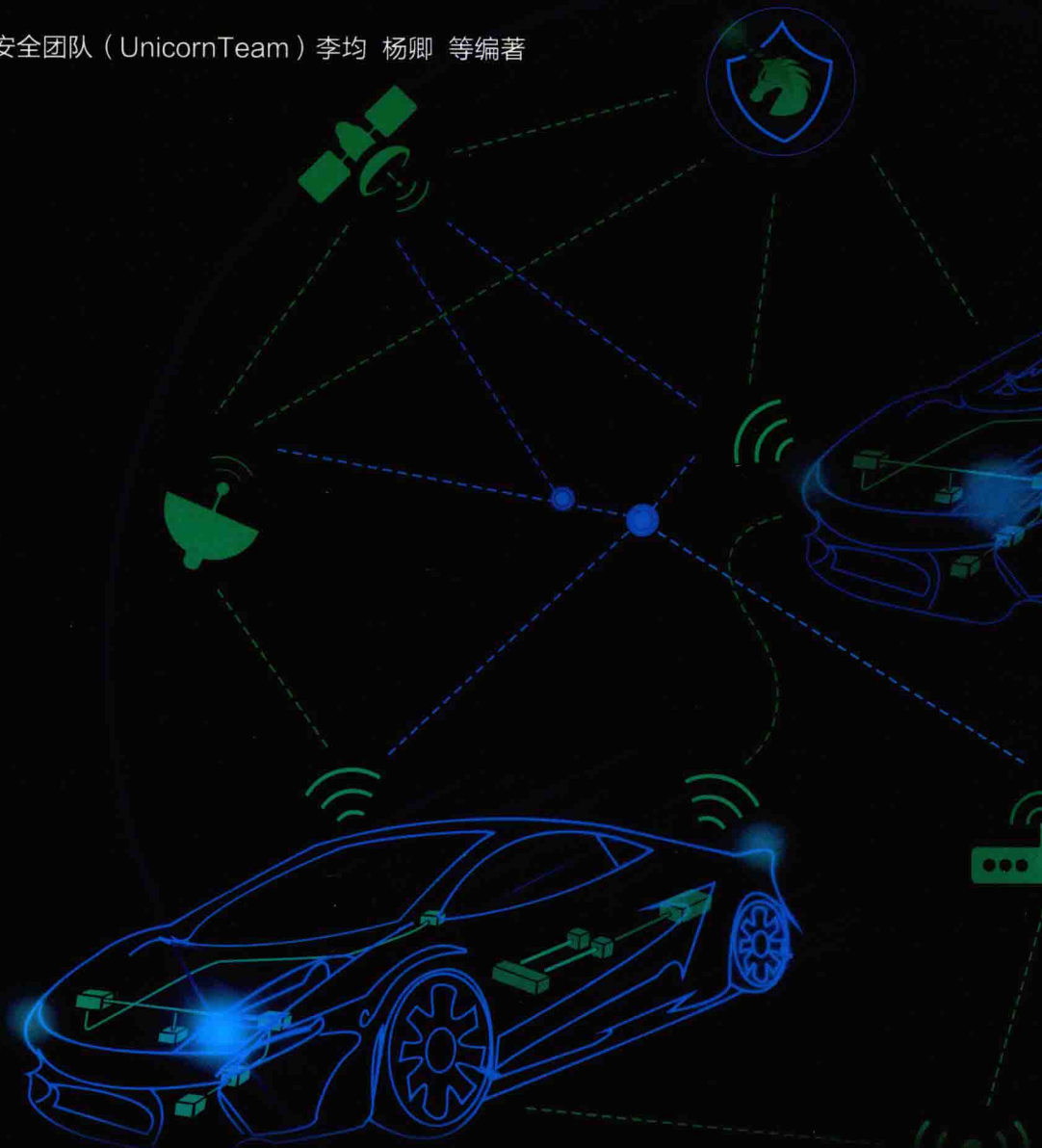
Broadview
www.broadview.com.cn

智能汽车安全攻防大揭秘

360独角兽安全团队（UnicornTeam）李均 杨卿 等编著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

