加速车辆信息安全

赢得车辆完整性和数据隐私性竞争

IBM 商业价值研究院

执行报告
汽车制造业

IBM 如何提供帮助

如今，车辆正逐渐从一种交通工具转变为新型的移动数据中心，车载传感器和计算机能够即时捕获有关车辆的信息。利用此类实时数据，IBM 可以帮助汽车制造业的高管提供全新的服务，满足互联互通时代的消费者对于车辆体验的新要求和期望。我们既拥有丰富的制造业经验，也拥有深厚的全球汽车行业专业知识，可以消除消费者对行车安全和车辆质量的顾虑。通过使用 Watson 等创新技术，我们可以满足汽车制造商 (OEM) 和供应商的各种需求，提供更安全可靠的产品和服务，从而实现更高的品牌忠诚度和客户满意度。请访问 ibm.com/industries/automotive

预防、检测和响应

*2014 年，IBM 发表了研究报告“促进安全：*新一代车辆的网络保障”，阐述了我们对于汽车信息安全的观点，介绍了汽车信息安全生命周期的“设计，制造，驾驶”方法。[1] 现在，我们希望更深入地推进这种方法。*尽管从“设计”阶段开始的汽车信息安全生命周期中，每个阶段都可能出现安全问题，但有关信息安全的大多数话题都主要聚焦于使用中的车辆和数据隐私所面临的威胁，也就是集中在“驾驶”阶段。因此，我们重点关注这个阶段，消费者可以轻松发现并评价汽车制造商如何利用技术来预防漏洞，检测可疑行为，以及通过稳妥安全的恢复措施应对威胁。*

执行摘要

消费者催生了互联互通式汽车。我们总是希望在行驶旅途中有美妙的音乐陪伴，曾几何时，我们在车上听的是 8 音轨磁带中的音乐，而现在，移动手机可以存储成千上万首歌曲，当然，要通过汽车的扬声器来播放。

这听起来很简单，但汽车与外部设备的连接还是存在一定复杂性的。如果汽车可以提供蓝牙服务，为什么不能作为 WiFi 热点为所有乘客提供服务呢？在我们最近的“人车新关系”调研中，我们发现 49% 的受访消费者希望未来 10 年内汽车可以成为物联网 (IoT) 中安全的集成设备。[2]

现代的出行者既希望在不同的交通方式之间无缝切换，又希望保持一致而个性化的数字化体验。许多技术共享有关出行者的信息，而且这些技术各自独立地参与联合运输体验，因此监管和隐私就成为需要关注的问题。当出行者从一种出行模式切换到另一种时，必须确保车辆上的个人数据被清除，并对旅行期间所捕获的持久数据进行适当保护和加密，在最终删除之前最大程度缩短数据保留时间。

好消息是到目前为止，互联功能还没有给威胁分子可乘之机。尽管研究人员最近的试验证明，控制车辆是可能的，但是车辆的漏洞还没有被广泛地利用。[3] 目前，通用的计算平台，例如台式电脑、笔记本电脑甚至是移动手机和平板电脑都很容易成为恶意软件和勒索软件的目标；然而，因为安全控制使得攻击者危害这些目标变得更加困难，所以他们将攻击目标转向物联网，包括互联互通的车辆。[4]

56% 的消费者表示信息安全和隐私保护将成为他们未来做出车辆购买决定时的主要考虑因素

在互联互通式汽车时代，**没有信息保护的车辆就不是完全安全的**

信息安全必须融入到企业的文化精髓之中，并在车辆的整个生命周期确保信息的安全性

在互联互通的汽车时代，不仅仅是消费者的安全和隐私处于风险之中，汽车制造商和移动生态系统中的其他参与者(例如电信和保险公司)更是责任重大。我们无法阻止攻击者和研究人员探测漏洞。汽车制造商需要尽自己最大的努力生产没有漏洞的产品，持续对产品进行全面测试，并随时准备好了解、修复和公开回应调查人员的发现以及出现的各种事故。随着汽车不断朝着“轮子上的数据中心”发展，亟需一种多学科的方法，涵盖传统和非传统的参与者以及各种能力，应对网络安全和数据隐私方面的挑战。

