听《Opportunities and Challenges of Side-Channel Security in the Era of Confidential Computing》有感

2019年3月22日，我有幸参加Yinqian Zhang博士关于机密计算场景下侧通道安全相关技术的分享。

Zhang博士是俄亥俄州立大学计算机科学与工程系的助理教授。他的研究兴趣一般在于计算机安全。他最着名的研究主题是侧通道安全，特别是在云计算，移动计算和机密计算方面。在过去十年中，他在众所周知的会议论文集和期刊上发表了大量高质量的同行评审研究论文。作为系统安全和辅助渠道方面的专家，他经常被邀请担任顶级安全场所的技术计划委员会成员，如IEEE S＆P，ACM CCS，Usenix Security和NDSS。2013年获得安全奖学金，2018年获得国家科学基金会颁发的职业奖，2019年获得俄亥俄州立大学颁发的Lumley研究奖和教师教学奖。同时，Zhang博士被认为是安全最具影响力的AMINE学者之一在2018年。

机密计算利用现代处理器的新兴安全组件（如英特尔SGX和AMD SEV）在不受信任的软件堆栈上安全地执行应用程序。通过机密计算使得各种隐私敏感应用（例如，机密云计算和隐私保护区块链）成为可能。但是，先前的研究表明，机密计算容易受到各种侧通道攻击。 本演讲总结了Zhang博士最近在这方面对侧通道的研究，并重点介绍了我们提出的一些解决方案，这些解决方案为具有机密性要求的应用提供了侧通道弹性。

所谓侧通道攻击是指不直接读取比如账号的密码之类的信息，另辟他路。举例来说，目标设备旁边的磁探针去测量设备在执行加密操作时泄露的电磁辐射，从中提取出加密重要数据的密钥。研究人员称他们能完整提取出运行在iOS设备上的OpenSSL和 CoreBitcoin签名密钥，部分提取出Android设备上的 OpenSSL密钥。

对智能卡的旁路攻击，是上世纪 90 年代末提出的。攻击者在智能卡的 VCC 或 GND 上串联一个小的电阻，使用示波器测量该电阻上的电压降，测量的电压降和芯片的能量消耗成正比，因此可以将电压降作为能量消耗来处理，并将对应的曲线波形视为功耗曲线。同样的道理，探测电磁变化获取智能卡芯片的功耗曲线也能进行攻击。这类旁路攻击叫做能量分析攻击（Power Analysis Attack）。能量分析攻击又分为简单能量分析攻击和差分能量分析攻击，其中简单功耗分析（Simlpe Power Analysis, SPA）攻击是从密码芯片运算的功耗波形上能够直接找出一切密钥信息的攻击方法。因为在芯片中，密钥位为 0 时运算的功耗和密钥位为 1 时运算的功耗存在差异，通过这样的差异分析出密钥位的值，按照一定规律组合得到完整的密钥。而差分功耗分析（Differential Power Analysis, DPA）攻击是需要知道算法的明文（输入）和密文（输出），通过对一系列的功耗轨迹进行分析和计算，重现加密密钥的攻击方法。

相比于直接窃取密码，侧通道攻击更加难以防范，硬件的厂商需要投入额外的大量经费。随着物联网的普及与发展，硬件设备安全将是未来重要的一环，而测通道攻击的防范也将是限制其发展的一堵大墙。