车灯突闪、车门被解锁、发动机莫名熄火……

如何防止汽车被黑客攻击?

宁波这场车联网安全攻防挑战赛有答案

如今,智能网联汽车越来越多,许多汽车连上网络后,可能进行实时路况导航、下载视频音频、引进语音交互。同时车内的空调、天窗,甚至如刹车、变速箱都可以由计算机控制。但您有没有想过,这些功能除了带来生活出行的便利之外,也增添了许多安全隐患。理论上,黑客可以通过网络攻击任意一台网联汽车,窃取车内数据,甚至夺取驾驶控制权。

为了提升汽车网络安全技术,加强汽车网络安全防范,7月23日,由国家互联网应急中心、国家市场监督管理总局缺陷产品管理中心、中国网络空间安全协会、中国互联网发展基金会指导,宁波市互联网信息办公室、宁波市经济和信息化局、国家互联网应急中心浙江分中心联合主办第二届车联网安全攻防挑战赛在宁波举行,10支来自全国的车联网安全领域的团队通过车联网攻防实战演练的方式,探索汽车网络安全领域的新技术和新突破。

□记者 乐骁立

智能网联汽车方便多多,但隐患也不少

黑客入侵车辆已不是新闻

车灯突然闪烁、车门毫无征兆的被解锁、发动机在运转中熄火,随着手指不停敲击键盘,一行行代码在车辆大屏的翻滚,随之而来的是汽车出现的各种变化。这就是车联网安全攻防挑战赛现场真实出现的情况。每一种情况的发生都代表着车内计算机系统被攻破、挟持、夺取控制权。

这种情况不仅出现在实战攻防的大赛现场,日常生活中也正在发生这种事件。2015年,两名白帽黑客Charlie Miller和Chris Valasek远程入侵了一辆正在路上行驶的切诺基(自由光),并对其做出减速、关闭引擎、突然制动或者制动失灵等操控。事件一出业界震惊,克莱斯勒为了防止汽车被黑客攻击,共在全球召回了140万辆车并安装了相应补丁。这两名白帽黑客也"自荐"成功,目前就职于通用的自动驾驶子公司。

去年,腾讯网络安全实验室的研究人员还成功远程入侵了一辆特斯拉Model X,实现对多个ECU(行车电脑)的操控,并在没有车钥匙的情况下实现开闭车门,控制灯光系统,播放音乐等功能。过去几年间,除了上述事件之外事实上还发生了几百起黑客操控汽车的案件,涉及诸多品牌和车型,包括丰田、比亚迪等一些我们熟知的品牌。

表1-1 部分汽车网络安全研究和事件

序号	时间	研究和事件描述
1	2013年	Charlie Miller & Chris Valasek通过OBD接口破解了丰田普锐斯;
2	2014年	360公司破解了Tesla汽车远程控制功能;
3	2015年	宝马汽车ConnectedDrive功能存在漏洞,需要进行大规模的远程修复;
4	2015年	Samy Kamkar破解了通用安吉星OnStar系统;
5	2015年	360公司破解了比亚迪汽车云服务,远控驾驶功能;
6	2015年	360公司破解了Tesla汽车毫米波雷达系统;
7	2015年	Charlie Miller & Chris Valasek远程破解了JEEP汽车,导致其召回140万辆汽车;
8	2016年	日产LEAF汽车API遭泄露,黑客可远程控制;
9	2016年	Troy Hunt发现了日产聆风手机App存在漏洞,全球停止NissanConnect服务;
10	2016年	腾讯科恩实验室实现了远程无接触式破解Tesla,可以在驻车状态和行驶状态下远程控制;
11	2017年	腾讯科恩实验室再次实现了远程无接触式破解Tesla。

来源:中国信通院汽车电子网络安全标准化白皮书2018

通信和娱乐系统最容易受攻击

那么,黑客是怎么入侵我们的车辆的呢?

国家互联网应急中心车联网安全工作组高级工程师、本届大赛裁判范乐君介绍,首先,车上最容易受攻击的是通信和娱乐系统,因为这些系统连接着外部网络,通过运营商的网络、WiFi、蓝牙的通道,就可以入侵,并找到一些车载APP的漏洞,攻入这些APP。而后,黑客能获取用户在这些App上的隐私数据、历史记录、使用数据,比如入侵电话软件,就听实行监听,入侵导航软件就能获取用户定位,或者给出错误的导航数据,诱使车辆偏离路线。

如今,越来越多的新能源车,全车装有大量电子器件,一旦电子器件间的网关有漏洞,黑客就可能通过这些通信娱乐软件入侵车辆内部,但这种情况比较少。

目前,要进入车辆内部,控制行车电脑和动力域,即动力系统、制动系统、转向系统,基本需要物理连接。汽车上有个接口叫OBD设备,是厂商用来诊断汽车的各种数据,这个接口集成了很多ECU的CAN总线接口,因此OBD也成了黑客攻击的主通道。通过OBD接口可以变向的访问汽车其他设备,比如雨刷,空调和动力总成等。

此外,还可以通过攻击TBOX,来入侵ECU。因为,传统汽车的联网是由TBOX来提供,TBOX类似于电脑网卡。大家都知道电脑插上网卡就能联网,汽车也是一样,通过TBOX汽车可以按照指定协议访问TSP服务器,并进行数据的收发。而对黑客而言,这个信息传输的通道,就变成了他们"拦路打劫"的要道,路上充满着"收获"的惊喜。他们可以通过这个数据通道植入病毒或程序,从而获得汽车的控制权。

如何保障汽车网络安全呢?

随着5G时代的到来,汽车网络安全的话题越来越受关注,因为这跟每个人的生命都密切相关。那么,如何提高汽车网络安全防护呢?

与会的嘉宾介绍,目前能做的就是控制权限,加强加密工作,并且建立一套完整的安全网络体系。

首先是软件开发公司要的软件开发中的安全,减少代码的漏洞,把漏洞封杀在摇篮里。

然后是每个数据接口要加强加密工作,同时对车内网络总线的要进行保护监控,并对汽车健康数据进行实时监控。此外,车辆要加装安全模块,就像杀毒软件一样,比如trustzone等硬件保护。还有就是,加强云端服务器的数据传输处理过程的保护。

以上这些都是车企、软件厂商能做的。对于普通人来说,要注意车载软件及时更新并及时关注厂家公告(软件更新可能会修复漏洞)。在对汽车原装软件进行修改时,应小心注意,给汽车连接第三方设备时应先确定其安全性,比如WIFI、蓝牙等;此外,当其余人用外部物理设备链接汽车时应小心警惕。最后一点最重要,离开车时切勿忘记锁车。

"我们也将多举行这种实战攻防演练,进一步提高应对车联网黑客攻击的能力。"范乐君说。