汽车制造商还必须确保涉及行车安全、信息安全和隐私保护的工作公开透明。56% 的受访消费者表示，安全和隐私将是他们未来做出车辆购买决策时的关键考虑因素。[5] 尽管消费者需要最新的技术，但是他们也希望这些技术以确保行车安全、信息安全和数据隐私为前提。

为成功打下坚实基础

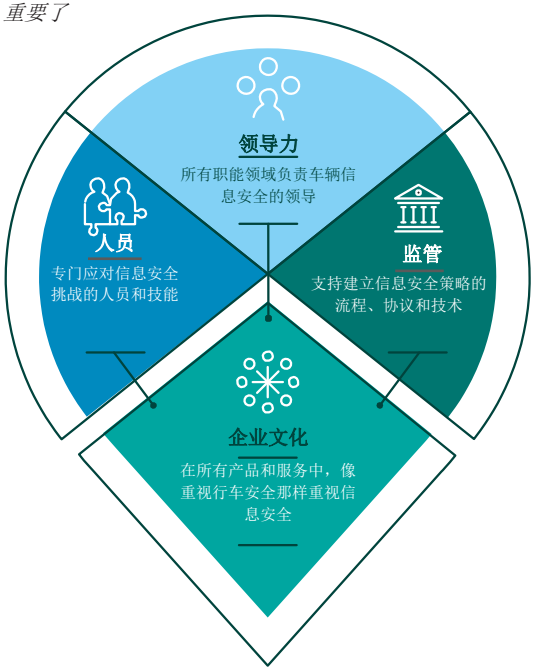
如果汽车制造商能够做好充分准备，那么他们在设计有效的信息安全解决方案时就能取得最大的成功。成功的基础主要有两个方面：一是确保将信息安全融入企业的文化精髓之中；二是为汽车制造商和消费者（尤其是后者）建立强大的数据模型，能够全面理解数据使用、隐私和所有权等各个方面。只有这样，汽车制造商才能真正落实“设计，制造，驾驶”信息安全方法所有阶段，尤其是“驾驶”阶段，从而能够有效预防、即时检测和从容应对各种威胁。

将信息安全融入企业的文化精髓之中

互联互通汽车的信息安全始于企业层面，应当渗透到汽车制造商的企业文化之中，上至领导，下至员工，贯穿整个监管领域（见图 1）。“设计，制造，驾驶”方法需要一种新的观念，将信息安全上升至与行驶安全相同的重要性水平，在物联网时代，没有信息安全就没有行驶安全，也就不可能实现互联互通汽车。信息安全并非大多数员工固有的关注点，包括有些身处领导岗位的人员；因此他们必须学着将信息安全作为优先任务来抓。特别是汽车制造商，需要将信息安全落实到每个流程之中，通过反复强调，使之成为员工的自然条件反射。

图 1

如果汽车制造商接受信息安全观点，并在企业文化中践行这个观点，车辆信息安全就变得与行车安全一样重要了



欢迎非传统的行业参与者

汽车行业无疑非常清楚自己的技术和行车安全模式，但信息安全研究人员则更了解网络安全形势和威胁分子。在 IBM 商业价值研究院的最新报告“2025 汽车展望：大业无疆”中，我们发现与消费者最有共鸣的数字体验都是由外部合作伙伴而不是汽车制造商所设计。[6] 这是因为，这些接口基于消费者的设备，比如移动手机，能够营造更亲密的用户互动体验。以下是一些建议：应当与非传统的行业参与者合作，因为他们拥有深厚的多学科专业知识，可以设计出最理想的解决方案。

因为设计、制造和管理车辆的整个周期非常复杂，涉及许多不同的组织实体，所以必须有一个主体单位来定义信息安全战略和实践，并监管各个实体的实施和协作。这个主体的负责人通常被称为“网络安全沙皇”，无论叫什么，这个职位必须有权与设计、生产和服务等各个组织实体开展合作。该主体必须确保在各个实体中进行宣传和沟通，鼓励每个人在“设计，制造，驾驶”阶段创建和管理方案时，考虑安全问题和威胁模式。

