智能网联汽车的安全威胁研究

荀毅杰[1]，刘家佳[2]，赵静[1]
（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；
2. 西北工业大学网络空间安全学院，陕西 西安 710072）

摘 要：智能网联汽车正成为未来汽车行业的主流，而汽车安全问题也逐渐成为汽车工业中不可忽视的难题。详细分析了智能网联汽车中存在威胁的攻击面，总结了一些具有代表性的攻击方法。在此基础上，讨论了一个利用控制器局域网络总线和汽车远程服务提供商漏洞对纳智捷 U5 汽车进行攻击的实际案例。实验结果表明，智能网联汽车中存在很多可以被利用的攻击面。最后，针对智能网联汽车中存在的威胁提出了一些可行的防御措施。

关键词：智能网联汽车；远程服务提供商；控制器局域网络总线；电子控制单元；安全威胁
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2019.00134

Research on security threat of intelligent connected vehicle

XUN Yijie[1], LIU Jiajia[2], ZHAO Jing[1]
1. School of Cyber Engineering, Xidian University, Xi'an 710071, China
2. School of Cyber Security, Northwestern Polytechnical University, Xi'an 710072, China

Abstract: Intelligent connected vehicle (ICV) is becoming the mainstream of automotive industry in the future, and automobile safety has gradually become a problem that cannot be ignored in the automotive industry. The threat attack surfaces in ICV were analyzed in detail, and some representative attack methods were summarized. On this basis, a practical case of using the vulnerabilities of controller area network bus and telematics service provider to attack the Luxgen U5 car was discussed. The experimental results show that there are many attack surfaces that can be used in ICV. Finally, some feasible defensive measures against the threats in ICV were put forward.

Key words: intelligent connected vehicle, telematics service provider, controller area network bus, electronic control unit, security threat

1 引言

智能网联汽车（ICV，intelligent connected vehicle）正成为未来汽车行业的主流。许多先进的技术，如云计算、人工智能、V2X（vehicle to everything）通信和高级驾驶员辅助系统等，正越来越广泛地被应用于汽车中，使得网联汽车能够更加智能地为人们提供舒适的服务并保证司机和乘客的安全[1]。如别克、大众等汽车中普遍配备有自动泊车和自适应巡航功能，极大地减轻了司机的驾驶负担；特斯拉 Model 3 提供了远程云服务功能，司机利用手机可以直接对汽车车门开关、空调开关等进行远程控制；沃尔沃研发的自动防撞系统可以自动检测可能与汽车相撞的车辆、行人或其他障碍物，从而保证

收稿日期：2019−07−24；**修回日期：**2019−09−05
基金项目：国家自然科学基金资助项目（No.61771374，No.61771373，No.61801360，No.61601357）；中央高校基本科研业务费资助项目（No.3102019PY005，No.JB181506，No.JB181507，No.JB181508）；中国“111 计划”资助项目（No.B16037）
Foundation Items: The National Natural Science Foundation of China (No.61771374, No.61771373, No.61801360, No.61601357), The Fundamental Research Fund for the Central Universities (No.3102019PY005, No.JB181506, No.JB181507, No.JB181508), 111 Program Subsidized Projects of China (No.B16037)

驾驶员、乘客和行人的安全。

汽车与智能设备之间的多功能连接虽然能够为用户提供更多的便利和更好的驾驶体验，但也为恶意攻击者带来了大量入侵入口[2]。近年来，汽车与外界的互联互通已成为目前及未来汽车的发展趋势。大量接口被用于连接外部智能设备的同时，也可能被恶意攻击者用来实现对车辆内部网络的访问。一旦车辆内部网络被恶意攻击者入侵，不仅会造成驾驶员隐私信息丢失，还会使车辆被攻击者控制[3]。因此，研究 ICV 中存在的漏洞，并针对漏洞提出相应的防御措施是学术界和工业界中重要的研究课题。

ICV 安全已经引起了大量研究人员的关注，他们已在相关方面取得了显著成果。如 Enev 等[4]利用机器学习算法，对汽车控制器局域网络（CAN，controller area network）总线数据进行特征提取，实现对汽车驾驶员的身份识别，证明了用户隐私存在被泄露的风险。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、车身控制模块（BCM，body control module）和自动驾驶控制单元，证明了汽车中存在很多安全隐患[5]。Zeng 等[6]使用便携式 GPS 欺骗器实现了非法篡改车辆的 GPS 路线，严重威胁了车载 GPS 安全。Miller 等[7]在 DEFCON 会议中指出，ICV 中存在大量可被利用的攻击面，如远程无钥匙进入（RKE，remote keyless entry）、蓝牙、Wi-Fi、车载资讯系统、互联网、APP 等，都有可能使用户隐私泄露，甚至导致车辆被远程控制。

