汽车智能化的安全思考

闫 琛 徐文渊
浙江大学

关键词：智能汽车 安全 攻击 防护

引言

汽车智能化发展迅速，许多领域的成熟技术已被融合到汽车里。最典型的莫过于汽车移动通信的无线技术：蓝牙实现了免提通话，GPS 实现了汽车的定位与导航，蜂窝网络中的 3G 技术使汽车成为手机一样的移动数据终端，Wi-Fi 为车载娱乐系统提供了便捷渠道……

殊不知，汽车的智能化发展，在提升人们驾乘体验的同时，也引入了很多安全隐患。其中最大的威胁来自汽车电子控制单元 (Electronic Control Unit, ECU) 与通信总线组成的分布式网络结构。它是汽车中使用最广泛的总线，攻击者通过控制一个电子控制单元就可能影响到总线上的其他所有电子控制单元，包括引擎、制动、方向盘等。

汽车电子系统结构及其安全隐患

为了提高汽车系统的安全性，我们必须对汽车的电子系统结构有基本的了解，包括功能、基本控制单元和通信方式。

汽车智能化

汽车智能化的发展已经是不可阻挡的趋势。自动泊车、无人驾驶、车道保持、碰撞检测、车载移动互联系统等已成为新的热点。其发展方向可以总结为“三高一低”：安全性的提高、舒适性的提高、移动通信能力的提高和驾驶难度的降低。依赖于汽车移动通信能力的车联网 (V2V, V2I/I2V)[1] 已经应用于一些车型，一旦普及，将会极大地提高交通安全和效率，并推动自动驾驶汽车的应用。

汽车的智能化意味着新功能和信息接口的引入，而它们的实现依赖于汽车的电子控制单元。

汽车电子控制单元

现代一辆高级汽车通常含有超过 75 个的电子控制单元[2]，上千万行的代码，覆盖汽车几乎所有的功能：引擎、变速器、制动、车内温控、娱乐系统、灯光和安全气囊等等，如图 1。

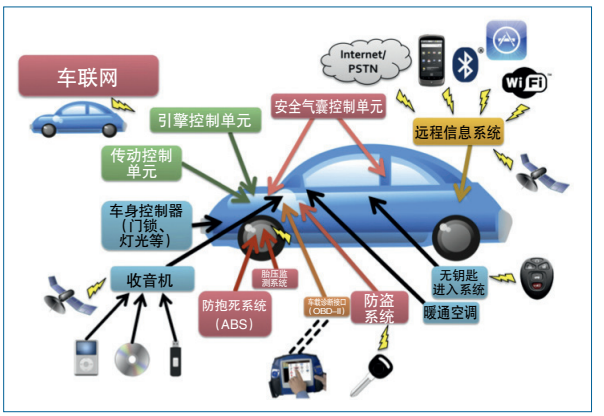

图1 汽车的主要电子控制单元模块[6]

[1] V2V，Vehicle to Vehicle，车对车；V2I，Vehicle to Infrastructure，车辆与基础设施间（通信）。

[2] “This Car Runs on Code.” http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code。

这种嵌入式控制系统的设计极大地方便了汽车的生产和维修。

车内通信总线

电子控制单元之间通过通信实现合作功能和信息共享。以自动泊车系统为例，需要多个电子控制单元分别实现如下功能：处理超声波传感器的信号并判断汽车周围环境；控制方向盘助力器实现指定的转向角度和速度；控制引擎输出动力和制动；计算汽车姿态和轨迹并向其他控制单元发送执行指令。各个控制单元之间的数据和指令传递需要采用可靠和高效的通道，因而引入了汽车的通信总线。总线结构可以减少线束，并且可统一通信协议。

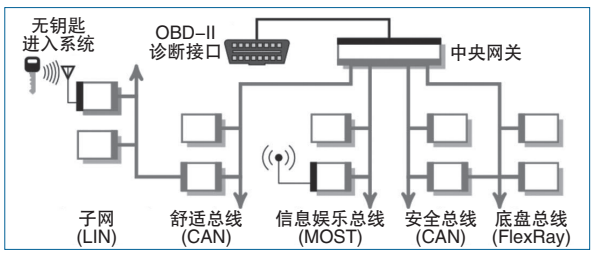

图2　汽车总线结构[10]

