新闻热线：010—58884062
E-mail：adaxuqian@126.com
■责编 许 茜
科技日报 2018年8月15日 星期三

小心，你的联网车副驾驶可能“坐”着黑客


视觉中国

本报记者 **张盖伦**

百度公司董事长兼CEO李彦宏曾经在两会上畅想过智能车的未来：只要把车开上高速，你就能吃着火锅唱着歌，被车轻轻松松地从北京载到上海。

360集团董事长兼CEO周鸿祎后来在公开场合“皮”了一下：有一天，你吃着火锅唱着歌，可能智能车就被黑客劫持了。

周鸿祎素来喜欢“放炮”，但他描述的画面，并非耸人听闻。

前不久，以色列一家汽车联网安全公司的CEO阿米·多坦说了这么一番话：自动驾驶汽车系统可能会充满漏洞且易被黑客攻击。

当车辆接入网络，也就给了黑客远程攻击的机会。360智能网联汽车安全实验室负责人刘健皓被称为“破解特斯拉第一人”，他曾发现特斯拉Autopilot（自动驾驶系统）存在传感器漏洞并将漏洞提交给了特斯拉公司的安全部门。刘健皓在接受科技日报记者采访时表示，漏洞不可避免，也不可能被完全清除，信息安全攻防是一场动态的持久战。

存在漏洞、错误是代码的通病

阿米·多坦给出了这样一组数字：“联网汽车每1800行代码就会存在一些错误，其中80%是安全漏洞。”他还表示，一辆联网汽车和一辆自动驾驶汽车的潜在安全漏洞数目分别为5000和15000。

这是怎么算出来的？

北京理工大学网络攻防对抗技术研究所所长闫怀志告诉科技日报记者，国际著名的CMMI（软件能力成熟度集成模型）将软件能力成熟度分为5级，其中1级最低，5级最高，4级和5级的千行代码缺陷率分别为0.92‰和0.32‰。联网汽车“每1800行代码就存在一些错误”，表明其软件能力成熟度大致在CMMI 4级和5级之间。“虽然联网汽车代码成熟度达到了较高水平，但显然还有一定的提升空间。”闫怀志说。

闫怀志认为，软件代码出现漏洞，是由软件开发和应用过程中的不正确或遗漏行为所造成的，也就是在软件设计、实现或应用过程中有意或无意导致软件架构或其具体实现与期望不符。“漏洞的出现是所有软件代码的通病，不仅仅局限于联网汽车与自动驾驶应用领域。”不过，漏洞出现的频率又跟软件研发和保障水平密切相关。比如，在级别不同的CMMI研发保障能力下开发出来的代码质量和漏洞数量会有显著差异。“自动驾驶软件属于典型的工业应用软件之一，其安全漏洞的潜在危害性，尤其是对人和物理环境的破坏性都极大，和普通软件的危害不能同日而语。”闫怀志强调。

有漏洞不是稀奇事。中国科学院微电子研究所副研究员王云表示，随着汽车智能化水平的提高，一辆车上的代码可能有几千万甚至上亿行，存在错误和漏洞是肯定的。“不光自动驾驶行业，传统软件行业都会有各种错误，不管是Windows还是iOS。”

车载娱乐系统易成被侵入对象

漏洞是如何被发现和修复的？

王云介绍，成熟的软件开发都会有标准流程，会对需求、架构设计方案、代码模块设计接口、代码机制等环节进行代码测试与评审。通过规范的流程，大部分代码漏洞可以被发现，但是依然有少部分漏洞不会被测试用例覆盖。

“联网汽车涉及各种协议或操作系统、应用软件，存在漏洞的地方更多。目前被发现的漏洞涉及TSP（内容服务提供商）平台、APP应用、Telematics Box（T-BOX）上网系统、车机IVI系统CAN-BUS车内总线等各个领域和环节。”王云表示，协议、操作系统存在的漏洞都可能被利用，造成的危害也不一样：有的能让黑客窃取用户信息，更严重的能让黑客控制汽车。

