智能汽车安全风险与对策研究报告

360 公司&互联网实验室

2014 年 8 月

前言

当前智能汽车与车联网正在成为业界热点，很多 IT 厂商、汽车厂商正在致力于提升汽车的智能化程度，这对于消费升级和经济发展都有积极意义，但安全风险也不容忽视。智能汽车使传统网络安全问题向现实世界扩散，用户在驾车过程中面临网络攻击的威胁，可能引发车辆失去控制、拒绝服务等严重情况，影响用户生命财产安全。在智能汽车产业爆发前夜，有必要理清其背后的安全风险并加以防范，保障用户利益和产业健康发展。

本报告由 360 公司与互联网实验室联合推出，旨在揭示汽车智能化背后隐藏的安全风险，并希望各界共同努力，构建智能汽车产业安全防护体系，打造安全的智能汽车生态系统。

目 录

图表目录

第一章　智能化热潮开启汽车产业新时代

“智能汽车”是以传统汽车为基础，加装传感器（雷达、摄像）、控制器、执行器等设备，通过车载传感系统和信息终端实现与人员、车辆、环境的智能信息交互，使汽车具备感知能力，自动分析汽车行驶的实时状态，使汽车按照人的意愿做出行驶、停靠、加速、刹车等行为，最终实现替代人操作驾驶的目的。简而言之，智能汽车就是将传统汽车智能化，将车辆中由人和机械控制的部分功能乃至全部功能交由信息系统、信息技术来处理，将人从汽车操作中解放出来。

智能汽车在形成一股热潮，智能化程度不断提升，也不断有厂商加入到该领域。智能驾驶、生活服务、安全防护、位置服务以及用车服务等，都是智能汽车较为成熟的或可预期的功能。智能汽车技术正在赋予传统汽车以新面貌、新活力、新定位，进一步提升车主的生活品质。

1.1IT 技术驱动汽车智能化

IT 技术正在大量使用于汽车工业，使汽车智能化程度不断提升，目前智能系统只是辅助车辆行驶，未来将实现彻底的无人驾驶。

当然，汽车智能化是个渐进的过程，美国高速公路安全管理局将智能汽车定义为五个层次阶段：无智能化、具有特殊功能的智能化、具有多项功能的智能化、具有限制条件的无人驾驶、全工况无人驾驶。

图表 1：智能汽车发展阶段

制图：互联网实验室

可以看到，IT 技术与传统汽车相结合，将使汽车越来越智能越来越易操作。智能汽车前两个层次的“辅助驾驶技术”和“半自动驾驶技术”已经得到广泛应用，并成为汽车厂商提升产品档次和市场竞争力的重要手段。当前业界正致力于第三个层次“高度自动驾驶技术”的实用化研发和产业化。沃尔沃推出的堵车辅助系统、奥迪等公司推出的自动转向、加减速、车道引导、自动停车、自适应巡航控制等技术都属于第三层次的智能汽车技术。

图表 2：现阶段智能汽车简要构造

制图：互联网实验室

汽车的智能化是 IT 系统不断接入传统汽车的结果。如上图所示，目前阶段的智能汽车基本都配备了发动机控制系统、车载控制系统、车身控制器、变速箱控制单元等，实现部分操作的智能化控制，并通过 3G、蓝牙等与外部网路连接，通过 V2V 技术实现车与车之间的通信。

与传统汽车相比，智能汽车将给用户带来更好的体验，部分甚至全部的操作可以通过智能系统来完成，降低了汽车的操作难度与使用门槛，被解放的用户可以将事件用于休息、娱乐、办公，提升生活与工作效率。智能驾驶、生活服务、安全防护、位置服务以及用车服务等，都是智能汽车较为成熟的或可预期的功能。智能汽车技术正在赋予传统汽车以新面貌、新活力、新定位，进一步提升车主的生活品质。

目前智能汽车正在形成一股业界热潮，智能化功能在不断拓展，很多汽车厂商、IT 厂商都在该领域不断推出新产品或技术试图在这一蓝海领域占得先机。

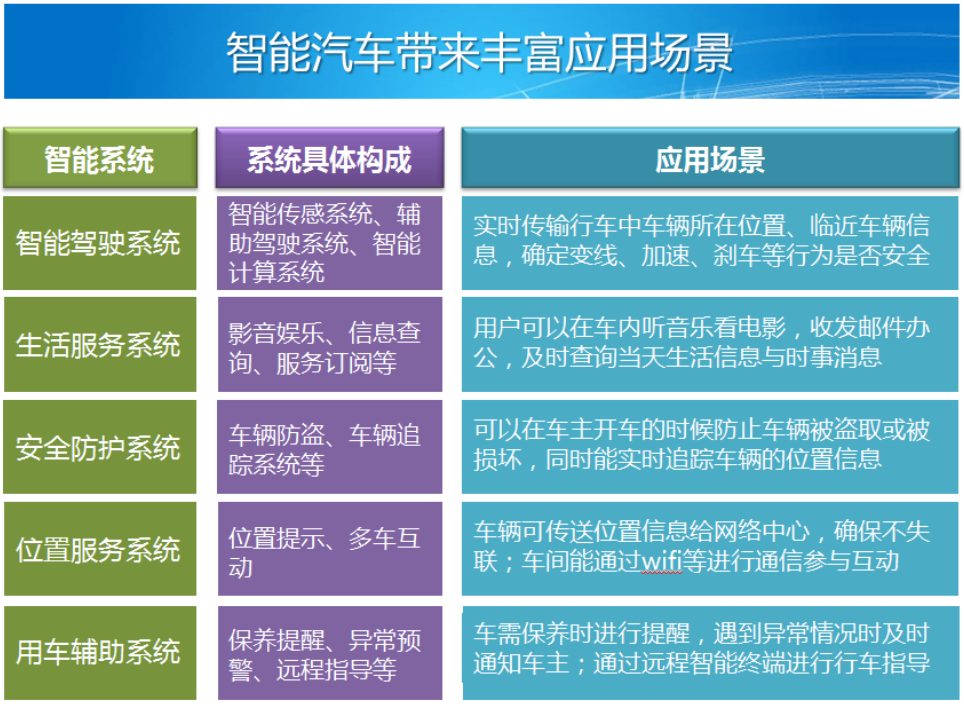
1.2 智能化或将重构汽车产品与汽车行业

传统汽车是一种机械，一种代步工具，使人从长途跋涉的艰辛中解放出来。智能汽车则将重新定义汽车产品，使汽车不再是单纯的代步工具，不仅可以减少汽车的操作难度，使用户更容易、更便捷地使用汽车，更轻松地到达目的地，还可以提供娱乐、办公、生活助手等服务，使用户多功能地使用汽车。智能汽车可以说是汽车的历史性跨越，使汽车不再是简单的代步工具，更是移动的家、移动的办公室。另外，随着与网络更深度、更频繁的连接，汽车也将成为一个网络终端、信息产品。

（1）智能化提升促使传统汽车进化为操作便捷、功能全面的交通、娱乐、办公平台

相较于传统汽车，智能汽车通过提高智能化程度可以给用户带来更大效用。它通过智能驾驶系统、生活服务系统、安全防护系统、位置服务系统、用车辅助系统来提升用户使用汽车的舒适性、便捷性、安全性。

图表 3：智能汽车增强汽车功能提升用户效用



制图：互联网实验室

总结来看，智能汽车给用户增添更丰富的应用场景，提升用户效用。带来的效用增加主要体现在：

（1）更轻松驾驶。通过辅助驾驶系统等使汽车部分操作由人通过智能系统来控制机械系统完成，降低汽车的操作难度，提升驾驶操作的自动化与舒适度，使用户驾车更轻松；

（2）多功能使用。用户可以通过智能汽车更方便地上网浏览信息、收发邮件、听音乐等，全面提升汽车行驶中的乐趣与时间使用效率；

（3）提升汽车安全性。通过智能传感系统、位置服务系统、数据处理系统、网络连接系统等将汽车自身参数与周边环境数据上传至数据中心，数据中心测算出行车中的安全数据并回传至汽车，汽车依据安全数据自动调整行车速度、实施变线、躲避对方等，达到车与周边环境的和谐统一，使行车更安全。

