基于威胁建模的智能汽车网络安全风险防护设计

徐 辉

（江铃汽车股份有限公司 南昌 330000）

摘 要 随着智能汽车产业的发展，其网络安全问题愈发凸显。据统计，智能网联汽车中涉及车辆操控、车载通信以及数据存储的核心漏洞已超3 700个，2023年至2024年9月间，国内发生20余起车企相关数据泄露事件，暴露出行业在安全防护方面的严峻挑战。在这一背景下，威胁建模技术以其对潜在风险的系统化分析和评估能力，成为网络安全防护的关键工具。目前，STRIDE模型、攻击树等经典建模方法在风险识别和分析中表现出一定优势，但其对智能汽车特定场景的适配性有限，难以涵盖复杂的车联网交互及数据流动场景，且与后续的防护设计缺乏有机衔接。因此，文中探讨了基于威胁建模的智能汽车网络安全风险防护设计问题，以期提升智能汽车网络安全风险防护水平。

关键词： 车载通信；风险防护；网络安全

中图分类号 TP309

Design of Intelligent Automotive Network Security Risk Protection Based on Threat Modeling

XU Hui

（Jiangling Motors Co., Ltd., Nanchang 330000, China）

Abstract With the development of the intelligent automobile industry, its network security issues have become increasingly prominent. According to statistics, there are over 3700 core vulnerabilities related to vehicle control, in vehicle communication, and data storage in intelligent connected vehicles. Between 2023 and September 2024, there were more than 20 data breaches related to car companies in China, exposing severe challenges in the industry's security protection. In this context, threat modeling technology has become a key tool for network security protection due to its ability to systematically analyze and evaluate potential risks. At present, classic modeling methods such as STRIDE model and attack tree have shown certain advantages in risk identification and analysis, but their adaptability to specific scenarios of intelligent vehicles is limited, making it difficult to cover complex scenarios of vehicle networking interaction and data flow, and lacking organic connection with subsequent protection design. Therefore, the paper explores the design of intelligent vehicle network security risk protection based on threat modeling, in order to improve the level of intelligent vehicle network security risk protection.

Key words Vehicle communication, Risk prevention, Network security

1 基于威胁建模的智能汽车网络安全框架

1.1 威胁建模框架的构建

威胁建模作为网络安全分析的基础工具，在智能汽车网络中具有重要的地位。其核心在于通过分析可能的威胁路径和攻击目标，系统性地识别并评估潜在的风险[1]。当前，国际通用的威胁建模方法包括STRIDE模型、攻击树分析和HEAVENS框架等，这些方法分别从欺骗、篡改、抵赖等维度或攻击路径的多样性入手，为风险评估奠定了理论基础[2]。在智能汽车这一复杂的“车-路-云”体系中，传统威胁建模方法需要进行针对性优化，以适应其多维度的网络架构和动态通信特性。为此，本文提出了基于ISO/SAE 21434标准的资产-威胁-安全属性三维模型。该模型通过识别关键资产、界定潜在威胁，并匹配对应的安全需求，构建了一个更适用于智能汽车环境的威胁分析框架。具体而言，“资产”包括智能汽车中的ECU、T-BOX等硬件，车载系统及数据资源；“威胁”涵盖通信劫持、数据篡改及权限提升等多种形式；“安全属性”则聚焦于完整性、真实性与抗重放能力。

此外，结合TARA（威胁分析与风险评估）流程，进一步构建了适用于智能汽车的威胁建模实施流程。（1）以数据流图（DFD）为核心，描绘系统的通信和操作路径。（2）通过攻击树模型量化不同攻击路径的可能性。（3）利用风险矩阵对威胁进行分级分析。智能汽车的威胁与风险评估模型如图1所示。

作者简介：徐辉（1982—），本科，研究方向为网络安全、大数据、AI。

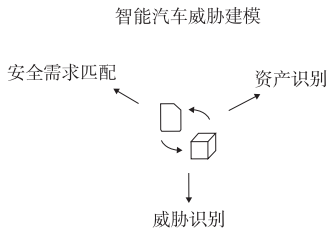

图1　智能汽车的威胁与风险评估模型

1.2　威胁建模驱动的网络安全需求分析

在威胁建模驱动的风险评估过程中，攻击路径分析被视为识别高优先级威胁的核心步骤。每一条攻击路径可以被分解为若干个具体的攻击步骤，从起点的目标资产（如车载模块或敏感数据）开始，经过多个可能的攻击手段，最终指向预定义的网络安全目标，针对攻击路径的分析过程主要包括以下几个阶段。首先，在风险评估中，攻击路径的可能性是确定风险等级的关键。根据智能汽车的实际场景，本文对攻击路径进行了分类（见表1），从几乎不可能完成的“非常低”到几乎肯定能完成的“高”，明确了每个等级的具体定义。

