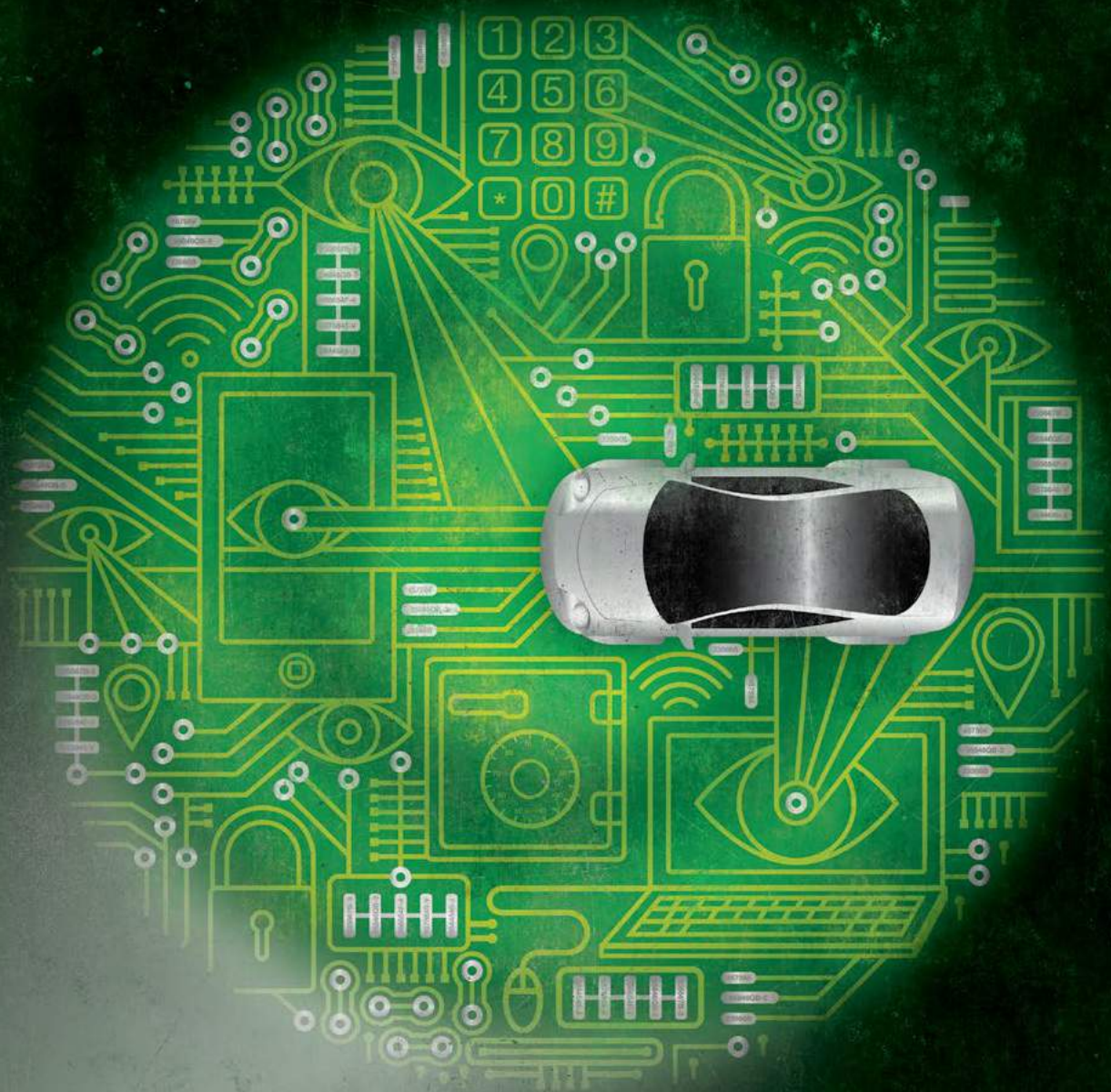
Deloitte.
University Press



保障未来移动出行的安全

应对自动驾驶汽车内外的网络安全风险

德勤未来移动出行系列

保障未来移动出行的安全

德勤综合研究中心专注于为跨行业与职能部门的重要商业问题提供一个全新视角，该视角将贯穿新兴技术的快速变化到人类行为的一致性因素。我们以研究报告、小视频以及研讨会等多种形式阐述我们对商业变革的观察，并为我们的客户提供深入严谨的见解。

封面图片：TRACI DABERKO

目录

简介

不速之客

驾驶汽车长期以来一直属于比较危险的人类行为之一——比如，最广为人知的是开车去机场这段路程是飞机旅行中最不安全的一环。[1]因此，自动驾驶汽车的安全性作为最常被提及的优点之一，这也就不足为奇了。事实上，许多人期望，拥有更多路况信息和自动驾驶技术的新兴移动出行生态系统[2]可几乎完全杜绝常见交通事故。

旨在改进人们出行方式的这一创新却带来了头号网络安全挑战。

但是，未来移动出行不仅带来潜在商业发展机会和新的价值创造来源，也带来了新的风险。旨在改进人们出行方式的这一创新却带来了头号网络安全挑战。那些人们拍拍脑袋就能想象得到的危险——例如自动驾驶汽车被黑客入侵后撞毁[3]——还只是冰山一角；实际上，这些危险甚至还不是风险程度最高的威胁。共享车辆可以储存数百位用户的数据，这自然成为令数字窃贼垂涎欲滴的作案对象。接入了互联网且自动化程度越来越高的汽车成为恶意勒索软件新的泛滥之地。随着出行运营管理商提供从起点到终点的路线规划，他们可以对人们的生活有更全面的认识——去哪里、什么时候去、以及去干什么。这样一来，用户信息就会越积越多，危险也越来越大。