智能汽车安全攻防大揭秘

360独角兽安全团队（UnicornTeam）
李均 杨卿 曾颖涛 郑玉伟 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书首先针对汽车研发人员介绍了一些安全基础知识，如加密解密、安全认证、数字签名、常见攻击类型和手段等，然后针对安全研究人员介绍了一些智能汽车的工作原理，如汽车的内网协议、网络架构、X-By-Wire 线控系统原理、常见潜在攻击面等，最后对一些实际的汽车攻击或安全测试案例进行详细分析，并在分析过程中对案例里涉及的漏洞进行防御分析。本书的特点是由浅入深，为读者提供详细的实际案例分析和防御建议。

本书的目标读者为智能汽车或者网联汽车研发人员，希望进行智能汽车安全研究或渗透测试的安全研究人员等。

图书在版编目（CIP）数据

智能汽车安全攻防大揭秘 / 360 独角兽安全团队（UnicornTeam），李均等编著. —北京：电子工业出版社，2017.10

ISBN 978-7-121-32497-0

Ⅰ. ①智… Ⅱ. ①3… ②李… Ⅲ. ①智能控制—汽车—计算机网络—网络安全 Ⅳ. ①U469-39②TP393.08

中国版本图书馆 CIP 数据核字(2017)第 197071 号

策划编辑：郑柳洁
责任编辑：郑柳洁
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×980　1/16　印张：14.25　字数：280 千字
版　　次：2017 年 10 月第 1 版
印　　次：2017 年 10 月第 1 次印刷
定　　价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

前　言

当 Tim Berners-Lee 在 1989 年发明互联网时，他可能没想到网络威胁会像现在所面临的这样严峻，而网络连接会像物联网时代这样深入而广泛。同样，当智能汽车被发明时，它的发明者可能也没想到智能汽车会像今天一样遭受黑客攻击等网络安全威胁。近年来，互联网汽车、自动驾驶汽车、智能交通等发展非常迅速，就连互联网公司也纷纷加入汽车研发与制造业，传统汽车制造商积极地将自家产品加入互联网连接功能和辅助驾驶功能，以期通过联网后实现的新功能吸引消费者。在各家车厂如火如荼地研发智能汽车的同时，我们也看到各种各样通过网络对智能汽车发起攻击的漏洞案例，这些案例中有的通过网络解锁并启动汽车威胁到财产安全，有的甚至可以通过网络远程控制汽车的物理功能，直接威胁到驾乘人员的生命安全。所以在智能汽车或网联汽车如火如荼发展的同时，我们需要对汽车潜在的网络安全问题足够重视，做到防患于未然。

传统车厂往往对网络安全缺乏足够的认识，而安全研究人员对汽车的控制原理了解也不够充分，作者在汽车行业和安全行业都有从业经验，所以希望通过本书连接汽车研发人员和安全研究人员，为汽车安全贡献一份绵薄之力。

关于本书

从答应写这本书开始，有四个多月作者都没有下笔，不是因为太忙没时间，而是因为一直在想如何下笔，作者一直在收集相关资料和研究案例。作者希望写一本经典的参考书，能够让安全人员通过本书了解汽车的构造原理及漏洞原理，如线控系统、汽车总线、ECU 闭环控制原理等，能够让汽车行业从业者了解到他们设计生产的汽车及汽车配套的网络服务在推上市场后将面临怎样的安全考验，帮助他们建立安全概念及安全思维方式，了解常规的防护手段，比如加密解密、安全认证、数

字签名等概念。本书书名《智能汽车安全攻防大揭秘》，从名字上看好像是专门讲解如何攻击汽车的，但实际上如何防御攻击也是本书的重点，本来攻击与防御就是紧密联系的。此外，由于汽车是一个非常复杂的系统，涉及的技术非常多，不可能用一本书囊括所有内容，所以有的概念或者技术没有提到也请读者原谅。本书主要分析汽车上可能或者已经遭到攻击的电子系统，让安全研究人员了解汽车攻击原理和可能的攻击面，让汽车行业的从业人员建立起基本的安全概念。

本书分为基础篇和案例分析篇。基础篇中会介绍一些与汽车安全相关的概念，例如针对汽车行业的从业人员介绍加密算法、认证协议、攻击类型等基础知识；针对安全从业人员介绍汽车构造、汽车电子系统原理、汽车各类总线协议、汽车安全研究发展、汽车可能暴露的各种攻击面等。理解了这些基础知识有助于理解后续篇章的内容。

