GSMA 物联网

汽车物联网安全

如何应对最常见的攻击形式

汽车物联网安全

如何应对最常见的攻击形式

不断进化的攻击者

过去几十年，信息安全领域出现了一种模式：攻击者总是能够成功，而且成功的速度越来越快。如今，市面上用于入侵计算机系统的工具、信息和技术空前增多。同时，计算机系统的防护工作因需要经常投入大量的精力、弹性硬件架构以及大批技术精湛的工程师，其成效总是不尽如人意。

5 年前，Lab Mouse Security（鼠标安全实验室）的 Don A. Bailey 首次在拉斯维加斯召开的 Black Hat Briefings（黑客简报大会）上演示前所未有的远程汽车黑客入侵。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越来越感兴趣，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。一旦发现薄弱环节，不法之徒便会闻风而来，破坏控制，从中渔利。

某些攻击者开始使用一种称为“勒索软件”的新型恶意软件，禁用关键系统，要求受害人支付费用。许多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即被安装某种恶意软件，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、毁坏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攻击者何时会针对其物联网解决方案发起攻击，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解决方案，这些方法大多针对构成物联网的行业和技术。

物联网本质上是云、网络连续性和嵌入式技术的组合应用，用于物理连接计算机系统，以便提供创新服务。也就是说，物联网利用现有技术，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，发现物联网解决方案中的漏洞。

图 1 展示了汽车物联网解决方案中可能包含的组件

图 1 - 常见的汽车物联网组件及其功能

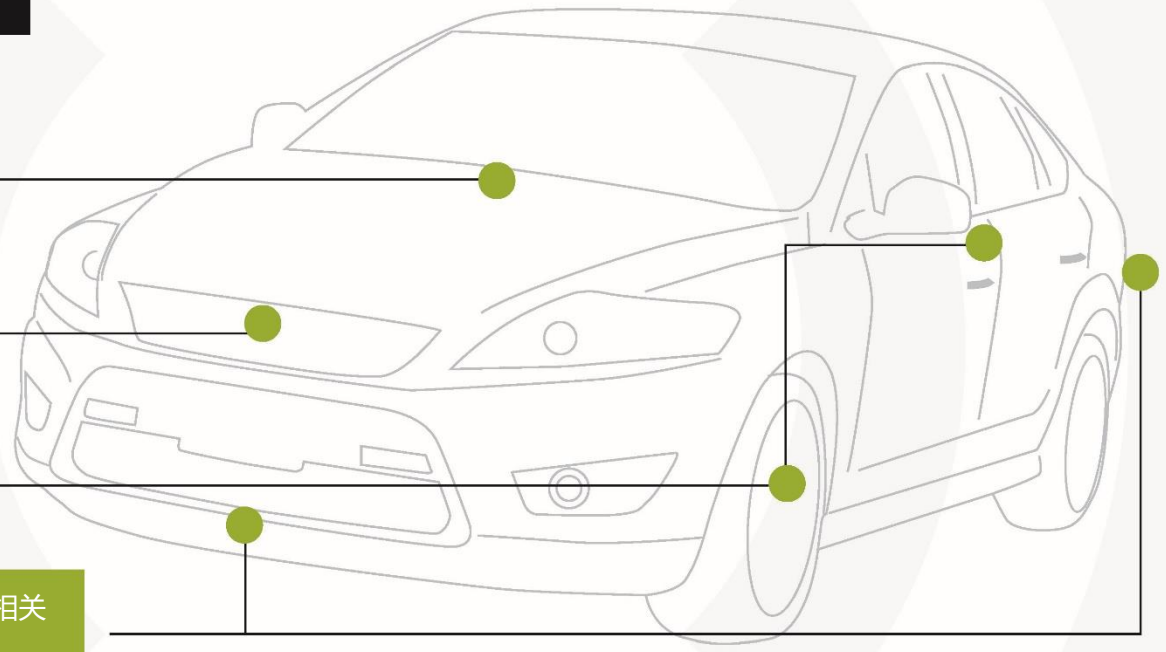
现代汽车物联网功能

现代车联网系统收集数据、提供娱乐、显示诊断系统

中央计算系统指导实时决策

传感器帮助司机安全协调路况

无线通信系统与附近的对等方进行交互，转发安全相关指标和警报



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

每个有见识的攻击者都知道，物理设备是任何独立通信网络最薄弱的进入点。保障物理设备的安全非常困难，因此利用网络通信或物理终端的薄弱环节是攻陷物联网生态系统最简单的方法。

