黑客远程操控可致车祸或“劫”车

美国菲亚特克莱斯勒汽车公司召回140万辆面临黑客攻击风险的汽车，被网络安全专家视为“大事”。随着电脑和网络技术的应用，汽车正变得更加智能，但也暴露在黑客的攻击之下。

用科罗拉多州安全公司LogRhythm首席信息安全官詹姆斯·卡德尔的话说，不同于人们普遍认知的“黑客攻击危及知识产权”，这次发现的汽车网络安全漏洞事关“140万个处于危险中的生命”。

这件“人命关天的大事”具体意味着什么？你如果听说过时下越来越热的新名词“物联网”，再看看接下来要举的这些例子，或许会有进一步的认识。

手段不止“劫”车

首先要举的例子当然是这次汽车召回的直接导火索——美国网络安全专家查利·米勒和克里斯·瓦拉塞克“黑入”一辆切诺基吉普车的实验。两人在家利用笔记本电脑，通过这辆吉普车的联网娱乐系统侵入其电子系统，远程控制车的行驶速度，操纵空调、雨刮器、电台等设备，甚至还把车“开进沟里”。

米勒和瓦拉塞克认为，吉普车上的互联网连接功能对黑客来说是非常理想的漏洞，只要找到车的IP地址，侵入系统，就能“劫持”车辆，而菲亚特克莱斯勒生产的47.1万辆车都存在这种漏洞。

实际上，黑客攻击时不一定要“劫持”汽车或引发车祸，用其他手段也会对车主造成麻烦和损失，比如利用汽车导航系统跟踪车主行踪、远程操控车内话筒录下车主对话等。

网络安全研究者说，目前已经出现盗窃者利用无线电信号解锁并盗走汽车的案例。今后可能出现的手段包括：黑客在车中植入恶意软件，导致引擎失灵，以此敲诈车主；或是利用所谓“车联网”，即实现车辆与周边环境联网以改善交通状况、防止车辆相撞的无线连接技术，使每一辆驶经的汽车都可能被侵入或置入病毒。

目标不限汽车

既然说到“车联网”，不妨看看涉及范围更广的“物联网”。汽车作为物联网的重要组成部分，是较受黑客欢迎的攻击目标，但可能成为攻击目标的显然不止汽车。

2008年，波兰一名14岁少年用一个改装过的电视遥控器控制了波兰第三大城市罗兹的有轨电车系统，导致数列电车脱轨、人员受伤。

2010年，美国得克萨斯州奥斯汀市汽车经销商“得克萨斯汽车中心”接到大量客户投诉车辆故障，包括喇叭无故半夜鸣响、车辆无法发动等。调查发现，“得克萨斯汽车中心”一名前雇员远程入侵这家经销商的电脑系统，通过其与车辆间的联网设备遥控车辆，而这名20岁男子的动机竟是发泄被炒鱿鱼的不满。

2011年，3名美国网络安全研究者宣布，他们成功入侵用于控制监狱大门的网络系统，能够任意远程开关这些大门。他们还发现，其他不少机械控制系统也存在类似薄弱环节。

无人机也是黑客感兴趣的目标。伊朗2011年俘获美国RQ-170“哨兵”无人侦察机，据称就是伊朗网络专家远程控制了这架飞机的操作系统。2013年，美国知名黑客萨米·卡姆卡尔在“优兔”网站发布一段视频，展示他如何用一项名为SkyJack的技术，使一架基本款民用无人机能够定位并控制飞在附近的其他无人机，组成一个由一部智能手机操控的“僵尸无人机战队”。

在引发“物联网”意义上“物质损害”的重大网络攻击中，伊朗核设施遭遇的“震网”病毒袭击算是典型案例。计算机专家认定，这次袭击致使核电站离心机因转速失控而受损，导致伊朗核计划被显著拖延。

此外，2007年，时任美国副总统迪克·切尼心脏病发作，被怀疑缘于他的心脏除颤器无线连接功能遭暗杀者利用。这被视为物联网攻击造成人身伤害的可能案例之一。

“物联网”的“宿命”？

《华盛顿邮报》报道，2010年全球联网设备数量为20亿台，这一数字预计在2020年剧增到250亿台。网络专家认为，随着联网设备越来越多、技术越来越普及，“物联网”遭“黑”是“必然出现”的问题，甚至已经有专家把“物联网”戏称为“攻击目标之网”。

究其原因，互联网本身就具备“不安全性”：目前的互联网基于诞生于数十年前的技术，那时黑客、网络安全等概念甚至都没有出现。要在这种“有缺陷”的技术基础上实现大量设备高度互联，有效的安全措施难以跟上。

以汽车为例：目前市面上出售的汽车已经不只是代步工具，而是“车轮上的电脑”，各系统内外相互连接。遥控钥匙、卫星电台、远程信息处理部件、蓝牙连接、仪表盘联网、无线胎压监测等功能使汽车与外部联通，也都可能成为黑客攻击的突破口。在汽车内部，各系统相互联通使外来攻击有了跨越系统的路径，而各系统间通信依靠的仍是创立于20世纪80年代的计算机协议，不具备“验证”消息来源的能力。

原美国国防部高级研究项目局网络安全研究负责人派特尔·扎特克说，汽车上述系统的整体安全“可能比目前(计算机)操作系统的安全状况落后15或20年”。

原福特汽车公司技术专家约翰·埃利斯说，“物联网”连通性和新功能的增速远快于对攻击有效防范措施的增速，而汽车制造业研发周期较长，导致填补汽车网络安全漏洞或以新车型替换存漏洞车型耗时长、难度大。

“不是车的问题”

米勒和瓦拉塞克2011年受扎特克委托，开始研究汽车网络安全。他们研究车型除了吉普切诺基，还包括丰田“普锐斯”和福特“翼虎”等。据他们统计，汽车电脑系统的数量近年来持续增加，2006年版普锐斯内含23个电脑系统，而2014年版包含40个。

随着各汽车制造商争相研发无人驾驶汽车，这一势头预计将加速发展。

实际上，一些“老车型”也通过车载自动诊断系统(OBD)接口，被加上无线连接设备，加入“物联网”。

然而，如果汽车防黑客措施如专家所说那样欠缺，汽车岂不是“越高配越危险”？

美国塔夫茨大学计算机科学教授和网络安全研究者凯瑟琳·费希尔认为，尽管汽车制造商面临计算机协议过时且存在缺陷的技术困境，但如果在安全措施研发方面投入更多时间和资源，汽车网络安全进一步完善在技术上而言“是可能的”。

但她指出，技术研发能否实现，还要看汽车制造商是否有足够“商业动机”。“他们(制造商)都很担心不安全，但难以独自承担(研发成本)。”

埃利斯认为，作为汽车制造商上游供货方的电脑软件制造商应该研发安全软件并做好维护和更新工作，但现有商业模式没有给予他们这样做的动力。“这不是车的问题，而是软件和商业模式的问题。”

(据新华网)