汽车制造企业还必须从行业外部聘用具备信息安全知识的人才担纲各种关键职位。此类专家能够发现信息安全实践的漏洞，推动改进措施，还能够向周围的人宣传信息安全理念。

汽车行业正不断扩大自己的边界，超越特定于汽车的技术，涉足汽车制造商所不熟悉的领域。汽车制造企业必须和物联网技术和信息安全方面的专家合作，包括软件和固件分析师、通信和网络工程师、云架构设计师、移动设备开发人员、威胁分析师以及数据科学家。汽车制造商还必须在汽车行业内开展合作，共享威胁情报，而且他们必须跨行业进行合作，以便尽早检测到常见威胁，例如国家的间谍活动。

合作还意味着邀请研究人员测试汽车产品，第一时间与汽车制造商分享他们的发现。可以通过表彰和奖金来激励研究人员：抓错奖励计划是一种有效的方法，鼓励他们发现更多的现实攻击情况，这不是内部质量评估团队可能找到的问题。

最后，消费者需要了解汽车制造商正在积极采取步骤，解决信息安全问题和提高信息安全水平，确保互联互通汽车的行车安全和隐私更有保障。汽车制造商必须做到公开透明，也就是要列出具体内容，比如漏洞的详细信息，并为客户提供工具，帮助他们确认车辆是否处于最新状态。与研究人员合作并与消费者联系，是建立信任关系和保持品牌忠诚度的关键。

评估数据使用和所有权

在评估信息安全和隐私保护时，强大的数据使用和所有权模式非常重要。这包括生成的数据以及有关收集、传输和存储数据的位置和方式等方面的信息。此外，汽车制造商必须对数据进行分类。数据是属于车辆使用者还是属于汽车制造商？如何根据这些信息保护数据安全？

汽车制造商一直在谁最终拥有数据的问题上犯难。比如天气和地图等信息很明显属于汽车制造商。手机联系人、通话记录和短信息很明显属于消费者。但谁是车内传感器遥测信息的所有者？除非法律特别规定，否则汽车制造商会认定这些数据属于车辆使用者，只有在消费者通过某种选择机制同意的情况下，他们才能对这些数据进行传输、存储和使用。[7]

可识别个人身份的敏感信息可能会归入“数字化个人”类别。举例来说：

- 汽车可能通过驾驶风格“了解”您的感受，并相应地做出响应。如果驾驶风格非常大胆奔放，汽车可能会从重金属电台切换到舒缓的爵士乐电台，帮助您平静下来。
- 汽车可能会在方向盘上安装心率监控器。如果监控器检测到您的心率出现严重异常情况，就会切换至完全自主驾驶模式，并发出紧急情况警报。

当今车辆中的个人数据

当今的车辆中，个人数据无处不在。例如，导航系统可能会收集车辆位置坐标数据，并将数据发送给汽车制造商的后台系统，以便对驾驶模式进行分析，然后反馈给导航应用。车辆必须将这些数据进行匿名化处理，删除有关车主或车辆使用者的个人信息。如果消费者将手机与车辆配合使用，并且同步联系人、通话记录和短信等信息，车辆必须对这些数据进行加密。车辆使用者离开该车，并且手机和车辆的距离超出一定范围时，车辆必须清除这些数据，这样，后来的使用者便无法访问这些数据。

- 如果您发生事故或遇到紧急健康问题，汽车可能访问您的病历，并将这些信息传输给急救人员。

对于汽车制造商来说，这个领域的复杂性只会越来越高。消费者直到确信自己的数据受到保护时，才会真正意识到互联互通汽车可以带来的好处。

接受“设计，制造，驾驶”信息安全方法

尽管本文的重点是深入探讨“驾驶”阶段，但是简单概括一下前两个阶段的关键组成部分也非常重要，因为所有三个阶段的工作结合在一起才能形成一个值得信赖的生态系统（见图 2）。

设计信息安全指的是规划如何抵御攻击，不仅仅是考虑车辆内部的信息安全，还包括车辆与基础架构之间互动的安全。实现这种信息安全的指导原则是假设最糟糕的情况，为应对故障而设计。例如，总线系统上的每次互动都可能会受到威胁，因此电子控制单元 (ECU) 不应盲目地对每条控制消息采取行动。

