互联
生活

汽车物联网安全

打击最常见的攻击模式

全球物联网应用呈现规模化发展态势，物联网接入设备数量快速增长，数据内容更加丰富和精准，物联网网络安全和信息保护面临严峻挑战。车联网是物联网中最具发展潜力的重要领域之一，由于车联网信息安全可能转化为物理伤害和人身伤害，其应用安全和隐私保护问题得到产业界高度关注。GSMA提出的《汽车物联网安全》报告对车联网应用面临的重点安全问题进行了分析，契合产业发展需要和技术演进趋势，对促进车联网重点安全技术突破，推动车联网应用规模化发展具有重要意义。

汤立波博士
车联网项目技术负责人
业务资源与物联网研究部副主任
中国信息通信研究院

汽车物联网安全

打击最常见的攻击模式

不断演进的攻击者

过去几十年间，信息安全领域涌现出一种模式：攻击者处于上风，而且获胜速度越来越快。如今，市面上用于计算机系统入侵的工具、信息和技术空前增多。而同时，因需要投入大量的精力、弹性硬件架构以及大批技术精湛的工程师，计算机系统的防护工作成效总是不尽如人意。

5 年前在拉斯维加斯召开的黑客简报大会上，Lab Mouse Security（鼠标安全实验室）的 Don A. Bailey 首次演示了如何远程遥控入侵汽车系统。如今，DEF CON 大会（世界上最大的黑客大会之一）成立了一支汽车黑客研究小组，专门提供硬件工具、免费软件技术以及压缩技术，用于绕开复杂的安全控制系统。

随着人们对入侵行为的兴趣与日俱增，并非每个人都能遵守专业信息安全研究员制定的道德标准。某些人会选择越过禁区。一旦发现薄弱环节，不法之徒便会聚拢，夺取控制权用于他们自身的目的。

某些攻击者开始使用一种全新的恶意软件 - “勒索软件”，禁用关键系统，要求受害人支付费用。大多数这类攻击行为会导致严重的后果。

例如，2015 年 12 月，乌克兰某小区供电设备被安装了某种恶意软件，继而导致为期三周的停电事故。2007 年起，这款恶意软件便开始活跃于网络系统，近期经过更新后，开始用于破坏控制系统和工业控制系统中的硬件。这是世界上第一例由黑客引起的停电事故。

随着物联网 (IoT) 的发展，工业系统之间的联系越来越密切，发生这类攻击的概率大大增加。工程师和高管需要考虑的是攻击者何时会攻击物联网 (IoT) 解决方案，而不是考虑他们是否会发起攻击。有效防御此类攻击以及确保总体技术可恢复的唯一方法是在解决方案开发伊始，就绷紧安全神经。

攻击模式

攻击者倾向于综合使用多种方法攻击物联网 （IoT) 解决方案，这些方法大多针对构成物联网 (IoT) 的行业和技术。

物联网本质上是云、网络持久性技术和嵌入式技术的组合应用，令计算机系统能够进行物理连接，以便提供创新服务。也就是说，物联网 (IoT) 利用现有技术，实现交互性和自动化。