图 2 中的方块代表汽车的电子控制单元模块，根据重要性和功能被分成多组，每组都由一条总线连接，不同的总线之间通过中央网关进行通信。不同的通信特性和速率需求可能会导致汽车中存在着不同的总线，包括控制器局域网络总线、LIN 线（Local Interconnect Network，本地互联网络）、MOST（Media Oriented System Transport，面向媒体的系统传输总线）、FlexRay 和以太网等。最常见的是控制器局域网络总线。

控制器局域网络产生于 20 世纪 80 年代，在 90 年代中期被引入汽车，是一种事件驱动的多主机串行现场总线，协议标准为 ISO 11898。控制器局域网络总线可靠性高、性价比高、便于故障诊断，是被各大汽车厂商采用的标准总线结构。它具有完善的通信协议，采用广播通信方式，常见传输速率是高速 (500Kb/s) 和低速 (100Kb/s)。

但是对于一些传输速率要求更高的应用，如信息娱乐系统，控制器局域网络总线的传输速率则相对有限，因此需要采用速率更高的总线，如面向媒体的系统传输总线、FlexRay、以太网等。著名的特斯拉汽车就使用了罕见的以太网，其独特的总线结构（图 3）已引起许多安全研究者的注意。

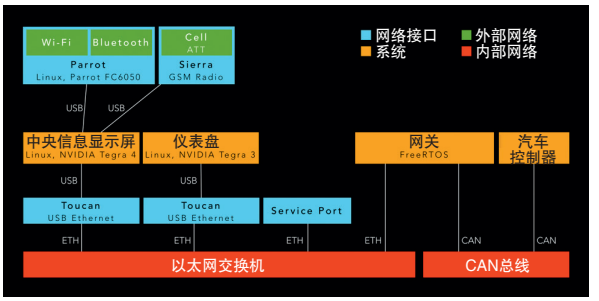

图3　特斯拉Model S的总线结构(https://blog.lookout.com/blog/2015/08/07/hacking-a-tesla/)

控制器局域网络总线因其细致完善的通信协议和高可靠性被工业界公认为最有前途的现场总线之一，但其安全性一直以来都为人诟病。有学者在理论层面分析过包括控制器局域网络在内的汽车中的多种总线[3]和电子控制单元可能存在的安全问题[4]，他们认为现代汽车有许多特征让未授权的访问变得简单，例如汽车控制器间的所有通讯都是未加密的明文，控制器也无法验证传入信息的来源是否真实。

汽车最大的安全威胁还是来自总线的互联，基本上每个 LIN、控制器局域网络、MOST 线上的控制器都能够向其他控制器发送消息。因此，如果任何一条总线遭入侵，整辆车的通信网络都会受到威胁。例如多媒体系统与汽车控制网络的连接可能会使恶意软件（蠕虫、病毒、木马等）通过 CD/DVD、电子邮件等渠道侵入汽车并造成严重后果。

汽车安全分析

随着现代社会对汽车依赖性的提高，人们开始意识到汽车被恶意攻击和控制带来的巨大危险。尽管有相当多的计算机领域的经验可以借鉴，但汽车对于大多数安全研究者来说仍是一个棘手的对象。汽车电子控制单元是分布式的嵌入式系统，具有十分有限的输入 / 输出接口和不易读取的固件系统。

市面上基本没有现成的工具或软件，汽车厂商对技术细节也守口如瓶，大部分信息只能通过逆向工程获得，这些都增加了研究的难度。

攻击接口

除了与外界的物质交换，汽车还有许多信息接口。这些信息接口大部分采用无线通信方式，从用途上讲可以分为两类：第一类属于与驾驶相关的功能类系统，用于汽车诊断和辅助性驾驶等，这对汽车安全起到至关重要的作用；第二类属于与用户相关的体验类系统，主要是信息娱乐系统。

