简译版

黑客仅需几秒就能克隆特斯拉 Model S 的钥匙

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	Hackers Can Clone Tesla Key Fobs in Seconds		
原文作者	Eduard Kovacs	原文发布日期	2018 年 9 月 11 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	https://www.securityweek.com/hackers-can-clone-tesla-key-fobs-seconds		
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 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 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。 • 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。 • 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。 • 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。		

黑客仅需几秒就能克隆特斯拉 Model S 的钥匙

Eduard Kovacs

2018 年 9 月 11 日

研究人员声称发现了一种新的攻击方法，可用于快速克隆特斯拉 Model S（可能还有其他汽车）的遥控钥匙。

许多高端汽车使用“无钥匙进入和启动系统”（Passive Keyless Entry and Start System，PKES）打开车门和启动发动机。该系统依赖于靠近车辆的配对钥匙。

众所周知，PKES 易受中继攻击，攻击者经常利用该方法窃取高端汽车。这些攻击涉及汽车和智能钥匙之间的中继消息：攻击者靠近特斯拉 Model S，利用黑客设备收集电子锁信号；接着靠近车主（钥匙），收集密钥信号。之后，攻击者就可以打开车门、启动发动机了。然而，在这些中继攻击中，汽车只能被解锁并启动一次，而且需要合法的钥匙在一定的距离内。

比利时鲁汶大学（KU Leuven University）计算机安全及工业加密研究小组（COSIC）的几位研究员发现了一种新的攻击方法，可以在几秒钟内克隆钥匙。之后，攻击者就可以随时解锁和启动一辆汽车了。

“在正常操作期间，汽车会定期广播其识别符（ID）。钥匙接收到汽车的 ID，如果它是预期的汽车 ID，钥匙就会回复，表示它已准备好接受质询。”研究人员在博客中解释说。“在下一步中，汽车向钥匙发送随机质询。钥匙计算出一个响应并回复给汽车。在收到钥匙的响应后，汽车必须对其进行验证，然后才能打开车门。这种质询-响应不断重复，直到汽车启动。”

研究人员指出，在此过程中存在一些安全问题。例如，没有很强的验证措施，使得一般人都能轻易获得钥匙的响应内容。这是因为只要获得汽车的 ID 就可以，而这个 ID 是由汽车自身定期主动广播的，易于获取。

还有一些与加密相关的问题：钥匙使用 DST40（40 位加密密钥）来计算响应，安全性较低。十多年前，研究人员发现，使用至少两个质询响应对就可以恢复加密密钥。

鲁汶大学研究人员描述的攻击主要有四个阶段。在第一阶段，攻击者获得汽车广播的 ID。然后，利用该 ID 冒充目标车辆并向钥匙发送两个质询。

获得响应对并恢复 40 位加密密钥后，攻击者可以冒充钥匙，解锁并启动汽车。

攻击者可以使用售价 400 美元的 RFID 分析工具 Proxmark 3，从 1 米（3 英尺）外执行攻击。然而，专家认为，如果使用专门构建的天线和传输硬件，这一距离可以增加到 8 米（26 英尺）。

该研究主要针对特斯拉 Model S 使用的 PKES 系统。然而，该 PKES 系统由 Pektron 制造，并被其他几家汽车制造商使用，包括 McLaren、Karma 和 Triumph，这意味着他们的汽车也会受到影响。

特斯拉与研究人员合作，实施防止攻击的措施，但其他汽车制造商尚未对该漏洞做出回应。

特斯拉于 2017 年 8 月首次收到关于此漏洞的通知，直到最近几周才解决了这一问题，推出了改进的钥匙加密技术，并引入了一项可选的“PIN to Drive”功能，该功能要求在仪表板显示器上输入 PIN 码，匹配成功后才能驾驶汽车。

可以将钥匙放在屏蔽 RF 信号传输的特殊盒子或袋子中，来防止此类攻击。然而，这违背了无钥匙进入和启动系统的目的。

研究人员并不打算公开他们开发的工具，但很快会发布一篇包含技术细节的论文。

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，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，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“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