（4）远程控制汽车。通过手机与远程控制系统，人在远离汽车时也能控制汽车，进行开门关门、开关空调等活动，对汽车的掌控力没有了空间限制。

在未来，智能汽车还会有更多颠覆性的应用出现，如无人驾驶，使用户可以从劳累的操作中解放出来；智能汽车可以被用户远程控制来从事更多活动，如用于接受快递、去指定地点接人等。信息技术的功能演进使智能汽车未来具有无限想象力。

（2）智能汽车将成为继电脑、手机、电视之后的又一重要网络终端

汽车智能化水平不断提升给用户带来更舒适的使用体验，汽车厂商与 IT 厂商也加速在智能汽车领域布局，未来用户驾车行为将进一步数字化、网络化、信息化，用户在行车过程中通过传感器、无线网络实现车与车、车与网的无缝网络连接，汽车大量接入网络，并向网络传输数据，同时也从云端接收数据，智能汽车最终会成为继电脑、手机、电视之后的又一个重要的网络终端。

当前的时代是网络化推进的时代，网络全面接管用户的工作与生活。传统的汽车成为新兴的网络接入终端，可以说是汽车产业的一次飞跃。智能化进一步拉近了汽车与用户的连接，使汽车也进入网络化时代，成为收发数据的新工具，在用户生活中的地位也会进一步提升。目前手机是用户使用频繁的网络设备，智能汽车兴起后，用户通过汽车接入网络的时间与频率会不断增长，汽车在网络社会的地位与作用将更加显著。

可以想象，在未来会有更多网络活动通过智能汽车进行，也会有越来越多的针对智能汽车的应用程序、应用商店、智能硬件，并逐步形成一个以智能汽车为核心的生态系统。

1.3 汽车巨头与 IT 厂商角力智能汽车

由于智能化可以给汽车用户带来更大效用，汽车智能化程度在未来很有可能成为衡量汽车性能的重要参数，是夺取未来汽车市场的关键策略。受此影响，在汽车领域智能化正在成为研究的重点。业界广泛引用的数据显示，近年来，汽车产业领域超过 90%的创新都与汽车智能化系统相关[1]。

目前已经有不少汽车厂商通过自主开发或与 IT 厂商合作的方式将先进的信息技术整合到汽车系统中。很多 IT 厂商与汽车厂商为在智能汽车领域占据一席之地，都在进行相关的技术储备或推出各种智能化产品。

[1]数据来源：一汽副总工程师李骏等。http://www.motorlink.cn/html/exhibition/1000013b0061db7f-3-1-38.html

图表 4：部分汽车厂商在智能汽车领域的布局

汽车厂商	在智能汽车领域的探索与布局
奔驰	✧ 推出了与其车型互联的 Pebble 智能手表，可通过振动的形式来提醒驾驶员前方的交通事故、道路修缮以及抛锚车辆等实时路况信息 ✧ 位于硅谷的研究中心正在开发可以令驾驶员在驾驶时更加惬意的接收消息推送的方法
奥迪	✧ 推出一款基于安卓系统的 10.2 英寸车载平板电脑，可通过车内无线网实现与其他乘客间的互动，并为乘车者提供导航、网络浏览、媒体播放等功能 ✧ 奥迪同苹果公司达成协议，将从后年起把苹果 CarPlay 车载操作系统搭载于量产车型
福特	✧ 宣布一系列车载智能系统发展计划，包括导入 MyFord Touch、发布九款基于 Applink 平台智能电话应用，并与百度和中国联通整合更多在福特汽车内可以使用的声控应用程序。 ✧ 先后与微软、索尼合作打造 SYNC 系统以及影音系统，尔后又与谷歌、Facebook 等美国 IT 公司联手开发车载应用。
通用	✧ 拥有安吉星车载信息系统。 ✧ 开发未来意图引擎人工智能技术，能够对以往的驾车操作情况进行分析，结合当前车况和相关数据，推测驾驶者的意图
沃尔沃	✧ 与苹果 CarPlay 和谷歌 AndroidAuto 进行合作 ✧ 发布 SENSUS 创新科技子品牌及相应的智能车载交互系统，可提供包括互联、服务、娱乐、导航、控制在内的车载互联功能。
丰田	✧ 开发了 G-BOOK 车载信息服务系统，通过车上无线通讯终端机来提供互助信息服务，并且能连接各种兼容于“G-BOOK”功能的设备
特斯拉	✧ 推出基于 linux 的操作系统，具有地图、语音识别和音乐等应用 ✧ 配备了具有四级高度调节的空气悬架，在靠近汽车时，可伸缩的车门把手可自动弹出，并且选择了一套德国 BILSTEIN 的空气避震系统。 ✧ 在中央台拥有两个 iPad 般大小的大屏幕，除此之外没有任何其他按键，这块屏幕可以控制特斯拉几乎所有的功能

制表：互联网实验室

可以看到，诸多知名汽车企业已经拥有车载系统，或支持谷歌、苹果的车联网系统，对汽车各类智能化功能进行底层支持，并开始研究一系列语音控制、车主意图识别、用户数据处理等方面的前沿技术，使汽车更智能更理解用户。

图表 5：部分 IT 厂商在智能汽车领域的布局

IT 厂商	智能汽车领域的布局
Google	✧ 推出基于安卓的车载系统，成立“开放性汽车联盟”，其目标是将 Android 系统的体验带到汽车导航和资讯娱乐系统当中 ✧ 开发无人驾驶汽车 ✧ 内置应用商店可以下载相关汽车应用，或者让自己的 Android 设备与汽车相连，实现众多功能 ✧ 谷歌收购在线地图公司 Waze，完善导航服务

苹果	✧ 推出 Car Play 车载系统，通过和手机相连来获得语音搜索和导航服务 ✧ 已与丰田、福特、宝马、雪佛兰、日产等公司达成合作意向，后者已经宣布支持 CarPlay 系统
阿里巴巴	✧ 阿里与上汽集团就“互联网汽车”战略合作，充分集成阿里“YunOS”操作系统、大数据、阿里通信、高德导航、阿里云计算、虾米音乐等资源和上汽集团的整车与零部件开发、汽车服务贸易等资源
百度	✧ 开发一款名叫 carnet 的车载智能平台，可将用户的智能手机与车载系统无缝结合，实现“人、车、手机”之间的互联互通 ✧ 正在进行无人驾驶汽车的研发
腾讯	✧ 发布车联网硬件结合产品路宝盒子与腾讯路宝 APP，能够提供传统的地图导航功能，还可通过云端计算，会产生出对用户非常有用的数据
360 公司	✧ 安全研究团队发现黑客可借此远程控制车辆，操控开锁、鸣笛、闪灯、开启天窗等。目前正在探索进入汽车行业的具体形式，在汽车系统安全领域，360 愿意和厂商进行合作

制表：互联网实验室

IT 厂商入局智能汽车领域的主要举措包括推出车载系统并与汽车厂商合作推广，开发导航、语音识别、娱乐、安全等方面应用程序和应用技术。

可以看到，智能汽车的良好前景已经是业界共识，智能汽车已经在业界形成开发热潮，各方都不希望错过这场汽车与网络信息技术交汇带来的市场盛宴。传统汽车厂商积极探索智能汽车领域，通过推出车载系统等行为加强对智能汽车的主导权；互联网 IT 厂商看到了智能汽车的良好前景，也积极介入智能汽车领域，寄望通过利用自身在信息技术领域的优势开发更智能的车载系统以及提供更丰富的网络内容等手段，试图切入智能汽车领域，甚至有谷歌等 IT 厂商已经在开发无人驾驶汽车。这些布局形成了智能汽车开发热潮，也凸显了业界对于汽车智能化前景的高度认可。

