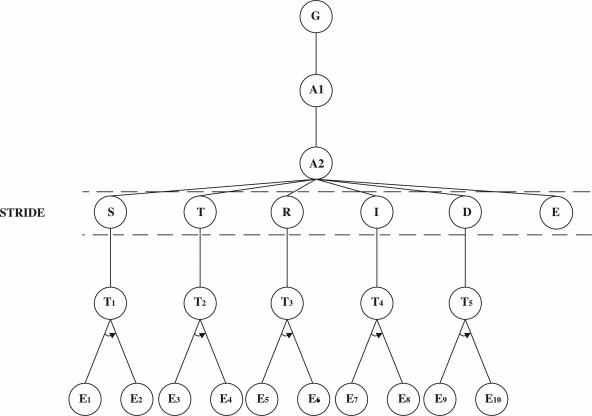


图 4.4 实例节点定义图

表 4.3 攻击树节点定义表

|  |  |  |  |
| --- | --- | --- | --- |
| 节点 | 定义 | 节点 | 定义 |
| G | 攻击车载网络 | E2 | 插入虚假数据 |
| 1  A | 攻击网络通信 | E3 | 非法物理访问 |
| 2  A | 攻击 CAN/CAN FD | E4 | 数据修改 |
| T1 | 欺骗攻击 | E5 | 非法物理访问 |
| T2 | 篡改攻击 | E6 | 重放数据 |
| T3 | 重放攻击 | E7 | 非法物理访问 |
| T4 | 嗅探攻击 | E8 | 监听和拦截数据 |
| T5 | 拒绝服务 | E9 | 非法物理访问 |
| E1 | 非法物理访问 | E10 | 连续发送高优先级数据包 |

表 4.4 攻击序列评分表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 攻击序列 | 专家意见 | TOE | 最佳时机 | 装备资产 |
| P1{E1, E2} | 2 | 4 | 2 | 2 |
| P2{E3, E4} | 2 | 2 | 4 | 2 |
| P3{E5, E6} | - | 2 | 4 | 2 |
| P4{E7, E8} | - | 2 | 4 | 2 |
| P5{E9, E10} | 2 | 2 | 4 | 2 |

安全属性权重，得到它们的模糊判断矩阵如下:

|  |  |  |
| --- | --- | --- |
| 0.5  l  l  0.4  RP1 =  0.6  0.4  「  0.5  0.5  RP3 =  0.7  「 0.5 | 0.6 0.4 0.6 」 l 0.5  0.5 0.3 0.5 0.4  , RP2 =  0.7 0.5 0.7 0.6  「  0.5 0.3 0.5 0.4  0.5 0.3 0.5 」 l 0.5  0.5 0.3 0.5 0.6  , RP4 =  0.7 0.5 0.7 0.8  0.5 0.3 0.5  「 0.6  l 0.5 0.5 0.3 0.5 」  0.5 0.5 0.3 0.5  RP5 =  0.7 0.7 0.5 0.7  「 0.5 0.5 0.3 0.5 | 0.6 0.5 0.7 0.5  0.4 0.5 0.7 0.5 |

上述模糊判断矩阵都满足模糊一致性判断矩阵的条件，

|  |  |
| --- | --- |
| 0.4  0.3  0.5  0.3  0.2  0.3  0.5  0.3 | 0.6 」  0.5  0.7  0.5    0.4 」  0.5  0.7  0.5 |

因此不需要通过等式

4.5 进行一致性转换。

然后我们直接用等式 4.7计算所有攻击序列的安全属性权重向量。结果如公式

表 4.5 基于 FAHP 的攻击序列可能性表

|  |  |
| --- | --- |
| 攻击序列 | 可能性 |
| P1 | 0.372 |
| P2 | 0.372 |
| P3 | 0.413 |
| P4 | 0.492 |
| P5 | 0.413 |

4.9 所示。

0.267 0.267

l

「

0.200 0.200

WPi =

0.333 0.333

0.200 0.200

将等式 9 和表 5 中的值代入等式 1，

0.217 0.167 0.217 」

0.217 0.233 0.217

(4.9)

0.350 0.367 0.350

0.216 0.233 0.216



可以获得每个攻击序列的概率。结果如表

6 所示。从表 6 中的数据可以看出， 攻击序列 P4 出现的概率更高， 这意味着嗅探 攻击比其他攻击更简单、更容易执行。因此， 在 CAN/CAN FD 中考虑和部署安全 机制时，我们应该首先关注这个问题。

**4.3.2** 有效性比较

我们通过 FAHP和传统的 AHP 进行比较， 证明使用 FAHP 的优点和和有效性。 在 AHP 中， 用判断矩阵 R 来表达问题中各个因素或方案之间的相对重要性。矩阵 R 满足判断矩阵需要满足的数学性质是一致性、对称性和正定性。其中， 一致性是 AHP 方法的核心， 它要求判断矩阵中的每个元素都必须符合矩阵的逻辑关系， 否 则就存在矛盾和不一致性。即以下数学表达式：

Tii = 1, i = 1, 2, . . . , n (4. 10)

Tij =  ,

i, j = 1, 2, . . . , n (4. 11)

与 FAHP 不同，表 4.6 中所示的 1-9 标度标准用于比较攻击序列的四个安全属

表 4.6 重要性比例标度标准

|  |  |  |
| --- | --- | --- |
| 比例 | 定义 | 描述 |
| 1 | 同等重要 | 这两个因素同等重要 |
| 3 | 稍微重要 | 其中一个元素比另一个 稍微重要一些 |
| 5 | 明显重要 | 其中一个元素显然比另 一个更重要 |
| 7 | 更重要的 | 一个元素比另一个更重 要 |
| 9 | 极重要的 | 一个元素比另一个元素 极其重要 |
| 2 ，4 ，6 ，8 | 相反比较 | 如果将元素 ai 与元素 aj 进行比较， 则得到判断 rij。那么， 如果 aj 与 αi 比较，则判断为  rji = 1/rij |

性的权重。根据标度准则， 我们把上节中所用到的五个攻击序列比较了每个攻击

」

 」

序列的安全属性权重。判断矩阵如下获得:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| l  R1 =  「 l  R3 =  「 l  R5 =  「 | 1  1/3  3  1/3  1 1  1 1  5 5  1 1  1 1  1 1  5 5  1 1 | 3 1/3 1 1/5 5 1 1 1/5  1/5 1  1/5 1 1 5 1/5 1 1/5 1 1/5 1 1 5  1/5 1 | 3 」  l  1  , R2 =  5  1  「  」 l  1  3  , R4 =  7  「 3  」 | 1  1/3  3  1/3  1/3 1 5  1 | 3 1/3 3 1 1/5 1 5 1 5 1 1/5 1  1/7 1/3  1/5 1 1 5  1/5 1 |  |

然后，我们需要根据等式 12 来判断上述矩阵的一致性。

CR =  < 0.1

(4. 12)

其中， CI 表示一致性指标， RI 表示随机一致性指标。

一致性指标 CI 可以通过计算特征向量的最大特征值 λmax 和判断矩阵的大小

n 得到：

CI =

λmax − n

n − 1

(4. 13)