在设计安全的汽车时，设计流程必须从一开始就关注信息安全问题。这包括定义一系列手段和方法，用于测试在车辆使用期间可能收到的威胁。整个设计团队都应该能够使用这些威胁模型。接下来，在设计安全的基础架构的过程中，不但需要考虑车辆，还要考虑与车辆进行通信的所有基础架构组件，比如交通信号灯、收费路段以及其他车辆等。设计必须保证所有组件之间互动的完整性，这至关重要。

图 2

需要采用全面的信息安全方法，满足当今互联互通汽车的需求

要制造安全的汽车，不仅需要关注供应链和生产环境，还要关注连通消费者的所有分销渠道。要建立可信的供应链，就必须确保完整性 – 这意味着需要防止假冒伪劣或恶意组件进入汽车部件供应链，确保部件在从工厂装运到汽车安装的过程中不会受到篡改。

要控制生产环境，就需要确保 IT 和生产系统的完整性。通过了解每个系统的功能、应用、接口和协议，制定安全策略，设置访问和安全控制，从而保护生产环境。建立可信的分销渠道与供应端流程类似，但是它关注的是汽车在生产、经销商和最终的消费者之间的流转环节。当车辆交到第三方供应商（例如，物流公司）手中时，必须实施控制措施，防止车辆被篡改。

必须清楚，信息安全的控制范围不仅仅在于车辆和汽车制造商。它还涉及经销商和服务中心，以及第三方供应商等等。该行业必须检测和监控**生态系统**环境，确保一切流程可信。这样就可以实现一种端到端的信息安全方法，满足当今需求，并为将来做好准备。因此，生态系统中的每个领域都必须是值得信赖的环境，需要建立各种安全控制措施，包括加强认证和访问规则、强化系统以及实施密钥管理。

尽管汽车制造商拥有对车辆的控制权，但许多参与方都希望与车辆建立连接。连接点提供了一个开放的平台，但同时也形成了安全专家所称的“广泛的威胁面”。汽车制造商必须考虑每种连接技术的影响，选择那些与能够提供强大安全保障的大多数潜在第三方兼容的连接技术。

放心地驾驶

如果汽车制造商接受了我们建议的基本注意事项，那么他们在提高“设计，制造，驾驶”方法第三个阶段的信息安全方面就能够取得更大的成功。在“驾驶”阶段，车辆行驶在路上，驾驶员希望通过技术和服务预防漏洞，检测可疑行为，并通过妥善安全的恢复方式作出响应（见图 3）。车辆、汽车制造商和参与管理车辆的第三方都必须尽可能地执行这种全面的方法，避免加重车主的负担 – 除非车主要求参与进来。只有在极端情况下，才希望驾驶员做出有关行车安全、信息安全和隐私保护方面的决策。

预防漏洞

认证实体

认证是验证身份的过程。需要对车辆以及 Web 门户网站和移动应用等界面进行身份认证。车辆中的组件也需要对车辆基础架构进行认证，各个组件之间还需要相互认证。目的是确保来自人员、应用和组件的命令都经过授权。身份认证会主动确定人员或组件的身份。但是，它并没有规定什么人或什么组件可以进行访问。

可信的身份不仅仅是用户名和密码那么简单。在互联互通汽车环境中，可信的安全模块不可或缺。该模块必须；

- 为交互式登录提供认证功能，为非交互式的组件（例如 ECU）提供明确的身份识别功能。
- 在出现疑问时证实身份。
- 自身具备证书和密钥的存储、签署和管理功能，并实施强大的认证功能，例如双重认证和带外机制。
- 灵活可扩展地实施 OAuth 和 SAML 等开放标准。[8]

图 3

“放心驾驶”阶段的组成部分

互联互通汽车中的可信身份

下列是一些互联互通汽车生态系统中可信身份认证和使用的例子：

- 用户在移动应用或 Web 浏览器中进行认证，然后通过这些应用或浏览器与后台系统进行通信；此外还在拥有的车辆中进行身份认证。然后，用户就可以监视和控制车辆。
- 智能交通信号灯和路边基础设施可能指示车辆采取特定的行动，例如在急转弯时减慢车速。基础设施组件必须提供可信的身份，防止不法分子滥用信号指示机制。
- ECU 和控制组件必须具有可信的身份，有权发送消息。这样可以阻止非法设备发送恶意命令。
- 在本地安装或通过无线方式安装的更新都必须具有可信的身份，以避免安装恶意软件。
- 服务机构、修理中心以及内容供应商等第三方也必须拥有可信的身份。
- 应用必须可信。