第二章　智能汽车背后的信息安全风险

传统产品在智能化进程中将不可避免地面对信息安全问题。传统的功能手机在智能化之前很少有信息安全问题，智能手机产业爆发以后，随着而来的是大量的手机病毒、恶意攻击、个人资料泄露。汽车业也将如此，在智能汽车全面兴起后，病毒、恶意攻击、隐私泄露等安全问题也将如影随形。

智能汽车在提升交通安全、给用户带来更舒适操控体验的同时，也带来比较严重的信息安全隐患，形成安全悖论。正常运行的智能汽车信息系统会提升乘车安全性，研究表明，在智能汽车的初级阶段，通过先进智能驾驶辅助技术发挥作用，有助于减少 50%-80%的道路交通安全事故[2]。如果实现无人驾驶，甚至可以完全避免交通事故；但信息系统可能出问题，PC 端、手机端的病毒、网络攻击都有可能被复制到汽车领域，如果行驶中的汽车被黑客控制，出现刹车、变线等操作失控等问题，会严重影响用户生命财产安全。

智能汽车存在安全问题已有例证。国内安全厂商 360 发现特斯拉汽车应用程序流程存在设计缺陷，攻击者利用这个漏洞，可远程控制车辆，实现开锁、鸣笛、闪灯、开启天窗等操作，并且能够在车辆行驶中开启天窗。在国外，Charlie Miller 和 Chris Valasek，两位专业黑客曾轻而易举地攻克丰田普锐斯以及福特翼虎（Escape）的核心操作系统，随意篡改刹车、加速以及转向等指令。

智能汽车安全问题不容忽视。因此，智能汽车的发展需要在智能化程度与安全之间做出平衡，没有绝对安全的智能系统，只有在智能化与安全之间找到一个厂商、用户都认可的支点，智能汽车产业才能健康发展。

2.1 风险来源

从根源看，智能汽车的信息控制系统带来了网络连接，隐含了系统漏洞，为安全埋下隐患。从直接来源看，猖獗的外部攻击与用户自身的不当操作（如通过网络不慎下载病毒）都会将以往 PC、手机互联网时代的安全威胁带到汽车领域。

[2]来源：中国汽车报；http://www.cnautonews.com/zlpl/201404/t20140408_300931.htm

图表 6：智能汽车信息安全问题的简要脉络

制图：互联网实验室

2.1.1网络数据交换是产生安全风险的根本原因

智能汽车安全问题的深层根源在于汽车的信息化。智能汽车与传统汽车区别在于安装了传感器、车载软件等电子信息产品，实现了智能化控制。这一过程中伴随着与外部的网络连接和数据交换。智能汽车实现了车与数据中心、车与车之间、车与智能手机等外部硬件的数据交换，这个过程中伴随着风险，使得电脑、手机终端面临的信息安全风险也会移植到汽车领域。同时车载 IT 系统难免面存在漏洞。这就为产生安全问题埋下伏笔。

图表 7：数据流入流出带来智能汽车安全问题

制图：互联网实验室

如图所示，接收的数据包含了从云端下载的内容，网络连接端口处恶意软件植入汽车网络的数据同样可能包含其中，因此大大增加了汽车网络被黑客攻击的风险。

发出的数据包括汽车及用户数据可能需要在云端处理，以便提供包括个性化投保方案、定制资讯内容以及广告等众多服务。如果数据被黑客获取，用户隐私面临泄露风险，如果黑客依据数据对汽车实施攻击，也将加剧安全风险。

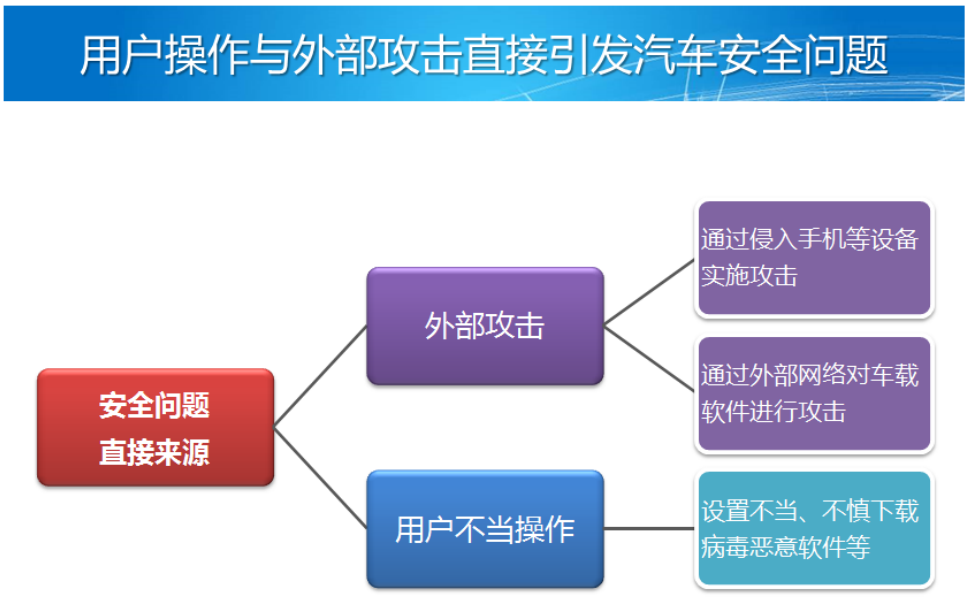
接收的数据包括经 ECU 不同部分计算处理过的数据或流经车载娱乐系统 ECU 的用户数据群。由于接收到的数据可能并不安全，这可能导致数据处理发生错误。同时汽车的联网和信息娱乐系统在受到代码篡改以及用户数据人为操控等作用时很容易出现崩溃。

总之，汽车实现了与外部的网络连接，为病毒木马入侵汽车领域打开了方便之门，也使黑客找到了网络攻击的入口。车载系统技术漏洞的存在则很容易被不法分子利用，进行网络攻击进而达到其控制车辆、窃取隐私等目的。