当使用公式 4.13 时， 需要先计算出矩阵的最大特征值 λmax ，然后使用该公式 计算出置信区间 CI。这个置信区间的含义是， 以给定置信水平(例如 95%) 对最 大特征值进行估计时， 真实值落在此区间的概率是给定置信水平。如果置信区间 越小， 就意味着估计的精度越高。此外， 随机一致性指标 RI 是通过参考随机一致 性指标表格中如表 4.7 所示的数值得到的。如果一致性比例 CR 小于 0.1，则认为

判断矩阵具有可接受的一致性，否则需要重新构建判断矩阵。

表 4.7 随机一致性指标表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| RI | 0 | 0 | 0.58 | 0.9 | 1.12 | 1.24 | 1.32 | 1.41 | 1.45 |

经检验， 上述判断矩阵均满足一致性条件。因此可以计算出矩阵的归一化特 征向量，这就是我们需要的权向量。结果如等式 4.14 所示。

|  |  |  |  |
| --- | --- | --- | --- |
| 0.250  l  0.095  Wi =  0.560  「 0.095 | 0.250 0.095 0.560  0.095 | 0.128 0.128 0.639  0.105 | 0.062 0.151 0.636  0.151 |

|  |  |
| --- | --- |
| 攻击序列 | 可能性 |
| P1  P2  P3  P4  P5 | 0.318  0.318  0.340  0.372  0.340 |

0.128 」

0.128

(4. 14)

0.639

0.105



(4. 15)

攻击序列的安全属性得分与 FAHP 一致。因此， 每个攻击序列的概率也可以 通过将等式 4.14 代入等式 1 并结合表 5 来获得。结果如表 4.15 所示。两种方法的 比较结果如图 8 所示。可以看出， 两种方法评价结果的趋势大致相同。 P1 和 P2有 相同的概率。在这两种情况下， P4 的可能性最大。成功攻击可能性较高的攻击序 列所代表的攻击行为能够被反映出来， 说明了两种方法的有效性。但由于两者的 权重向量不同， 具体概率值也不同。构造判断矩阵时， 考虑各属性的重要度梯度较 小， 权重值应与重要度一致。显然， FAHP 的梯度小于层次分析法的梯度。在权重 方面， FAHP 比层次分析法更客观， 但层次分析法的缺点， 如判断矩阵的一致性难 以检查， 在这里没有太大影响。在我们的方法中， 两者都可以用来计算攻击事件发

生的概率。

**4.3.3** **SATT** 威胁建模与其他威胁建模对比评估

首先，我们考虑 STRIDE 模型和我们提出的 SATT威胁建模方法的优劣。 STRIDE 模型易于理解和教授， 因此在非安全和非技术团队成员中应用广泛。它能够快速 识别可能影响正在建模的系统的高级威胁， 并且具有较快的执行速度。相比之下， SATT 模型不仅包括 STRIDE 模型， 还通过攻击树模型进行威胁分析。 SATT 模型 的场景涵盖了很多安全场景， 因此更适用于对复杂场景进行验证， 化繁为简。特别 是在智能网联汽车场景下， SATT 模型表现更出色。

其次， 与常用的基于 AHP 的攻击树模式相比较， SATT 模型首先将 STRIDE 的 元素添加到攻击树中， 通过对资产威胁进行分类， 减少了构建攻击树的盲目性。此 外， 该方法为攻击事件分配多个属性， 并定量描述每个属性的重要性， 然后使用数 学方法计算权重， 最终得到叶节点所代表的攻击事件的概率。相比基于攻击场景 或历史数据的方法， 该方法具有一定的灵活性和优势。因为历史数据有时难以获 得， 可能需要长时间的大量实验或统计， 并且还需要对复杂数据进行分析处理。我 们的 FAHP 方法基于专家评分和严格的数学计算， 使计算攻击事件的概率变得更 加容易。此外， 我们考虑各种因素， 包括攻击者的能力， 而不仅仅是攻击场景。但 是， 与基于数据的方法相比， 该方法的主观性不可避免， 因为它涉及各种因素的相 对权重和攻击事件的得分，这些大多依赖于专家的主观判断。

**4.4** 本章小结

在这一章中， 重点对智能网联汽车领域的威胁建模分析进行了阐述， 以传统 的 STRIDE模型和攻击树模型为基础， 提出了一种被称为 SATT 全新的威胁建模方 法。详细阐述其建模原理和步骤， 并利用实际商用的汽车进行威胁建模； 然后还对 实例威胁车载网络进行了威胁建模分析， 对威胁进行了更深一步的判断， 同时为 第五章的远程控制攻击提供理论依据； 最后对比分析了传统 STRIDE 威胁建模以 及 SATT 威胁建模方法优缺点。

第五章 仿真实验风险评估和远程入侵渗透测试

**5.1** 实验环境

本章节首先将介绍某款智能网联汽车上的可利用漏洞信息， 以及通过 Isograph AttackTree+ 对其进行安全威胁建模并对其进行风险评估的实例。其次通过远程入 侵渗透测试实现远程获取汽车信息和控制汽车。

**5.1.1** 实验对象

实验环境包括某知名品牌汽车一台， Windows 系统 PC 电脑和无线路由器一 台。软件环境： 手机环境为安卓 5.9.1，手机智能互联 APP)。由于车辆本身就具备 了通过车连 APP 远程控制的功能， 因此， 在第四章提出的实例威胁建模后， 我们 对它进行了一个基于模型的仿真实验， 结果表明， 目前 ICV 的应用还存在很多安 全隐患。

**5.1.2** 车辆内部架构

**5.1.3** 实验工具

Isograph Attack+ 是著名的安全行业 Isograph 公司推出的基于攻击树的系统漏 洞建模工具。该软件通过建立系统漏洞模型，利用威胁分析和攻击树提高安全性。构 建旨在减少成功攻击的措施的图形表示， 并使用缓解树。根据 ISO 26262、ISO/SAE 21434、J3061、DO-356 和 ED-203 等标准， 该软件可以通过威胁分析和攻击树来确 定系统易受攻击的位置， 进而提高资产和 IT 系统的安全性。使用缓解树的图形化 表示， 我们能够快速构建模型， 并且采用 AttackTree 的高级 GUI 特性进一步优化 模型。此外， 我们还可以链接到需求管理工具， 如 Jama Connect® ，以进一步提高 产品的安全性和可靠性。该公司产品自上世纪 80 年代以来一直处于不断的发展过 程中，是安全和可靠性专业人士公认的标准。

该软件具有以下优势和特色：



图 5.1 测试车辆

• 可视化潜在的攻击场景： 攻击树分析提供了一种以易于理解的图形方式对系 统威胁进行建模的方法。如果我们了解系统受到攻击的方式， 我们就可以制 定对策来防止这些攻击实现其目标。

• 可以在其中快速构建和分析攻击树模型， 并以易于理解的格式呈现结果。 **At-** **tackTree** 还允许用户定义量化攻击成本的指标、发动攻击的操作难度以及可 能感兴趣的任何其他相关量化指标。

• 可以构建缓解树。其功能是用来构建减少攻击带来的影响因素。比如现实生 活中公关部门如果通过有利良好的发言可以减缓银行抢劫带来的影响， 反之 则不然。我们通过构建缓解树模拟现实中这种情况。

