

简译版

## 研究人员发现操纵道路导航系统的新方法

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Researchers Stealthily Manipulate Road Navigation Systems		
原文作者	Eduard Kovacs	原文发布日期	2018 年 7 月 16 日
作者简介	Eduard Kovacs 是 SecurityWeek 的特约编辑。		
原文发布单位	SecurityWeek		
原文出处	<a href="https://www.securityweek.com/researchers-stealthily-manipulate-road-navigation-systems">https://www.securityweek.com/researchers-stealthily-manipulate-road-navigation-systems</a>		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。</li> <li>本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。</li> <li>译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。</li> <li>本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。</li> </ul>		

## 研究人员发现操纵道路导航系统的新方法

Eduard Kovacs

2018 年 7 月 16 日

**来自弗吉尼亚理工大学、中国电子科技大学和微软研究院 (Microsoft Research) 的一组研究人员发现了一种新型 GPS 欺骗方法，该方法已被证明对道路导航系统非常有效。**

GPS 欺骗已经出现多年。理论上说，这种攻击方法可以诱骗驾驶员开往任意目的地，但实际上，被误导导航系统提供的指令经常与实际道路相矛盾(例如在直行的高速公路上左转)，这使其不太可能应用于现实场景。

如今，研究人员发现了一种更有效的、更不容易引起怀疑的方法。使用该方法，攻击者可以诱骗受害者驶入错误的路线(例如，使救护车和警车不断转圈)，使目标车辆开往特定目的地，或使目标车辆驶入危险的环境中(例如，逆向驶入高速公路)。

为了使攻击有效，攻击者需要知道目标的大概目的地。该技术最可能的受害者是不熟悉目的地区域的驾驶员。

基于曼哈顿和波士顿的 600 条出租车运行路线，研究人员创建了一种算法，可以生成模拟真实道路状况的虚拟路线。这种攻击最有可能在道路网密集的城市中发挥作用。

攻击者创建假的 GPS 信号，将受害者的目的地设置为邻近的“虚拟目的地”(ghost location)。导航系统会重新规划新路线——“虚拟路线”(ghost route)，指示受害者一步一步地到达虚拟目的地。

为了避免引起怀疑，研究人员根据收集到的出租车运行路线生成虚拟路线。他们在每个路段运行搜索算法，以确定所有可能的攻击路线。在测试期间，该算法为每个目标旅程平均找到了 1500 个潜在的攻击线路。



(a) 初始导航路线  $P \rightarrow D$  ; (b) 虚拟目的地 B ; (c) 受害者的实际路线  $A \rightarrow C$

“该算法精心设计一些 GPS 信息输入，传送给目标导航设备。这样触发的导航指令和地图上展示的路线就能与实际道路网保持一致了。”研究人员在他们的论文中说。

在某些情况下，如果初始目的地不在通往虚拟目的地的路线上，导航系统可能会重新规划路线。但是，研究人员的调查显示，这不会引起太多怀疑，因为现实中经常发生这种情况。

可以使用成本大约为 200 美元的便携式 GPS 欺骗器执行此类攻击。攻击者可以将其放置于目标车辆上，进行远程控制；或者将其放置于距离目标车辆 40-50 米（130-160 英尺）的尾随车辆上。

研究人员使用自己的汽车在现实场景中测试了此类攻击。为避免造成麻烦，他们选择午夜后在郊区进行测试。他们还邀请 40 名参与者（美国和中国分别 20 名）使用可以通过新方法攻击的驾驶测试模拟器。测试表明，此类攻击的成功率高达 95%，只有 1 名中国参与者和 1 名美国参与者发现了攻击。

## 安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队,安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队,为用户提供端点防护、流量监测、快速处置、深度分析等产品,以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门,提供高级威胁和新兴威胁解决方案和能力体系,产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点,全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴,安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可,安天已连续五届蝉联国家级安全应急支撑单位资质,亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点,在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面,提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动,进行了深度的解析,对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上,安天创始人、首席技术架构师作为网络安全领域的发言代表,向习总书记进行了汇报。2016 年 5 月 25 日,习近平总书记在黑龙江调研期间,视察了位于哈尔滨科技创新城的安天公司,对安天负责人说,“你们也是国家队,虽然你们是民营企业”。

安天实验室更多信息请访问: <http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问: <http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问: <http://www.avlsec.com>