安全小课堂第五十四期【汽车的网络安全问题】

京东安全应急响应中心 2017-04-21

近年来，物联网的应用逐渐扩散到消费领域，汽车工业就是一例。汽车制造商不断改进技术，完善互联汽车的效能，并让驾驶者能够及时获知潜在的危险。车主还能通过智能手机应用远程解锁汽车、查看引擎状态或定位车辆所在。JSRC **安全小课堂第五十四期**，我们来聊一聊互联汽车面临着哪些安全隐患?，本期小课堂邀请到了**曾颖涛**、**李均**师傅进行分享。感谢JSRC白帽子们的精彩讨论。

《速度与激情8》中远程控制汽车的桥段是否真的可以实现?

京安小妹

远程控制是可以实现，但是只针对部分车型，前提是汽车的控制系统要有线控功能,然后汽车必须联网了。

讲师：曾颖涛、李均

远程控制汽车需要满足什么样的条件?

京安小妹

就是要能够有如wifi 蓝牙，蜂窝网之类的连接,通过这些连接接入汽车内网，内网上有各种控制器，比如变速器控制器、发动机控制器,想办法控制这些控制器来实现加速啥的动作最终实现远程控制。

讲师：曾颖涛、李均

白帽子提问:通过外网攻入内网有哪些姿势?

外网攻入内网还是讲个例子吧,比如有wifi你先连上去扫描一遍看看开放啥端口没有或者把车机的固件读出来分析固件看能不能找到负责处理这些连接的代码的漏洞如果车机有漏洞你可能会取得车机控制权,下一步要看车机是否接入了汽车内网如果接入了看是什么接口。

讲师：曾颖涛、李均

白帽子提问:有没有用http接口的地方?

车机与服务器之间就可能会用到http接口。

讲师：曾颖涛、李均

除了电影中的桥段，汽车被黑还有什么样的风险？

京安小妹

1.个人隐私数据信息泄露。
2.你的位置被泄露。
3.你的通话记录信息泄露。
4.汽车容易损坏。

讲师：曾颖涛、李均

挖掘汽车的网络安全漏洞的思路是怎样的？

京安小妹

这个你就得看你擅长的是哪方面了,比如你擅长web,那么汽车联网后都有服务器.比如你擅长移动，你就分析一下配套app,如果你擅长通信安全，那么蜂窝网。

讲师：曾颖涛、李均

汽车企业在需要注意什么才能避免汽车被黑?

京安小妹

当然是员工的安全意识提高啊，和安全厂商多合作，提高安全等级。
举几个例子,宝马connecteddrive 系统的安全等级就不够，采用了密码次的方式来轮换使用固定的一些秘要，虽然有安全意识但是没料到人家通过硬件提取密码的方式把密码池给找出来了，而且发现这个密码池通用于其他车。
员工安全意识，比如JEEP那个Uconnect 漏洞案例中，明明有认证机制的却没有使用。
和安全厂商多合作是对的，换一拨专门找茬的人来从新审视一遍方案肯定能够大大提高安全性，系统隔离,在汽车设计的时候一定要想好了再搞，不要赶时髦，觉得买个通信模块就可以入网了。

讲师：曾颖涛、李均

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文