对 ICV 的安全威胁进行研究十分必要且具有重要价值。虽然越来越多的研究员开始关注 ICV 的安全问题，但在相关文献中却鲜有综述。鉴于此，本文首先介绍了 ICV 的车辆内部网络和无线通信网络的拓扑结构；其次，详细分析了 ICV 中存在威胁的攻击面和攻击实验，并总结了一些具有代表性的攻击方法；在此基础上，对纳智捷汽车的 CAN 总线和汽车远程服务提供商（TSP，telematics service provider）的威胁漏洞进行了全面研究，证明了 ICV 中存在很多可以被利用的攻击面；最后，针对 ICV 中存在的威胁，提出了一些可行的防御措施，可以给新研究员提供一些基本指导。

2　ICV

ICV 的网络拓扑结构大致由车辆内部网络和无线通信网络两部分组成。车辆内部网络由 CAN 总线和电子控制单元（ECU，electronic control unit）组成，其功能是监控车辆状态、控制车辆行为；无线通信网络由 TSP 和车载终端（T-BOX，telematics BOX）组成，是车辆与远程云服务器之间数据交互的通道。

2.1　车辆内部网络

目前的汽车结构中，车辆内部网络主要由 CAN 总线和 ECU 组成，ICV 的网络拓扑结构如图 1 所示。CAN 总线是国际标准化组织定义的串行通信总线[8]，具有比特率高、抗磁干扰能力强、检波率高等特点，是一种通用、高效、可靠、经济的平台，应用于汽车业、制造业和航天工业中[8]。ECU 是嵌

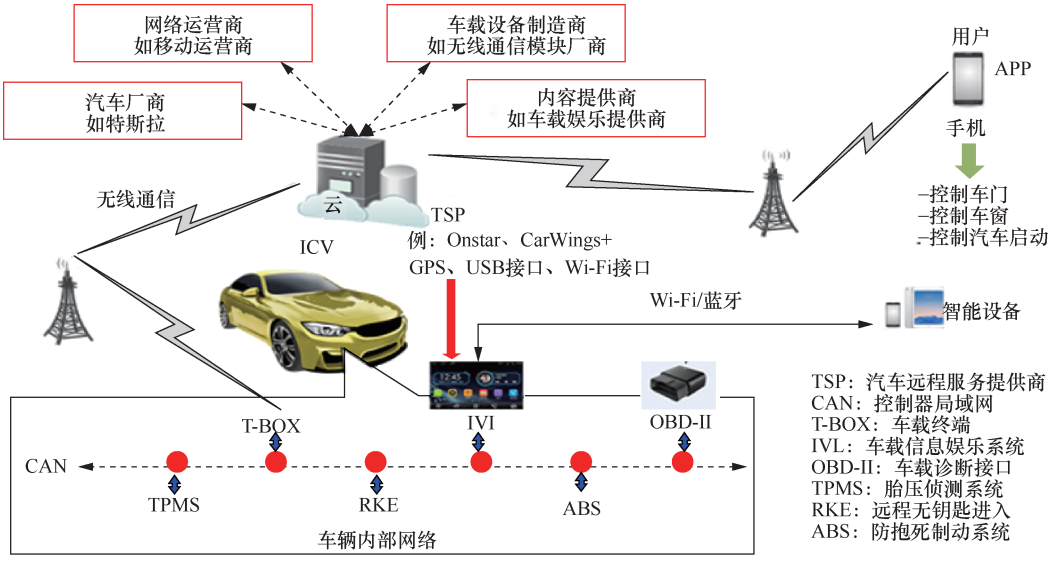


图 1　ICV 的网络拓扑结构

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，如图 1 所示。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[8-9]。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。

2.2 无线通信网络

除了嵌入大量的智能电子设备外，ICV 还普遍配备有 TSP 功能，旨在提供远程控制、第三方服务等功能，为乘客带来更舒适的驾驶体验[10]。如别克君威汽车中配备有自适应巡航、坡道起步辅助系统以及安吉星（Onstar）TSP 服务系统等智能设备。其中，Onstar 可以提供远程信息服务，包括紧急救援服务和防盗。ICV 可以利用 T-BOX 与 TSP 连接，以获取远程信息服务，如图 1 所示。