刘健皓把漏洞比喻为银行的后门。大门处有重兵把手，但后门可能就是防护真空。有心人士能通过后门大摇大摆进来“搞事情”。而且，很可能银行自己都不知道有这个后门。

车联网及自动驾驶软件，实现了车—车之间、车—人之间、车—路之间的高效互联互通与信息共享，并为车联网智能决策和优化提供了基础支撑，但它也让联网车在信息安全、功能安全及隐私保护等方面，面临着前所未有的严峻挑战。闫怀志说，黑客可以利用车载终端系统、车联网云平台、移动APP、OBD（车载诊断系统）等系统的漏洞对车辆实施攻击，实现对智能车辆的操作控制。不安全的代码也可能在无攻击的情况下“自行”失效，导致车辆行为失控。

“有通信、接口的地方就容易遭到攻击。”刘健皓说，黑客攻击车辆可以分为物理接触、近场控制、远程控制3种。在智能网联时代，黑客能“顺着网线”悄无声息地进入你的车。

在测试联网汽车时，刘健皓团队也发现，车载娱乐系统易成为被侵入的对象。如今，汽车的中控系统做得越发酷炫，为了给用户更为高科技的人机交互体验，一些实体控制按钮被集成到了车载娱乐系统当中，该系统通常也要为用户提供互联网内容。于是，黑客就能通过车载娱乐系统的漏洞一举控制车辆的仪表盘甚至制动系统。

从已有的案例来看，最夸张的情况是，黑客能控制车辆动力和转向系统。比如远程启动一下发动机，比如让你的方向盘有“自己的想法”。而且，如果黑客破解了某车厂的后台，他就能用同样的方法横向批量影响到所有该品牌的汽车。

所以，如果有汽车在道路上集体“抽风”，也不是不可能。

打一场动态信息安全攻防战

当然，如果真“集体抽风”就成了公共安全事件，一切都要防患于未然。联网车并不只是黑客的猎物，实际上，车厂也会采取种种措施升级自己的防护机制。与入侵者斗智斗勇，本身就是一个你来我往、你攻我挡的动态平衡过程。

“安全防护不只是防护某个‘点’，一定要做到全面。”刘健皓说。所谓的全面，指的是在云（云服务）、管（通信）、端（车载终端）、控（控制系统）上全面保驾护航。

闫怀志表示，代码错误的避免和纠正，需要标本兼治，且应以治本为主，治标为辅。“标”是采用各种漏洞挖掘、分析、测试及修复手段来避免或减缓其安全威胁；“本”上还是应该严格遵循软件安全工程规范，从源头上解决问题。尤其是对于车联网和自动驾驶这种工业软件来说，要特别重视功能安全与信息安全二者的结合，从其全生命周期统一考虑各种安全因素。“具体来说，是识别工业应用软件的危险，定义其安全需求，然后进行安全设计、安全编码及安全测试，进行有效的缺陷管理，即实施基于功能安全与信息安全融合的工业应用软件安全工程方法。”

闫怀志介绍，在进行具体安全设计和代码编写时，可参考多种安全编码标准和指南。比如，汽车行业可以参考汽车电子功能安全标准（ISO 26262），还可以参考国际著名的MISRA（汽车工业软件可靠性联合会）的工业C编程规范。“该规范为汽车嵌入式系统编码提供了有关安全可靠性的最佳实践。”闫怀志说。

王云透露，国际组织（ISO/SAE）正进行21434（道路车辆—信息安全工程）标准的制定。该标准主要从风险评估管理、产品开发、运行/维护、流程审核等4个方面来保障汽车信息安全工程工作的开展。

在具体实践上，360智能网联车安全实验室给车企的建议是——“逆向思维”。在车辆正式推出之前，他们会对合作车企车辆进行测试，模拟黑客对车辆进行攻击；发现漏洞后，让车企对薄弱环节进行修正。车辆上市后，团队会为车辆做全生命周期的安全管理，监控和防护其可能遭到的攻击。