**5.2** 实验过程

我们通过 Isograph AttackTree 实现攻击建模，流程如图 5.2 所示

**5.2.1** 攻击路径分析

攻击场景选择以恶意攻击 IVI 系统作为攻击目标， 其可能的攻击类型目前选 用了四种：欺骗攻击、篡改攻击、重放攻击、嗅探攻击。

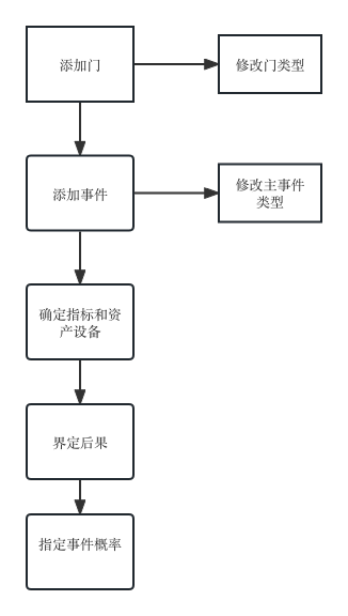


图 5.2 软件建模流程图

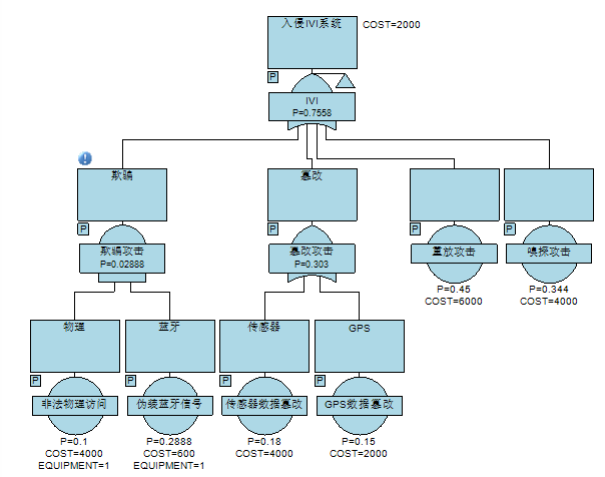


图 5.3 attack tree 仿真实验结果图

**5.2.2** 构建攻击树

使用 Attack Tree 工具对上述攻击入口进行构建攻击树模型并编译， 根节点定 义为恶意攻击 IVI 系统，叶子节点代表了攻击事件。

**5.3** 实验结果分析

我们把攻击序列重新评分了一张表， 并按照第四章提出的 SATT 威胁建模风 险评估方法， 求出了每个攻击序列的发生概率和， 再通过 Attack Tree+ 编译结果如 图 5.3 所示。可以看到综合攻击成本等因素通过 GPS 篡改信号的攻击路径发生概 率最大。由以上仿真实例可知， SATT 安全威胁模型可以为风险评估人员提供更可 靠的风险信息，使他们能够更方便地制定下一步的应对策略。

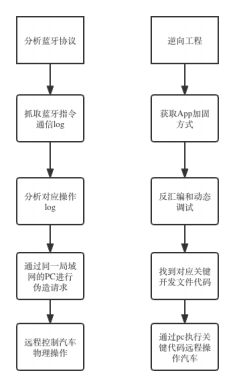


图 5.4 漏洞挖掘和攻击步骤图

**5.4** 远程渗透及攻击测试

我们通过几个攻击入口试图对车辆进行远程渗透和攻击测试， 整体的流程如 图 5.4 所示。大致分为蓝牙信号截取、请求伪造、和逆向工程几个步骤。我们通过 多次可重现实验确定该车存在以下安全漏洞； 首先在近距离通信使用蓝牙伪造请 求攻击, 具体来说首先分析蓝牙协议配对握手协议， 然后找到对应指令操作请求通 过同一局域网 PC进行伪造请求从而达到远程控制智能网联汽车的目的； 在逆向工 程部分， 下载反编译工具， 如 apktool、dex2jar 和 JD-GUI 等。接着获取 APK 文件。 然后使用 apktool 解压 APK 文件， 得到 smali 代码和资源文件。使用 dex2jar 将 DEX 文件转换成 JAR 文件， 得到 Java 代码。使用 JD-GUI 查看 Java 代码， 并进行修改。 最后从中验证并找到对应关键代码。

**5.4.1** 蓝牙近距离通信漏洞利用

Bluetooth 是一种近距离数据交换的通信方式， 攻击者可以利用其攻击智能网 联汽车。利用 Bluetooth 技术， 攻击者可以对汽车上的IVI 信息系统进行恶意编程， 从而入侵汽车网络。文献 [[41](#_bookmark248)] 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。如利用蓝牙技术可实现连接手机或其他设备， 实现 对汽车的解锁、启动等功能， 蓝牙钥匙功能的优点在于便携、安全， 避免了传统车 钥匙的遗失和被盗风险，同时增强了用户的驾驶体验。

蓝牙通信前置知识

在将手机与系统正确连接后， 蓝牙允许的功能是通过车辆通过仪表板、控制屏 幕、方向盘按钮或语音命令完全无线访问手机的呼叫功能。蓝牙既是无线标准又 是通信协议， 使用一套既定的硬件和编码在您的汽车和手机之间来回发送呼叫和 数据，安全可靠。使用 2.4 GHz 至 2.485 Ghz 的频率，蓝牙硬件以相对较低的功率 进行广播——提供仅几英尺(或在某些情况下可达 100 米) 的范围， 同时节省手机 的电池电量并减少暴露于潜在有害辐射. 为了将手机(如 iPhone 或 Android 智能手 机) 与车辆的蓝牙系统一起使用， 需要与系统“配对”——本质上是批准双向通信和 远程操作。设备配对一次后，系统会记住它，每次都自动连接。

如图 5.4 这里简短的说下蓝牙协议的类型: 其实我们蓝牙协议主要分为传统 蓝牙和低功耗蓝牙。对于传统蓝牙来讲， 当提出主动连接的设备(搜索设备) 和 被连接的设备(被搜索设备) 打算进行连接时， 搜索设备会以极快的速度进行跳 频， 被搜索设备会以极低的速度跳频， 这样两个设备一定会同时跳跃到同一频段 (79 个频段中的一个) 。随后， 搜索设备和被搜设备进行连接， 并会将连接信道按 照跳频图(由发起连接的设备) 进行有规律的变化。当中， 发起连接的一方被称 为 Master，接受连接的一方称为 Slave 此外， 在建立连接后， 双方根据已建立逻 辑、基于 BR/EDR controller 的 l2cap 可以沟通各自是否具备可以使用的 Altemate 的 AMP Controllers，具备的话则会判定是否将传输的 data，转移到这些 Controllers (极大提供蓝牙传输效率)。对于低功耗蓝牙来讲，同样存在两方，称为 Adversting 的一方， 发送 adversting packets (广播包) ，接收的一方称为 Scanner ，当 Scanner

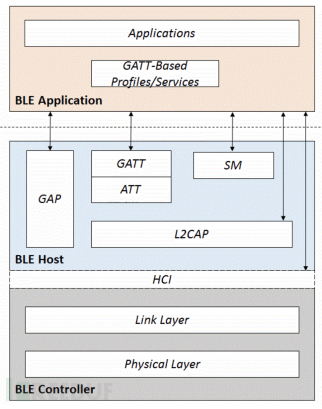


图 5.5 蓝牙握手协议示意图

接受到”connectable advertisingpacket” 回应”connection request” 建立起点对点链接 (Initiators)， Initiators 发起连接即为 Master ，Scanner 为 Slave。频道的选择则是在 有 Master 生成的 Hopping Pattern 决定。这里解释下几个专用名词:

• ATT (Attribute Protocol : 最终生成 STK 用户建立加密连接， 建立加密连接 后再自行生成 LTKS, 通过 Transport Specific Key Distribution 共享双方生成 EDIV 和 Rand 用于索引 LTK

• LTK: 长期密钥

• IRK: 身份解析密钥当私有地址周期性变化时可通过 IRK 并依据 list 对周期性 变化的地址向 MAC 地址映射(BLE 地址随机性)

• CSRK ：连接签名解析密钥连接使用数据签名来保护连接(其提供了完整性 和认证)

蓝牙协议配对流程

• 配对发起者(Initiator，总是 Master) 和配对的回应者(Responder，总是 Slave) 可以交换足够的信息， 以决定在阶段 2 使用哪种配对方法、哪种鉴权方式。 配对方法： LE legacy pairing 和 LE Secure Connections (新方法优先支持)

• 鉴权如果双方都支持 OOB 鉴权， 则选择该方式(优先级最高) 否则， 如果双 方都支持 MITM 鉴权， 则根据双方的 IO Capabilities (并结合具体的配对方 法)，选择合适的鉴权方式

• 获取密钥: 最终生成 STK 用户建立加密连接， 建立加密连接后再自行生成 LTKS, 通过 Transport Specific Key Distribution 共享双方生成 EDIV 和 Rand 用 于索引 LTK

当我们都配置好了就可以手机汽车 app 抓包了。运行手机汽车互联 app 就可 以被 fiddler 所截取到数据包了。通过检测配对的蓝牙协议中， 并未发现使用 SMP， 所以 BLE 模块和 APP之间并不会进行安全的权鉴, 如图 5.6

通过蓝牙实现伪装请求攻击

具体攻击思路参考这篇文献 [[42](#_bookmark249)]:

• 让安卓设备抓取到发送的信息

• 拿到蓝牙信息进行 wine shark 过滤出关键信息

• 让电脑设备的 linux 进行数据读写, 达到蓝牙操控的目的

(1) 安卓设备首先获取 root 权限进入文件目录, 在设备里进入蓝牙目录, 找到 bt\_stack.conf 蓝牙配置文件， 然后在在开发者选项里打开蓝牙 HCI 信息收集日志此 时若继续蓝牙收发数据可观测到控制台出现了/btsnoop\_hci.log 文件, 这里有我们所 需要的打印信息, 如图 5.5

(2) 通过 adb 命令进行手机的连接, 导出我们的.log 文件 (3) 通过从手机设置里 找到对应的 mac 地址我们通过工具过滤出来该设备的蓝牙传输信息。

当我们在手机 APP 下发” 开锁” 命令时: 通过打印工具发现发现: 对应 Handle 字段为:’0x0019’,value 是: 313233, 当我们在手机 APP 下发” 解锁” 命令时: 通过打

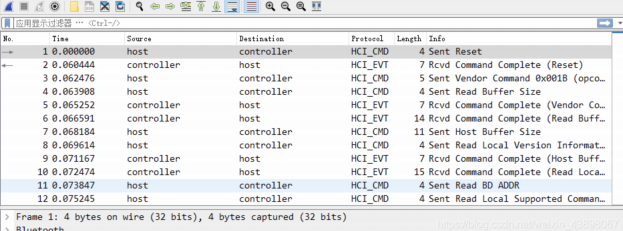


图 5.6 蓝牙传输数据打印文件图

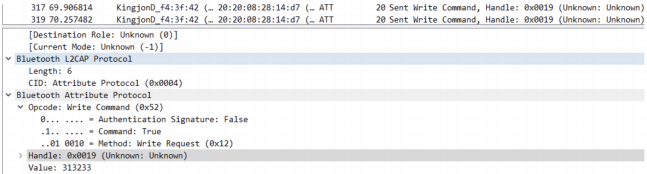


图 5.7 蓝牙对应操作数据字段图

印工具发现: 对应 Handle 字段为:’0x004e’,value 是: 000000。根据对应字段参数规 则， 我们可以伪造请求参数 [[43](#_bookmark250)]，任意的通过 pc给配对中的智能网联汽车发送操 作指令从而达到远程恶意控制该智能网联汽车的目的。此外经过研究和攻击我们 还可以通过蓝牙协议对该智能网联汽车进行更多危险的操作。

**5.4.2** 逆向工程 **APP** 和破解请求加密

我们通过对 App 进行反编译 [[44](#_bookmark251)]，可以获取车联网 APP 源码和对应的接口从 而伪造请求获取关键代码。 Android 应用程序包(英语： Android application package， APK) ，APK 是 Android 应用程序的安装包文件的扩展名。这是一种用于 Android 操作系统的应用程序包格式， 它包含了应用程序的代码、资源文件和 AndroidMan- ifest.xml 等元数据文件。 APK 文件是开发者将 Android 应用程序编译后生成的文 件， 也是用户安装应用程序的方式之一。用户可以从各种应用商店、网站或其他来



图 5.8 反编译命令执行行图

源下载 APK 文件并手动安装应用程序。

工具准备

• apktool ：资源档案，可撷取影像档案及版式档案，供使用者浏览。

• dex2jar：将 APK 反编译成 Java 源码(classes.dex 转化成jar 文件)。

• 查看APK 中 classes.dex 转化成出的jar 文件，即源码文件下载 apktool、dex2jar、 jd-gui，完成后将三个文件放在同一文件中， 并解压 dex2jar、jd-gui 压缩包， 这一步是为了方便进行反编译。

执行 **APK** 反编译

获取反编译成功后文件： 打开对应的文件夹可以看到反编译后生成的文件， 在 这些生成的文件和文件夹当中， 我们关心的是 res 文件夹中和 AndroidManifest.xml 文件， 打开 res 文件夹， 里面存放了我们所关心的 xml 文件， 如图 5.8 所示：图中 展示了 APK 文件反编译后的资源文件，下面对这些文件做一个简单的介绍:

• META-INF：保存 APP 的签名信息。

• AndroidManifest.xml：Android 清单文件， 向 Android 系统提供应用的必要信 息。

• classes.dex：文件包含了应用程序中所有的 Dalvik 可执行代码， 包括应用程 序的所有类、方法、字段以及其他的 Java。

• assets ：存放一些资源文件字体，声音等。

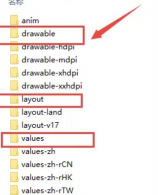


图 5.9 apk 开发文件列表图

• lib: 存放第三方库。

• original：存放未经过反编译的等 AndroidManifest.xml 文件。

• res ：存放资源文件，例如图片、颜色、字符等。

• smali：存放 Java 编译成的 smali 代码， smali 相当于 Android 虚拟机上运行的 语言。

解析加固 **APK**

( 1 ) APK 加固即通过消除漏洞和增加安全层来“强化”或保护应用程序免受入 侵。加壳后的 DEX, Android 虚拟机首先对其进行解密操作， 再加载到系统内存中 运行。其中加壳过程如图 5.10 所示在图中， 简易的描述了加固的原理， 首先我们会 拿到一个需要加固的源 apk 文件， 然后需要加固这个源 apk，我们就会写一个对应 的壳程序， 然后我们需要将两个 apk 合并， 为了让程序能够正常运行， 我们就需要 将源 apk 文件和壳程序的 dex 文件进行合并， 然后用合并之后的 dex 文件将可程序 的 dex 文件替换掉， 这样我们的壳程序就会照成运行。这里说明下什么是Dex 文件: 我们都知道 apk 的本质是一个压缩包， 当我们直接将.apk 的后缀改为.zip 的时候， 是可以直接解压出里面的文件的 (甚至有些压缩软件可以直接解压.apk 文件， 例如 bindizip)。那么 app 为什么能在手机中运行呢， 靠的就是.dex 文件， 在 Windows 端 的可执行文件是.exe 文件， JVM 的可执行文件是.class 文件， 那么在 Android 中的 dalvik 或 art 虚拟机上运行的可执行文件就是.dex 文件。

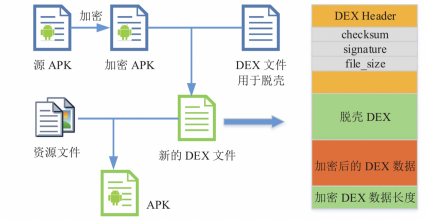


图 5.10 目标 APK 加固分析

脱壳加固 **APK**

脱壳是把加在软件上的保护程序 Dex 去掉直接能看到对应的源码。跟java 类 似，安卓的 class 都是由 Classloader 的 loadClass 方法加载的。跟java 不同的是， 每一 个 class 对象都会有对应的 dex 对象属性跟相应的 dex 文件关联起来。利用xposed， 将 loadClass 方法劫持住， 每当 loadClass 方法调用完成后， 用 xposed 执行后置方 法。获取方法加载的 class 对象， 然后调用 getDex 方法。拿到对应的 dex 文件引用， 最后将 dex 文件序列成 byte 数据， 写到自定义保存文件里面去。就能拿到脱壳后 的 dex 文件。我们通过”反射大师” 这款软件来进行脱壳处理, 其需要在 Xposed 环 境中使用，支持市面上大多数加密壳。

• 手机或模拟器安装 xposed 环境

• 安装反射大师， xposed 内部勾选反射大师模块，重启模拟器。

• 打开目标 app 进入到主界面。

• 选择当前 ACTIVITY 长按写出 Dex 约两秒后释放， 然后点击确定。 dex 文件 可以直接拉到jadx 查看源码

分析关键操作代码

|  |
| --- |
| p r i v a t e v o i d i n i t L o c a t i o n S t y l e ( ) {    1  2  3  B i t m a p D e s c r i p t o r d e s c r i p t o r = B i t m a p D e s c r i p t o r F a c t o r y . fr o m R e s o u r c e (  R . d r a w a b l e . m a i n \_ l o c a t i o n \_ i c o n ) ;  M y L o c a t i o n S t y l e m y L o c a t i o n S t y l e = new M y L o c a t i o n S t y l e ( ) ; |

4

5

6

7

8

9

10

11

12

13

14

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

|  |
| --- |
| m y L o c a t i o n S t y l e . m y L o c a t i o n I c o n ( d e s c r i p t o r ) ;  m y L o c a t i o n S t y l e . i n t e r v a l ( 2 0 0 0 ) ;  m y L o c a t i o n S t y l e . m y L o c a t i o n T y p e ( M y L o c a t i o n S t y l e . LOCATION\_TYPE\_FOLLOW  ) ;  m y L o c a t i o n S t y l e . m y L o c a t i o n T y p e ( M y L o c a t i o n S t y l e . LOCATION\_TYPE\_LOCATE ) ;  m y L o c a t i o n S t y l e . s t r o k e C o l o r ( g e t R e s o u r c e s ( ) . g e t C o l o r ( R . c o l o r .  c o l o r P r i m a r y ) ) ;  m y L o c a t i o n S t y l e . r a d i u s F i l l C o l o r ( g e t R e s o u r c e s ( ) . g e t C o l o r ( R . c o l o r . c o l o r P r i m a r y \_ 5 0 ) ) ;  mMapView . getMap ( ) . s e t M y L o c a t i o n S t y l e ( m y L o c a t i o n S t y l e ) ;  mMapView . getMap ( ) . g e t U i S e t t i n g s ( ) . s e t M y L o c a t i o n B u t t o n E n a b l e d ( t r u e ) ; mMapView . getMap ( ) . s e t M y L o c a t i o n E n a b l e d ( t r u e ) ;  } |

获取汽车初始化地理位置代码

根据上述代码块只是分析过程中一个关键的部分代码截图， 从图中可看出该初始 化了汽车的地理位置以及该文件一系列关于获取地理位置的方法函数, 我们可以通

过调用对应方法获取汽车位置信息。

|  |  |  |  |
| --- | --- | --- | --- |
| p u b l i c c l a s s G e o L o c a t i o n {   |  |  |  | | --- | --- | --- | | / / 高 德 秘 钥  p r i v a t e s t a t i c | f i n a l S t r i n g APP\_CODE\_GAODE = ” 44 |  |   a a 4 b 2 a 7 7 7 2 5 0 4 9 6 0 b 6 9 1 c fb 9 8 0 2 ” ;  p u b l i c s t a t i c S t r i n g G e t L o c a t i o n B y A d d r e s s ( S t r i n g a d d r e s s , S t r i n g  c i t y ) {  l o g . i n fo ( ” 地 理 编 码 ： a d d r e s s =” + a d d r e s s + ” ， c u r r e n t C i t y =” +  c i t y ) ;  t r y {  HashMap< S t r i n g , O bj e c t > p a r a m e t e r s = new HashMap < > ( 3 ) ; p a r a m e t e r s . p u t ( ” a d d r e s s ” , a d d r e s s ) ;  p a r a m e t e r s . p u t ( ” c i t y ” , c i t y ) ;  p a r a m e t e r s . p u t ( ” key ” , APP\_CODE\_GAODE) ;  / / 高 德 获 取 地 理 信 息  S t r i n g r e s p o n s e = H t t p U t i l . g e t ( ” h t t p s : / / r e s t a p i . amap . com / v3 / g e o c o d e / geo ” , p a r a m e t e r s ) ;  JSONObject r e s p o n s e J s o n = J S ON U t i l . p a r s e O bj ( r e s p o n s e ) ;  S t r i n g s t a t u s = r e s p o n s e J s o n . g e t ( ” s t a t u s ” ) . t o S t r i n g ( ) ; |