在未来的发展之路上，我们应该全面关注网络安全问题，让联网的汽车和其相关生态体系更安全、更警惕、更有韧性。这可能将彻底改变企业的网络安全策略：

安全性。围绕最敏感的资产实现风险集中控制，从而降低风险，确保生产效率，提高业务增长，实现成本优化。

警惕性。为关键业务流程制定监控方案。在汇总威胁数据、信息技术数据和业务数据之后，公司可以生成丰富的警示信息，帮助确定事件的优先级，简化事件调查步骤。

韧性。快速适应和响应内外各类变化，比如商业机会、业务需求、中断或威胁，并能保持持续运营，缩小对业务的影响。

未来移动出行最大的威胁可能还是网络风险。对用户和企业而言，在此过程中数据管理、用户隐私和数据保护至关重要。正如防撞预警系统和防抱死制动器并没有能够消除所有的交通事故一样，共享汽车和自动驾驶汽车也不会毫无风险。对于移动出行生态系统中的参与者而言，最关键的挑战是将风险维持在消费者和监管者都能接受的水平。随着汽车制造商、技术公司、政府等都为未来移动出行生态的发展纷纷加大投入，可是如果他们对网络威胁没有足够的了解，或没有具体的应对策略，这些巨额投入可能就会打水漂。

风险之所在

上个世纪人们主要专注于解决工程方面的问题，而现如今汽车制造商正面临新一轮的挑战。其他行业也在积极应对网络安全问题，移动出行生态系统中的参与者可以向这些行业寻求类似的解决方案，不过这些解决方案的具体实施还是需要精心调整，以满足汽车行业的特殊需求。

至于企业采取什么措施，还是要看他们在整个生态系统里扮演什么角色。在《未来移动出行》一文中，我们预想了未来移动出行的四种共存情境：其中一些与如今现状非常类似，而另一些则对未来共享交通和自动驾驶的可能性进行了大胆的设想（见图1）。[4]

这四种未来出行情景分别带来了不同的与数据相关的风险和挑战，因而需要一系列的应对措施。

未来情景1：这是最为保守的情景，车辆基本上和今天一样，依然是自己的车自己开。不过，预计车辆会有更多连接和数据（创建、消费、分析等），也会采用先进的驾驶辅助技术（但并非完全自动化）。随着汽车设计的进步，安全功能也会相应革新。升级后的安全功能将可能基于现有的车载技术和功能。不过升级后的技术在保障现有的技术和功能安全的同时，也要不断改进提升，以适应第一种未来情景所带来的变化。

图1.未来移动出行情景

来源：德勤分析

内部威胁

无论怎样发展，未来移动出行很有可能会引入新的基础设施，更多依赖数字化网络，而非实体设施。[5]随着车辆与其他车辆及周围环境的数字化连接越来越多，车联网的应用会逐渐扩展到很多方面，从帮助应急车辆重新规划路线、缓解交通拥堵，到指引车辆停泊以及电动车辆充电。

类似于眼下的智能手机开发，未来软硬件供应商很可能会联手开发新型车辆及其配套基础设施。先让我们想象这样的场景，假设软件开发商与车联网设备制造商合作，由后者负责运输和装配联网设施。当软件开发商的骨干工程师离开这家公司，他带走了手头上的商业机密和车联网系统的后门信息。可能出于对前雇主心怀不满，他泄漏了这些机密信息，数十万的设备将会门户洞开，任人鱼肉。一开始，这些攻击可能还只是一些恶作剧，但事态很快就会升级：黑客们可以操纵整座城市的交通信息，向交通软件或共享汽车通告每条路都在施工，引发事故，导致市政应急服务能力严重下降。接着，他们又可以远程操控将电动汽车充电站的电流提升四倍，进而引起火灾。

当然，企业要努力保障安全，避免单个人为破坏行为造成大面积损失，但总有缺漏。近期，制造业生产力与创新联盟和德勤联合开展了一项调查，结果显示：制造业高管们追查出有42%的网络事故源自于“内部威胁”。[6]

泛汽车行业可以向诸如北美电力可靠性公司之类的企业学习如何制定标准和规范，指导关键电力系统的安全研发。在标准委员会的带领下，行业志愿者和公司员工共同起草，北美电力可靠性公司着眼于系统可靠性和市场影响性制定了一套准则。这些准则同样适用于移动出行系统。[7]随着汽车和交通基础设施开始与周边环境以及其他系统整合，政府和系统开发商应考虑像保护其他公共设施一样保护这些移动出行的基础设施。

制定标准时，可参考美国国家标准与技术研究所的《信息技术系统安全性准则与规范》。[8]就像安全内容提供商可以通过加密和认证来保护公共设备那样，重要基础设施的保护工作通常除了物理防护和公共安全措施外，还要求开发相应的安全防护软件。这是因为监管部门（如美国运输部以及美国国家公路交通安全管理局） 认识到，如今他们监管的这些设备越来越复杂，而且还支持远程控制，那它们面临的危险也就相应地增加了。同样需要关注的还有联网车辆和相关设备，它们也是新的移动出行生态系统中的关键基础设施。

如今，美国国家公路交通安全管理局正为了将来的发展铺平道路。在2016年10月，管理局为了提高网络安全，向汽车行业提出了一系列建议，重点“确保汽车系统在遭受攻击后还能采取适当安全的操作”。[9]