2.1.2用户不当操作与网络攻击是最直接的威胁

就具体的安全问题来源看，用户的操作与外部攻击都可能给智能汽车带来信息安全问题。将较而言，外部攻击更为频繁直接，也更难以预防。

图表 8：用户的操作与外部攻击直接引发智能汽车安全问题



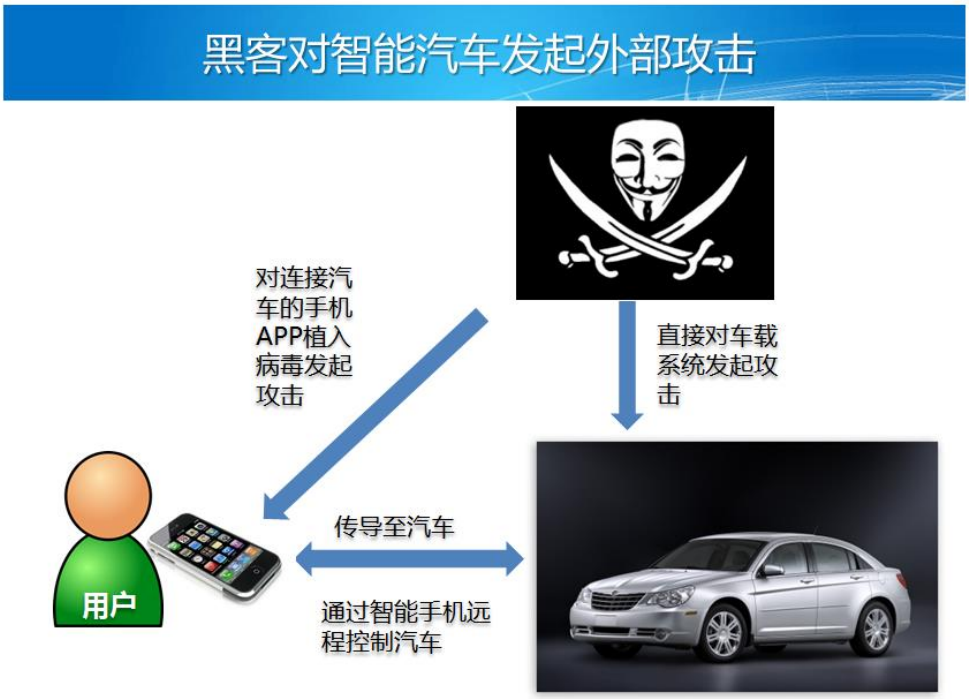
制图：互联网实验室

（1）外部攻击将严重威胁智能汽车安全

黑客通过对智能汽车实施外部攻击可以控制车辆，阻碍其正常行驶，并窃取用户信息。外部攻击

途径包括通过入侵外部连接设备实施攻击、通过外部网络直接对车载软件实施攻击。

图表 9：黑客对智能汽车发起外部攻击的途径



制图：互联网实验室

通过入侵外部连接设备来实施的攻击目前来看主要是通过控制智能手机实施的攻击。特斯拉汽车就是通过手机应用程序来远程控制汽车，进行开启车门、开关空调等操作，黑客可以通过攻击手机应用程序来控制智能汽车。未来随着智能可穿戴设备的快速发展与普及，智能眼镜、手环、车钥匙等便携式可穿戴设备也可以与汽车实现连接，对汽车进行控制。黑客也可以通过攻击这些设备达到其非法目的。

通过汽车的外部连接设备（如智能手机）实施的攻击模式可以有很多种，比如向与汽车连接的智能手机植入病毒，通过网络连接将病毒传导至汽车，进而影响汽车信息系统正常运行；还可以发掘智能手机应用程序存在的漏洞并加以攻击，以智能手机为跳板，外部攻击者给车载设备和车载导航仪系统造成损害，或是经由智能手机泄露车内信息，侵犯驾驶员的隐私。

除了通过入侵外部连接设备，恶意攻击者远程可以通过网络直接对智能汽车展开攻击。现阶段汽车上有很多使用通信的装置，例如智能钥匙、轮胎压力监测系统（TPMS）、路车间通信等。这些使用短距离无线通信的功能，就有可能受到通信被窃听、被恶意中断等威胁。 而且目前汽车连接外部网络的环境日益完善，汽车可以通过 3G 等方式实现网络连接，未来可鞯会出现 WIFI 连接网络等形式，网络连接越来越通畅、便捷，恶意攻击者也就有更多的机会进行恶意侵入。另外现在车载信息服务开始普及，从外部网络实施攻击的威胁已成为现实。未来专门针对汽车的 APP 将会越来越多，不法黑客也会有越来越多的攻击点可选择。

国外已经对智能汽车外部攻击有很多研究。例如，美国研究人员返现，黑客通过胎压力监测系统（TPMS），可以伪装 TPMS 的压力报告消息，随时点亮警报灯。另外研究显示，攻击者为实施远程攻击，利用逆向工程技术，通过解析通信及信息终端，开发出了针对特定车型的入侵代码和可执行代码。

通过外部攻击，黑客可以制造的威胁包括三大类：控制、篡改、窃取。

图表 10：外部攻击带来的直接威胁

威胁类型	威胁形式	具体威胁
控制汽车系统	DoS 攻击	通过非法或过多的连接要求造成系统瘫痪、服务受阻的威胁
	非法利用	无正当权限者通过伪装和攻击产品漏洞，利用汽车系统功能的威胁
篡改	非法设置	无正当权限者通过伪装和攻击产品漏洞，非法变更汽车系统设置数据的威胁
	虚假消息	攻击者通过发送虚假消息，使汽车系统执行非法动作和显示的威胁
	记录丢失	删除或篡改操作记录等，使用户之后无法查看的威胁
	非法转播	通过控制通信途径，劫持正规通信、夹杂非法通信的威胁
窃取泄露信息	信息泄露	汽车系统中应当受到保护的信息落入非法人员之手的威胁
	窃听	车载设备之间的通信、汽车与周边系统的通信遭到窃听、截取的威胁

制表：互联网实验室

通过网络攻击，黑客可以控制智能汽车部分功能，修改设置，向汽车发出错误指令，这些都会令车主陷入危险境地；黑客的窃取隐私、窃听行为也使车主的个人信息保护面临尴尬。

（2）用户不当操作带来风险

用户本身的操作也会带来安全风险，情形主要包括两种：一是用户经由汽车内的用户接口，错误实施操作、设置引发的威胁；二是通过用户从外部带入的产品和记录介质，车载系统感染病毒和恶意软件引发的威胁。

智能汽车是个非常复杂的技术体系，包含多种信息控制系统，每类系统会有不同的安全参数设置，如果用户的设置不符合安全原则，可能会影响系统正常运行，带来安全隐患。当然，只要用户合规操作，这类风险可以避免。

用户不慎使系统感染病毒与恶意软件将使汽车陷入危险境地。虽然目前针对智能汽车的病毒尚未出现，但这是基于智能汽车尚未普及的原因。未来随着市场上智能汽车存量的增大以及用户使用汽车智能系统频率的增加，针对智能汽车实施攻击越来越有利可图，专门针对智能汽车的病毒与恶意软件也一定会出现。未来用户在智能汽车上会有很多网络操作，如观看视频图片、收发邮件、通过应用商店下载 APP 等，都隐藏着被病毒感染的风险。

2.2 风险表现：带来人身安全、隐私、经济损失等诸多危害

国内安全厂商 360 公司发现特斯拉应用程序漏洞的消息引发了业界关于智能汽车安全的大讨论。汽车的智能化为生活带来方便的同时，也为黑客提供了更多的攻击对象。一旦智能汽车被黑客控制最后失去的就可能是用户宝贵的生命。从这个角度看，智能汽车信息系统出现安全问题其危害将远超以往 PC、手机互联网时代。智能汽车的安全性必须在产业发展之前加以深入研究。

总体来看，智能汽车潜在风险体现在用户人身安全、隐私、经济利益三方面。

图表 11：智能汽车带来的三类安全问题

制图：互联网实验室

（1）人身安全类

智能汽车引发的人身安全问题是指智能汽车信息系统被病毒感染、被黑客攻击，出现拒绝服务、失去控制等状况，影响用户人身安全。

具体来看，有些安全漏洞将削弱关键系统的安全性，将乘车人、外部行人和周边环境置于危险当中，可能导致的后果包括在驾驶途中突然熄火、车辆行驶中被黑客控制肆意改道等。黑客控制车辆就等于是放任汽车被别人驾驶，将车在没有人的情况下开到别的地方去，驾驶中可进行急转弯，急刹车，

急加速，爆胎等操作。

还有一些非关键安全系统受影响将导致汽车拒绝服务或进行不必要的操作。如造成刹车失灵，选择性爆破轮胎，停止发动机，而且有可能在车内绕过基本的网络安全保护，在车内恶意地桥接两个内部子网。

此外，在尚未实现完全无人驾驶的智能汽车内，随着车内娱乐、办公功能的丰富，用户极有可能在驾驶过程中出现注意力不集中，进而出现车祸事故。

上述问题都会导致汽车行驶过程中用户对其失去控制，给用户造成人身伤害，甚至使用户失去生命。

（2）隐私类

隐私类风险指的是安全漏洞可能导致个人信息、车辆信息被窃取，并被滥用或篡改。中国工程院院士郭孔辉透露的数据显示，目前智能汽车上至少有超过 80 个智能传感器，每天向智能汽车云端传输的数据达到 100 兆，这些数据涵盖了汽车和驾驶者个人的各类信息，包括位置信息、操作记录、驾驶习惯等。如果信息泄露，意味着用户隐私被侵犯。

智能汽车运行形成的数据类型众多数量巨大，通过对各类数据进行分析，可以对车主与汽车形成较为完整的形象素描，进而可以进行隐私泄露和特定攻击等行为。总体而言数据可以分为事关用户的数据和关于车辆的数据。

