通过分析智能手机电磁辐射来寻找安全漏洞
由卡三和 CSIC（高等科学研究委员会）研发的新项目

马德里卡洛斯三世大学（卡三）和高等科学研究委员会（CSIC）的研究人员正在研发一个新的应用。该应用可分析手机是否可能遭受网络攻击，从而通过电磁辐射获得加密密钥。

该项目的目的是通过使用加密技术，完善手机和其他电子设备的安全性。该发明在加拿大最近举办的物联网安全与隐私国际研讨会（Workshop on Security and Privacy on Internet of Things）被提出。

该研究集中在我们了解的“侧通道攻击”—“当某种情况可以被利用（这里具体指任何电流产生一个磁场）而获得非法利益（这里具体指攻击者试图提取私有的理论上无法访问的加密密钥）。”研究人员之一，卡三计算机安全实验室（COSEC）的何塞· 玛利亚· 德· 福恩特斯（José María de Fuentes）解释。

传统上，加密算法被尝试攻击—即保护信息的过程通常具有复杂的数学基础。然而渐渐的，这种类型的侧通道攻击已经发展到寻找其他方式来违反安全，而无需“破坏”维持它的数学。“当设备运行时，它们使用能量并产生电磁场，而我们试图捕获它们的踪迹以获得加密密钥，并且反过来解密数据。”另一位研究员，同样是卡三计算机安全实验室小组成员的罗莱纳· 冈萨雷斯（Lorena González）表示。

数字漏洞

“我们要证明这类设备是否有漏洞，因为如果它们可以被某些不法分子攻击—即如果有人计算出你手机上正在使用的密码，那手机就非常容易被攻击，并且数据将不再是私密的。”另一位研究人员，CSIC 物理和信息技术研究所（ITEFI）的路易斯· 埃尔南德斯· 恩希纳斯（Luis Hernández Encinas）表示。

该研究的根本目的是检测并确认电子设备或其芯片是否有漏洞，从而无论是用户对软件还是硬件的开发都可以采取适当的对策来保护其安全。“接下来我们的工作是验证这是否已正确执行，并再次尝试检查是否还有其他类型的漏洞。” 路易斯· 埃尔南德斯· 恩希纳斯补充说明。

研究人员认为，该项目最重要的一点是开发一个可以继续探索此类侧通道攻击的架构和工作环境。实际上，存在从其他数据中提取加密信息的可能性，如设备的温度变化，功耗或者芯片处理计算所花费的时间。

该项目在 CIBERDINE（网络安全：数据、信息和风险）—一项由马德里大区教育、文化和体育厅与欧盟结构基金会联合拨款的研究发明与创新（I+D+i）项目的框架下研究。其最主要的目的是开发技术工具，使网络空间成为公共管理、公民及企业更安全可靠的环境。为了实现这个目的，研究主要有三个大方向：网络数据的大量分析、合作性网络安全以及该领域的决策帮助系统。

参考书目：

《从密码设备获取和分析痕迹的框架》：*A Framework for Acquiring and Analyzing Traces from Cryptographic Devices*
作者：A. Blanco Blanco， J.M. de Fuentes， L. González Manzano， L. Hernández Encinas， A. Martín Muñoz ， J.L. Rodrigo Oliva 和 I. Sánchez García
物联网安全与隐私研讨会 （SePrIoT） 2017
第 13 届 EAI 国际通信网络安全与隐私大会
2017 年 10 月 25 日，尼亚加拉大瀑布，加拿大
http://www.seg.inf.uc3m.es/~lgmanzan/docs/SCAP.pdf

更多信息:

CIBERDINE 项目： http://www.seg.inf.uc3m.es/ciberdine

Atención a medios de comunicación
T: 91 624 90 35 / 639 906 177
medios@uc3m.es