案例分析篇中会分析一些经典汽车网络攻击案例。这些案例涉及安全的方方面面，比如硬件安全、通信安全、云端安全等。在分析案例的同时会讲到对应的防御措施，了解攻击者在这些案例中采用的攻击手段和对应的防御措施，有助于读者将所学知识应用于安全测试或安全开发中。

致谢

感谢朋友和家人一直以来对作者的全力支持。

感谢 360 独角兽安全团队、无线电安全研究部及 360 集团的同事们。

感谢 Charlie Miller、Chris Valasek、Marc Rogers 等汽车安全研究人员对本书内容的贡献。

感谢领导及朋友杨卿先生的指导和栽培。

感谢谭晓生先生引荐我到 360 公司并在工作中给予我们的支持。

作者：李均

目　录

汽车安全基础篇

案例分析篇

汽车安全基础篇

在基础篇我们会介绍一些与汽车安全相关的概念，例如加密算法、认证协议、汽车构造、汽车电子系统原理、汽车安全发展等。理解这些基础知识有助于读者理解后面案例分析篇的内容。

第 1 章　智能汽车相关基础概念介绍

“智能”这个概念的具体定义非常具有争议性。现在市面上涌现了很多智能硬件、智能家居、智能机器人等，但具体什么是智能则各家说法不一。很多人将智能等同于可以用手机或其他终端通过网络远程控制，或者能够根据传感器感知环境数据并通过人工智能系统处理这些数据进而执行相应动作。根据这样的套路，智能汽车可被定义为在普通车辆的基础上增加了先进的传感器（雷达、摄像头等）、控制器、执行器等装置，通过车载传感系统和信息终端实现与人、车、路等的信息交换，使车辆具备环境感知能力，能够自动分析车辆行驶的安全及危险状态，并使车辆按照人的意愿到达目的地，最终实现替代人工操作的目的。

然而在国外，事实上没有准确的所谓“智能汽车”的概念。与国内笼统的智能汽车概念相比，作者认为国外的一些相关定义更准确、更精细。下面我们来看看与“智能汽车”相关的一些重要概念。

1.1　网联汽车

联网的车（Connected Car）：又称网联汽车，即这些车具有网络连接功能，通常还具有 Wi-Fi 热点功能用于和其他设备分享车载网络连接。具有网络连接功能的汽车通常还会扩展出其他功能来充分利用网络连接带来的优势，例如车祸自动报警求救、远程控制、远程升级［Over the Air（OTA）Update］、安全预警等。

1.2　V2X

V2X（Vehicle to X）通信：表示车与 X 通信，X 可以是车（Vehicle）、路（Road）或者其他相关基础设施，相应地也就有了 V2V（Vehicle to Vehicle，车与车通信）、V2I（Vehicle to Infrastructure，车与基础设施如道路、服务器等通信）、V2P（Vehicle

to Pedestrian，汽车与行人通信）等概念。V2X 的典型应用有左转辅助、紧急刹车提示、闯红灯警告、过弯速度警告、施工路段提醒、实时天气信息提醒等。

1.3　高级辅助驾驶系统

高级辅助驾驶系统（ADAS，Advanced Driver Assistance System）：ADAS 是在驾驶过程中辅助驾驶员的系统，它的功能包括安全告警功能、自适应控制功能、信息提示功能等，可在通过传感器检测到可能的危险时对驾驶员发出告警或者接管汽车某些控制功能（比如紧急刹车功能），以及根据环境自动对汽车的某些功能进行控制，比如根据环境亮度自动调节车灯亮度、自适应巡航控制、盲点警告、自动变道等。ADAS 技术通常依赖于各种传感器和通信技术，例如依赖雷达或者摄像头检测与前车的距离，依赖 V2V 获取附近车辆信息，依赖摄像头检测车道等。表 1-1 所示为一些 ADAS 的例子。

表 1-1　ADAS 举例

Adaptive Cruise Control	Adaptive High Beam	Glare-free High Beam	Automatic Parking	GNSS	Blind Spot Monitor	Collision Avoidance System	Forward Collision Warning	Intersection Assistant
自适应巡航	自适应远光灯	防炫目远光灯	自动泊车	全球卫星定位导航系统	盲点检测	防碰撞系统	碰撞预警	交叉路口辅助系统
Traffic Sign Recognition	Wrong-way Driver Warning	Intelligent Speed Adaptation	Lane Change Assistance	Pedestrian Protection System	Lane Departure Warning System	Hill Descent Control	Vehicular Communication Systems	Driver Drowsiness Detection
交通信号识别	错误驾驶习惯告警	自适应速度控制	变道辅助系统	行人保护系统	车道偏离预警系统	下坡辅助控制	车载通信系统	驾驶员疲劳检测