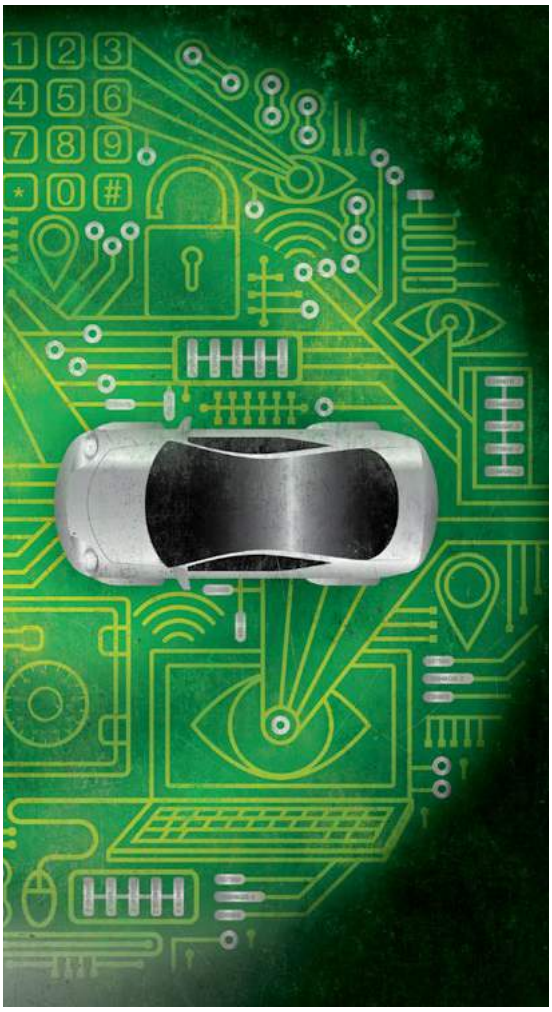
即使在今天，很多车辆严重依赖于一些专有软件，而这些软件在黑客面前已经是漏洞百出。就一般的新汽车而言，上面配备的电脑系统都会用到上亿行代码，[10]这些代码使得汽车可以互联互通且更加精细复杂，但同时也更易受攻击（见辅文，《内部威胁》）。而且这还不单单是代码数量的问题——质量也是个大问题。企业加速变革和创新的目的是在竞争中脱颖而出，为在竞争中胜出，却往往倾向于牺牲端对端开发和测试的严谨性。这种目光短浅的做法会增加系统错误率或使系统安全失去保障，说不定最后导致产品召回，商业信誉受损。新功能不可避免地整合多种来源的集成代码，也存在更多的潜在漏洞，汽车制造商和软件开发公司相应地需要在整个汽车组件的集成、安全和测试上多花点功夫。[11]

同样，随着汽车缺陷更多的来自代码而非零件，监管机构也面临挑战。有些人已经认识到这一难题。美国国家公路交通安全管理局局长Mark Rosekind直截了当地说：“几百万行代码……都讨论多少次了？我们就是搞不定。”[12]

未来情景2：尽管车辆仍然由人工控制，但随着“共享经济”和各大汽车共享服务公司的兴起，共享出行将进一步发展。

我们现在瞥见一下未来的情景，大致了解下潜在的网络安全问题。然而，如果在技术创新上一味求快，会大幅增加网络威胁的规模、强度和复杂度。随着社交媒体、拼车软件及其他移动应用程序的激增，连接消费者的智能设备会暴露更多的风险。

保护司机和乘客的个人信息是重中之重。心怀不轨的人可能会想办法搞到这些信息，因此对拼车服务公司的系统虎视眈眈。支付系统可能也会泄露个人信用和银行信息。导航和位置信息则可能泄露客户隐私，这就要求厂商确保车载通信的安全。



现在，汽车公司和科技公司都试图进军共享出行领域，[13]他们应该考虑到这个业务模式的风险和网络威胁。

数据饕餮

正如飞行数据记录器会记录驾驶舱发生的事情，联网汽车也会记录车主和乘客的一举一动。但车载技术还可以编纂和分析数据，得出一些更具洞察力的结论：例如，设备可以仅根据刹车踏板数据对用户进行分类。[14]而对于共享汽车而言，深层数据挖掘可能会越来越频繁，以满足客户对服务无缝对接的渴求。现在很多公司（如数据中介和保险公司）都在期待着可以无限制地访问这些数据，但另一方面，数据匹配正在以新的方式从这些数据里面提炼金矿。一些拼车服务提供商已经可以实现乘车过程中同步乘客的音频服务系统。[15]

现在，想象一下有人在垃圾场搜集零件，她直接忽略了挡泥板、车门和气囊。真正有价值的东西还是在CPU模块里面——并不是用于维修或备用，而是里面的数据。每个模块都可能包含大量有价值的信息——比如，每一辆共享汽车的数据记录器都可能储存着之前用户的智能设备信息，包括地址和身份证号，还记录着这辆车报废前去过的每一个地方，甚至包括数百个账号和日志，这样就暴露了乘客的电话号码、地址和支付记录。一套完好的个人数据放到网上卖，价格会比单独转售一个零部件高得多。

在未来，汽车会越来越了解自己的主人及乘客——对很多人而言，这个趋势让他们越来越担心。这些数据是归制造商所有吗？那车主呢，或者借车的人，抑或只是乘客呢？我们的法律制度会怎么界定数据的所有权？当车辆开过不同的辖区时又会是何种情形呢？对于事故车辆，警察又会怎么处理车上的数据？车辆报废之后，谁又会负责清除报废车辆的数据记录？