图表 12：智能汽车形成的数据

	数据类型	数据具体内容	通过分析可获知的信息
关于用户的数据	用户信息	用户（驾驶员和乘员）的个人信息、认证信息、缴费信息、使用记录和操作记录等	对用户基本情况可以形成初步认识
	用户关注内容	视频、音乐、地图之类的应用数据	通过分析这类数据可以知晓用户在娱乐等方面的喜好
关于汽车的数据	基本控制功能的运行	基本控制功能的连贯性和可用性，基本控制功能的执行环境和使其运行的通信	汽车的性能，智能信息系统的运营状况，据此可做针对性攻击
	汽车固有信息	包括汽车车体中固有的信息（车辆 ID、设备 ID 等）、认证信息码、行驶及运行记录等积累的信息	车辆基本信息，可以对车辆进行身份识别、定位
	汽车状态信息	表示汽车状态的数据、位置、车速、目的地等	汽车行驶中，通过这些数据可以更加精准地实施攻击
	软件	ECU 的固件等关系到汽车基本控制功能和扩展功能的软件	汽车的智能化程度
	设置信息	硬件和软件的运行设置数据	汽车软精件具体的设置情况，可发现用户的使用偏好

制表：互联网实验室

可以看到，智能汽车运行会产生各种类型的数据，涉及到汽车硬件配置、软件信息、系统设置、用户个人信息等多个层面，如果这些数据被盗取，可以对用户形成较为精准的形象素描，进而可以对用户形成深层次骚扰，如以隐私泄露相要挟、利用行车信息向用户发出恶意广告、利用车辆软硬件信息与用户操作习惯实施网络攻击等。

（3）经济类

经济类风险指用户可能遭受经济损失，包括篡改授权或敲诈勒索等形式。在无人驾驶过程中，黑客可将车辆行驶到无人寻到的地方从而进行敲诈勒索车主的行为，或者直接把车辆占为己有也是有可能的，这都给车主造成了经济损失。

另外值得注意的是干扰胎压监测系统，提示驾驶员胎压有问题，让驾驶员产生心理恐慌。国外有研究显示，通过异常胎压导致汽车爆胎，爆胎情况下会紧急制动，再加上气囊弹出把门打开，可确保人安全地出去。由于在这个过程中都是以一种假象出现的，所以这时黑客可进行偷车等行为。

可以发现，与 PC、手机互联网时代相比，汽车智能化、网络化将可能给用户人身安全构成严重威胁，这是以往的信息安全问题所不具备的危害。如果车辆因被黑客控制出现撞车等事故，造成的经济损失也非常大。未来智能汽车如果出现安全问题，其危害将远超 PC、手机互联网时代。

2.3 风险走向：市场爆发将伴随安全问题的大爆发

在未来，智能汽车爆发产品实现普及后，攻击智能汽车对黑客越来越有吸引力，而网络连接的增多也将加大感染病毒的风险，另外车载系统的统一与开放使病毒与恶意攻击的打击面增大，如果智能汽车领域的安全防护做得不够好，安全问题会快速增长。

图表 13：智能汽车的崛起将伴随着安全风险的增加

制图：互联网实验室

2.3.1使用量越大，数据积累越多，对黑客的吸引力越大

不法分子攻击智能汽车，原因主要来自于三点：炫耀技术、打击车主、谋取经济利益。未来随着智能汽车市场的爆发，这个三方面动机都有可能被不断激发出来，针对智能汽车的攻击将越来越多。

第一，汽车智能化是大趋势，未来智能汽车保有量将不断增加，智能汽车这种产品的影响力也将越来越大，成为一种重要的信息终端。对于要炫耀技术的不法分子而言，攻破智能汽车信息系统意味着较高的成就感，这将刺激部分黑客发起针对智能汽车的攻击；

第二，随着智能汽车的普及，智能汽车越来越成为大众产品。意图攻击车主的犯罪行为也会由其他领域转移到智能汽车。对汽车的攻击成为谋财害命的手段；

第三，智能汽车大量普及，车载数据越来越庞大。在未来的大数据时代，巨量的用户数据将会是重要的资产。通过盗取用户数据进行分析会成为一条灰色产业链。车载数据涉及到用户日常的车辆信息、车主信息、行车路线、日常喜好等，对于黑客来说，可以通过售卖车主各类数据来牟利。基于此，以盗取隐私数据为目的的黑客行为也会越来越多。

以上三种动机不断发酵，将使越来越多的不法黑客将犯罪触角延伸到智能汽车领域，对于智能汽车的攻击会越来越多。

2.3.2网络服务越频繁，外部数据接收越多，感染病毒风险越大

随着智能化的提升，汽车与外部的联系越来越多，积累的数据越来越多，风险也会大量增加。智能汽车发展使车载数据密度巨变，将加剧智能汽车安全风险的自增长趋势。

在智能汽车上，电控单元将与控制器局域网、车载网络标准及内部互联网等汽车网络相连接，从APP、应用商店等处接受数据，也将与提供自动紧急呼叫系统、远程诊断和数据交换等功能的车内电子设备和汽车制造商端口的连接，实现行车信息与数据的接收，未来还会实现车与车之间的相互通信，进行操作系统生态数据的无缝交换。随着信息娱乐系统和连通性技术的不断改进，车载数据在数量和方向上将发生很大改变，驱使智能汽车安全风险急速增长：

在数量上看，车载数据将随着用户使用的增加而大幅增长，达到惊人的量级；从方向上看，从外部接受的数据会越来越多，包括来自网络内容服务商的数据、来自汽车厂商安全控制中心的数据，来自网络运营商的数据，等等。

未来的智能汽车将是一个数据收发器，每时每刻都接受大量数据，联网的加深与数据的流动都会加深智能汽车的信息安全隐患，大量使用网络将加大感染病毒与恶意软件的风险，接收的数据中可能含有病毒木马、恶意广告等恶意程序。

2.3.3车载信息系统的开放与统一将放大智能汽车安全风险

目前车载信息系统格局较为分散，很多汽车厂商都有自己的一套技术标准与产品体系，这在一定程度上抑制了产业发展，但也加大了黑客破解的成本。随着汽车越来越智能化，智能汽车将越来越符合 IT 市场格局的规律---“70-20-10”法则，即市场越来越集中于一家独大的厂商，份额达到七成左右，处于次席的厂商能拥有 2 成左右的份额，其他厂商占据剩下的 10%份额。也就是说市场上的信息系统产品与技术标准将越来越趋向于统一。同时由于 IT 厂商不会直接去造汽车，更多是会和汽车厂商合作，这就使得车载信息系统越来越开放，为更多厂商所使用。

这种情形有利于智能汽车市场的快速崛起，但在一定程度上不利于安全防护。车载信息系统的开放与统一将使黑客实施破坏的平均成本降低，也使单个病毒或恶意攻击的影响面极大拓展。一种病毒可能会影响使用相同系统的几万辆汽车。

2.4 安全与智能，智能汽车产业发展的平衡之战

汽车智能化正在成为业界热潮和重要趋势，正在重新定义汽车行业。未来智能化程度还会成为用户选购汽车的重要指标。但由于智能汽车出现问题可能导致用户生命财产受到严重威胁，安全也会和智能化一样成为未来智能汽车产业发展的重大主题，只要实现安全与智能的平衡，智能汽车产业发展才能又快又好。

（1）信息系统安全性将与智能化程度并驾齐驱，成为判断汽车竞争力的重要指标

汽车智能化可以显著提升用户效用，使汽车更能满足用户在网络时代的全面需求。但智能汽车潜在安全问题不容忽视，车联网时代安全问题严重性远远超出了以往 PC、移动互联网时代的安全问题。用户显然会注意到这一点。着眼于未来汽车用户的需求，智能汽车需要在智能与安全之间做出平衡。