表1　攻击可行性等级

等级	描述
FL4-高	攻击路径可见且容易实现或几乎肯定能完成
FL3-中	通过非直接的攻击方法，攻击路径是可行的
FL2-低	攻击路径在理想情况下可实现
FL1-非常低	攻击路径在理论上可实现但几乎不可能完成

这些等级对应于威胁建模中路径步骤的成功概率，如式（1）所示：

$$P(A)=\prod_{i=1}^{n} P_i \tag{1}$$

其中，$P(A)$为攻击路径A的整体成功概率；P_i为路径中每个步骤i被攻破的独立概率；n为路径中的步骤总数。

以未授权访问T-BOX通信为例，若攻击路径可行性为中等（FL3），则攻击步骤可能通过组合路径实现，具有较高的成功概率。其次，风险值的计算直接决定了防护需求的优先级。根据TARA流程，风险值R可通过威胁影响S和发生可能性P的乘积计算。本文以风险矩阵（见表2）的形式对风险值进行直观量化。矩阵横向代表攻击可行性（FL1到FL4），纵向代表潜在影响等级（IL1到IL4），两者交叉生成的风险值为1~5，分别表示从最低风险到最高风险。

表2　风险判定矩阵

风险值	FL1	FL2	FL3	FL4
IL1（最低影响）	1	1	2	3
IL2	1	2	3	4
IL3	2	3	4	5
IL4（最高影响）	3	4	5	5

为应对智能汽车复杂动态的网络环境，风险评估可进一步结合动态权重调整机制优化需求分析。调整因子w被引入风险值的计算式中，用以反映攻击态势实时变化对风险等级的影响，如式（2）所示：

$$R'=w\times S\times P \tag{2}$$

其中，w依据实时监控数据动态调整。

在通信负载显著增加或威胁监测频率提高时，可适当提高，以确保安全需求的优先级与实际风险动态匹配。上述方法通过风险矩阵将风险值可视化，交叉分析威胁发生概率和影响程度，以确定优先防护区域。

1.3　智能汽车网络安全防护设计

在智能汽车的网络安全设计中，“车-路-云”多层次架构的复杂性要求制定动态且分层的防护策略，以应对可能的安全威胁和多样化攻击路径。基于威胁建模驱动的设计理念，从车载通信安全、动态协同防护和嵌入式代码加固3个维度进一步构建智能汽车的网络安全体系。首先，车载通信安全设计是整车网络安全的基础环节。针对传统CAN/CAN-FD网络及车载以太网通信的特点，安全通信技术需同时满足真实性、完整性和抗重放的需求。在车载CAN网络中，通过引入基于消息认证码（MAC）的消息鉴别技术，可有效防止数据篡改与伪造。同时，在车载以太网中，广泛采用TLS协议作为传输层加密机制，不仅保护了V2X通信的安全性，还增强了节点间数据交换的抗监听能力。此外，结合动态密钥管理策略，可确保加密和认证技术在资源有限的车载环境中高效运行。其次，动态协同防护策略是应对复杂攻击态势的关键。通过“云-管-端”协同架构，建立多层次的入侵检测和响应体系。在终端，可以基于轻量级的入侵检测模块，实现对通信异常的本地监测；在管控层，部署差异化检测功能，对跨域流量的异常行为进行实时分析；在云端，通过车辆安全运营中心实时聚合多源数据，并结合机器学习算法生成全局威胁态势。基于威胁建模生成的攻击路径数据，协同架构可动态调整防护策略，对高风险路径实时加强安全防护。在OTA更新过程中，云端可优先验证更新包的完整性，并对高频访问路径增加认证强度。最后，在嵌入式代码安全加固方面，由于车载设备的软硬件资源受限且实时性要求较高，传统代码加固技术需适配嵌入式环境。本文提出的基于代码混淆的安全加固方法，通过对控制流的扁平化处理和指令集的随机化，显著提升了逆向工程和漏洞利用的难度。在嵌入式处理器中采用多维度评估模型，综合分析代码安全性、功能一致性、资源开销及性能损耗，并通过实验验证其有效性。

2　仿真分析

2.1　实验设计

为了验证威胁建模与网络安全防护设计的有效性，本文设计了一系列覆盖典型场景的实验方案，重点关注OTA升级和车路协同两个高风险、高复杂度的应用场景。在OTA升级场景中，攻击可能集中于更新包的完整性与可信性验证，而在车路协同场景中，威胁则更多来自实时通信的