TSP 主要由车载设备制造商、内容提供商、网络运营商和汽车厂商 4 部分组成[10]。设备制造商负责为汽车提供 TSP 硬件和软件支持；内容提供商为用户提供 GPS 导航、娱乐和多媒体信息等服务；网络运营商包括移动运营商、固话运营商和卫星运营商，旨在为 ICV 和 TSP 之间提供通信基础设施[10]；汽车厂商负责实时监控汽车异常，保护用户的生命安全。TSP 如 Onstar、智行+（CarWings+）和智能副驾（G-Book）等是汽车与外部设备通信的桥梁。TSP 通过集成内容提供商、网络运营商等众多资源，将外部设备和车辆紧密地结合起来，实现智能设备和汽车之间的无线通信，如 TSP 利用第三方云平台的电子地图可以实时计算和规划司机的最优路线。

此外，T-BOX 作为汽车与 TSP 通信的核心设备，向 TSP 上传车辆状态信息和用户信息以实现云端对汽车的跟踪和保护。同时，T-BOX 也可以接收并处理来自 TSP 的控制指令，实现远程控制汽车车门开关、点火/熄火和打开后备箱等操作。TSP 为用户提供了更方便、安全和可靠的服务。然而，一旦 TSP 被攻破，用户隐私和车内数据就会被恶意攻击者窃取，甚至导致目标车辆被攻击者完全控制。

3 ICV 中的潜在威胁和攻击方法

本节详细介绍了 ICV 中存在威胁的攻击面和相应的攻击实验，ICV 中的潜在威胁如表 1 所示。同时，针对 ICV 的攻击实验，总结了一些具有代表性的攻击方法。

3.1 ICV 中的潜在威胁

3.1.1 远距离通信的潜在威胁

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。文献[7]破解了汽车固件（V850），实现了对汽车设备（方向盘等）的远程控制。文献[11]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[5]和文献[12]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。

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[13]揭露了针对新兴互联车辆的交通信号控制的拥塞攻击。

表 1　　ICV 中的潜在威胁

距离	入侵入口	被攻击设备	攻击方法/威胁	文献
远距离通信	蜂窝网络	T-BOX	未经授权的权限升级 不安全的系统接口和配置	[7,11]
	Wi-Fi	ECU	不安全的身份验证 未经授权的权限升级	[5,12]
	OBU/RSU	IVI	数据欺骗	[13]
	GPS	IVI	流量劫持	[6]
近距离车外通信	蓝牙	IVI	不安全的系统接口和配置	[14]
		ECU	无线电信号干扰	[11]
	高频无线电	RKE	软件定义无线电欺骗	[15-16]
		TPMS	无线电信号干扰	[17]
车辆内部网络	USB	IVI	数据欺骗	[11]
	CAN 接口	ECU	未经授权的权限升级 不安全的系统接口和配置 边信道攻击	[4,7]

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[6]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。

3.1.2　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[14]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。文献[15-16]通过软件无线电欺骗实现了对 RKE 系统的攻击，文献[17]则使用软件无线电欺骗实现了对汽车 TPMS 系统的攻击。

3.1.3　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　ICV 中典型的攻击方法

1) DDoS 攻击/EDoS 攻击

DDoS（distributed denial of service）攻击是指在不同位置（IP 地址）的多个攻击者向相同的攻击目标发送常规的服务器请求，服务器资源因请求超载而瘫痪。其中，不同的源 IP 地址可以进行伪造，使

得入侵检测十分困难，因此，DDoS 攻击是一种很难防范的攻击。EDoS（economic denial of sustainability）攻击是由 DDoS 攻击衍生的一种攻击方法，其目的是通过定制或租用僵尸网络的 DDoS 攻击，熟练地实时消耗受害者的通信链路，给攻击目标造成巨大的经济负担，文献[18]详细介绍了 DDoS 攻击和 EDoS 攻击对云安全的威胁，并提出了相应的防范措施。

2) 侧信道攻击

侧信道攻击（SCA，side channel attack）是基于目标设备的物理信息（电流、电压、电磁辐射、执行时间、温度等）与保密信息之间的依赖关系，实现对保密信息的获取。这种攻击方式对加密设备造成了严重威胁，如文献[19]通过映射内部云基础设施，使虚拟机（VM，virtual machine）与目标机共存，从而实现跨 VM 的侧信道攻击，成功提取同一目标 VM 上的数据信息。

3) 中间人攻击

中间人（MITM，man-in-the-middle）攻击是一种针对通信链路的间接攻击方式，利用技术手段将攻击者置于通信链路中，如车辆攻击中，攻击者通常将自己置于 TSP 和 T-BOX 之间，然后以 MITM 身份与通信双方建立正常连接，实现对通信双方数据欺骗。文献[20]指出亚马逊 EC2 的 Java 库及其云客户端易遭受 MITM 攻击。

