攻击者可以利用键盘上的热成像窃取口令

简译版

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	Attackers could use heat traces left on keyboard to steal passwords		
原文作者	Tomáš Foltýn	原文发布日期	2018 年 7 月 6 日
作者简介	Tomáš Foltýn 是一位安全作家。 https://www.welivesecurity.com/author/tfoltyn/		
原文发布单位	WeLiveSecurity		
原文出处	https://www.welivesecurity.com/2018/07/06/thermanator-attackers-heat-keyboard-password/		
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。		

攻击者可以利用键盘上的热成像窃取口令

Tomáš Foltýn

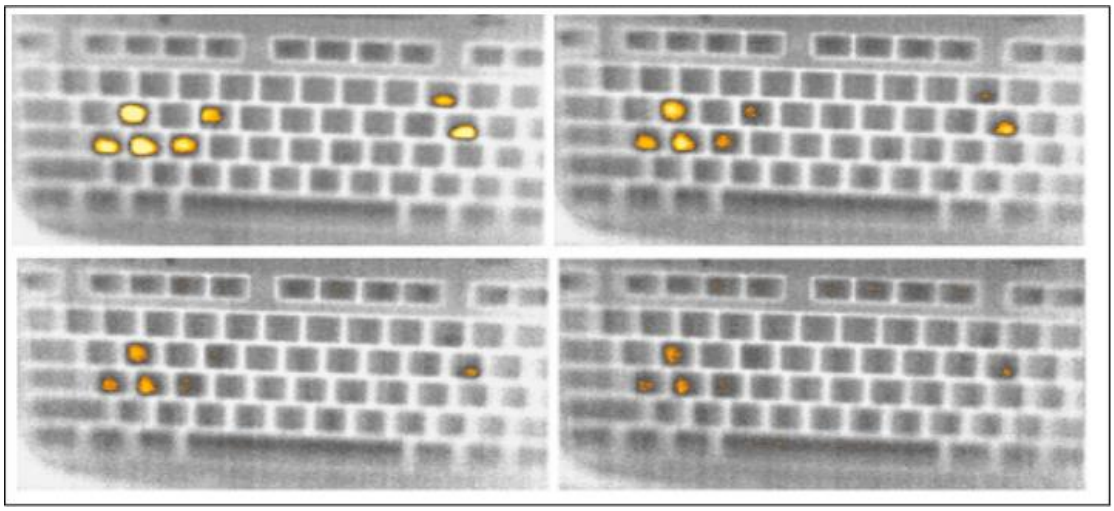
2018 年 7 月 6 日

这种名为“热终结者”（Thermanator）的攻击可以利用手指余温的热成像，窃取你在电脑键盘上输入的凭证或任何其他短字串。

加州大学艾尔文分校（UCI）的学者提出了一种新的攻击方式：使用者在键盘上输入口令后，攻击者可以利用热成像摄影机搜集到键盘上的余温，从而窃取输入的口令——1 分钟之内这个方法都可行。

在测试中，研究人员让 30 名参与测试的人员在 4 款普通外界键盘上输入 10 组不同的口令（包括强口令和弱口令），之后使用热成像摄像机扫描键盘余温。在测试的第二阶段，8 名未经专业训练的使用者充当“攻击者”，根据热成像数据得出输入的口令——结果都挺靠谱。

研究人员在一篇名为《热终结者：键盘口令输入的事后余温攻击法》的论文中指出，在按下第一个键的 30 秒之内，测试者可以还原完整按键；在按下第一个键的 1 分钟内，则可以还原部分按键。由此获得的部分按键可用于口令破解攻击。



口令“passw0rd”输入 0、15、30 和 45 秒后，键盘上余温的热成像（加州大学艾尔文分校提供）。

“如果你输入口令后马上走开，攻击者就可以窃取你的口令了。”该论文的一位作者吉

恩·图斯迪克（Gene Tsudik）说。

“作为恒温动物，人类喜欢低于体温的环境。”论文写道，“由于这种热差异，我们不可避免地会在经常触摸的许多物体上留下余温，尤其是徒手接触时。”

2011 年的一项研究表明，通过分析自动取款机按键上的余温，可以恢复输入的密码。

与此同时，对 Thermanator 的研究还表明，由于单指或双指打字（hunt-and-peck）会留下较大的指纹和热痕迹，因此 Thermanator 攻击对此类人群特别有效。盲打（touch typist）需要将手指放在“home 键”，会产生更多的热噪声，因此更加安全。（译者注：在盲打中，两个大拇指控制空格键，左手另四指分别放在 A、S、D、F 四个键上，右手另四指分别放在 J、K、L、；四个键上。）

要想攻击有效，还需要满足一些条件。最重要的是，受害者必须在输入敏感信息后立即离开或被引诱离开，而且热成像摄像机必须能看清整个键盘。

该论文指出，这种“事后内部攻击”对基于口令的系统带来了新的威胁，其中一个原因是“过去昂贵的侦测设备越来越便宜”。

缓解措施

该论文提出了一些缓解措施，能够加大攻击者还原击键的难度，甚至使他们无法收集数据。这些措施包括：输入口令后用手在键盘上抹几下；或者随机多按几个键，以便增加“热噪声”。

还可以使用鼠标点击虚拟键盘输入口令。然而，这可能会增加“肩窥”（当你输入敏感信息时，有人越过你的肩膀偷看）攻击的风险。

另一个不太实际的措施是：戴上绝缘手套，甚至假指甲。研究发现，丙烯酸塑料指甲足以应对 Thermanator 攻击。当然，如果你不选择这种方法，也没什么可责怪的。

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*