因此，攻击者可利用明确的方法和现有工具，发现物联网 (IoT) 解决方案中的漏洞。

图一展示了汽车物联网解决方案中可能包含的元件。

图 1 - 常见的汽车物联网元件及其功能

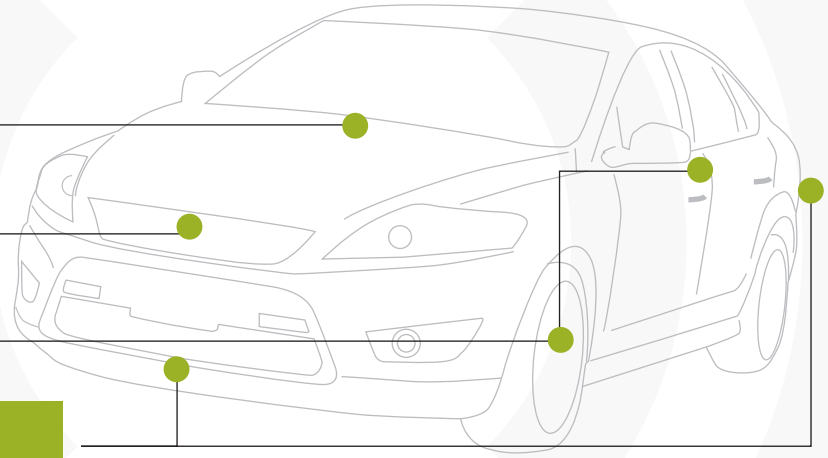
现代汽车物联网功能

现代汽车远距离通信系统；功能：收集数据、娱乐以及查看诊断系统

中央计算机系统；功能：提供实时决策指导

传感器；功能：帮助司机了解安全的路况信息

无线通讯系统；功能：警示行人，播报安全关键指标和警报



攻击物联网技术的常用策略包括

- 利用对等实体认证中的薄弱环节
- 篡改实用加密
- 终端完整性中的缺口
- 未对关键和非关键应用程序加以区分
- 软件应用程序中的缺陷
- 业务逻辑薄弱环节

每个有经验的攻击者都知道物理设备是所有通信网络中最薄弱的环节。由于物理设备安全性极具挑战性，所有利用网络通讯或物理端点中的薄弱环节是最有效的方法。

虽然可以敦促出色的工程师维护核心远距离通信系统，但由于成本高昂、技术复杂，维护汽车计算机系统中的传感器或电子控制单元 (ECU) 端点安全是一个巨大的挑战性。

图 2 显示了几种攻击汽车物联网解决方案的方式。

图 2 – 几种常见的汽车系统攻击模式

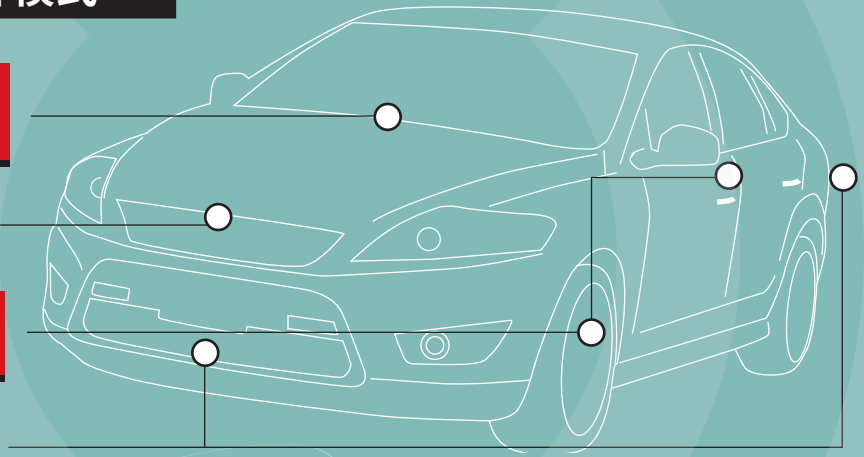
攻击汽车物联网功能的几种模式

模拟远程信息后台服务、操纵固件升级、利用信息安全漏洞以及利用第三方应用程序“越狱”

利用本地或远程 CANbus 工具控制 ECU 决策制定过程

通过标准无线协议的弱点执行远程代码或假冒传感器数据

通过滥用安全证书或密钥体系控制关键通讯渠道



高性价比的解决方案

以上所述问题并非系统性问题，也并非无法解决。事实上，有许多防止攻击物联网解决方案的有效方法。

由于管理安全界面多通过产品或服务架构实现，我们可以通过以下四种方式保护终端设备的管理界面。

- 使用可信计算基搭建网络和应用程序安全体系
- 确保所有网络通讯保持机密
- 限制应用程序的运行
- 执行防干扰措施

1. 使用可信计算基

可信计算基 (TCB) 是所有安全策略、程序和技术的集合，加强了重要加密应用程序的使用和安全性。它是定义平台可信性的基础。如果将可信计算基 (TCB) 应用于核心产品，那么该产品将在这一领域大获成功。可信计算基 (TCB) 的功能：

- 减少甚至消除硬件拷贝或诈骗所带来的潜在风险
- 在服务器内部强制使用可信的组成部分
- 提高现场或远程更新应用程序的成本效益
- 增强服务器不同组成部分的互操作性和可信性
- 延长产品的使用寿命

GSMA 物联网安全指南可提供有关可信计算基的更多信息， 下载地址为 **http://www.gsma.com/connectedliving/iot-security-guidelines**

2. 安全网络通讯

物联网安全的第二个重要因素是网络通讯。网络内部的所有组成部分均须能互相验证并在适用时秘密传播数据。这些组成部分沟通时，其完整性均须经过验证，以确保数据不会遭受截取、更改或假冒。

如没有了可信计算基 (TCB)，确保网络通讯的安全将面临很多问题，并将导致生产环境产生意料之外的运转情况。例如，许多新物联网产品利用个人局域网络 (PAN) 的通讯技术，如低能耗蓝牙技术 (BLE)、无线个域网以及线程。

此类产品包括新安全功能，能够在不可信赖的网络中确保网络同伴间会话的安全。
尽管这些更新协议（如，椭圆曲线迪菲- 赫尔曼密钥交换）为确保会话安全而使用的密码规则系统，在数学上完全正确，但并不能确保其数据的机密性和完整性。