- 包含加密处理器。
- 必须具备防篡改能力。

身份认证还必须提供特定于车辆的功能。例如驾驶行为模式分析、确定驾驶员体重的座位传感器，以及依赖进门密钥或移动手机特征码的确认功能。

管理访问权限

访问权限管理控制车内以及车辆与外部组件之间的活动。定义这些活动的执行许可时，必须考虑请求方和目标方的身份、请求类型（例如，控制消息、读取请求或写入请求）以及环境（例如，车辆的速度或所处地理位置）。

在车辆内部，ECU 最有可能成为恶意活动的目标。为了支持 ECU 访问规则，必须建立实施点。由于 ECU 处理能力有限，因此在这么多的端点上管理这些规则可能会非常复杂。但确实存在一些用于实施访问规则的策略，例如按子系统功能（例如，刹车和方向盘）对组件进行划分。

加密数据

加密技术可以保护数据本身，包括配置文件、遥测数据和消费者数据，例如电子邮件、短信和联系人信息等。数据可能（静态地）存储在汽车、汽车制造商的服务网络（云端）以及各种合作伙伴的许多位置中。数据也可能（动态地）通过移动网路、WiFi、蓝牙或使用专用短程通信 (DSRC) 在车辆的运行网络中传输。

加密技术在应用于控制器区域网络（CAN）总线时，可能会消耗过多的处理器资源，或者造成延迟。目前，这还不是可行的选择。在车辆系统中设计加密技术时，汽车制造商必须评估风险，而不是一味地追求所有组件的绝对安全。

加密技术依赖于之前提到的安全模块。对消费者数据的另一个要求就是加密技术必须采用“零知识”模式。这意味着汽车制造商和第三方不能解密数据；数据受到端到端的保护，只有消费者有能力解密这些数据。许多云供应商开始采用“零知识”模式。

最近，汽车制造商开始强调车辆入侵检测和预防系统（IDPS），以此作为防御攻击的一种方法。他们希望自己能够采取与之前应对机械挑战相同的工程设计方法，借助单个组件或功能应对所有信息安全挑战。

这种方法有两个缺点。首先，保护机制是基于规则的，因此只能在“预期的”攻击类型发生时才能进行干预。如果攻击者找到了规则没有覆盖的新方法，会发生什么情况呢？第二，攻击者也许不会攻击对于行车安全至关重要的组件而对乘客的生命安全造成威胁，他们却可以使用勒索软件或通过锁定支付数据而获得钱财。

有效的预防始于端到端的安全策略，以集成方式发挥作用。这种策略应当基于分层方法，让各种因素相互作用，相互补充。

访问权限管理的实际运用

以下是互联互通汽车生态系统中访问权限管理的一些例子：

- 只有经过授权后，防锁死的刹车系统（ABS）才可以向刹车 ECU 发送控制消息；任何其他系统必须向 ABS 请求这些操作，而 ABS 作为仲裁者，必须包含访问权限管理控制规则。这些刹车 ECU 本身必须包含简单的控制规则：除非消息来自 ABS，或者确认身份可靠，否则会忽略所有访问权限控制消息。
- 如果设置为代客模式，那么存储空间会保持锁定，车辆的行驶范围可能限制在半英里内，而且时速无法超过 25 英里。
- 只有直接参与电子邮件、短信和通话的人或组件才能访问这些数据。汽车制造商的服务云可能访问车辆的运行遥测数据，包括位置、速度和里程表读数，但是不能访问从驾驶者移动手机上同步的数据。但是，车主可以自行选择允许汽车制造商或第三方维护服务供应商访问他们的日历，以便安排预约。

检测可疑行为

揭示异常现象

检测可以提供预警，支持自动化系统和手动协议在攻击危害到行车安全、信息安全和数据隐私之前加以干预阻止。

入侵检测依赖于车辆内部关键位置的检测功能。这可能包括车载信息娱乐（IVI）系统、总线系统、中央网关、域控制器（在新一代汽车架构中）或者 ECU 本身。收集到的数据可能包括这些组件产生的事件，例如来自 IVI 的日志活动或者在受控总线上监控到的通信。