4) 云中人攻击

云存储已经成为物联网中的一部分，是云服务的一项重要功能。汽车向云端发送实时数据时，需要利用一个令牌进行身份验证，这种身份验证方法使得传输和存储大量数据变得越来越容易。考虑大多数云服务系统不检测令牌是否被盗，通过云中人（MITC，man in the cloud）攻击可以很容易地利用虚假令牌实现身份冒用[21]。攻击者一旦非法获得令牌，就可以访问云账户，窃取汽车数据甚至更改车辆信息。

5) 基于 Web 页面的注入攻击

当手机 APP 与 TSP 云端进行无线通信时，可以通过数据库解释器、利用用户输入数据时的漏洞执行注入攻击。注入攻击能够绕过身份验证直接访问云端信息、修改数据，甚至破坏数据库。腾讯科恩安全实验室的研究员就是利用 Web 页面的注入攻击实现了对特斯拉汽车的远程访问控制[5]。

6) 车载僵尸网络

攻击者利用各种方式传播僵尸程序，在互联网上感染大量智能设备。被感染的设备通过控制通道接收并执行攻击者的指令，致使大范围的目标设备瘫痪，从而形成僵尸网络攻击。文献[22]展示了一种僵尸网络攻击方式，可以在自动驾驶汽车场景中致使车辆瘫痪，造成严重的交通拥堵。

7) 绕过身份认证

为了保证车辆内部网络数据传输的高效性，汽车数据的加密/认证过程需要简化，这带来了许多安全隐患。攻击者能够利用这些漏洞破解数据信息，甚至能够绕过身份认证入侵车辆内部网络，文献[7]利用汽车诊断功能的漏洞绕过认证，成功实现了对汽车车速的控制。

8) 植入恶意软件

恶意软件可能以各种形式存在，如病毒、蠕虫、间谍软件等。在汽车中，攻击者可以通过无线远程信息系统（如媒体播放器、USB、Wi-Fi）的接口注入病毒，发动恶意攻击。根据文献[11]，针对媒体播放器固件的输入漏洞，研究人员将恶意软件添加到音乐文件中，当 IVI 播放这些音乐时，恶意软件就会运行并向车内网络发送恶意 CAN 消息。

9) 嗅探攻击

嗅探攻击是对汽车 CAN 总线数据分组、网络数据分组或蓝牙数据分组的一种拦截分析方式。在嗅探攻击下，汽车设备之间的通信可能被窃听，甚至数据被篡改。由于汽车 CAN 总线中的数据是以广播的形式传播，嗅探攻击是 CAN 总线攻击方式中使用最普遍、最有效的攻击方法。

4 实验研究

为了验证 ICV 中存在很多容易被利用的漏洞，在纳智捷 U5 SUV 汽车中进行了安全测试实验研究，纳智捷 U5 SUV 汽车如图 2 所示。纳智捷汽车不仅配备了巡航控制系统、自动变速器系统、车身控制系统和自动停车系统等大量辅助智能系统，还配备了 TSP、T-BOX 等远程通信模块，智能化程度高，是进行安全测试的理想车辆。纳智捷汽车安全测试实验分为两部分，包括 CAN 总线安全测试实验和 TSP 安全测试实验。

4.1 CAN 总线安全测试实验

在 CAN 总线安全测试实验中，利用嗅探攻击、重放攻击和绕过身份认证等攻击方式实现了对汽车仪表盘数据的篡改、汽车车门的开/关和灯光、雨刷等模块的控制。实验中使用的 OBD-II 诊断设备如图 3 所示。

图 2　纳智捷 U5 SUV 汽车

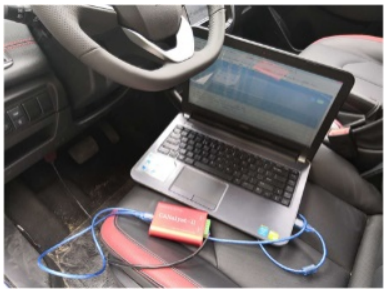


图 3　OBD-II 诊断设备

4.1.1　汽车仪表盘数据的篡改

仪表盘是司机在汽车行驶过程中最依赖的工具之一，它可以显示汽车速度、发动机转速和行驶里程等当前行车状态信息，司机能够根据行车状态信息对汽车状态进行相应调整。因此，一旦仪表盘数据被恶意篡改，可能会导致司机决策失误，甚至造成车祸等灾难性后果。