从安全分析的角度来看，这些信息接口都存在被攻击的风险，一旦被攻击者利用，将会直接引起其所在电子控制单元模块的工作异常，可能造成财产损失、信息泄露或危险驾驶。因此，我们按照攻击者所在的位置，将汽车常见的信息接口分为内部和外部两类（见表1）。表1中系统类别一栏指信息接口所在系统功能类别。

其中研究最广泛的是OBD-II和信息娱乐系统。

OBD-II是汽车控制器局域网络总线诊断接口，通常位于方向盘下方，是汽车的标准配置。汽车工程师通过将诊断设备与该接口连接，进行汽车调试或获取故障信息。但是绝大多数汽车并没有对该接口进行保护，这使得攻击者可以通过车载诊断接口监听汽车的控制器局域网络总线通信，从而通过逆向调试获得数据包，进而伪造数据包，并利用总线的广播模式影响其他电子控制单元。例如攻击者可以在踩刹车的同时通过车载诊断接口进行监听，从中筛选出控制制动的数据包。如果攻击者在之后重放数据包，就可以控制汽车的制动。

信息娱乐系统集成了蜂窝、广播、GPS、Wi-Fi、蓝牙、USB和CD等大量信息接口，为汽车提供了丰富的数据来源，但也给攻击者带来了丰富的攻击源。该系统常被设计为用户的中控界面，因此许多汽车将该系统作为高速和低速控制器局域网络总线的网关，这意味着控制它便可以同时获得对多条总线的控制权。

尽管这些信息接口都存在被攻击的可能性，但

表1 汽车信息接口

位置	系统类别	信息接口	接口描述
内部	汽车诊断	OBD[3]-II	用于汽车诊断与配置的控制器局域网络总线接口
	信息娱乐系统	USB[4]	连接USB移动存储设备
		CD	对CD中的特定文件格式进行解码
	发动机防盗锁止	RFID[5]	通过射频识别检测钥匙真伪
外部	传感器[6]	遥控钥匙	通过射频信号控制汽车车门开启或启动
		胎压监测	通过射频信号传递胎压信息
		超声波	利用超声波的反射探测汽车周围近距离物体
		毫米波雷达	利用微波的反射进行路况检测
		激光探测与测量	利用红外光的反射进行路况检测
		摄像头	通过图像处理进行路况检测
	信息娱乐系统	蜂窝网络	提供移动数据流量
		广播	包括模拟广播和数字广播
		GPS	全球定位系统，用于导航和定位
		Wi-Fi	接入Wi-Fi网络或自建热点
		蓝牙	用于与车内手持设备的无线连接
	车联网	DSRC[7]	通过射频信号传递安全及交通信息
	云端服务	手机应用	实现远程汽车监测或控制

[3] On Board Diagnostics，车载诊断。

[4] Universal Serial Bus，通用串行总线。

[5] Radio Frequency Identification，射频识别。

[6] 测量对象为汽车内部参数的传感器不做讨论。

[7] Dedicated Short Range Communications，专用短程通信技术。

不同汽车所具有的信息接口和采取的实现方法又不尽相同，因此对不同汽车的安全性不能一概而论。一般而言，对于初期调研和选取实验对象来说，拥有信息接口越多的汽车越具有被攻击的可能性。有研究者对 20 多款车型的电子系统结构和功能进行了调研[9]，以寻找可能的远程攻击接口并评估攻击的难度。他们认为最容易被攻击的汽车是 2014 款吉普切诺基、2015 款凯迪拉克凯雷德和 2015 款英菲尼迪 Q50，它们的共性是都具备高级的功能、丰富的攻击接口和简单的总线结构。

威胁模型分析

为了更直观地对威胁进行分析，可以依据通信距离对攻击接口进行简单分类，见图 4。图中有 4 类区域，分别是远距外部接口、近距外部接口、内部物理接口、内部网络，它们之间的分界线代表信任边界，越顶端的是越不受信的区域，越底端的是越受信的区域。若一个通信信道跨越的信任区间越多，则该信道的风险就越大。这是因为攻击接口距离对象汽车越远，该攻击的隐蔽性就越好，而且攻击者的自由度越大。攻击者位于汽车内部的攻击行为虽然并不具有太大的现实意义和可行性，但有助于攻击者理解汽车内部网络。