在未来发展的道路上，汽车制造商和共享出行服务提供商可能会指望企业信息技术部门。很多公司在租赁到期或合同到期时，会清理员工的电脑、手机等电子设备上的残余数据，具体可包括：数据加密、恢复出厂设置或其他数据安全清除。在一项调查中，超过半数的受访者表示，他们的公司有配备信息资产处置规定。[16]车辆所有权变更或者车辆报废时都可以参考采用类似的程序。

未来情景3：这种情景中采用了个人所有、完全自动驾驶的汽车。尽管大部分自动驾驶技术的核心功能都是车内标配（这样相对来说不容易受到攻击），但自动驾驶汽车总归还是要通过传感器、车联网技术、GPS软件等系统和外部世界进行信息交流。与第一种情景一样，如果一切顺利的话，这些联网汽车可能会改善乘客体验，但也可能带来新的威胁。去年，安全研究人员就已经能够利用车载应用程序里的漏洞攻击电动汽车的电池，可以使汽车熄火。[17]虽然后来漏洞修复了，但这个例子也让我们意识到连接性的增加会导致威胁升级。在自动驾驶汽车里，汽车系统将完全由汽车自主掌控，入侵攻击或系统漏洞所带来的损害都可能会危及生命。

为避免这些问题，自动驾驶汽车开发公司目前通过操作人员来控制应对系统崩溃或系统错误，但这种方法不适用于普通消费者。特别是如美国交通运输部制定的自动化车辆指南所指出的：“在制定保障机制时应当考虑到……人类驾驶员注意力不能集中的情况，如在酒精或其他因素影响下造成的困乏，或因其他方式造成的身体受损。”[19]除此之外，自动驾驶汽车可能在完全没有驾驶员接管的情况下发生故障——比如，自动驾驶汽车自己“开”去进行保养。该政策没有明确规定自动驾驶车辆在这种情况下应如何行事，而自动驾驶汽车开发商和研究人员必须努力制定出安全的方法。

来自制造商的系统信息也未必安全

虽然自动驾驶汽车失控好像更能让人浮想联翩，但平日老生常谈的那几种威胁也绝对不容小觑。如今，说到和软件相关的安装和召回，很多汽车制造商会让顾客亲自把车送到经销商那里来完成。但要让车主主动配合这样的服务要求似乎很困难，特别是当车辆运行还正常时。

但随着越来越多的车载软件需要定期更新安全和导航信息，新的移动生态系统中的自动驾驶车辆可能会有专用通信线路与制造商进行交互，以便即时进行软件的召回和补丁安装。车载系统的更新其实和今天的智能设备以及电脑类似，从网上下载更新包，然后让相应的设备在闲置时自动更新。

在不远的将来，自动驾驶汽车可能需要对车载通讯系统进行细微更新。接受和安装更新包的设备会直接和汽车互联网络连接，然后让车载设备在停车之后自动启用更新程序。试想一下，如果这些接收信息的设备与智能设备共享的服务器被黑客入侵得手，这就意味着该设备（几乎所有配置了该设备的车辆）接收的可能就不是生产商的更新包，而是黑客上传的。技术熟练的黑客甚至可以在几千台汽车上安装勒索软件，这样一来，除非向黑客付钱，不然用户会被锁定或车辆被冻结。而且在专有通道被封锁之后，制造商也对此无能为力，车主甚至无法将车辆开到服务中心。这将是个大问题，因为售后市场体系一直以来都是汽车产业的传统基础，允许车主们改装和定制车辆以提高汽车的性能。随着越来越多的汽车上的各种部件也开始联网，车主可能会无意中引入漏洞。

每个新的连接功能会带来新的漏洞，这样又该如何保证安全？在防止篡改这个问题上，汽车制造商和软件开发商学习专线化内容传送的方法。卫星和有线媒体提供商为了解决这个问题，用上了数字继电器、故障记录器、设备诊断包、自动化设备、计算机、可编程逻辑控制器和通信接口等。[18]但这个过程是曲折的，而且通常也是特定的。内容提供商受到终端用户技术能力的局限。在过去，像卫星接收器这样的设备如果想要无线进行用户验证，势必就要降低内容的质量，就像如今的车辆网络为了保证车辆内部模块之间的通信一样。虽然随着现在的接收器功能越来越强大，安全性也稳步提升，但黑客还是能用接收器中同样的手段来避开安全系统。

除非汽车技术供应商采取措施，从其他领域的安全内容提供商那里获得经验教训，不然类似的情形很可能会在互联汽车和自动驾驶汽车上重演。为了保证内容传递安全，通常都会做双向加密，安全密钥也会滚动刷新，想要在指定的响应窗口破解密钥是不切实际的。因为系统访问通常会受到限制，而且会定期检查系统漏洞和远程篡改。

对一些消费者而言，想要他们把自身的安全全部托付给一台自动驾驶的汽车，首先就要让他们对车辆技术的安全性、完整性和功能性有起码的信任。自动驾驶汽车的车载系统本身就有许多遭到攻击的脆弱点，包括雷达、相机、GPS、超声波传感器、车联网等网络功能，更别提这些传感器所依赖的相关基础构件和技术。因此，全自动化汽车对架构和操作（监控、漏洞管理、安全运行等）的要求要远远高于部分自动化或具备辅助驾驶功能的汽车。利用可靠的汽车技术来确保网络安全和个人隐私乃是重中之重。