这是因为这些技术不可信，并未在防干扰存储领域存储密钥，也可能没有确保全部会话安全所需的某种制程能力。

由于任何潜在攻击者的首要目标是网络通讯分析，不可避免地，网络通讯安全就成为任何物联网产品或服务的关键方面。

3. 限制应用程序的运行情况

应用程序的安全尤其具有挑战性，甚至对经验丰富的公司也是如此。尽管制造商工程团队设计的核心应用程序会受到全面审计，现代架构通常允许第三方应用程序加载至物联网端点。由于应用程序商店使得用户能够查看或许成千上万的第三方应用程序，这些程序几乎不可能全部通过全面审计。

确保应用程序安全的正确方式是将其通过封锁、虚拟机或其他提取方式进行隔离，限制它们的功能以及查看关键系统设备或资源的权限。

通过这种方式，软件的瑕疵不会导致攻击者突破应用程序并查看关键资源，如 CANbus（控制区域网络总线）。特别是，确保应用程序的以下方面至关重要：

- 减少甚至消除硬件拷贝或诈骗所带来的潜在风险
- 在服务器内部强制使用可信的组成部分
- 提高现场或远程更新应用程序的成本效益
- 增强服务器不同组成部分的互操作性和可信性
- 延长产品的使用寿命

实施这些规则时，即使攻击者通过利用第三方应用程序获得可执行代码，或如果该应用程序为“软件后门”，其影响也是可以量化且仅限于受损的应用程序。任何其他应用程序、子系统或主操作系统在任何方面均不会受到影响。

4. 执行防干扰

因为大多数攻击物联网的行为都是通过实体设备，阻止这些设备的分析能切实可行地降低攻击的可能性。

虽然攻击者所控制的实体设备始终处于受损的危险之中，实体防干扰可将攻击流程复杂化并提高相关费用至某一点，使得攻击不再可行或划算。

例如，若打开某设备的容器，其光敏性保险丝能删除储存。同样，可在设备外壳中嵌入电路，若打开该设备，此电路将切断纽扣电池电源并删除关键存储组件。

其他方法也可用来创建有效划算的措施，导致攻击者成功实现逆向工程或破坏设备安全所需的时间、费用和装备大幅增加。

图 3 列举一系列策略，用于确保汽车物联网解决方案的实施。

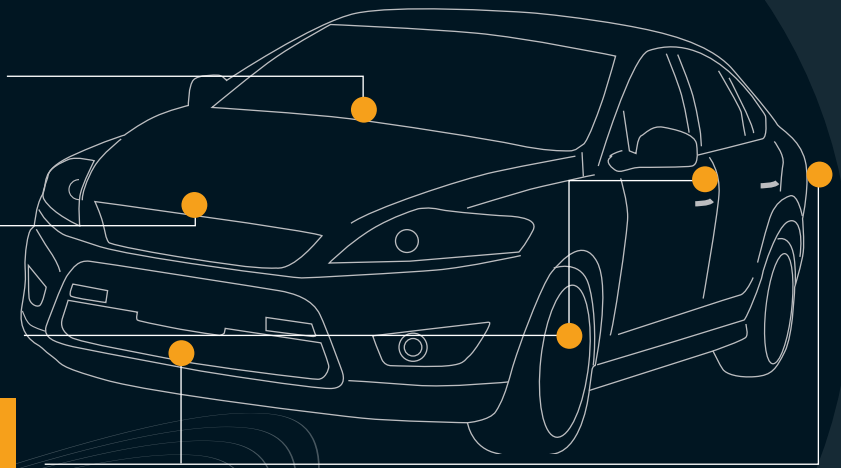
切实有效的汽车物联网安全解决方案

即使因漫游或协议降级导致移动网络安全变得不稳定，汽车物联网解决方案也可以通过加强应用水平的通信安全，来保证高度的保密性和完整性。

汽车物联网解决方案通过与核心架构之间建立信任，来降低长期工程造价并延长设备寿命

甚至在轻质传感器终端亦部署了同行认证、保证数据保密性和信息完整性。

如果某一客户应用程序受到损害，关键应用和非关键应用将会相互剥离，这样可以减少攻击者对核心部件的破坏性



总结

不论媒体如何炒作，物联网解决方案都具有其安全性。从架构层级开始我们就已建立了一个高性价比的安全体系。 微小的改进便可保证整个物联网产品或服务生态系统免遭破坏。但是，为了这细微的改进，工程团队必须花时间，从无到有，将安全体系植入进去。在物联网解决方案中，安全体系决不是一个附加装置，相反，它是物联网的根基。

更多有关降低常见物联网风险的建议， 请参考 GSMA 物联网安全指南。
http://www.gsma.com/connectedliving/iot-security-guidelines

了解最新的 GSMA 互联生活新闻：

请访问我们的网站 **www.gsma.com/connectedliving**
订阅我们的电子报 **http://www.gsma.com/connectedliving/sign-up-for-newsletter/**
关注我们的 LinkedIn: **http://gsma.at/LinkedInConnectedLiving**