虽然可以通过出色的工程技术保护核心车联网系统，但由于成本和复杂性原因，保护组成汽车计算机系统其他部分的传感器或电子控制单元（ECU）终端安全却十分困难。

图 2 显示了几种攻击汽车物联网解决方案的方式。

图 2 - 汽车环境中常见的攻击模式。

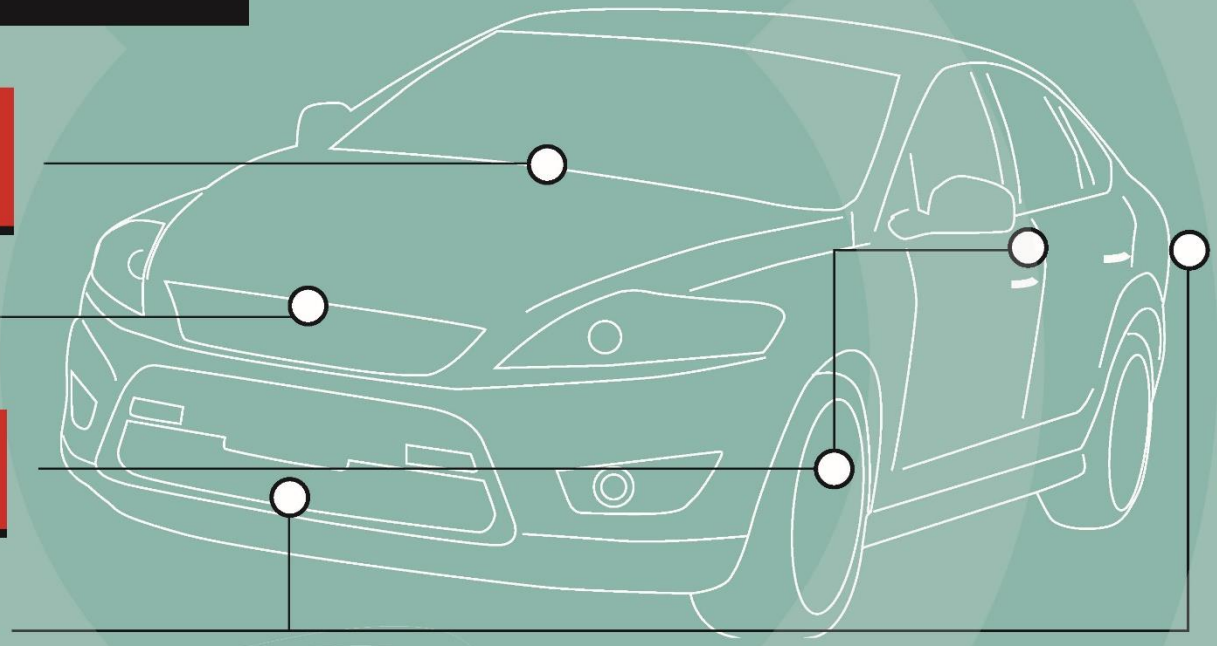
针对汽车物联网功能的攻击模式

模拟车联网后端服务、操纵固件更新、通信安全漏洞以及第三方应用程序“越狱”

通过本地或远程 CANbus 仪表控制 ECU 决策

通过标准无线协议的弱点远程执行代码或模拟传感器数据

通过滥用安全证书或关键层级来操纵关键通信渠道



经济有效的解决方案

上述问题既不是系统性问题，也并非无法解决的。事实上，有许多非常经济有效的方式可以防止对物联网解决方案的攻击。

由于管理界面安全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。

- **需要使用可信计算基以保证网络和应用程序安全**
- **确保所有网络通信的机密性和完整性**
- **限制应用程序的行为**
- **实施防篡改措施**

1.使用可信计算基

可信计算基（TCB）是策略、程序和技术的集合，强制使用重要加密应用程序并确保其安全性。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 物联网安全指南提供了有关可信计算基的更多信息，下载地址为：**http://www.gsma.com/iot/iot-security-guidelines**

2.保护网络通信

物联网安全的第二大重要属性是网络通信。网络内部的所有组件都必须能够互相验证，并在适用时秘密传送数据。这些组件通信时，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。

如果没有设计良好的可信计算基（TCB），在保护网络通信安全时可能会面临很多问题，往往导致生产环境出现意外情况。例如，许多新型物联网产品利用个人区域网络（PAN）的通信技术，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。

这是因为这些技术没有信任根，没有在防篡改存储领域存储密钥，可能也没有确保全部会话安全所需的某种处理能力。

由于任何潜在攻击者的首要目标是网络通信分析，因此必须将网络通信安全视为任何物联网产品或服务的关键环节。

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，甚至对于经验丰富的公司也是如此。尽管可以对制造商工程团队设计的核心应用程序进行全面审核，但现代架构通常会允许物联网终端加载第三方应用程序。应用程序商店使得用户有可能访问数十万第三方应用程序，几乎不可能对所有这些应用程序进行全面审核。