尽管之前提到的车辆 IDPS 方法非常好，但是它在检测阶段也有一些限制。IDPS 是基于规则的，主要检测和推理 ECU 之间通过车辆的 CAN 进行的通信。尽管这些信息非常重要，特别是当 IDPS 应用精心设计的方法时，但是获得的洞察仅代表车辆环境内部相关信息安全事件的一小部分。有关 CAN 总线的情报主要关注于行车安全方面。尽管这些信息对于保护生命安全至关重要，但是它不会提供针对其他网络或操作系统数据的可疑或异常活动的全方位视角。针对车辆的某些攻击也许可以通过这种方法检测到，但是许多复杂的攻击仍然无法被察觉。

应用安全分析和情报

安全分析必须发现针对个别车辆和整个车辆网络的完整性发起的攻击。通过对收集到的数据进行取证分析，根据历史数据进行仔细筛查，发现和了解攻击者所采用的途径。

汽车制造商正在大规模使用分析技术，例如车辆预测性维护分析。他们知道机械部件可能出故障 – 甚至知道何时出故障，出何种程度的故障。相同的预测性技能必须应用到信息安全分析方面，通过用例和威胁模型获得洞察。

他们采用基于环境的全面检测解决方案，在本地执行某些数据收集和处理工作，并接近实时地向中央分析平台发送一系列可处理的事件。这个流程使有限的车内计算能力和向后台系统发送所有数据点的带宽限制之间达到平衡。

控制版本

版本保证是重要的安全保障措施，它结合了安全模块的要素和检测功能，确保车辆内的所有组件都处于最新版本并且安装了最新的安全补丁程序。它还保证所有组件都未受篡改。

版本保证系统首先必须自身是可信的。其次，这种系统必须确认所有组件的身份可信，并对照由汽车制造商提供的主数据库进行数字特征符检验。IVI 本身非常复杂，包括许多开放源码软件库。库的版本和特征符必须定期进行维护和测试。为了保持透明度，汽车制造商必须为消费者提供某种形式的保证，最好在仪表板或 IVI 中提供。定期发送简单的消息，例如“所有车辆模块均有效并且处于最新版本”，可以保持消费者的长期信心。

对漏洞进行分类

各种漏洞的成因和后果各不相同，汽车制造商和立法者必须开展合作，为车辆漏洞建立分类系统，根据严重性划分责任大小。举例来说，伤害乘客的严重性要高于数据丢失。必须根据每种漏洞的类别做出不同的响应。

通过妥善安全的恢复方式作出响应

管理漏洞

尽管功能更新会给消费者带来不便，但是安全更新对于消费者的行车安全、信息安全和数据隐私至关重要。当汽车制造商发现车辆内部或支持基础架构中存在漏洞时，他们必须开发补丁程序并部署到每辆车上，以防攻击者有机可乘。

汽车制造商可能决定通过无线方式 (OTA) 进行更新，也支持消费者自行到服务中心（例如经销店）进行更新。汽车制造商必须事先征得车主的同意，才能提供 OTA 更新，以及收集有关车辆运行方面的特定数据。每当车辆的所有权发生变化时，汽车制造商都必须征得新车主的同意，也许就是在 IVI 上或 Web 门户网站上轻轻点击一下“同意”这么简单。

OTA 更新的细节非常复杂。汽车制造商与车辆之间的安全传输介质对于防止更新失败非常重要。更新后需要使用可信模块进行签名验证。最后，安装更新之后还必须进行测试。

在 OTA 更新开始之前，车辆需要处于合适的状态。例如，在车辆行驶过程中更新动力系统组件就是非常不谨慎的做法。如果在更新截止日期之前，无法找到安全的环境，那么车主需要使车辆处于安全模式，或是将车开到服务中心，完成这次更新。