在汽车运行过程中，汽车速度、发动机转速、灯光和喇叭等多种 ECU 会将自身状态通过 CAN 总线传输到仪表盘的接收器。随后，仪表盘中的数字信号处理器将接收的信号进行解析，并将解码数据传输到仪表盘的显示器中。因此，在上述过程中，恶意攻击者能够利用 CAN 诊断设备捕获相关数据并进行分析。在纳智捷汽车中，ID 为 0360 的数据分组代表仪表盘上的显示速度，数据分组格式为：[$\boldsymbol{X_3X_2\ X_1}$0 00 00 00 2$\boldsymbol{Y}$ 00 $\boldsymbol{MN}$]，其中，$X_3X_2\ X_1$ 为当前车速，取值范围为 0x000~0x5DA，表示车速范围是 0~199 km/h。Y 与压力传感器有关；MN 是一个与车速有关的计数器。根据数据格式和规律，利用式(1)推导出实际速度

$$车速(km/h)=34.5\times X_3+2\times X_2+X_1/8 \tag{1}$$

破解 CAN 总线中的车速编码后，可编写脚本生成一组 CAN 控制指令，并利用 OBD-II 端口注入指令以实现对仪表盘的欺骗。注入的部分攻击数据如下

SEND 0x0360 Frame 8 17 10 00 00 00 20 00 A8
SEND 0x0360 Frame 8 **17 0**0 00 00 00 20 00 B8
SEND 0x0360 Frame 8 17 10 00 00 00 20 00 C6
SEND 0x0360 Frame 8 **17 0**0 00 00 00 20 00 D6
SEND 0x0360 Frame 8 17 10 00 00 00 20 00 E4
SEND 0x0360 Frame 8 **17 0**0 00 00 00 20 00 F4

其中，加粗部分“17 0”表示仪表盘显示速度为 34.5×1+2×7+0/8=48 km/h。在嗅探分析过程中发现，纳智捷汽车制造商在数据的末尾添加了与速度相关的计数器，以增强 CAN 数据的安全性。然而，在攻击实验中，放弃模拟计数器而直接攻击仪表盘的速度显示时，实验攻击仍然有效。

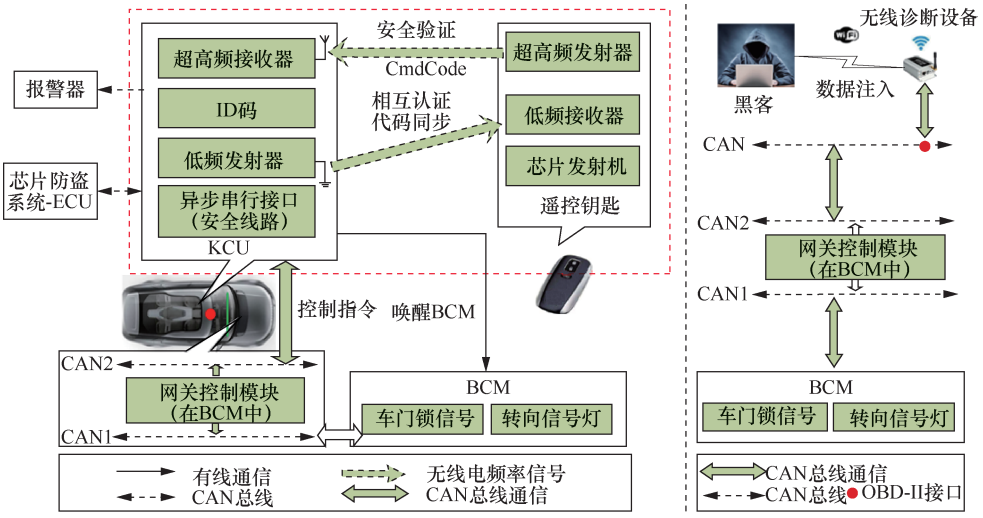
同理，可以利用相同的攻击方法实现对仪表盘中发动机转速、发动机温度等功能的控制。汽车仪表盘显示数据篡改实验结果如图 4 所示。在图 4 中，仪表盘显示当前车速为 161 km/h，发动机转速为 7 400 r/s，发动机温度为 0 ℃，安全带等指示灯均显示报错，这些情况在汽车正常行驶中是不可能同时出现的。

图 4　汽车仪表盘显示数据篡改实验结果

4.1.2　车身控制模块攻击实验

车身控制模块是汽车 ECU 的控制中枢，负责控制与车身相关的功能（如车大灯、雨刷、窗户、门锁等）。BCM 的出现不仅解决了 ECU 之间布线复杂的难题，减少了汽车制造成本，还降低了车辆的故障率。因此，车身控制模块逐渐成为汽车设计中不可或缺的部分。然而，BCM 在为汽车带来便利的同时，也存在很大的安全隐患。对车身控制模块的结构进行了分析，成功利用车身控制模块的漏洞实现了对汽车门锁开关、灯光和雨刷的控制。