未来情景4：最后，随着共享出行业务的扩张以及自动驾驶技术的成熟，我们可能会实现一个“车辆高度自主”的出行模式，乘客只需从附近的自动驾驶车队叫来一辆车便可到达目的地。这种模式最有可能从大城市的上班族开始，但随着能力扩大和用户消费意愿增强，这种模式就会迅速蔓延至各地。采用这些技术会催生一个综合多式联运化的生态系统，提供更安全、更环保、更便宜和更便利的交通服务。

这种情景与其他情景一样，也存在同样的安全漏洞和个人信息被盗的问题，而且将面临着更大数量级

操纵汽车控制系统和传感器

用户们常常会希望，智能设备上的一个应用软件就能无缝地控制拼车服务，并对接其他的交通出行工具。不出意外的话，你可以很方便地叫来一辆共享自动驾驶汽车，然后解锁上车，设定路线，到达目的地后支付车费。除了Wi-Fi和短程通信功能之外，汽车本身还可以接收来自蜂窝网络和卫星网络的信号；用户在付费后可以直接上车同步自己的个人内容，如便携式扬声器或智能电视机。

然而无缝化就很难避免风险。首先，黑客可能会偷偷安装监控设备，用收发器提取用户数据，或将恶意数据传入汽车网络。接下来客户就会不知不觉地将所有信息（从个人信息到付款明细）发送给黑客。更糟糕的是，黑客还可能会将错误的传感器及导航信息传到汽车网络，使车子转弯躲避并不存在的障碍物，或者把乘客送去错误的目的地。

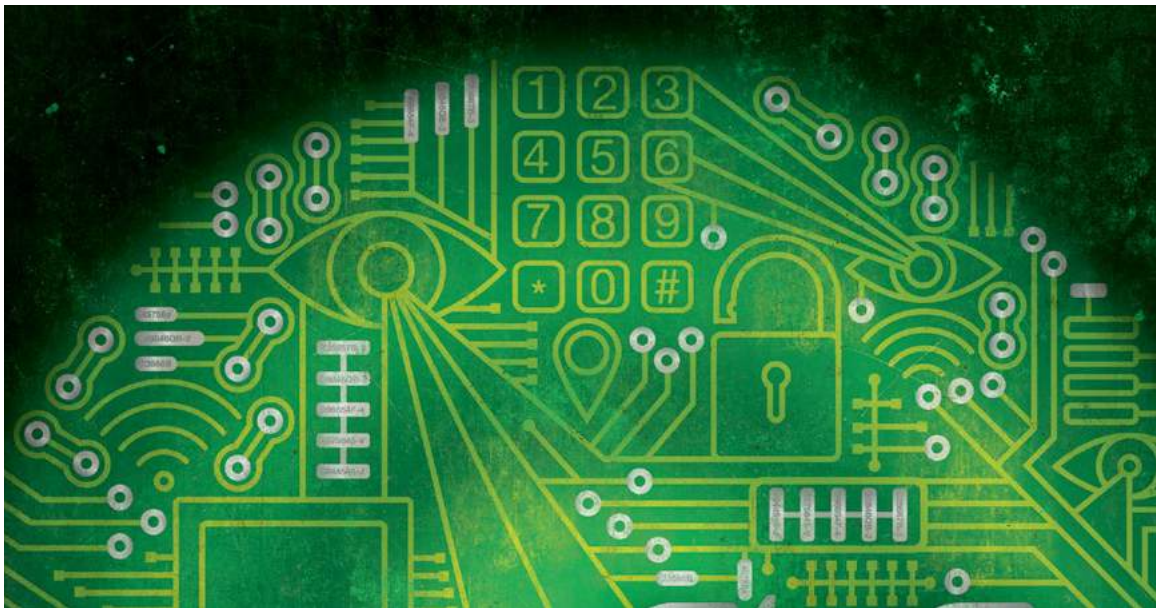
启用汽车网络与智能设备通信会让黑客们有机可乘，增加数据丢失的风险。关键和非关键的车载信息线路相互混杂在一起，会让信息注入器将不需要的数据传送到车辆设备中。理论上，控制车内灯光和音乐的设备不能与控制刹车和油门等关键任务的系统进行通信。而现在，这些车载网络已经与车载通讯系统或车身控制单元进行了连接，从而允许数据在网络之间进行传播。

网络安全行业正在努力解决这些问题。为了保护持卡人的数据，如今的支付卡处理器遵循既定的数据安全标准（DSS），旨在保护处理数据的设备。[20]数据安全标准虽然不是由政府机构强制执行，但也为业界提供了规范和指引，例如“系统密码或其他安全参数不要使用出厂初始默认设置”，以及“使用公用网络传输持卡人的数据时一定要加密”。支付卡行业中的企业可以自愿选择是否遵从，但如果公司加入支付卡行业联盟，则必须签署合同协议并满足数据安全标准。违规行为将会受到罚款、上调手续费或者终止服务等惩罚。

在泛汽车行业建立和实施一套安全标准时，不妨可以参考类似于DDS标准的规范，它将适用于汽车电子或基础设备供应商。这些规范也可应用于联网车辆储存和传输数据。目前大多数的车载网络架构无法处理入侵检测或威胁监控，更不用说实现认证或加密。一个现代黑客如果能入侵一辆车，通常来说，只要他知道这辆车的通信模式，他就可以随心所欲地从汽车网络发送或提取任何信息。随着汽车的功能越来越多，黑客能攻击的面也就会越来越广，这种问题就会越来越严重。在老一代汽车技术里面，汽车电子产品还比较单一，功能也比较弱，对黑客而言反而难以入侵。