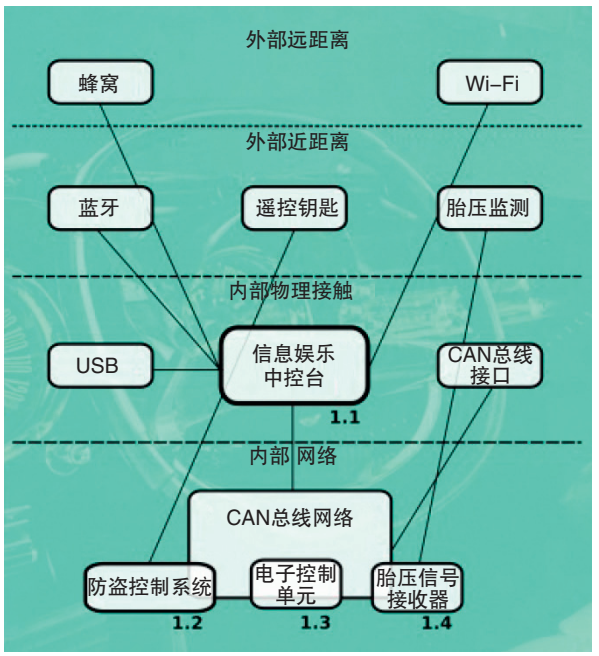

图4 汽车攻击接口分类（图片来源*Car Hacker's Handbook*. http://opengarages.org/handbook/）

从图 4 中也可以看出，有一部分电子控制单元（图中 1.3）是核心且相对封闭，例如引擎控制单元，除了控制器局域网络总线之外几乎没有其他的外部信息接口；还有一部分次要的，但是开放的，例如信息娱乐系统（图中 1.1）。虽然引擎控制单元很难从汽车外部直接攻击，但如果利用信息娱乐系统提供的大量外部甚至远程接口入侵汽车，再利用控制器局域网络总线无认证的广播机制发送虚假的引擎控制数据包，就可以实现对引擎控制单元的间接攻击，造成严重的后果。

目前最典型的汽车威胁是，发现一个可被利用的攻击接口，通过重刷固件等方式获得对某电子控制单元的控制权，再通过控制器局域网络总线广播伪包，最后影响其他电子控制单元。威胁的关键因素有：可被利用的攻击接口、有缺陷的电子控制单元固件、不合理的总线信息隔离以及缺乏安全机制的控制器局域网络通信协议。

由于每款汽车的电子结构并不完全相同，因此不一定同时具备以上所有被威胁因素。更为常见的是只利用部分因素，例如通过传感器提供的信息接口破坏该传感系统的功能，或者利用信息接口进行被动式窃听，但这些攻击都不会涉及总线。

攻击方法

“汽车攻击 (car hacking)”的说法早在十几年前就已经存在，当时指的是对汽车引擎的个人调校行为[8]，调校师通过修改汽车引擎控制电子控制单元的固件参数，以发掘引擎的最大动力潜能。有人通过对电子控制单元的修改使混合动力汽车更多地依靠电力行驶[9]。

[8] “How to Hack Your Car.” http://www.forbes.com/forbes/2002/0708/148.html。

[9] “Hacking the Hybrid Vehicle.” http://archive.wired.com/science/discoveries/news/2005/11/69519。