现代汽车大多采用智能 RKE。当驾驶员使用遥控钥匙控制车门时，遥控钥匙发送信号，汽车的 KCU 接收输入信号并对随机校验码进行安全校验。如果随机校验码正确，KCU 将车门锁控制指令通过 CAN 总线发送给 BCM，BCM 就可以控制汽车落锁/开锁。其中，BCM 和 KCU 工作原理如图 5 所示，智能遥控钥匙工作原理如图 5(a)所示。



(a) 智能遥控钥匙工作原理　　(b) 黑客攻击车门锁原理

图 5　BCM 和 KCU 工作原理

遥控钥匙与汽车之间存在的随机校验码校验机制使得无线电攻击方式变得十分困难。然而，通过对 KCU 的工作原理进行详细分析，发现汽车 KCU 和 BCM 之间的通信存在很大的安全隐患。攻击者可以绕过随机校验码校验机制，从 CAN 总线捕获 BCM 和 KCU 之间的车门锁控制指令，并将控制指令通过 CAN 总线直接发送给 BCM，黑客攻击车门锁原理如图 5(b)所示。所以，黑客可以直接通过 CAN 总线将车门锁控制指令发送到 BCM 中，从而绕过智能钥匙和汽车之间的安全校验机制。

利用类似的攻击方法，攻击者能够从 CAN 总线中嗅探汽车车灯、雨刷的控制指令，并将指令重放，来实现对汽车车灯和雨刷的控制。

4.1.3　洪水攻击

CAN 总线采用优先级策略进行数据转发。在 CAN 总线中，当多个 ECU 同时发送消息时，CAN ID 越低，数据在 CAN 总线中传输的优先级就越高。依据这一特性，攻击者可以通过向 CAN 总线发送大量 ID 为 0000 的数据分组，使得 CAN 总线数据过载，导致 CAN 总线拒绝服务。而当其他 ECU 无法接收、发送消息时，汽车将陷入瘫痪状态。

4.2　TSP 安全测试实验

在TSP安全测试实验中，发现了纳智捷汽车TSP云端的验证漏洞，验证了 TSP 云端用户数据存在被泄露的风险。不仅如此，攻击者还可以在未授权的情况下登录 TSP 服务器，通过向 TSP 发送虚假指令实现对车辆的控制，TSP 攻击流程如图 6 所示。

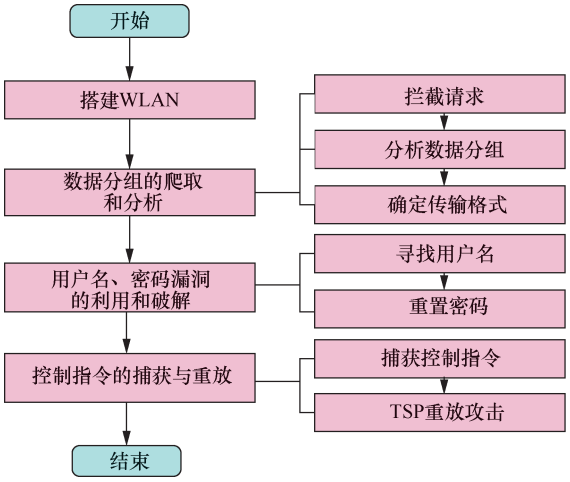


图 6　TSP 攻击流程

4.2.1　TSP 攻击流程

1) 搭建 WLAN 和数据分组的爬取及分析

为了嗅探 TSP 和纳智捷云控 APP 之间的数据分组，需要利用无线路由器搭建一个无线局域网。然后，在局域网中利用 Ettercap 或 Burpsuite 嗅探所有请求/响应数据分组，对数据分组中部分未加密的数据进行分析。最后，编写 Python 脚本以确定 APP 请求登录的格式。

2) 用户名、密码漏洞的利用和破解

在确定了 APP 的正确请求登录格式后，需要解决用户名、密码的破解问题。研究发现，当攻击者输入已注册的用户名时，云端会返回密码错误或登录成功的响应；当用户名不存在时，云端将返回用户名不

存在的响应。根据不同的反馈，可以利用大量手机号码依次请求登录，寻找已注册的纳智捷云控 APP 的手机号码。由于实验攻击过程是违法的，因此，在实验中只使用与实验车辆绑定的手机号进行了测试，验证了攻击方案的可行性。在现实生活中，如果车主在汽车中放置一个标有挪车电话的卡牌，那么攻击者则可以利用挪车电话找到目标攻击车辆的用户名。