的难题，因为黑客可以入侵“智能”基础设备或者大型共享自动驾驶车队，从而带来更大的损害。[21]

在每一种未来情景下，汽车和乘客可能需要给予车载技术更多的信任，提高车辆网络安全。安全研究人员着重强调了汽车存在的漏洞，吸引了各方的关注（乃至想象），包括公众、监管机构、公职人员等。要想成功解决这些风险问题，我们不仅要在行业标准上达成共识，更要一起努力，确保未来移动出行的安全、警惕和韧性。



发展之路

大局：达成共识

虽然未来移动出行生态的发展会面临诸多潜在的威胁，但这些危险并非难以克服，部分原因是公众、各级政府、监管部门以及标准制定部门对网络安全越来越重视。举个例子：2016年，联邦调查局和美国国家公路交通安全管理局向公众和汽车、汽车零部件和售后设备制造商发出警示，以敦促他们“对互联汽车技术带来的潜在问题和网络安全威胁保持警惕”。[22]美国国家公路交通安全管理局还于2016年1月召开了一个公开座谈会，以促进各利益方商讨汽车网络安全问题。与会者包括17家汽车主机厂代表、25个政府组织和13个行业协会。[23]

安全意识的提高正合时宜。随着私营企业和政府努力实现未来移动出行的新愿景，泛汽车行业急需建立网络安全标准，作为行业的安全基线，同时也为未来的软件开发和分销做好准备。幸运的是，初步的努力已经开始了。2015年，为了加强网络安全意识，分享网络风险信息，提高全球汽车行业的协作能力，汽车信息共享与分析中心应运而生。[24]同时，美国汽车制造商联盟和全球汽车制造商协会也制定了《汽车网络安全最佳实践框架》。[25]

> 为了有效地制定标准，衔接未来各种移动出行方式，需要有更多的行业参与进来。

但这还远远不够。目前的这些工作都还是自愿性质的，参与者也只是汽车主机厂和供应商——考虑到未来移动生态系统预计将跨越各个传统领域，包括科技、电信、媒体、保险、金融等等，如今的参与者的阵容还是太小了。为了有效地制定标准，衔接未来各种移动出行方式，需要有更多的行业参与进来。事实上，鉴于这一新技术浪潮还处于起步阶段，目前的技术供应商似乎有能力塑造相关的标准。

在过去很多时候，科技行业已经给我们展示了未来发展路径。一个不错的例子是，当初通信行业的参与者联合成立了蓝牙技术联盟。蓝牙技术联盟是一个非营利的非股份制机构，负责监管蓝牙标准的制定和蓝牙技术和商标的授权工作。[26]现在，任何需要将蓝牙无线技术纳入其产品的公司，必须先成为联盟成员。

蓝牙技术联盟能取得如此成功，归根结底还是因为它对蓝牙技术规范的控制，要求成员认证其产品符合标准。技术联盟成员须声明他们会遵守蓝牙专利/版权许可协议和蓝牙商标许可协议。[27]通过确认所有的蓝牙产品达到合格标准，申报程序齐备，品牌标注符合要求，这一实施计划有助于保护所有技术联盟成员的权益。这一计划还会监督市场动态并每月进行审

核，以确保成员根据蓝牙品牌指南使用商标，销售的商品和服务已成功完成蓝牙认证和申报流程。[28]

通过确认所有的蓝牙产品达到合格标准，申报程序齐备，品牌标注符合要求，这一实施计划有助于保护所有技术联盟成员的权益。

诚然，为互联车辆和自动驾驶汽车创建类似的组织并不简单——这需要将无数独立开发自动驾驶系统的企业联合起来，并就某些基本功能达成一致。但是，联盟的意义不容小觑，特别是，有助于让公众确信开发商的确采用了严格的工序，建立了自动驾驶系统的安全性和完整性。

细节：建设防护措施

单单是制定几条标准还不足以为未来移动出行的发展保驾护航：汽车制造商和其他制造商仍然需要构建安全组件并保障信息交互安全。行业标准是在每个组件的基础上对车辆部件进行测试，评估软硬件、无线升级以及通讯渠道的漏洞。通常来说，单独的模块都会由特定的专家负责，因此不同的组件会引入多个合作伙伴。将这些独立开发的组件整合成一个产品，这会带来多重挑战。首先，独立测试中不存在的攻击漏洞，可能会在组件之间进行通信的时候出现。比如，如果发送的信息无效或格式错误，这个模块就可能会失效。其次，非正常的信息传输可能会使生产商或其合作伙伴的知识产权遭到恶意攻击。如果不能安全集成这些组件，将会很容易被攻击。

图2.展现了一辆完整的互联车辆，显示出各个组件如何彼此交互。单个组件的故障通常也导致连锁反应，使驾驶员和其他人员处于危险之中。

将这些独立开发的组件整合成一个产品，这会带来多重挑战。

例如，如果车辆信息交互线路崩溃，则车辆实时系统就不能向车辆高级智能系统传送重要的状态信息。而如果车辆高级智能系统没有接收到这些信息，那么控制诸如刹车、加速/减速、防撞组件的集成车辆安全系统就不会有任何动作。

以下对车辆组件进行了简要说明，可以全面了解每个组件的主要功能和相关风险。.