虽然这些不是严格意义上的攻击行为，但所使用的修改电子控制单元固件的方法却是相同的。

内部攻击接口

1.OBD–II

OBD-II 是汽车安全研究的首选接口，虽然并非最佳的攻击接口，但由于它提供了所有总线的接口，因而对于研究总线的数据流量具有重要意义。

研究者选取车窗、警示灯、安全气囊和网关等组件来搭建模拟的汽车环境 [7,8]，并通过实验验证了对控制器局域网络总线的信息注入会造成电子控制单元工作异常。美国华盛顿大学和加州大学圣地亚哥分校的研究人员在真实车辆上进行了实验 [5]，发现通过向控制器局域网络总线注入假包可以控制汽车的仪表盘显示、灯光、雨刷，甚至引擎和刹车等。他们的目标是，在获得了对汽车内部网络的物理访问权限后，研究可能实现的恶意攻击效果。其研究对象是两辆相同的 2009 年款汽车，实验场景分为三种：工作台，即单独移出车内的硬件，在实验室中测试；静车，即将汽车固定后，连接 OBD-II 诊断端口进行实验（如图 5）；动车，即在一条封闭的路段上驾驶汽车进行实验。研究者开发了 Car Shark 软件，用以分析和注入控制器局域网络数据包。

对于单个组件的攻击，文献 [5] 主要描述了以下方法：(1) 数据包侦听和定向探测。通过数据重放和试探，确定了收音机、仪表盘和一部分车身控制模块的通信和控制方式。(2) 模糊攻击。随机构造大量数据帧，就完全可以造成严重的危害。(3) 逆向工程。对于部分电子控制单元，通过控制器局域网络总线的 Read Memory 服务可导出固件，并能使用反汇编工具进行分析。

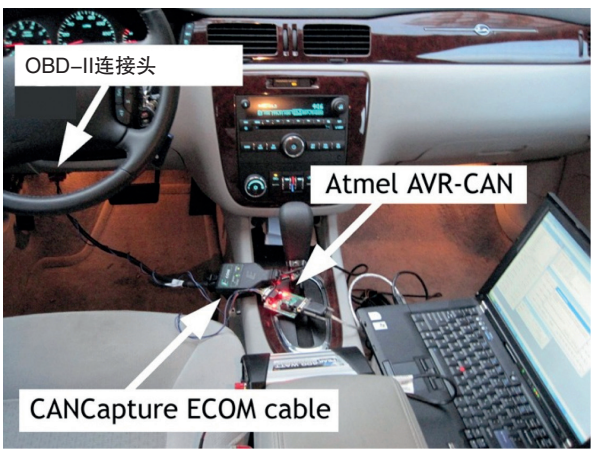

图5　实验环境[5]

在静车条件下对收音机、仪表盘、车身控制、引擎、制动、空调分别进行的攻击和对控制器局域网络总线的拒绝服务 (Denial of Service, DoS) 攻击，都达到了使其功能失效或显示错误的结果。在动车实验中，文献作者发现了许多静车时无法展现的攻击效果。

对于多个组件，他们发现汽车安全的防护并不仅仅是分别保护好单独组件的问题。他们进行了一系列复合攻击，实现了结合多总线、多组件的攻击效果。他们发现实验车的远程信息处理单元 (telematics unit) 具有同时连接高速和低速总线的特性（即网关），因此可以通过接入低速总线的电脑对其类 Unix 的固件系统重新编程，将它变成可以向高速总线传递低速总线信息的通道，这样与低速总线连接的后装电子控制单元就可以绕过网关的阻拦影响到高速总线上的重要组件。

2.USB/CD

大多数汽车娱乐系统都提供 CD 播放器和 USB 接口。攻击者可以将恶意程序伪装成音乐文件，或者植入到用户的移动设备中，在接入汽车时对娱乐系统发动攻击。文献 [6] 发现娱乐系统存在固件更新的漏洞，某一特定命名的文件可以触发更新，用户如果没有按下正确的按键，系统就会重刷。经过逆向工程，研究者发现可以构造一个特殊的 WMA（Windows Media Audio，微软音频）文件，在电脑上能正常播放，一旦在汽车上播放就会造成系统的缓冲区溢出，从而执行任意代码，向控制器局域网络总线发送假包。

3.射频识别

使用“热连线 (hot-wiring)”的方式可以在没有钥匙的情况下启动汽车，但是现在的大部分汽车都装有使用射频识别的防盗点火装置，只有匹配的钥匙才能启动汽车。射频识别虽然极大地降低了汽车的盗窃率，但系统并不绝对安全。约翰霍普金斯大