在确定了攻击目标车辆的用户名后，需要正确的登录密码和与用户名绑定的车架号才能够成功登录汽车 APP。在实验中利用嗅探工具成功获取了汽车的车架号信息，并利用重置密码漏洞实现了对登录密码的更改。在进行重置密码实验时，TSP 云端收到重置密码请求后，会给绑定手机发送一个 6 位数字校验码，数字校验码在 5 min 内输入有效，输入错误并不影响再次输入。因此，可以利用软件工具重复向 TSP 端发送 6 位数字的校验码，直到校验成功以进入更改密码界面。

3) 指令的获取与重放

当纳智捷云控 APP 向云端发送打开/关闭车门、点火/熄火、鸣笛等指令时，嗅探工具能够准确地捕捉到相应的请求指令。随后，利用 Python 工具编写用户登录脚本和指令控制脚本，使用 MITM 攻击方法，向云端发送登录请求和控制请求，从而实现对纳智捷汽车的攻击。

4.2.2　TSP 攻击实验结果

通过 TSP 安全测试实验可以发现，纳智捷云控 APP 和云端之间存在用户隐私被泄露的风险。TSP 攻击实验结果如图 7 所示，图 7(a)为纳智捷云控 APP 状态，图 7(b)为非法获取的车辆隐私信息，图 7(c)为非法获取的当前车辆位置信息。此外，攻击者还能非法窃取纳智捷云控 APP 的用户名、密码，并实现对车辆车门开启/关闭、点火/熄火和鸣笛等功能的控制。

5　防御对策

1) 诊断端口访问控制

大量 CAN 总线威胁研究实例表明，OBD-II 诊断端口是最容易被攻击者利用并实施攻击的一个端口。因此，对 OBD-II 端口实施访问控制，同时不影响汽车诊断功能的正常使用是一个亟需解决的问题。

2) 网络分割

现在很多车辆中已经采用了网络分割的方式来保护 CAN 总线的安全。网络分割是指将关键 ECU 和非关键 ECU 划分在不同的网段中，并用网关严格限制不同网段之间的数据传输。攻击者则无法通过外部 ECU 直接与关键 ECU 进行通信，攻击难度将成倍增加[23]。

3) 入侵检测系统/入侵防御系统

CAN 总线入侵检测和 TSP 入侵检测是当今汽车安全领域的热门话题。入侵检测系统的实施，如针对 TSP 数据分组进行流量分析或针对目标 ECU

(a) 纳智捷云控 APP 状态　　(b) 非法获取的车辆隐私信息　　(c) 非法获取的当前车辆位置信息

图 7　TSP 攻击实验结果

ID 的传输周期进行分析等，能够直接、有效地监测来自汽车外部的恶意入侵，是如今汽车安全中最有效的防御手段之一[24]。

4) 数据加密

在 CAN 总线和 TSP 的数据传输中，需要对关键数据进行加密。在传输时，加密数据即使被攻击者捕获，也无法轻易破解数据（即逆向困难），有效地保护了汽车数据的安全。

5) 强认证

在 TSP 安全测试中发现，云端针对不同的登录错误返回不同的请求以及修改密码时对安全校验码的输入次数没有设置限制等，都是 TSP 攻击中可被利用的攻击面。为解决此类问题，TSP 可以在用户登录错误时返回相同的错误反馈，同时，对安全校验码的输入次数加以限制以及对关键安全功能的认证使用双向认证、动态认证等。

6 结束语

ICV 正成为未来汽车行业的主流，汽车安全问题也逐渐成为汽车工业中不可忽视的难题。本文详细分析了 ICV 中存在威胁的攻击面和相关的攻击实验，并总结了一些具有代表性的攻击方法。在此基础上，对纳智捷汽车的 CAN 总线和 TSP 的威胁漏洞进行了全面研究，证明了 ICV 中存在很多容易被利用的攻击面。最后，针对 ICV 中存在的威胁，提出了一些可行的防御措施。

参考文献：

[1] XUN Y J, LIU J J, NING J, et al. An experimental study towards the in-vehicle network of intelligent and connected vehicles[C]//2018 IEEE Global Communications Conference. IEEE, 2018.

[2] XUN Y J, SUN Y Y, LIU J J. An experimental study towards driver identification for intelligent and connected vehicles[C]//2019 IEEE International Conference on Communications. IEEE, 2019.

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

[4] ENEV M, TAKAKUWA A, KOSCHER K, et al. Automobile driver fingerprinting[J]. Proceedings on Privacy Enhancing Technologies, 2016(1): 34-50.

[5] NIE S, LIU L, DU Y. How we remotely compromised the gateway, BCM, and autopilot ECUS of tesla cars[C]//2017 Black Hat. 2017.