- **车辆通讯总线**。供应商应严格测试控制器局域网、互联网协议、2Wire、以太网和其他供应商指定的通信总线系统，以识别影响软硬件之间通信的安全漏洞。
- **手机应用**。手持设备上的车辆远程应用以及与其相连的车载仪表盘应用应当被仔细评估以确保点对点交互的安全性。现在手机应用软件越来越多，

图2. 互联车辆评估

来源: 德勤分析

汽车的高级智能系统集成度越来越高，风险也越来越大。

- **互联汽车服务**。企业服务、传感器通信、无线固件更新、V2V和V2X通信都可能存在漏洞，提供商应对这些点对点安全漏洞进行审查。其他容易遭受攻击的还包括车辆定位器，远程解锁和启动功能，以及车队健康监控。
- **综合车辆安全**。供应商和汽车制造商应该想办法阻止针对车辆物理安全系统（如防盗器、报警系统和解锁系统）的攻击。此外，应考虑到并尽力减轻针对无线电频的攻击，如重放攻击和拒绝服务攻击。

- **信息娱乐系统**。汽车音响主机，如导航系统、USB、CD/DVD等物理接口都暴露在外，这就容易让黑客有机会直接入侵核心组件和固件。
- **无线通信**。Wi-Fi、蓝牙、近场通信和移动互联网技术为入侵互联车辆提供了更多的途径，因此这些技术都应该仔细检查，定位相关的漏洞。
- **高端/自动驾驶车辆系统（包括半自动和完全自动驾驶）**。高级智能互联车辆系统，如雷达、摄像头、驾驶和停车辅助系统以及防撞系统，让黑客得以把网络攻击变成对车辆本身的攻击。在黑客的控制之下，这些系统可以严重影响车辆安全。因此，系统的完整性对汽车的整体安全至关重要。
- **固件**。黑客可以提取和分析电子控制单元固件。这样黑客就可以找出这些固件中的漏洞，并且提取敏感数据，如加密密钥。确保这些文件受到保护并且防止其被篡改是保证整个系统安全的关键。

在整个发展过程中，公司应努力实现网络风险管理的三大基本目标：安全、警惕、韧性。

在整个发展过程中，公司应努力实现网络风险管理的三大基本目标：安全、警惕、韧性。抱着“预防”比“治疗”更重要的想法，要进行有效的危机管理，首先就要保护好关键部件，并防止系统数据泄露或系统损害。保证系统安全并不是一劳永逸的事。随着时间的推移，硬件和软件都会“老化”，并且攻击的性质和强度都会改变。因此，供应商应该在保证安全的同时，还要保持警惕性——持续监控系统，以确定系统是否安全或已被损坏。最后，如果已经制订了相应的流程来快速处理威胁，防止扩散并且迅速恢复，万一受到攻击时，止损和恢复就会容易很多。[29]

结论

保护新兴的移动出行生态安全还任重道远，风险很高。在瞬息万变的世界，未来移动出行想必会更加复杂，许多问题还未得到解答，却有更多未知问题等着我们。尽管许多汽车制造商和技术公司都争相进军这一领域，但时下消费者还是对自动驾驶汽车的前景持观望态度。[30]如果车辆的安全得不到保障，这些投资就会打水漂。

幸运的是，未来移动出行所面临的许多网络风险，我们并不陌生。

幸运的是，未来移动出行所面临的许多网络风险，我们并不陌生。通过借鉴其他行业辛苦得来的经验教训，泛汽车行业就能比黑客和其他对手领先一步。可以采纳以下几个步骤：

- 利用企业信息技术流程解决数据隐私防护和数据废弃处置问题
- 实施加密和代码签名机制，保护系统软件的完整性
- 为关键车辆系统安全开发制定实践标准
- 要求供应商执行已制定的标准，类似于支付卡行业的安全标准DSS

通过从其他行业那里学习保护重要数字基础设施的经验——包括眼下为保护互联汽车所做出的努力——全球泛汽车行业一定可以像当年成功推广传统汽车那样，把共享自动驾驶汽车也变成全人类所共享的福音。

尾注

1. Aurelio Locsin, “Is air travel safer than car travel?,” *USA Today*, http://traveltips.usatoday.com/air-travel-safer-car-travel-1581.html.
2. See Scott Corwin, Nick Jameson, Derek M. Pankratz, and Philipp Willigmann, *The future of mobility: What’s next?*, Deloitte University Press, September 14, 2016, http://dupress.deloitte.com/dup-us-en/focus/future-of-mobility/roadmap-for-future-of-urban-mobility.html; and Scott Corwin, Joe Vitale, Eamonn Kelly, and Elizabeth Cathles, *The future of mobility*, Deloitte University Press, September 24, 2015, http://dupress.com/articles/future-of-mobility-transportation-technology/.
3. Lorenzo Franceschi-Bicchierai, “Car hacking looks much cooler in ‘Fate of the Furious’ than it does IRL,” *Motherboard*, March 9, 2017, https://motherboard.vice.com/en_us/article/fast-and-furious-8s-car-hacking-might-be-the-most-credible-stunt-in-the-movie.
4. Corwin et al., *The future of mobility*.
5. Simon Ninan, Bharath Gangula, Matthias von Alten, and Brenna Sniderman, *Who owns the road? The IoT-connected car of today—and tomorrow*, Deloitte University Press, August 18, 2015, https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-automotive-industry.html.
6. Carol Mangis, “How to recycle old electronics,” *Consumer Reports*, April 22, 2016, www.consumerreports.org/electronics-computers/how-to-recycle-old-electronics/.
7. North American Electric Reliability Corp., “Standards,” accessed October 26, 2016, www.nerc.com/pa/stand/Pages/default.aspx.
8. Marianne Swanson and Barbara Guttman, “Generally accepted principles and practices for securing information technology systems,” National Institute of Standards and Technology, September 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.
9. National Highway Traffic Safety Administration, “U.S. DOT issues federal guidance to the automotive industry for improving motor vehicle cybersecurity,” October 24, 2016, www.nhtsa.gov/press-releases/us-dot-issues-federal-guidance-automotive-industry-improving-motor-vehicle.
10. David Gelles, Hiroko Tabuchi, and Matthew Dolan, “Complex car software becomes the weak spot under the hood,” *New York Times*, September 27, 2015, https://nyti.ms/2mF6Teu.
11. Kenneth van Wyk, “The true root causes of software security failures,” *Computer World*, May 21, 2013, www.computerworld.com/article/2497957/security0/the-true-root-causes-of-software-security-failures.html.
12. Pete Bigelow, “NHTSA mulls role of car-hacking researchers, but time’s ticking,” *AutoBlog*, October 10, 2015, www.autoblog.com/2015/10/10/nhtsa-car-hacking-researchers/.
13. Joshua Jamerson, “Verizon to buy Fleetmatics for $2.4 billion,” *Wall Street Journal*, August 1, 2016, www.wsj.com/articles/verizon-to-buy-fleetmatics-for-2-4-billion-1470055429.
14. Miro Enev et al., “Automobile driver fingerprinting,” *Proceedings on Privacy Enhancing Technologies*, 2016 (1), pp. 34–51, www.autosec.org/pubs/fingerprint.pdf.
15. Uber, “Uber & Spotify = Music for your ride,” November 17, 2014, https://newsroom.uber.com/uber-spotify-music-for-your-ride/.