“没有一个安全公司能够保证车辆百分之百安全，跟黑客对抗的过程是动态防护的过程：发现攻击、阻断攻击、下发更新策略……”刘健皓强调，“我们希望为每个车厂建立一套安全的运营体系，实现自主品牌车辆的安全运营。”

牵手区块链，能让密码更安全吗

行业观察

实习记者 **于紫月**

“区块链概念持续升温，这股热潮也涌进了商业密码行业，目前市场上出现了很多做区块链密码的创业公司。”众享比特科技有限公司高级顾问陈红在近日举办的商用密码高性能技术创新发展论坛上对科技日报记者说。

作为炙手可热的比特币的底层技术，区块链技术具有去中心化、无法篡改、可追溯等特点。区块链上的每个用户均可参与到数据库的记录工作，在没有权威中间机构的统筹下，也可实现信息的传递与交换。

近三年来，区块链技术的研发与应用步入了快车道，它已与通信、医疗、金融等多个领域进行结合。如今，它又将触角伸向了商业密码。

加持以安全著称的区块链，强强联合之下，能让密码更安全吗？


视觉中国

“在区块链技术的支持下，商业密码无需再依赖第三方机构，能大大降低被篡改或被恶意攻击的风险，使密码的安全性得到大幅提升。”众享比特科技有限公司副总裁陈鸿刚对科技日报记者说，以身份认证为例，过去一旦存储密码的服务器遭到破坏，就可能导致大量用户密码泄漏，后果十分严重。而在采用区块链技术后，可将用户密码的存储模式改为分布式，进而大大降低“拖库”“撞库”等网络攻击的概率，即便部分区块链节点失效也不会对整个系统认证造成影响。

此外，商业密码也能提升区块链技术的使用效率。

“如今虽然区块链技术炙手可热，但它并非完美无瑕。”陈鸿刚表示，其区块容量有限、确认耗时长、能耗大等问题一定程度上限制了它在商业领域的应用。

陈鸿刚进一步解释，由于区块链存储数据量有限，且数据添加需要在链上的每个节点进行记录和认证，所以在存储图片、视频等大文件时，区块链的工作效率会大幅降低。但倘若与商业密码算法相结合，这个问题就会迎刃而解。

商业密码的常用算法是哈希算法，这一算法可将大文件转换成独有的哈希值，再将这一数值上传至区块链。哈希值通常为数字，占用空间极小，如此一来，区块链的效率将大幅提升。

不过，区块链与密码的结合也存在着一些障碍。

首先是应用场景。“商业密码是避免信息泄露的有效途径，其核心技术在于算法。对所有用户透明、公开的区块链技术在有些特定场景中并不适用。”陈鸿刚说，例如涉及商业机密或军事信息，这就需借助算法对链上数据进行加密存储，设定用户访问权限，在分享数据的同时加强隐私保护。

其次是技术衔接问题。陈鸿刚认为，对现有非区块链密码系统进行改造、升级的难度颇大。在推广的过程中，缺少“一键式”的替换方案，使得用户密码升级程序多、情况复杂。此外，目前国内缺少相关详细的法律规范及技术标准指引，行业规范有待进一步加强。

硬件设施落后也是现阶段的一个难点。“不过，硬件基础薄弱或许是件好事。因为以前都是围绕着国外现有的基础架构在进行思考，现有的架构限制了科研工作者的思路。”渔翁信息技术股份有限公司总裁郭刚对科技日报记者说，“走完全自主、可控的道路才是王道。”