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

|  |
| --- |
| i f ( ! ” 1 ” . e q u a l s ( s t a t u s ) ) {  l o g . e r r o r ( ” 列 表 信 息 获 取 失 败 ， 关 键 字 ： ” + a d d r e s s + ” 城  市 ： ” + c i t y ) ;  r e t u r n n u l l ;  }  JSONArray g e o c o d e s = r e s p o n s e J s o n . g e t J S ON A r r a y ( ”g e o c o d e s ” ) ;  r e t u r n J S ON U t i l . p a r s e O bj ( g e o c o d e s . g e t ( 0 ) ) . g e t ( ” l o c a t i o n ” ) . t o S t r i n g ( ) ;  } c a t c h ( E x c e p t i o n ex ) {  l o g . e r r o r ( ” 调 用 接 口 失 败！ ” + ex . g e t M e s s a g e ( ) ) ;  r e t u r n n u l l ;  }  }  p u b l i c s t a t i c S t r i n g G e t A d d r e s s B y L o c a t i o n ( S t r i n g l o c a t i o n ) {  l o g . i n fo ( ” 逆 地 理 编 码 ： l o c a t i o n =” + l o c a t i o n ) ;  t r y {  HashMap< S t r i n g , O bj e c t > p a r a m e t e r s = new HashMap ( 1 6 ) ; p a r a m e t e r s . p u t ( ” l o c a t i o n ” , l o c a t i o n ) ;  p a r a m e t e r s . p u t ( ” key ” , APP\_CODE\_GAODE) ;  / / 高 德 获 取 地 理 信 息  S t r i n g r e s p o n s e = H t t p U t i l . g e t ( ” h t t p s : / / r e s t a p i . amap . com / v3 / g e o c o d e / r e g e o ” , p a r a m e t e r s ) ;  JSONObject r e s p o n s e J s o n = J S ON U t i l . p a r s e O bj ( r e s p o n s e ) ; S t r i n g s t a t u s = r e s p o n s e J s o n . g e t ( ” s t a t u s ” ) . t o S t r i n g ( ) ;  i f ( ! ” 1 ” . e q u a l s ( s t a t u s ) ) {  l o g . e r r o r ( ” 列 表 信 息 获 取 失 败 ， 经 纬 度 ： ” + l o c a t i o n ) ;  r e t u r n n u l l ;  }  JSONObject r e g e o c o d e = r e s p o n s e J s o n . g e t J S O N O bj e c t ( ”  r e g e o c o d e ” ) ;  r e t u r n r e g e o c o d e . g e t ( ” fo r m a t t e d \_ a d d r e s s ” ) . t o S t r i n g ( ) ; } c a t c h ( E x c e p t i o n ex ) {  l o g . e r r o r ( ” 调 用 接 口 失 败！ ” + ex . g e t M e s s a g e ( ) ) ;  r e t u r n n u l l ;  }  }  } |

代码块 2: 获取汽车经纬度地理位置

编写远程控制脚本

( 1 ) 车辆位置实时追踪。汽车上的导航系统主要依赖 GPS，如果天气恶劣， 还 可以利用内置 SIM 卡的无线网络基站进行辅助定位。汽车还配备了 SIM 卡和导航 地图， 可以帮助司机在最短的时间里， 找到正确的路线。如果有了网络， 就可以连 接到云端， 通过在该路段上行驶的车辆的数目来判定前面的道路是否拥堵。根据代 码分析， 这辆车可以连接到高德地图的 API。这个 ICV 的位置经纬度判断是 GPS 来确认，最终把数据存储到 TSP 云端数据存储中。

我们通过上节逆向工程 APK 文件编写了定位追踪代码， 进行越权操作包括： 定位追踪、敏感信息获取， 以及调用的 API 的密钥。这里， 编写的脚本首先需要越 权获取车辆经纬度， 经纬度可以从 TSP 云端数据中通过接口得到， 也可以通过调 用高德地图 API 获取车辆实时定位。最后我们通过 pc 电脑执行代码远程获取了对 应车辆的位置信息和其他身份等更敏感信息。如代码块 2 所示

**5.4.3** 流量抓包和远程登录

在本节我们通过搭建无线局域网实现 APP 发送 HTTP 指令抓包分析, 从而伪 造请求参数达到远程向智能网联汽车发出指令的目的。 Cookie 是一种存储在客户 端的文本文件， 用于跟踪和记录用户的会话信息， 例如登录信息、购物车内容等。 Cookie 的工作原理是在客户端(例如浏览器) 和服务器之间建立一个状态管理机 制， 使得服务器可以在多次 HTTP 请求中识别同一用户的身份和状态。当用户首 次访问网站时， 服务器会返回一组 Cookie，包含一些用户信息和一个唯一的标识 符。当用户再次访问该网站时， 浏览器会将 Cookie 发送给服务器， 服务器通过解析 Cookie 来获取用户的会话信息。 session 本意是指客户端与服务器的会话状态， 由 于凭证存储到了服务端， 后来也把这些存在服务端的信息称为 session。现在服务 器决定自己维护登录状态， 仅发给客户端一个 key，然后在自己维护一个 key-value 表， 如果请求中有 key，并且在表中可以找到对应的 value，则视为合法 图 5.11 为 HTTP 请求返回验证 Cookie 流程。所以， 当我们获得另一个客户机的 cookie 时，我 们可以冒充攻击。我们先用抓包工具开始抓包 HTTP 请求， 然后查看 cookie。接着 在抓包工具复制对应的 HTTP 请求头数据携带该 cookie 在程序中发送HTTP 请求，

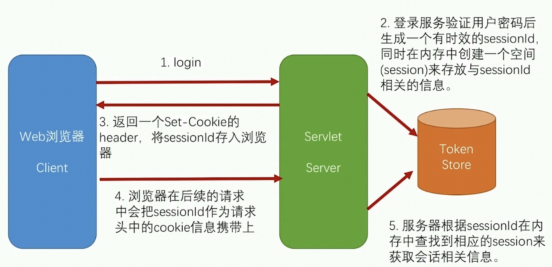


图 5. 11 HTTP 请求返回验证 Cookie 示意图

就能让程序伪装 APP通过改变参数发出特定的请求操作。

对数据的抓包流进行分析。这里我们采用 Fiddler[[45](#_bookmark252)] 这款软件来进行数据抓取， Fiddler 不仅可以抓 web 页面的 HTTP/HTTPS 的数据报文, 也可以抓取我们手机移 动端的数据报文。在攻击目标与服务器之间中介， 嗅探两者之间的数据流量， 从而 窃取用户的数据资料。具体步骤如下:

• 将手机设置为使用 Fiddler 作为代理服务器， 并且确保手机和计算机在同一 个网络中。

• 配置手机 App 代理： 将手机 App 代理设置为 Fiddler 的代理， 以便所有的网 络流量都通过 Fiddler 进行捕获和分析。

• 查看抓包结果： 在 Fiddler 工具栏上， 点击“Inspectors”选项卡，可以查看捕获到 的请求和响应。在“Inspectors”选项卡下，可以查看不同的视图，如“Raw”、“Head- ers”、“JSON”等。

• 分析抓包结果： 通过分析请求和响应， 可以了解每个请求的内容、响应时间、 状态码等信息，从而识别出潜在的问题或性能瓶颈。

在设置好了 Fiddler 之后， 我们通过车联网 APP 进行了查看车辆信息 (车辆四 门开关状态、行驶里程、剩余流量、续航里程、发动机状态) 的操作与此同时 APP 发起了 HTTP 请求， 通过 Fiddler 我们成功了侦测到了该请求以及返回数据。如图