[6] ZENG K C, LIU S, SHU Y, et al. All your GPS are belong to us: towards stealthy manipulation of road navigation systems[C]//27th USENIX Security Symposium. 2018: 1527-1544.

[7] MILLER C, VALASEK C. Remote exploitation of an unaltered passenger vehicle[C]//Defcon, 2015: 1-91.

[8] BOSCH R. CAN Specification Version 2.0[S]. 1991.

[9] 程军，崔继波，苟凯英. 车辆控制系统 CAN 总线通信的实施方法[J]. 汽车工程, 2003(5): 300-305.
CHENG J, CUI J B, GOU K Y. Implementation method of CAN bus communication in vehicle control system[J]. Automobile Engineering, 2003, (5): 300-305.

[10] LI Y S, LUO Q, LIU J J, et al. TSP security in intelligent and connected vehicles: challenges and solutions[J]. IEEE Wireless Communications, 2019, 26(3).

[11] CHECKOWAT S, MCCOY D, KANTOR B, et al. Comprehensive experimental analyses of automotive attack surfaces[C]//USENIX Security Symposium. 2011, 4: 447-462.

[12] NIE S, LIU L, DU Y. Free-fall: hacking Tesla from wireless to can bus[C]//2017 Black Hat. 2017: 1-16.

[13] CHENG Q A, YIN Y, FENG Y, et al. Exposing congestion attack on emerging connected vehicle based traffic signal control[C]//2018 Network and Distributed Systems Security (NDSS) Symposium. 2018.

[14] LUO Q, CAO Y, LIU J, et al. Localization and navigation in autonomous driving: threats and countermeasures[J]. IEEE Wireless Communications, 2019, 26(4): 38-45.

[15] BENADJILA R, RENARD M, LOPES-ESTEVES J, et al. One car, two frames: attacks on Hitag-2 remote keyless entry systems revisited[C]//11th USENIX Workshop on Offensive Technologies (WOOT 17). 2017.

[16] GARCIA F D, OSWALD D, KASPER T, et al. Lock it and still lose it-on the (in)security of automotive remote keyless entry systems[C]//25th USENIX Security Symposium (USENIX Security 16). 2016.

[17] ISHTIAQ ROUFA R M, MUSTAFAA H, TRAVIS TAVLORA S O, et al. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study[C]//19th USENIX Security Symposium. 2010: 11-13.

[18] SOMANI G, GAUR M S, SANGHI D, et al. DDoS attacks in cloud computing: issues, taxonomy, and future directions[J]. Computer Communications, 2017, 107: 30-48.

[19] RISTENPART T, TROMER E, SHACHAM H, et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds[C]//Proceedings of the 16th ACM conference on Computer and Communications Security. ACM, 2009: 199-212.

[20] GEORGIEV M, IYENGAR S, JANA S, et al. The most dangerous code in the world: validating SSL certificates in non-browser software[C]//Proceedings of the 2012 ACM conference on Computer and Communications Security. ACM, 2012: 38-49.

[21] LIANG X, SHETTY S, ZHANG L, et al. Man in the cloud (MITC) defender: SGX-based user credential protection for synchronization applications in cloud computing platform[C]//2017 IEEE 10th International Conference on Cloud Computing(CLOUD). IEEE, 2017: 302-309.

[22] GARIP M T, GURSOY M E, REIHER P, et al. Congestion attacks to autonomous cars using vehicular botnets[C]//NDSS Workshop on Security of Emerging Networking Technologies (SENT). 2015.

[23] 张德干, 赵彭真, 高瑾馨, 等. 面向车联网的智能数据传输新方法[J]. 物联网学报, 2019, 3(2): 89-99.
ZHANG D G, ZHAO P Z, GAO J X, et al. A new intelligent data transmission method for intelligent and connected vehicles[J]. Chinese

Journal on Internet of Things, 2019, 3(2): 89-99.

[24] 余辰, 张丽娟, 金海. 大数据驱动的智能交通系统研究进展与趋势[J]. 物联网学报, 2018, 2(1): 56-63.
YU C, ZHANG L J, JIN H. Research progress and trend of intelligent transportation system driven by big data[J]. Chinese Journal on Internet of Things, 2018, 2(1): 56-63.

[作者简介]

荀毅杰（1994− ），男，山西晋中人，西安电子科技大学博士生，主要研究方向为智能网联汽车安全和机器学习。

刘家佳（1984− ），男，湖北荆州人，西北工业大学网络安全学院教授、副院长，主要研究方向为无线移动通信、Wi-Fi 和物联网等。

赵静（1996− ），女，贵州遵义人，西安电子科技大学硕士生，主要研究方向为智能网联汽车安全。