1.4　自动驾驶汽车

自动驾驶汽车（Automated Driving Car）：自动驾驶汽车依靠人工智能、视觉计算、雷达、监控装置和全球定位系统的协作，让计算机在没有任何人主动操作的场景下，通过汽车线控（X-By-Wire）系统自动安全地操作机动车辆。

自主驾驶汽车（Autonomous Car）：作者刻意避免使用自动驾驶汽车这个概念，是想将现在的汽车所具备的智能驾驶功能与自动这个概念做些区别，自动可以定义

为根据预先设定的程序对环境做出预先设定的反应，而自主驾驶汽车能体现出汽车可以在一定的权限内自主做出一些决定，因为汽车采用了很多人工智能里的学习算法，这些算法模型会在汽车整个生命周期中不断自我学习升级，会越来越“聪明”。

经过前面的介绍，可以将智能汽车广义地定义为具有全部或者部分上面提到的这些功能的汽车。智能汽车又因为智能程度的不同分为表 1-2 所示的不同级别，这个级别分类来自于 SAE［参考 adaptive-ip.eu 和美国汽车工程师协会（Society of Automotive Engineers，简称 SAE）标准 J3016］。

表 1-2　自动驾驶的分类

SAE 级别	SAE 名字	SAE 定义	转向和加速及减速	驾驶环境监控	失效备用	系统能力	BASt 级别	NHTSA 级别
人类驾驶员负责监测驾驶环境			人	人	人	N/A	只是人	0
0	无自动化	全程由人控制						
1	驾驶员辅助	转向或加减速由一个辅助驾驶系统根据环境信息完成，并需要驾驶员控制其他方面	人和系统	人	人	一些驾驶模式	辅助驾驶	1
2	部分自动化	转向和加减速都由辅助驾驶系统根据环境信息完成，并需要驾驶员控制其他方面	系统	人	人	一些驾驶模式	部分自动化	2
自动驾驶系统负责监测驾驶环境			系统	系统	人	一些驾驶模式	高度自动化	3
3	一定条件下自动化	自动驾驶系统控制驾驶的所有方面，但是期待驾驶员在系统发出干预请求时能够正确响应						
4	高自动化	自动驾驶系统控制驾驶的所有方面，即使驾驶员在系统发出干预请求时不能够正确响应	系统	系统	系统	一些驾驶模式	全自动化	3/4
5	完全自动化	任何时候任何条件下汽车的任何方面都由系统控制	系统	系统	系统	所有驾驶模式	——	