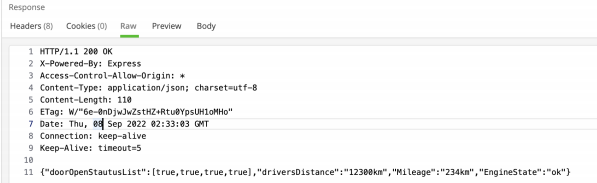


图 5. 12 Fiddler 抓取 HTTP请求车辆状态信息接口图

5.12 所示: 我们发现手机 APP 有控制车门开关功能， 因此我们通过手机 APP 点击 关门， 此时 Fiddler 也同样侦测到了请求如法炮制我们利用 Fiddler 中的 Composer 功能自定义服务请求发送到服务器， 可以手动创建一个新的请求， 也可以在会话表 中， 拖拽一个现有的请求并进行修改； 因此 Composer 可以篡改 Cookie 中的数据。 也就是说， Inspectors 篡改的是我们输入的数据, 这里类似 Web 安全中 CSRF 请求 攻击 [[46](#_bookmark253)]，主要操作步骤如下:

• 首先定位到那条开车门请求记录， 然后用鼠标将该条请求记录的位置拖拽到 Composer 中接口。 Composer 会自动读取到该条请求的所有数据。

• 篡改数据。直接在 Composer 中的 Request Body 或者是请求头信息中修改数 据

• 点击“Execute”按钮执行发送请求。

由于” 开门”“关门”操作是同一个 HTTP 请求接口只是参数不同, 因此我们可以任意 的篡改参数任意实现开关门。

**5.5** 防御措施

对于上述远程攻击，我们提出了一些解决方案，仅供参考。

(1) 接口加密关键数据

IVI 系统只对某些重要的数据进行了加密， 所有接口都会暴露敏感的消息息， 并且有可能会收到恶意的攻击。所以， 要实现车载 TSP 系统和远程设备之间的安 全通讯， TSP 必须做到以下几点： 加密更多关键信息， 或者尽量降低已加密数据与

纯文本的耦合。

(2) 安全认证和访问控制。

TSP 一般存在不合理的云身份验证结构， 造成用户名泄漏以及修改口令。黑客 可以通过假冒用户的身份进行非法登陆， 从而对用户的安全造成极大的威胁。通 过 HTTP ( S) 来阻止对某个 IP 的处理也能避免黑客行为以及提升系统防火墙以及 提高对 SQL 注入的认知都能提升系统的安全性。

(3) 应用逻辑混淆和安全加固。

在应用程序中集成混淆工具如 Proguard 等， 这能极大的增加黑客的破解难度； 将代码的最重要部分保留在 C/C++ 开发代码中， 这样即便黑客攻克了开发代码也 很难获取我们的关键代码； 使用 MD5、AES 等加密算法加密重要的 api 密钥等， 这 样和安全接口的身份凭证相结合能提升接口安全性；

**5.6** 本章小结

本章首先通过 Isogrash AttackTree 这款软件对商用汽车进行了仿真实验， 验证 了我们提出的安全威胁模型的可行性。其次， 再进行真实的远程渗透攻击的实验。 先进行蓝牙近距离通信伪造操作请求成功的发送伪造请求解锁了车辆车门； 然后 破解解析车联 App，从而获取车主个人信息及汽车内部信息和状况; 最后我们通过 抓包手机互联 APP 发送的汽车操作 HTTP 请求获得了登录凭证 Token 通过该凭证 我们实现了伪造请求远程操控智能网联汽车的入侵行为。

第六章 总结与展望

**6.1** 工作总结

论文从智能网联汽车的安全架构开始， 首先展示现有 ICV 领域使用的通信技 术、基础设施以及网络拓扑； 然后通过大量的调查对 ICV 面临的安全威胁进行系 统分类和展示， 列出多种典型的攻击和威胁面； 并用传统 STRIDE 给智能网联汽车 的 IVI 系统进行了威胁建模， 第四章提出了自己的威胁建模方法并进行了实例验 证， 最后给出了和 STRIDE 模型的对比评估； 最后通过漏洞挖掘和利用， 编写渗透 脚本， 成功对一款新型 ICV 实施了远程入侵， 证明当前 ICV 确实存在诸多的安全 问题。本文也存在一些不足之处， 一是只是从 TSP 系统的远程攻击的角度去进行 渗透攻击， 限于篇幅， 没有对其他方向的攻击和威胁进行深入研究和探讨， 日后需 要加强 ICV 其他领域的窥探； 二是新提出的威胁建模方法， 只是成功的应用在了 ICV 领域，至于其他场景的此新型威胁建模方法，有待验证和改进。

本文在对 ICV 进行了远程攻击的基础上， 对当前 ICV 存在的许多安全问题进 行了分析探讨。文章也有不足之处， 一是只对 IVI 系统的远距离攻击做了较深的探 讨； 由于篇幅所限， 并没有对其他方面的攻击和威胁进行详细的分析和探讨， 今后 还需要对车联网、物理等方向的远程攻击等进行进一步的研究。第二， 我们提出的 安全威胁建模有效性尚待验证与改进，并且希望可推广到更多安全威胁建模领域。

**6.2** 未来展望

通过对威胁模型的分析， 表明了智能网联汽车的安全性目前还不算高， 本文 提出的问题都会间接或直接地造成车辆被非法使用和远程操控； 虽然本文进行的 是车载网络的安全威胁分析， 但是这种方法并不局限于汽车领域。它也可以应用 于其他信息物理系统。未来， 我们将优化方法， 进行全面的安全威胁分析， 有助于 在汽车网络安全的发展中更早地发现威胁和漏洞。

参考文献

[1] SCHMITTNER C, MA Z, REYES C, et al. Using SAE J3061 for automotive se-

curity requirement engineering[C] // International Conference on Computer Safety, Reliability, and Security. 2016 : 157 – 170.

[2] SCHNEIDER U. ISO/SAE 21434-The Standard for Security in Connected Cars[J].

ATZ worldwide, 2022, 124(4) : 64 – 64.

[3] 中国智能网. 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. .

[4] 思维财经. 2023 年新能源汽车市场格局正在酝酿巨变 [C/OL] // 2023 年新能源 汽车市场格局正在酝酿巨变. .

[5] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive experimen-

tal analyses of automotive attack surfaces[C] // 20th USENIX security symposium

(USENIX Security 11). 2011.

[6] MILLER C, VALASEK C. Remote exploitation of an unaltered passenger vehicle[J].

Black Hat USA, 2015, 2015(S 91).

[7] 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.

[8] 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.

[9] 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.

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

[11] GU Z, HAN G, ZENG H, et al. Security-aware mapping and scheduling with hard-

ware co-processors for flexray-based distributed embedded systems[J]. IEEE Trans- actions on parallel and distributed systems, 2016, 27(10) : 3044 – 3057.

[12] MOUSA A R, NOURELDEEN P, AZER M, et al. Lightweight authentication proto-

col deployment over FlexRay[C] // Proceedings of the 10th International Conference on Informatics and Systems. 2016 : 233 – 239.

[13] GOSMAN C, DOBRE C, POP F. Privacy-preserving data aggregation in Intelligent

Transportation Systems[C/OL] // 2017 IFIP/IEEE Symposium on Integrated Net- work and Service Management (IM). 2017 : 1059 – 1064.