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。

这样，软件的缺陷就不会导致攻击者突破应用程序并访问关键资源，如 CANbus（控制区域网络总线）。
尤其是必须确保应用程序：

- 无法提高其影响主操作系统的权限
- 无法进入底层驱动或设备
- 无法影响其他关键应用程序的运行情况
- 无法储存至其他应用程序的存储或资源，或从中读取

实施这些规则时，即使攻击者利用第三方应用程序获得可执行代码，或该应用程序有“隐蔽后门”，其影响也可以量化，并且仅限于遭到入侵的应用程序。任何其他应用程序、子系统或主机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物理设备，所以阻止对这些设备进行分析能够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有遭到入侵的风险，但是可以使用物理防篡改措施，将攻击流程复杂化并提高相关费用，以至于攻击不再可行或划算。

例如，光敏性保险丝可以在打开设备外壳时擦除内存。同样地，可在设备外壳中嵌入电路，打开设备时，此电路将断开纽扣电池并擦除关键内存组件。

还可通过其他方法设计经济有效的措施，令攻击者成功逆向工程或破坏设备安全保障所需的时间、费用和设备大幅增加。

图 2 - 汽车环境中常见的攻击模式。

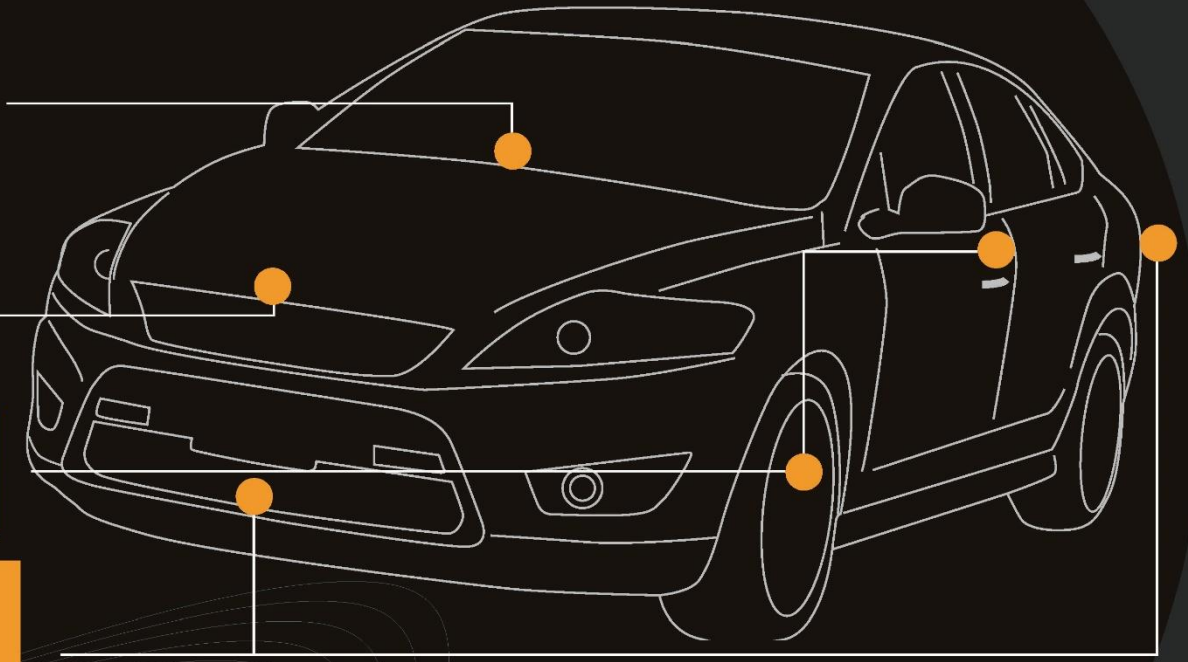
切实有效的汽车物联网安全解决方案

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

将关键应用和非关键应用彼此隔离开来，因为如果有定制应用遭到入侵，这样可以降低攻击者破坏核心部件的能力



总结

虽然媒体危言耸听，但物联网解决方案的安全是可以实现的。经济高效的安全体系要从架构层面开始建立。只需作出一些细微的更改，即可保证整个物联网产品或服务生态系统免遭破坏。但是，为了实现这些细微的更改，工程团队必须花费时间，从无到有地建立安全体系：在物联网解决方案中，安全体系不能作为附属物来实施。相反，它必须要成为基础。

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/iot/iot-security-guidelines

如需了解最新的 GSMA 物联网新闻：

请访问我们的网站：**www.gsma.com/IoT**

订阅我们的电子报：**http://www.gsma.com/IoT/sign-up-for-newsletter/**

关注我们的 LinkedIn：**http://gsma.at/IoT**