实施汽车安全运营中心

汽车制造商需要收集有关车辆运行情况的所有信息，进行分析、评估并据此采取行动 – 而且应该在指定的车辆安全运营中心 (VSOC) 执行所有的任务。VSOC 是互联互通汽车的行车安全、信息安全和隐私保护方面的任务控制中心。它是第一线的安全运营功能，可以监视针对一系列预定义车辆（例如，按照地理位置、型号和制造商定义）的网络威胁，分析各种事件，对安全事故进行分类和上报，以便做出响应和进行修复。VSOC 涉及大量人员、流程和技术，可以实施威胁监控、取证调查、事故管理和安全报告。

VSOC 的目的在于：

- 在集中位置监控威胁，综合各种威胁情报并采取相应行动。
- 为网络事故做好准备并做出响应
- 追溯完整的攻击活动
- 搜索违规迹象
- 实现业务连续性，高效地开展恢复工作
- 防止网络威胁损害车辆的基础架构
- 提供有洞察力的网络威胁与合规报告

尽管 VSOC 的安全分析师必须具备汽车行业深厚的技术领域知识，甚至要了解受到攻击的车辆的特定构造、型号和版本，但是它与传统的业务 IT SOC 方法相比，还是具有一定的优势。这些分析师还必须具备广泛的网络安全领域的专业知识。

持续改进

从所有流程中不断汲取的经验教训会持续反馈到整个周期中。例如，汽车制造商需要让先前描述的电子取证途径形成闭环，并将内部安全测试的结果反馈给研发中心，以便实现持续改进。这些措施有助于消除设计阶段之初所带入的设计缺陷。

汲取的某些经验教训有助于更好地了解攻击者以及他们的动机和策略。这种知识能够增强威胁模式，改进汽车信息安全的“设计”和“制造”阶段。汽车制造商还应该与行业协作流程（例如汽车信息共享和分析中心（Auto ISAC））以及互联互通汽车生态系统中的每个利益相关方共享反馈。同样，许多行业推动的计划都希望实现标准化或建立最佳实践，这包括“汽车开放系统架构”(AUTOSAR)、“电子安全车辆入侵保护应用”(EVITA) 以及为汽车网络安全提供指导的“SAE 国际标准 J3061”。在实现自主驾驶的征途中，我们期待看到更多针对互联互通汽车的 IT 安全和数据隐私方面的特定法律法规。

最终，汽车制造商必须为遵守更高的标准做好准备，实现更高水平的信息安全、隐私保护和行车安全。这样的汽车可以提供消费者期待的安全特性和便捷功能，同时还确保汽车的行车安全和信息安全定位准确，使消费者可以从互联互通汽车的真正力量中受益。

您的互联互通汽车上路了吗？

- 您将采取怎样的全面战略和方法，将车辆信息安全提升到与自身企业以及合作伙伴企业内的行车安全一样的水平？
- 如何利用互联互通汽车的历史和实时安全信息，了解恶意攻击的目的、途径以及存在的漏洞？
- 如何继续完善反馈闭环，改进车辆的安全态势？
- 如何以安全的方式与第三方及合作伙伴共享互联互通汽车数据？
- 采用哪些机制获得车辆信息安全专业知识，并与生态系统共享？

合作者

Arndt Kohler，IBM 欧洲安全事务，副合伙人

Yaron Wolfsthal 博士，以色列网络安全人才中心副总监

Yair Allouche 博士，以色列网络安全人才中心互联互通汽车安全首席技术官

Rob Carson，IBM 商业价值研究院，IBM 数字服务部内容战略规划师和撰稿人

April Harris，IBM 商业价值研究院，IBM 数字服务部视觉设计师

关于作者

Christopher Poulin 曾是 IBM X-Force 安全研究团队的研究战略家。他着重关注有关物联网环境（包括互联互通汽车）的威胁情报和信息安全技术。他在信息安全方面拥有超过 25 年的工作经验，最开始在美国国防部工作，担任过许多不同的职位，包括软件开发人员，还是一家高级安全保障咨询机构的创始人。

Giuseppe Serio 是 IBM 汽车、航空航天以及国防行业的网络安全全球解决方案负责人。他与全球客户的合作已经超过 20 年，拥有丰富的经验，主要负责与客户讨论各种信息安全项目和信息安全挑战，包括互联互通汽车的信息安全问题。他与其他 IBM 职能部门密切合作，包括 IBM 研究院、安全部门和物联网业务部门，共同开发和调整安全解决方案，使之适应特定行业的需求。在加入 IBM 之前，Giuseppe 是普华永道咨询公司的高级咨询师，在该公司管理多个国际业务转型项目。他的联系方式为 giuseppe.serio@de.ibm.com