[14] ALOMAR R, EL SADDIK A, MUHAIDAT S. Secure and efficient communication

for vehicular networks: a survey[J]. IEEE Transactions on Intelligent Transportation

Systems, 2017, 18(12) : 3374 – 3393.

[15] DENG X, LIANG X, LI X. Security and privacy in vehicular ad hoc networks: a

survey[J]. IEEE Transactions on Intelligent Transportation Systems, 2014, 15(2) :

686 – 696.

[16] PETER A, SCHÄFER G, TEWS E. Evaluation of Remote Keyless Entry Systems in

Modern Cars[J]. IEEE Transactions on Vehicular Technology, 2019, 68(5) : 4061 – 4072.

[17] KOHNFELDER L, GARG P. The threats to our products[J]. Microsoft Interface,

Microsoft Corporation, 1999, 33.

[18] LAUTENBACH A, ALMGREN M, OLOVSSON T. Proposing HEAVENS 2.0–

an automotive risk assessment model[C] // Computer Science in Cars Symposium. 2021 : 1 – 12.

[19] MOHSIN M, SARDAR M U, HASAN O, et al. IoTRiskAnalyzer: A probabilis-

tic model checking based framework for formal risk analytics of the Internet of

Things[J]. IEEE Access, 2017, 5 : 5494 – 5505.

[20] AGADAKOS I, CHEN C-Y, CAMPANELLI M, et al. Jumping the air gap: Mod- eling cyber-physical attack paths in the Internet-of-Things[C] // Proceedings of the 2017 workshop on cyber-physical systems security and privacy. 2017 : 37 – 48.

[21] UCEDAVELEZ T, MORANA M M. Risk Centric Threat Modeling: process for attack simulation and threat analysis[M]. [S.l.] : John Wiley & Sons, 2015.

[22] SHOSTACK A, STEWART C. VAST: a visual, agile, and simple threat modeling

methodology for security and privacy[J]. IEEE Security & Privacy, 2015, 13(1) :

52 – 57.

[23] LARRONDO-PETRIE M M, WHITEHEAD J, FLINN J, et al. TRIKE: A com-

prehensive threat modeling framework for embedded systems[J]. IEEE Security &

Privacy, 2013, 11(6) : 38 – 45.

[24] WOO S, JO H J, LEE D H. A practical wireless attack on the connected car and secu-

rity protocol for in-vehicle CAN[J]. IEEE Transactions on intelligent transportation systems, 2014, 16(2) : 993 – 1006.

[25] 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.

[26] AMOOZADEH M, RAGHURAMU A, CHUAH C-N, et al. Security vulnerabili-

ties of connected vehicle streams and their impact on cooperative driving[J]. IEEE

Communications Magazine, 2015, 53(6) : 126 – 132.

[27] 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.

[28] 腾讯网. 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.

[29] 荀毅杰. 使用便携式 GPS欺骗器篡改车辆的 GPS 路线 [R]. 2020.

[30] BERGHEL H, UECKER J. WiFi attack vectors[J]. Communications of the ACM,

2005, 48(8) : 21 – 28.

[31] NISSIM N, YAHALOM R, ELOVICI Y. USB-based attacks[J]. Computers & Se-

curity, 2017, 70 : 675 – 688.

[32] ALAMLEH H, ALQAHTANI A A S. A cheat-proof system to validate GPS location

data[C] // 2020 IEEE International Conference on Electro Information Technology

(EIT). 2020 : 190 – 193.

[33] RUDDLE A, WARD D, WEYL B, et al. Deliverable D2. 3: Security requirements for automotive on-board networks based on dark-side scenarios[J]. EVITA project,

2009.

[34] SAMUEL J, AALAB K, JASKOLKA J. Evaluating the soundness of security met-

rics from vulnerability scoring frameworks[C] // 2020 IEEE 19th International Con- ference on Trust, Security and Privacy in Computing and Communications (Trust-

Com). 2020 : 442 – 449.

[35] WINTERFELDT D V, FISCHER G W. Multi-attribute utility theory: models and

assessment procedures[J]. Utility, probability, and human decision making, 1975 :

47 – 85.

[36] LIU Y, ECKERT C M, EARL C. A review of fuzzy AHP methods for decision-

making with subjective judgements[J]. Expert Systems with Applications, 2020, 161 : 113738.

[37] KUBLER S, ROBERT J, DERIGENT W, et al. A state-of the-art survey & testbed

of fuzzy AHP (FAHP) applications[J]. Expert Systems with Applications, 2016, 65 :

398 – 422.

[38] DOMINIC D, CHHAWRI S, EUSTICE R M, et al. Risk assessment for cooperative automated driving[C] // Proceedings of the 2nd ACM workshop on cyber-physical systems security and privacy. 2016 : 47 – 58.

[39] REINDL A, WETZEL D, BALBIERER N, et al. Comparative Analysis of CAN

CAN FD and Ethernet for Networked Control Systems[C] // embedded world con- ference digital. 2021.

[40] ZAGO G M, de FREITAS E P. A quantitative performance study on CAN and CAN

FD vehicular networks[J]. IEEE Transactions on Industrial Electronics, 2017, 65(5) :

4413 – 4422.

[41] 安天实验室. 安天基于蓝牙协议漏洞的 BlueBorne 攻击综合分析报告 [R]. 2018.

[42] von TSCHIRSCHNITZ M, PEUCKERT L, FRANZEN F, et al. Method confusion

attack on bluetooth pairing[C] // 2021 IEEE Symposium on Security and Privacy

(SP). 2021 : 1332 – 1347.

[43] LU Y, MEIER W, VAUDENAY S. The conditional correlation attack: A practical

attack on bluetooth encryption[C] // Annual International Cryptology Conference. 2005 : 97 – 117.

[44] YANG T, YANG Y, QIAN K, et al. Automated detection and analysis for android

ransomware[C] // 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cy- berspace Safety and Security, and 2015 IEEE 12th International Conference on Em-

bedded Software and Systems. 2015 : 1338 – 1343.

[45] CRANE J. Fiddler crabs ofthe world: Ocypodidae: genus Uca : Vol 1276[M]. [S.l.] :

Princeton University Press, 2015.

[46] BLATZ J. Csrf: Attack and defense[J]. McAfee® Foundstone® Professional Ser-

vices, White Paper, 2007.

致 谢

经过这几年的学习和工作， 我结识了一群有趣的同学。虽然我们面临着学业 和工作的压力， 但是大家的陪伴让我们的生活充满了交流、玩笑、吐槽和鼓励， 增 添了不少乐趣。我感到非常幸运能够遇到你们。同时， 我也要感谢工作中遇到的同 事们， 实习的日子充满了干劲和欢乐， 让我有机会实践所学知识并不断成长。非常 感谢我的朋友们对我的鼓励和支持。当我遇到困惑、烦闷、失落时， 你们一直陪伴 在我身边， 倾听我的诉说和分享， 成为了我心中的港湾。特别感谢刘虹老师对我的 指导和帮助， 她总是耐心地解答我的问题， 并且那种乐观向上的态度也深深地影 响了我， 增强了我的信心。最后， 感谢我的家人， 他们在我最脆弱、焦虑、不安的 时刻一直陪伴在我身边，给予我无限的爱、支持和鼓励，是我坚强的后盾。