学的研究人员破解了德州仪器射频识别芯片的加密算法[10]。通过无线窃取并破解用户的射频识别信息，攻击者不仅可以绕过汽车的射频识别钥匙验证，还可以让用户为攻击者所加的汽油买单。

外部攻击接口——传感器

1.遥控钥匙

汽车钥匙的基本功能是射频遥控，它的功率更大、遥控距离也更远，已是汽车防盗系统的标配。遥控钥匙采用滚动码的加密机制以应对重放攻击，具有较高的安全性。针对它的攻击方法有：

干扰。利用汽车遥控钥匙的频段进行无线电干扰，影响锁车和开车。使用现成的干扰器就可以完成，技术含量不高。

重放攻击。在远离汽车的位置对钥匙信号进行记录，随后重放。只要重放信号没有被汽车接收过，攻击就是有效的。这种攻击需要掌握使用无线电设备的技能，只适用于车主钥匙保管不善的场景。

中继攻击。通过有线和无线方式，在物理层面对钥匙的射频信号进行中继，从而在车主携带钥匙远离汽车时进入并启动汽车。

破解算法。通过边信道攻击方法破解汽车钥匙常用的KeeLoq算法[11]，只要嗅探到两次信号就可以获得汽车密钥。

2.测距传感器

超声波传感器常用于汽车的近距离测距，是倒车雷达、自动泊车等功能的核心。毫米波雷达用于汽车的远距离测距，常见于防撞辅助、自动巡航等功能。激光探测与测量技术常应用于自动驾驶汽车的环境感知。它们的基本原理是分别通过测量超声波、微波和激光的反射时间来计算与周围物体的距离。对于这类传感器的攻击目前还比较少见，可行的攻击方法是干扰和欺骗。干扰可使传感器无法正常工作，而欺骗可以让传感器有错误的测量结果，造成事故。有研究者使用自制的激光设备对激光探测与测量信号进行了重放攻击，可以模拟汽车、行人甚至一堵墙[11]。这类攻击对于非常依赖传感器的汽车，特别是自动驾驶汽车来说，是非常大的威胁。

外部攻击接口——信息娱乐系统

1.蜂窝网络

蜂窝网络主要用于远程信息处理系统，可以通过蜂窝语音和数据网络支持求助、诊断、防盗和导航等。一旦该接口和信息娱乐系统存在可被利用的漏洞，就会带来被远程攻击的风险。

文献[6]通过逆向分析发现了某汽车的远程信息处理固件在执行aqLink协议时存在缓冲区溢出漏洞，可通过3G网络下载并执行恶意代码。他们还开发了兼容aqLink协议的PC端软件，能够自动呼叫该汽车并实现攻击。

近期有两位研究者查利·米勒(Charlie Miller)和克里斯·瓦拉塞克(Chris Valasek)通过斯普林特(Sprint)的蜂窝网络实现了对2014款吉普切诺基的远程攻击和控制[12]。他们的研究成果导致了菲亚特克莱斯勒在美国召回140万辆汽车，这也是全球首次由汽车攻击威胁引发的召回事件。

他们选择了该车的信息娱乐系统——Uconnect System作为攻击的对象，因为该系统同时连接了汽车的高速和低速控制器局域网络总线。Uconnect是一个运行在32位ARM处理器上的QNX操作系统，常见于菲亚特克莱斯勒汽车，固件很容易从网上下载。结合对固件的逆向工程，他们发现了车内Wi-Fi热点的密码设置缺陷，实现了IFS（Internet File System，互联网文件系统）越狱。通过端口扫描，他们发现了一个开放的6667 D-Bus端口和一种IPC[13]、RPC[14]的进程间通信机制，并且可以匿名登

[10] “RFID chips in car keys and gas pump pay tags carry security risks.” http://www.eurekalert.org/pub_releases/2005-01/jhu-rci012905.php。