IT辣评

点评人：本报记者 **王小龙**

Magic Leap推出首款产品 光说不练假把式，脚踏实地赢未来

炒作了好几年、钓了无数人胃口的AR头显Magic Leap one终于在近日正式发售了，售价为2295美元，首批公布的应用共有5款。

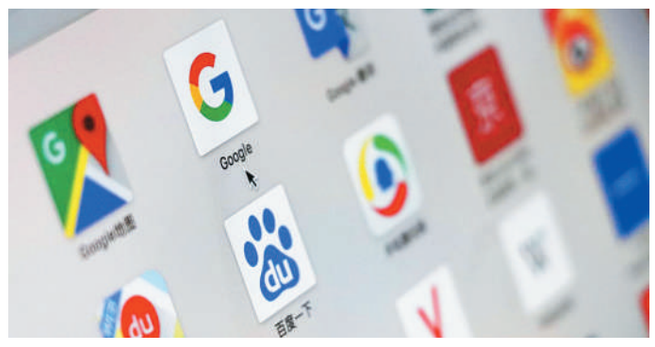
点评：成立7年，没有正式推出过任何一款产品，仅凭借几段Demo视频和几台样机就顺利拿到了超过23亿美元的融资，还得到了包括谷歌、阿里这些互联网巨头的支持……这样的事情或许只有Magic Leap才能做到。就在支持者们的信心快被消磨殆尽的时候，Magic Leap one姗姗来迟。非但如此，还挑了一个非常吉利的时间——8月8日。以AR和VR为代表的图像技术为我们勾画出了全新的交互方式，但“虚拟”终归还是要落在实处。创业不能只靠“画大饼”，过去吹过的牛总是要兑现的，即便不能100%实现，至少也得实现80%吧。在移动互联网时代，商家只有凭借过硬的技术实力和完美的用户体验才能最终赢得市场。

三星低调发布Galaxy Note9 电池变大、内存升级，可市场已不在

日前，三星电子正式发布旗下高端旗舰智能手机Galaxy Note9，新机升级到了4000毫安电池，一个完全重新设计的S Pen（手写笔），搭载最新的骁龙845芯片和高达8GB的内存和512GB的存储空间。此外，三星的DeX软件也已经内置在手机中，且不需要底座，就可以把它插到任何外部显示器上，获得类似传统PC的桌面体验。

点评：和以往的新机发布相比，今年Galaxy Note9的发布略显低调。三星没有大张旗鼓的宣传，市场反应更是出奇地冷清。曾经备受追捧的三星Note系列，如今在中国市场已被边缘化。5年前，三星在中国智能手机市场还占有20%的份额，而今年已降至不到1%。随着华为、小米、OPPO、vivo等国产手机品牌的崛起，三星手机的份额不断缩减。再加上除了S Pen手写笔外，Note9身上几乎看不到任何让人眼前一亮的创新点，被冷落自然也在情理之中。

传言谷歌计划重返中国大陆 时移世异，搜索不再是业务重心



前不久，《人民日报（海外版）》在社交媒体上刊文，文章针对近来传出的谷歌计划重返中国大陆的消息作出回应。文章称欢迎谷歌重返中国大陆，但前提是必须遵守中国法律。对此，百度创始人李彦宏在朋友圈表示：“如果Google决定回到中国，我们非常有信心再PK一次，再赢一次。”

点评：自从2010年谷歌宣布退出中国大陆以来，其重返的传闻就一直没有断过。这次“人民日报”和“李彦宏”这两个热词的加入，让“谷歌返华”再次登上了不少媒体的头条。网友纷纷站队，就百度能否再赢一次谷歌展开论战。辣评君以为，目前我们最应该讨论的不是谷歌是否会返回的问题，而是谷歌想做什么以及怎么做的问题。8年来，中国的互联网已经发生了翻天覆地的变化，早已从PC时代进入了移动互联网时代。而谷歌也早已把业务的重点转向了人工智能、无人驾驶等前沿领域。辣评君相信，即便谷歌返华，重点也不会是传统的搜索业务。前段时间，由谷歌开发的爆款人工智能小程序“猜画小歌”就是一个很好的例子。

（本版图片除标注外来源于网络）