16. Iron Mountain, “Enterprises have room for improvement in secure IT asset disposition,” May 8, 2014, www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/Sponsored/Enterprises-Have-Room-for-Improvement-in-Secure-IT-Asset-Disposition.aspx.

17. Troy Hunt, “Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs,” February 24, 2016, www.troyhunt.com/controlling-vehicle-features-of-nissan/.

18. Global Information Assurance Certification, “A content delivery case study,” June 23, 2003, www.giac.org/paper/gsec/3503/content-delivery-case-study/105714.

19. National Highway Traffic Safety Administration, *Federal Automated Vehicles Policy*, September 2016, www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.

20. Victor Oluwajuwon Badejo, “Case study: Payment card industry—data security standards (PCI–DSS),” March 11, 2016, www.slideshare.net/VictorOluwajuwonBade/case-study-on-pci-dss.

21. North American Electric Reliability Corp., “Standards.”

22. David Shepardson, “FBI warns automakers, owners about vehicle hacking risks,” *Reuters*, March 17, 2016, www.reuters.com/article/us-fbi-autos-cyber-idUSKCN0WK0BB.

23. Ryan Beene, “NHTSA chief vows action this year on cybersecurity,” *Automotive News*, January 19, 2016, www.autonews.com/article/20160119/OEM06/160119727/nhtsa-chief-vows-action-this-year-on-cybersecurity.

24. Automotive Information Sharing and Analysis Center, www.automotiveisac.com/, accessed March 27, 2017.

25. Auto Alliance, “Framework for automotive cybersecurity practices,” January 14, 2016, https://autoalliance.org/wp-content/uploads/2017/01/Framework.AutoCyberBestPractices.14Jan2016.pdf

26. Bluetooth, “Membership agreements,” www.bluetooth.com/membership-working-groups/membership-types-levels/membership-agreements, accessed March 27, 2017.

27. Ibid.

28. Bluetooth, “Qualification enforcement program,” www.bluetooth.com/develop-with-bluetooth/qualification-listing/qualification-enforcement-program, accessed March 27, 2017.

29. Irfan Saif, Sean Peasley, and Arun Perinkolam, “Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age,” *Deloitte Review* 17, July 27, 2015, https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-17/internet-of-things-data-security-and-privacy.html.

30. Craig Giffi, Joe Vitale, Ryan Robinson, and Gina Pingitore, “The race to autonomous driving: Winning American consumers’ trust,” *Deloitte Review* 20, https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-20/winning-consumer-trust-future-of-automotive-technology.html, accessed January 24, 2017.

中国汽车行业服务核心团队

何马克博士
领导合伙人
德勤中国汽车行业
电子邮件：mhecker@deloitte.com.cn

洪延安
领导合伙人
德勤中国汽车行业审计及鉴证
电子邮件：johnhung@deloitte.com.cn

虞正
领导合伙人
德勤中国汽车行业财务咨询
电子邮件：micyu@deloitte.com.cn

周梓滔
领导合伙人
德勤中国汽车行业风险咨询
电子邮件：totchow@deloitte.com.cn

肖天晶
领导合伙人
德勤中国汽车行业税务咨询
电子邮件：lixiao@deloitte.com.cn

中国网络安全服务核心团队

华北区

薛梓源
合伙人
电子邮件：tonxue@deloitte.com.cn

何晓明
合伙人
电子邮件：the@deloitte.com.cn

华东区

冯晔
合伙人
电子邮件：stefeng@deloitte.com.cn

施建俊
合伙人
电子邮件：alexshi@deloitte.com.cn

华南区

邓景山 (大陆)
合伙人
电子邮件：tertang@deloitte.com.cn

郭仪雅 (香港)
合伙人
电子邮件：evakwok@deloitte.com.hk

李卓伟 (香港)
合伙人
电子邮件：thomalee@deloitte.com.hk

Deloitte.
University Press

CQ-101SC-17

这是环保纸印刷品