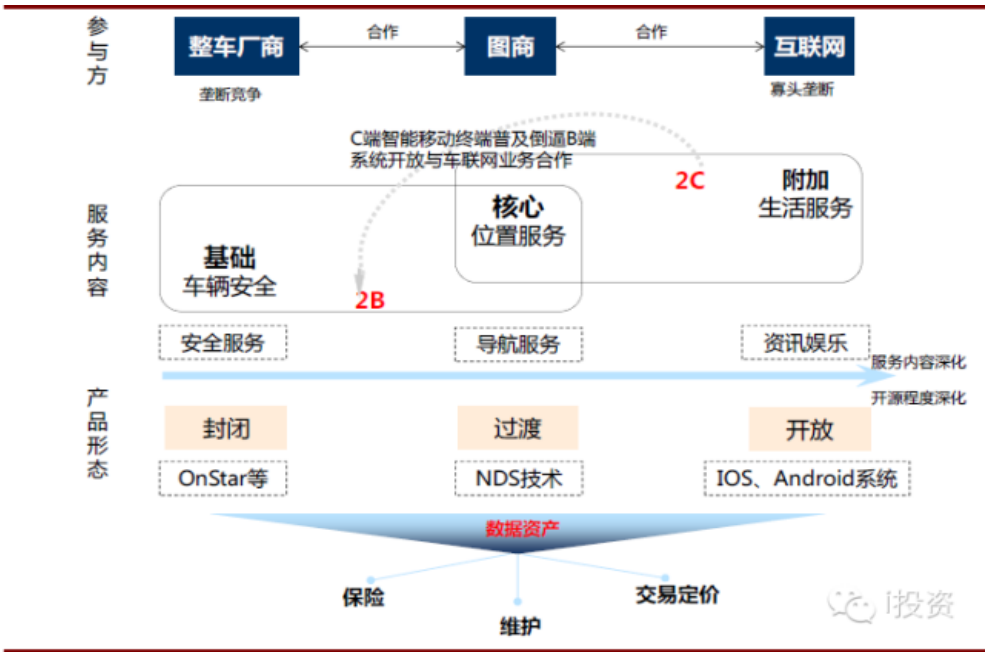
对于用户而言，令人眼前一亮的智能化功能当然很具吸引力，但用户显然也会关注安全问题，尤其是智能汽车涉及人身安全，不可不防。在 PC、手机互联网时代虽然也有比较严重的信息安全问题，但基本不会造成人身伤害，经济损失也往往有限，用户不会因安全问题而不使用 PC、手机。但智能汽车时代不会如此，如果安全程度不够将会影响生命安全。在未来智能汽车时代，用户对安全的关注度将超过以往 PC、手机网络时代。由此，智能化与安全都将是用户选购智能汽车时需要关注的最重要指标。重智能轻安全将无法有效获得用户青睐。

（2）IT 安全厂商未来将是智能汽车生态系统重要一环

围绕智能与安全的主题，未来智能汽车生态系统将包括整车厂商、零部件厂商、传感器厂商、操作系统/车载系统厂商、芯片厂商、汽车信息安全解决方案厂商、汽车应用程序开发商、网络运营商等多个主体。

在生态系统中，整车厂商、零部件厂商提供汽车的物理结构，传感器厂商提供识别、信号传输等服务，操作系统/车载系统厂商与芯片厂商提供汽车信息系统的底层构架，汽车信息安全解决方案厂商提供信息安全保障服务，汽车应用程序开发商为用户提供网络内容，网络运营商提供网络数据服务。

图表 14：智能汽车生态系统简图



来源：宏源证券研究所

在未来，安全厂商将在智能汽车生态系统中发挥重要作用。在智能汽车时代，不但要考虑汽车自身的物理安全，还要考虑软件层面的安全，即智能化背后所带来的信息安全。汽车越智能、越科技也意味着所面临的信息安全风险因素也就越多。汽车智能化无法绕过安全性问题。传统汽车厂商在汽车物理安全方面拥有多年的技术和数据积累，但在防范信息领域的病毒和网络攻击方面缺乏足够的优势。在未来会出现专门针对智能汽车与车联网的病毒，也会出现针对汽车信息系统的 APT 攻击，传统汽车厂商在这方面缺乏足够的经验，而这方面恰恰是 IT 安全厂商的优势。在 PC、手机互联网安全方面，IT 安全厂商已经积累了足够的技术、人才、数据优势，可以为智能汽车安全保驾护航。

第三章　构建智能汽车产业安全防护体系

目前国外对于智能汽车安全方面的探索处于初级阶段，还没有形成制度化、体系化的安全保障措施。鉴于安全主题在智能汽车领域的重要性，我国有必要加强研究，提前探索智能汽车的安全保障技术。

3.1 智能汽车安全领域的全球探索

在国外，随着智能化程度提升，一些安全隐患开始被黑客发掘，政府与议会等公共部门、行业组织、企业界都开始关注智能汽车安全，并有了一些初步探索。总体来看，业界对于智能汽车信息安全系统的探索目前还处于初级阶段，法规、行业标准、技术、产品还都未形成体系，这与智能汽车当前的发展状况密不可分。由于智能汽车远未普及，产品与技术都在探索中，政府、行业组织、企业目前考虑重点仍在于如何将智能汽车行业发展起来，安全还未提上重要议事日程。这就决定了目前全球智能汽车信息安全探索呈现零散化、碎片化特征。

具体而言，政府、议会等公共部门希望通过汽车智能化来减少交通事故，提升行车安全性，企业希望推出的智能汽车产品可以引爆市场需求，形成消费热点，行业组织希望某项标准或核心产品获得推广，各类主体对于信息系统安全的关注蕴藏于产品发展之中，并未与智能汽车发展摆在同一重要性级别上。

3.1.1公共部门对智能汽车安全的探索尚处于早期阶段

由于智能汽车在全球来说都是新兴事物，各国对于智能汽车安全的探索多限于业界，政府对此尚未有更多动作。主要国家政府对于智能汽车安全还没有系统的顶层设计出现，只有一些零散的规定。

（1）美国

在美国，智能汽车安全正在引起政界关注，包括参议院、FBI、国家公路交通安全管理局等都对智能汽车安全性表达了关注。

图表 15：美国公共部门在智能汽车安全领域的主要动向

机构或人物	主要动向
美国参议院商业委员会主席、参议员洛克菲勒	其向通用、丰田、谷歌、三星电子、美国电话电报公司以及苹果公司官员提请注意，表示他会加快车载技术标准的制定与实施，并建议规范手机与汽车娱乐系统互联在车内的使用来尽可能减少分心驾驶。
FBI	FBI 怀疑智能汽车的安全性，认为无人驾驶汽车可能在几年内可能被利用作为致命武器。无人驾驶汽车可能被犯罪分子控制，影响执法行为且执法对象可能使用这类汽车进行对抗。
国家公路交通安全管理局（NHTSA）	美国目前禁止无人驾驶汽车公开发售。NHTSA 公布了无人驾驶汽车规定，要求它们仅限用于测试，并且要求司机可以控制临时出现的故障[3]。

制表：互联网实验室

（2）英国

在英国，政府虽然已经允许无人驾驶汽车上路，但英国监管部门要求上路的自动驾驶汽车必须有人监控，并且随时可以切换到人工驾驶模式，以保障安全。

（3）日本

日本在无人驾驶汽车上路方面也比较保守。日本权威的国立研究机构----信息通信综合研究所研究员山口平八郎认为，实现自动驾驶还必须解决以下课题：一是完善法律。自动驾驶汽车发生事故应该由谁负责很难确定。针对事故的“汽车保险”也必须做出相应的改变。二是技术与安全。自动驾驶汽车与手动驾驶汽车在道路上共存可能带来问题。在十字路口右转弯等情况，手动驾驶司机是通过相互沟通来防止事故的，而自动驾驶汽车是通过道路基础设施传来的信息做出判断。除了自动驾驶汽车相互之间，还要开发人与自动驾驶汽车沟通的手段4。