[11] http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors。

[12] http://illmatics.com/Remote%20Car%20Hacking.pdf。

[13] Inter-Process Communication，进程间通信。

[14] Remote Procedure Call，远程过程调用协议。

入 Uconnect 系统。通过该端口可以追踪汽车位置，控制空调、音量和液晶显示屏。利用运营商蜂窝网络和 CAN 控制器的漏洞，攻击者甚至能够远程实现对汽车的完全控制，可以造成非常严重的后果。

2.蓝牙

一些熟悉蓝牙的研究者发现[15]，许多汽车生产商在它们的车载蓝牙模块中使用了“0000”或“1234”等极易猜出的弱口令，而这是汽车与蓝牙设备连接所需的唯一验证码。因此，研究者使用定向天线和自己开发的“Car Whisperer（车语者）”软件，注入或窃听其他汽车的蓝牙免提通话，甚至可以窃取从手机中导出的通讯录。这并不是由蓝牙协议的缺陷造成的，而是因为生产商忽视了蓝牙配置的安全隐患。

有研究者通过逆向分析发现[6]，某远程信息处理单元的固件在处理蓝牙配置命令时使用了不安全的 strcpy 函数，他们通过配对的蓝牙设备发起 shell 注入攻击即可执行任意代码。

汽车安全防护

虽然汽车的安全威胁可能来自方方面面，但其根本原因都是设置了不安全的信息接口、通信信道、电子控制单元固件以及总线结构。汽车信息安全防护的难度主要在于计算机领域的方法和经验不能很快应用在汽车上，因为决定物理安全的汽车实时性和可靠性可能会受到影响。

出厂检验

汽车在设计时需要考虑所有可能产生安全问题的因素，包括信息接口、通信信道、电子控制单元固件以及总线信息隔离等。

信息接口 一辆汽车具有的信息接口越多，它遭受攻击的可能性也越大。因此，需要尽量减少不必要的信息接口，特别是可以提供直接或间接的总线连接的接口。另外，还需要控制接口的开放时间，禁止在功能未经用户允许启用时开启相应接口，并对接口访问进行限制，提高用户的控制权限。

通信信道 无论是可以直接影响汽车执行系统的信道，还是向用户提供决策信息的信道，所有与行驶安全相关的信道都可以考虑加入加密和真实性校验，以应对干扰、窃听、欺骗和重放攻击。但是与之制衡的是对功能可用性与实时性的保证，例如方向盘和制动控制不能因此延迟时间过长。

电子控制单元固件 后果严重的汽车攻击都是由电子控制单元固件的缺陷造成的，这些缺陷使得攻击者可以执行任意代码或重刷固件。因此有必要设计一套对电子控制单元固件进行安全检查的系统或平台，对固件中可能存在的常见安全缺陷进行排查，其中包括不安全的函数、逻辑缺陷、无用的服务或端口等。此外，还要控制对电子控制单元进行固件重刷的权限和来源，加入数字签名等校验机制，通过代码混淆和加密增加逆向工程固件的难度。

总线 在设计总线结构时应注意不同总线之间的信息隔离，增强网关的安全性，并且对车载诊断接口进行访问限制，加入认证机制。

入侵检测

汽车厂商通常会大量采购其他厂家的电子控制单元组件，这为控制这些组件的安全性增加了困难。有必要引入汽车的入侵检测系统进行实时防护。

检测对象可以包括数据包频率、数据包 ID 、逻辑模式、物理层特征等。

总结

产品的智能化发展就像下跳棋，每前进一步，都会被对手利用和渗透，你费心搭建的棋路，也有可能成为对手长驱直入的捷径。汽车安全也是这样，新的功能在方便用户的同时，也往往为攻击者打开了大门。

汽车制造商将他们的产品变成与智能手机越来越相似的设备，但又普遍缺乏网络安全的经验，

[15] “Linux Bluetooth Hackers Hijack Car Audio.” http://www.theregister.co.uk/2005/08/02/car_whisperer/。

因此造成端口大开、漏洞频出的乱象。汽车行业迫切需要规范电子系统结构的设计，并对有风险的接口做好信息隔离，为核心动力操控系统建立起“信任区”。■

闫　琛

CCF学生会员。浙江大学博士生。主要研究方向为汽车与射频通信安全。

yanchen@zju.edu.cn

徐文渊

CCF专业会员。浙江大学教授、美国南卡罗来纳大学终身教授。主要研究方向为无线网络安全及隐私。

wyxu@zju.edu.cn

参考文献

[1] Ishtiaq Roufa, Rob Millerb, et al. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. 19th USENIX Security Symposium, Washington DC. 2010.