环境感知：前面提到的自主驾驶汽车或者 ADAS 的实现依赖于各种传感器对环境进行监测，图 1-1 所示为汽车配备的用于感知环境的传感器，这些传感器包括摄像

头、雷达等，其检测距离、精度及用途各有不同。

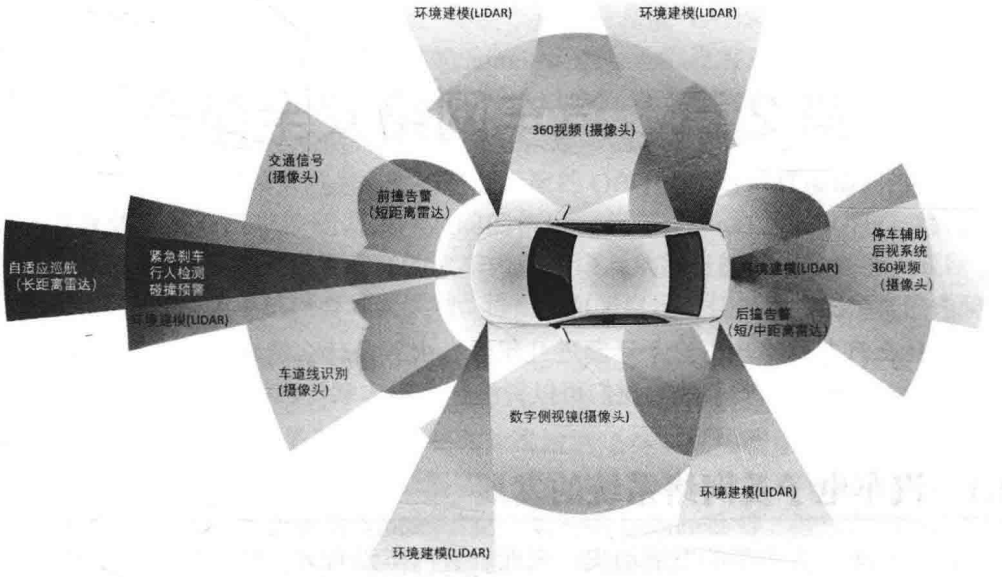


图 1-1　智能汽车传感器示意图

除了前面讲到的各种传感器之外，智能汽车还依赖高精度地图或超高精度地图。与普通的导航地图不同，高精度地图的精度要求非常高，通常要精确到车道级别，甚至厘米级别。

汽车在智能化、联网化、自动化等趋势下必须要考虑到被黑客攻击的可能性，汽车采用或者将要采用的技术如传感器、无线网络连接、云服务器等都可能遭到黑客攻击。本书会先分析一些针对汽车的攻击案例，然后讨论对应的防御方法。

第 2 章　汽车网络安全简介

为什么汽车网络攻击这个话题近几年这么火？是什么造成汽车受到网络攻击的威胁？面对汽车网络安全威胁我们可以做些什么？本章将回答这些问题。

2.1　汽车电子及网络系统的发展

纵观汽车一百多年的发展历史，表面上看汽车没有太大的变化，一个内燃机、一个变速器、四个轮子，加上通用的操作接口（一个方向盘、一个刹车踏板、一个油门踏板、一个离合器、一个变速杆等）。但其实在过去这几十年，汽车内部的控制系统发生了巨大变化。今天的汽车已经不再是简单的机械系统，今天的汽车配备了各种各样的电子控制模块（ECU，Electronic Control Unit）及传感器。这些电子控制模块相互协同，通过各种传感器和执行器对车辆的各部件、道路状况、驾驶员和乘客等进行持续的感知和控制。传统汽车上由机械控制的部件越来越依赖于电子系统来辅助控制（即线控，X-By-Wire），前者甚至会被后者取代。图 2-1 所示为汽车电子系统中采用的微处理器数量变化趋势，从中可以看出汽车越来越电子化。

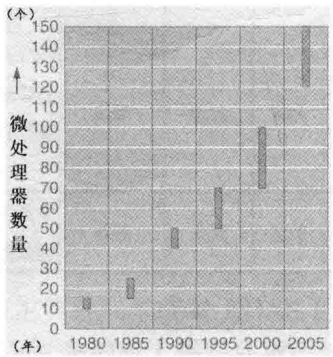


图 2-1　汽车中采用的微处理器数量变化

传统的汽车生产厂家其实一直非常重视汽车安全的研究，在汽车的安全方面投入了大量的人力物力进行研发。他们关注的往往是汽车本身的性能安全及操作安全，所以开发了很多功能来保证驾驶安全，如刹车防抱死系统（ABS）、安全气囊、预紧安全带等，这些都是安全功能（Safety Features），但是他们没有对汽车在越来越电子化、网络化的趋势下是否会遭受到同样可以威胁到汽车安全的网络攻击（Cyber Attack）引起足够重视。随着现代汽车集成越来越多的复杂的网络服务和通信功能，汽车所暴露的攻击面也越来越大，例如通过标配的 OBD 接口可以直接访问汽车内部网络，多媒体系统与汽车控制器内网之间的接口、蓝牙、Wi-Fi、SubGHz、蜂窝网（GPRS、3G、4G）等都提供了潜在的汽车内网入口。从网络的另一端来看，联网后的汽车和我们的 PC 或手机没有太大区别，将要面对来自世界任何地方的黑客的考验。

早期，像通用安吉星（OnStar）一类的车载信息系统（Telematics）通过无线网络为用户提供如碰撞自动求助、远程诊断等增值服务，要提供这些服务就需要将车载信息系统与汽车内部的子系统进行集成并通过网络与中央控制中心相连。现在各大汽车厂商都已经发布了自家的类似服务，甚至功能更多、控制更全面的服务，如宝马的 ConnectedDrive、奔驰的 Mbrace、克莱斯勒的 Uconnect 等。将来汽车与汽车、汽车与基础设施等的通信系统会得到大规模的部署及应用，这将为黑客通过无线入侵汽车提供入口，如图 2-2 所示。