可以发现，国外公共部门对于智能汽车安全目前多处于关注状态，没有系统性的政策出台，仅对市场关注度高的无人驾驶汽车有一些硬性规定，对于智能汽车信息系统的防护标准、智能汽车消费者权益保护等方面还没有专门的措施出台。

3.1.2企业界通过设置防火墙、严审应用程序等加强安全

（1）IT 企业：在车载系统、安全解决方案领域积极布局

很多 IT 企业将智能汽车作为下一个战略级市场，积极布局，相继推出车载系统、应用程序、安全解决方案等。相对于发展而言，安全是一个相对较小的关注点。

[3]来源：http://finance.chinanews.com/auto/2013/06-08/4910279.shtml
[4]来源：http://news.xinhuanet.com/world/2014-08/04/c_126827625.htm

图表 16：国外 IT 企业在在智能汽车安全领域的探索

IT 企业	在智能汽车安全领域的探索
苹果	加强对应用程序的审查
微软	使用 Mirrorlink 标准帮助智能手机与车载系统进行有效连接
英特尔	启动名为“保障联网汽车安全”的研究项目
VisualThreat	推出第一款针对智能汽车行业防 OBD2 攻击的智能汽车防火墙

制表：互联网实验室

苹果、谷歌、微软等企业发布应用了于智能汽车的操作系统。苹果于 2014 年 3 月推出 carplay 车载系统，以 Siri 语音助手为核心,将用户的 IOS 设备与车载设备相连接，可帮助车主安全驾驶,直接语音操作电话、短信、地图、音乐等服务。在安全方面，苹果突出对应用程序的审查，每一个 iOS 应用都得到过苹果 CarPlay 的批准，虽然 CarPlay 支持第三方应用，但需要面对严格的认证机制，应用首先需要经过 iOS 端认证、再进行 CarPlay 认证。目前只有少量的应用被 CarPlay 批准。

相比之下，谷歌推出的车载系统 Android Auto 其 SDK 完全开放，鼓励软件厂商加入，开发环境也相对自由，谷歌应用程序开发的干预很少，应用质量、设计语言是否统一，可能形成安全隐患。

微软也发布了新一代的车载系统 Windows in the Car。工作模式与苹果 CarPlay 基本一样，直接将智能手机操作界面投影到车载控制台上。该系统使用了 Mirrorlink 标准，这项协议可以帮助智能手机与车载系统进行有效连接。

移动安全供应商 VisualThreat 推出了第一款针对智能汽车行业防 OBD2 攻击的智能汽车防火墙产品。VisualThreat 于 2013 年创建于美国硅谷，是一家车联网安全防火墙提供商；

英特尔发布车载系统解决方案，并启动名为“保障联网汽车安全”的研究项目，这种技术可以与 IntelSecurity 提供的迈克菲(McAfee)技术一起使用。

总体来看，大型 IT 厂商如苹果、谷歌、微软等非常重视智能汽车领域，并试图将在电脑、智能手机领域的安全方案复制到汽车领域，对汽车领域的安全问题还没有专门的解决方案，安全探索还处于初级阶段。一些创业型公司 VisualThreat 已经开始在车联网安全领域推出专业防护产品，相信未来 IT 巨头也会逐步跟进。

（2）汽车企业：通过设置防火墙、审核应用程序等措施保障安全

汽车企业也看好智能汽车前景，通过自主研发或与 IT 企业合作等形式提升汽车的智能化程度。安全是信息化过程中的一个关注点，目前已有的安全措施包括设置防火墙、提高汽车应用程序安全要求等，但目前还并未形成规模化的智能汽车安全防护措施体系。智能汽车安全仍在探索阶段。

主流厂商发布的车载系统安全特点如下：

图表 17：主要车载系统安全保障情况

车载系统	安全保障
沃尔沃 Sensus 智能车载交互系统	该系统基于对大量真实交通场景的研究，以及长期来对用户驾驶习惯的研究和对消费者需求的把握。未来基于 Sensus 系统、汽车互联技术和云技术，海量数据可进行统一收集和实时的分析处理，创造更安全的运行环境。
福特汽车先后与微软、索尼合作打造 SYNC 系统以及影音系统	福特汽车就曾在 SYNC 系统中采取大量安全措施，其中包括只允许用户安装福特批准的出厂软件和安全设置，要求客户上网时输入随机给出的密码。汽车在路上行使时，为保护驾驶员安全，WiFi 热点功能会被激活，福特汽车还在 SYNC 系统上使用两款防火墙，一款类似于家庭 WiFi 路由器，一款为独立的 CPU，用来防止车内非法信息发送到其它模块。
通用 onstar 系统	通用向开发者开放数据接口，致力于打造开放平台。所有应用都必须符合两项特定要求：第一，应用必须符合美国国家高速公路交通安全管理局有关安全驾驶的规定；第二，应用必须提前说明，将会收集车辆的什么数据，如何利用这些数据，以及将为外部应用和服务提供什么样的访问权限。存在隐私权问题或导致安全问题的应用无法得到批准。

制表：互联网实验室

可以发现，汽车厂商通过严格审核认证应用程序、设置防火墙等措施来保障智能汽车信息系统的安全性。

另外，汽车的智能化不仅需要 IT 系统，还需要传感器、摄像头等其他设备。沃尔沃、奥迪、奔驰、宝马、丰田、日产、福特等汽车巨头在技术装置方面主要采用常规的雷达（厘米波、毫米波、超声波）相机（立体、彩色、红外）传感器（雷达、激光、超声波）摄像机等进行环境感知和识别，通过基于智能汽车的协同式辅助驾驶技术进行智能信息交互，结合 GPS 导航实现路径规划，且更加注重机电一体化系统动力学及控制技术的研发。

汽车厂商在研发智能汽车的过程中也设置了初步的安全控制措施，但这些措施还不够深入。目前智能汽车联网程度不够，面对的黑客攻击不多，病毒也还没有出现。智能汽车大量普及后可能会出现专门针对汽车的病毒和恶意攻击，汽车厂商目前的安全防护措施是否足够有效还不得而知。

3.2 我国智能汽车安全保障策略建议

智能汽车仍处于发展初期阶段，产品远未普及，很多安全问题也尚未显现，对于行业安全政策不必操之过急，但需要提前加以研究。信息技术发展速度很快，智能汽车市场爆发可能只需要两三年时间。达到一定普及度后，安全问题会越发凸显。如果没有技术与制度预案，可能会有一批智能汽车安全事件出现。我国需要对智能汽车的信息安全问题提前加以研究，做好预案。

我国智能汽车产业安全体系建设应充分发挥政府、行业组织、企业、用户等多方力量，形成合力，共同维护这一新兴领域的安全运行，并在新的产业发展机遇中实现健康发展。

3.2.1政府层面：推动安全软件预装与云安全系统的建立

通过总结国外状况可以发现，对于智能汽车安全，全球都在初步探索阶段，发达国家也并未大幅领先我国。我国应抓住历史机遇，在智能汽车安全领域形成技术与产品优势，使我国在未来智能汽车市场占有一席之地。应当看到，我国在整车研发制造、关键零部件研发制造、车载系统等关键领域都不具备足够优势，安全是我国在智能汽车领域需要紧紧把握的战略机遇。安全未来将是与智能化并重的智能汽车发展主题，而我国安全厂商在用户个人信息安全领域有足够优势，我国需要把握行业机遇，，对安全技术与制度方案提前加以研究，为行业爆发后的立法、监管做好准备。

在具体策略上，未来我国可以考虑统一智能汽车相关技术标准；明确将智能系统出现的问题列入三包系统；充分发挥车险在防范、处理智能汽车的作用；通过启动专项等方式支持国内安全厂商进入智能汽车领域。