Ben Stanley 是 IBM 商业价值研究院的全球汽车行业主管。他负责为 IBM 汽车行业事务开发思想领导力和战略业务洞察。Ben 拥有超过 39 年的汽车制造业工作经验，在业务战略和业务模式创新领域，与全球多家主要的汽车行业客户合作。Ben 曾受派遣到中国上海工作了五年，担任 IBM 汽车人才中心的负责人。Ben 的联系方式是：ben.stanley@us.ibm.com，Twitter 帐号是：@BenTStanley

更多信息

欲获取 IBM 研究报告的完整目录，或订阅我们的每月新闻稿，请访问：ibm.com/iibv.

从应用商店下载免费“IBM IBV”应用，即可在手机或平板电脑上访问 IBM 商业价值研究院研究报告。

访问 IBM 商业价值研究院中国网站，免费下载研究报告：http://www-935.ibm.com/services/cn/gbs/ibv/

选对合作伙伴，驾驭多变的世界

在 IBM，我们积极与客户协作，运用业务洞察和先进的研究方法与技术，帮助他们在瞬息万变的商业环境中保持独特的竞争优势。

IBM 商业价值研究院

IBM 商业价值研究院隶属于 IBM 全球企业咨询服务部，致力于为全球高级业务主管就公共和私营领域的关键问题提供基于事实的战略洞察。

注释和参考资料

1 Poulin, Christopher. “Driving security:Cyber assurance for next-generation vehicles.” IBM Institute for Business Value. 2014. http://www-935.ibm.com/services/us/gbs/thoughtleadership/automotivesecurity/

2 Stanley, Ben and Kal Gyimesi.” 人车关系新发展 – 全球消费者希望汽车如何适应自己的生活” IBM 商业价值研究院，2016 年。http://www-935.ibm.com/services/multimedia/a_new_relationship.pdf

3 Greenberg, Andy. “Hackers remotely kill a Jeep on the highway – with me in it.” Wired. July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

4 举例来说，Mirai 蠕虫病毒导致超过 100 万部互联的监视摄像头和数字视频录像机受损，而且其他恶意软件正在疯狂地攻击一切目标，包括家庭路由器、婴儿监视器，无所不包，目前路上行驶的车辆超过十亿部，想象一下，如果其中一辆被引入僵尸网络，并用于大规模的分布式拒绝服务 (DDoS) 攻击，会出现怎样的情况。

5 Stanley, Ben and Kal Gyimesi.” 人车关系新发展 – 全球消费者希望汽车如何适应自己的生活” IBM Institute for Business Value. 2016. http://www-935.ibm.com/services/us/gbs/thoughtleadership/autoconsumer/

6 Stanley, Ben and Kal Gyimesi. “Automotive 2025:Industry without borders.” IBM Institute for Business Value. 2015. http://www-935.ibm.com/services/us/gbs/thoughtleadership/auto2025/

7 数据所有权并不总是那么清晰明确。例如，一些零售商可能想知道他们的商店旁所经过的车辆 – 了解交通流量、车辆的品牌和型号（或许想衡量潜在消费者的财富情况），甚至想了解 VIN，以便跟踪经常出现的购车者。这类信息中的某些可能是公共可用的，例如交通流量数据，但是还有一些可能是特定于汽车制造商的，例如品牌和型号。这些数据中还有一些，比如 VIN，也许不能直接解析出消费者的身份，但可能被视为敏感信息。

8 OAuth（开发授权）是一种开放协议，支持针对 Web、移动和桌面应用进行安全授权；SAML（安全断言标记语言）是一种开放式的数据格式，支持在服务供应商和身份供应商之间进行身份验证和授权信息交换。

IBM Global Business Services, Route 100,Somers,NY 10589

美国出品，2017 年 1 月

国际商业机器中国有限公司
北京市朝阳区北四环中路 27 号
盘古大观写字楼 25 层
邮编：100101