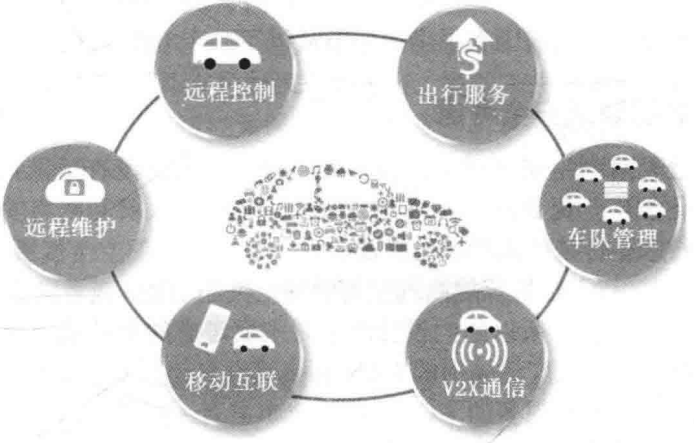


图 2-2　汽车将变得越来越网络化

另一方面，汽车也会快速向自主驾驶汽车方向发展。众所周知，要实现对汽车的自动控制要求汽车的很多物理功能（如加减速、刹车、转向等）能够被电子控制，在这样的发展趋势下，这些物理功能在汽车被黑客入侵后可能会被控制。

还有一个潜在趋势是汽车可能越来越开放，有趋势表明汽车将会成为和手机一

样的开放平台，应用开发者可以为汽车开发应用，用户可以随时为自己的汽车下载应用。这些应用可能会用到汽车内部的参数或者需要使用汽车的执行器，就像我们的手机应用程序要使用送话器、网络连接等外设模块一样，就会出现和现在的手机或者 PC 安全类似的问题，如木马、重打包的恶意软件等，而汽车面临的安全问题可能会威胁到驾乘人员的生命安全。

在功能不断增多，网络连接越来越普遍的发展趋势下，我们要看到汽车在这个发展过程中会暴露出越来越多的攻击点，并提出相应的预防措施，因为汽车不只像我们的个人电脑，汽车遭受网络攻击后可能会威胁到驾驶员的生命安全，例如 2015 年美国安全研究人员 Charlie Miller 和 Chris Valasek 通过无线入侵 Jeep 切诺基的车载信息系统后可以远程控制汽车加速、转向、刹车等，而整个过程不需要物理接触汽车或者提前对汽车进行改装。提到智能汽车不能不提特斯拉，特斯拉公司生产的多款电动车中 Model S 是最出名的一款，依靠各种传感器技术，Model S 可以感知汽车周围环境并实现有条件的自动驾驶功能，而特斯拉自动驾驶功能主要依赖的光学雷达（Lidar-Light Detection And Ranging）和摄像头也存在被欺骗或者干扰的风险。这些会在后续章节中讲到。

2.2 汽车安全的成因

汽车网络安全威胁的成因有很多，本节从以下几个方面分析。

2.2.1 设计之初缺乏安全考虑

汽车设计之初对网络安全威胁没有足够重视，原因是没有预见到汽车会像现在这样深度网络化发展。提到汽车安全，传统的汽车研发人员和网络安全研究人员可能会有不同的看法，传统的汽车研发人员也许会想到汽车的安全气囊、预紧安全带、ABS、碰撞安全性、行人保护等提高汽车驾驶安全性的功能，或者防盗器、GPS、SOS 等防盗或远程求救功能，所以他们设计汽车时主要考虑的是功能安全性，很少考虑到攻击情况，例如汽车上广泛采用的 CAN 总线就没有什么安全机制。网络安全研究人员会想到现代汽车上有很多的 ECU，而且汽车具有无线通信模块，因此他们会把汽车看作车轮上的计算机、车轮上的数据中心。

2.2.2 越来越广泛和深入的网络化

汽车接入网络是必然趋势，所以研究汽车安全势在必行。在国家推动万物互联的大背景下，各种家电设备都接入了互联网，汽车作为人们每天使用率高、使用时间长的基本交通工具理所当然地要接入互联网。汽车接入互联网后有很多好处，汽