（1）出台智能汽车领域相关安全技术标准，推动智能汽车上市前预装安全软件，并接入云安全系统

主管部门应跟进智能汽车领域的发展前沿动态，在智能汽车尚未普及之前就将安全技术的普及推广提上日程，争取形成较为成熟的、经验证可靠的行业标准，对智能汽车生态圈形成良性引导，使生态系统内成员都更加重视安全技术，也能依据行业标准形成可靠。可行的安全技术，为智能汽车安全保驾护航。

智能汽车安全问题主要来源于病毒、恶意软件、网络攻击。安全软件在 PC 和智能手机领域对于这些威胁起到了很好的防护作用。在智能汽车领域，也需要安全软件发挥作用。政府可以推动安全软件在智能汽车上的预装工作，鼓励企业建立云安全系统，并推动各系统之间的信息共享。

仅有安全软件还不够，还需要将汽车安全信息、攻击者信息、各种病毒数据上传至云安全平台，对各类数据进行系统分析，总结特点，对安全问题作出解读、预测，更好地左海安全管理工作。

（2）通过开展专项研究等形式启动对智能汽车安全领域的研究

目前国内安全厂商在智能汽车领域的布局还不多，这对于未来智能汽车用户比较不利。政府可以通过启动专项研究等形式鼓励国内安全厂商加速在智能汽车安全领域的研发与产品推广力度，使更多的在安全领域具有优势的安全厂商进入到智能汽车生态系统中来，推出适合汽车安全的产品，保障智能汽车安全。

智能汽车安全不仅需要汽车厂商增加信息系统的安全性，也需要第三次安全厂商提供防御网络攻击、及时发现漏洞等服务，智能汽车安全本质上属于个人级用户安全，我国安全厂商在这一领域有明显优势，可以充分发挥 360 等公司的技术优势，为智能汽车用户提供保障。

（3）智能汽车系统安全应纳入汽车“三包”

鉴于智能信息系统在汽车价值中的地位越来越重要，同时汽车智能系统也是新生事物，有别于以往的硬件质量问题，为维护用户利益，督促汽车厂商提升信息系统的安全性，有必要将智能汽车系统安全纳入“三包”。

智能汽车系统如果遭到黑客攻击而发生安全事故，属于第三方造成的问题，但也有汽车厂商背身系统存在漏洞的问题，汽车厂商不应以第三方攻击来推卸责任。将智能汽车系统安全纳入“三包”。可以督促汽车厂商开发更为安全、不易被攻击的控制系统，保障用户安全。

当然，具体问题非常复杂，智能汽车乃至无人驾驶汽车出现车祸如何确定责任等问题都需要有关部门提前加以研究，避免出现问题后没有规定可以参照。

（4）通过车险保障智能汽车用户利益

通过设计专门的保险产品来保障智能汽车用户的利益也是值得推广的方案。随着保障水平的提升，汽车智能系统遭受网络攻击总体来说会是小概率事件，可以通过保险产品来补偿受损失用户的利益。

目前已经有保险公司洞察到了市场的新趋势，专门服务于智能汽车的险种可能会出现。平安保险表示，以后会有专门针对智能汽车的险种。对于目前的智能汽车用户，如果用户加入外部设备后导致安全问题，保险公司已经有对应险种，而且汽车险种都会根据市场情况及时做出调整。当然对于智能汽车保险，更多保险公司选择观望，毕竟是技术问题、前沿问题，还需要进一步观察和探索。

在未来的智能汽车市场上，随着行业的进一步明晰，在市场激励和支付推动下，相信会有越来越多的有针对性的保险产品出现。有关部门可以组织业界对智能汽车保险前沿问题提前加以研究，如是否需要推出智能汽车强制险等。

（5）构建良好的漏洞发布机制

乌云网等漏洞发布平台聚集了我国比较有技术实力的白帽黑客，集中发布信息领域的技术漏洞，使各互联网平台及时修补出现的漏洞与设计缺陷，为维护我国网络信息安全发挥了独特的积极作用。在未来的车联网领域，也需要这类平台发挥积极作用，通过白帽黑客对漏洞的及时发掘、漏洞平台的及时发布，提醒汽车系统厂商及时修补，避免可能的安全问题出现。

（6）驾照考试科目应增加关于智能汽车安全相关的内容

汽车在智能化进程中，用户应当了解必要的安全知识，尤其是智能信息系统方面的设置、操作等具体细则，以便正确地使用智能系统。因此，在驾照考试科目中，应增加汽车智能系统远离、合理使用智能系统等内容，使用户对于智能汽车安全防护做到心中有数。

3.2.2企业层面：汽车生命周期全过程安全管理、推广APP白名单

（1）智能汽车策划、开发、使用、废弃的全过程都要着重考虑安全因素

智能汽车厂商应当进一步主动探索安全技术，提升信息系统的安全保障水平，从根本上保障汽车安全。在汽车从策划、开发、使用、废弃的各个阶段，都应坚持安全原则，加强安全管理。

在策划阶段，对于将要开发的系统，结合其使用方法和使用的信息，定义安全要件，应对与新技术相关的威胁。在项目外包过程中，要确定外包开发时的签约规则、能担保人员和委托品的安全品质的规则及筛选方法；

在开发阶段，要结合安全功能的安装方式和日志收集方式等进行设计，利用可防止漏洞出现的安全编码和编码标准，在测试环节利用源代码的复查和模糊测试等方式检验；

在使用阶段，要构筑发生事件时能快速采取应对措施的联络体制，要向用户和汽车相关人员提供信息，探讨在发现漏洞时向用户发布安全补丁和信息的方法，充分利用漏洞相关信息，合理使用漏洞相关信息，防止已经发现的漏洞再发、减少漏洞对于相关系统的危害。

在废弃阶段，应制定相应的废弃方针等，如在汽车废弃时提供信息删除功能，防止用户信息等落入他人之手，并公开删除方法。

通过智能汽车从策划到报废全过程的安全管理，可以在各个环节形成安全防护，尽最大可能消除安全隐患。

（2）通过减少接口等形式构建网络安全系统架构

在系统设计上，可以考虑减少接口的数量打造控制中心等形式，形成网络安全系统架构以及有效的工程解决方案。

安全漏洞随着允许汽车与外部设备或网络连接接口数量的增加而逐渐增多。对于汽车厂商而言，关键的安全架构方式是：减少接口的数量，并将剩余的接口整合成一个“控制中心”，而该“控制中心”将作为连通汽车内部网络和外部设备/网络之间安全、智能的大门。采用这种方式可以更好地保护汽车不受恶意软件的攻击，同时也阻止了敏感信息的内输和外露。

“控制中心”网络安全架构有几个关键要素：①受保护的关键入口：基于有线或无线接口的连接；②“封闭系统”：提供受限访问的预配置好的防火墙；③缜密的用户访问控制：不允许任何非授权用户访问隐私数据。

当然，建立以“控制中心”为首的汽车网络安全架构，在应对安全风险时可采取多种策略。如通过设立防火墙的方式来提供对其余网络的安全访问。

（3）汽车厂商、IT 系统厂商建立 APP 推广的白名单制度、恶意程序的黑名单制度

下载 APP 将是智能汽车拓展功能的重要载体，同时也是传播病毒的重要途径。在手机端，各类 APP 与开发者鱼龙混杂，形成了很多安全问题。在事关人身安全的智能汽车领域，汽车厂商、IT 厂商需要依据数据分析建立一套经过可信认证的 APP 白名单制度，在安全方面很少被恶意软件感染的 APP 可以进入白名单，重点推广，对于个人与小工作室开发的 APP 要谨慎推广，防止其借 APP 传播病毒。同时还可以建立针对开发者的黑名单制度，对于有侵犯安全过往历史的开发者，要提醒用户谨慎下载其开发的程序。

（4）编制更为详细、科学、易操作的使用手册，使用户正确使用智能汽车

智能化浪潮下汽车系统越来越复杂，对于用户而言，需要付出越来越高的学习成本。汽车厂商与 IT 厂商应当编制详细、科学、易操作的用户使用手册，使用户可以对汽车的构造、功能、技术参数、设置情况有更为清晰的了解和认识。