[2] Francillon, Aurélien, Boris Danev, and Srdjan Capkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. NDSS. 2011.

[3] Wolf, Marko, André Weimerskirch, and Christof Paar. Security in automotive bus systems. Workshop on Embedded Security in Cars. 2004.

[4] Wolf, Marko, André Weimerskirch, and Thomas Wollinger. State of the art: Embedding security in vehicles. *EURASIP Journal on Embedded Systems* 2007.1 (2007): 074706.

[5] Koscher, Karl, et al. Experimental security analysis of a modern automobile. Security and Privacy (SP), 2010 IEEE Symposium on. IEEE, 2010.

[6] Checkoway, Stephen, et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces. USENIX Security Symposium. 2011.

[7] Hoppe, Tobias, and Jana Dittman. Sniffing/Replay Attacks on CAN Buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy. Proceedings of the 2nd workshop on embedded systems security (WESS). 2007.

[8] Hoppe, Tobias, Stefan Kiltz, and Jana Dittmann. Security threats to automotive CAN networks–practical examples and selected short-term countermeasures. *Computer Safety, Reliability, and Security*. Springer Berlin Heidelberg, 2008. 235~248.

[9] Miller, Charlie, and Chris Valasek. A survey of remote automotive attack surfaces. Black Hat USA (2014).

[10]Sagstetter, Florian, et al. Security challenges in automotive hardware/software architecture design. *Proceedings of the Conference on Design, Automation and Test in Europe*. EDA Consortium, 2013

[11]Eisenbarth, Thomas, et al. On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme. *Advances in Cryptology–CRYPTO* 2008. Springer Berlin Heidelberg, 2008. 203~220.

CCF和IEEE-CS合作进入新阶段

中国计算机学会 (CCF) 和美国电气电子工程师学会计算机协会 (IEEE-CS) 日前签署战略合作备忘录，从 2016 年 1 月 1 日开始，双方将在服务会员、资源共享和出版等方面开展更深入合作。CCF 会员在享受 CCF 提供的优质服务的同时，可特价享受 IEEE-CS 提供的准会员服务。

IEEE-CS 提供的服务：

- 登录会员系统交纳人民币 65 元（学生会员 30 元），即可获得一年的 IEEE-CS 准会员资格 (Sister Society Associate Program, SSAP)，并获得唯一的准会员号。
- 可获得阅读 IEEE-CS 出版的 *Computer*、*IEEE Software* 和 *IT Pro* 等三种优秀刊物电子版权利；获得 *Newsletter* 等。
- 在出版物方面，CCF 会员可优惠订阅 *Computer*（英文版）及其他纸质版期刊。如果 CCF 从出版商那里购买了中文版 *Computer*，CCF 可提供会员阅读。
- 可享受 9 折优惠成为 IEEE-CS 会员。
- 学生会员可以 35 美元的价格同时成为 IEEE 和 IEEE-CS 的会员，并浏览 IEEE-CS 数字图书馆。

此外，CCF 还与 IEEE-CS 达成如下合作方案：

- “CCF 青年科学家奖”更名为“CCF-CS 青年科学家奖”，IEEE-CS 指派 1~2 人进入 CCF 评奖分委员会；双方在各自刊物上发布获奖新闻。
- 可邀请对方会员成为本学会理事会成员。
- IEEE-CS 将在 2016 CNCC 期间举办“Rock Stars”活动。
- 不定期互相交流访问。
- 在对方刊物上发表文章。

未来，双方还会以联合举办国际会议和联合设立奖项等方式进行广泛合作。