篡改与劫持。实验旨在评估威胁建模驱动下的防护策略在不同攻击路径中的实际效果，并量化其在检测效率、资源开销和响应延迟等指标上的表现。实验环境包括整车级虚拟测试平台和零部件级硬件模拟平台。虚拟平台基于车载以太网的核心协议栈，模拟车辆从T-BOX接收到OTA更新包直至完成验证和部署的全过程；硬件平台则采用真实的ECU节点和CAN总线，用于构建典型车内网络场景。实验采集的数据涵盖攻击路径的实时日志、网络通信流量以及在威胁建模基础上生成的风险矩阵。对于OTA升级的完整性验证，实验通过动态调整云端验证密钥的长度和频率，观察其对响应时间和加密成本的影响。在车路协同场景中，系统部署了多层次入侵检测模块，并结合实时生成的攻击路径数据进行高频访问路径的异常监测。

2.2 威胁建模验证

在设计实验中，结合OTA升级和车路协同两个典型场景，威胁建模的核心成果，包括风险矩阵和高风险路径的优先级划分，得到了系统性的验证。在OTA升级场景中，系统首先绘制了完整的通信数据流图，并基于攻击树模型提取关键的攻击路径。实验对路径可能性进行量化，并结合影响等级计算风险值。以更新包劫持为例，通过攻击路径的逐步分解，最终的整体路径成功概率为0.15（见表3），对应的风险值为0.60（中风险）。实验结果表明，风险矩阵的量化结果与实际攻击实验中的威胁表现一致，模型在高优先级路径的识别上表现出高度的准确性。

表3 OTA升级场景下的风险评估结果

攻击路径	可能性	影响等级	风险值
更新包劫持	0.15	4	0.60
中间人攻击	0.22	3	0.66
认证重放攻击	0.08	5	0.40

在车路协同场景中，通过对传输路径的实时监测，动态调整因子被引入风险计算。实验模拟了多种攻击场景，包括通信劫持和数据篡改，实验验证了动态调整机制在攻击态势突变时的高效性（见表4）。结合动态调整因子，风险值能根据攻击路径的变化进行实时更新，优先级调整的灵活性为防护策略优化提供了强有力的支撑。具体而言，在动态调整后，篡改攻击路径的检测率提高了25%，显著优于静态建模结果。

表4 车路协同场景动态调整机制的评估

攻击路径	静态风险值	动态风险值	攻击检测率提升
通信劫持	3.4	4.1	+21%
数据篡改	2.8	3.5	+25%
路径重定向攻击	2.5	3.2	+28%

以上实验结果表明，通过结合动态调整因子，威胁建模能适应攻击态势的实时变化，有效提升了高风险路径的识别能力和防护效率。

2.3 防护技术验证

实验对车载通信安全、协同防护以及代码安全加固技术的性能进行了量化验证，涵盖拦截率、误报率及资源消耗等关键指标。在OTA升级场景中，不同加密强度的消息认证码（MAC）和TLS协议被用于验证传输完整性保护的效果（见表5）。结果表明，拦截率随加密强度的提高从83%增长至97%，误报率则下降至1.6%。然而，资源消耗随着加密强度提升显著增加，CPU占用率达到35%，OTA更新延迟增长至17.8s，表明通信安全技术需在性能与资源消耗间平衡优化。协同防护策略通过“云-管-端”架构提升检测效率，通信劫持、数据篡改等攻击的检测率分别为93%和90%，动态调整响应时间保持在25 ms以内，资源占用低于15%，充分验证了协同防护体系的有效性。

表5 OTA场景下车载通信安全技术性能评估

加密强度等级	拦截率/%	误报率/%	CPU占用率/%	OTA更新延迟/s
低	83±2	2.3±0.5	15	10.3±1.2
中	91±3	1.9±0.4	23	12.8±1.0
高	97±1	1.62.3±0.3	35	17.8±1.5

3 结语

本文基于威胁建模构建了智能汽车网络安全框架，并通过实验验证了其有效性。模型结合ISO/SAE 21434标准，从资产、威胁和安全属性三维度系统性分析了攻击路径，提出了动态调整机制与风险矩阵，显著提升了风险评估的实时性与精准度。实验表明，车载通信安全技术在提高拦截率的同时保持着较低的误报率，但资源消耗随加密强度增加而显著上升，需优化性能。协同防护策略利用“云-管-端”架构，在检测效率和响应速度上表现优异，动态调整机制有效降低了高频攻击漏检率。代码安全加固技术进一步增强了系统抗攻击能力，平衡了资源消耗与安全性。

参考文献

[1] 范萍萍，刘怡婧，侯亚玲.智能网联汽车网络安全威胁建模平台研究[J].时代汽车，2023(23)：16-18.

[2] 郑磊，韩鹏军，田晨雨，等.基于威胁建模的网络安全日志自动化分析技术[J].微型电脑应用，2023，39(7)：154-156，180.