2021 年招收博士生、硕士研究生参与以下相关项目，有兴趣可联系张老师：

Email: zhangjiliang@hnu.edu.cn
Phone: 13875885226（微信）

项目 1: 计算机体系结构安全研究

简介: CPU 被认为是计算机的大脑，如果 CPU 存在漏洞，那么运行在其上的软件的安全性就难以保证。自 2018 年，主流高性能 CPU 上被曝出存在“史诗级”漏洞 Spectre 和 Meltdown 以来，对复杂通用计算机的侧信道攻击进入了一个新的阶段，各种攻击变体纷纷被提出。此类攻击主要利用了为提高处理器性能而提出的机制——分支预测与乱序执行。一个异常或错误预测的分支在提交指令之前，CPU 会继续执行一个瞬态指令序列。直到错误执行的指令退役时，CPU 发现异常/错误预测并刷新管道，以丢弃任何指令在体系结构上留下的“痕迹”。然而，指令造成的微体系结构信息变化却无法消除，攻击者利用时间差等信息可恢复出数据。现有的解决思路主要是消除时间差或在判断指令安全之前禁止敏感数据传播。主要的方案有分区、地址随机化、跟踪信息、阻止信息更新或传播等，但这些方法通常开销很大，难以部署；或者它们通常只解决攻击的一方面，仍留下其他可能的攻击面。发现新的漏洞并解决这些漏洞已经成为学术界和工业界研究的新课题，这对解决计算机系统安全问题具有重要意义。

项目 2:深度神经网络安全之对抗样本构建与防御

简介: 随着人工智能时代的到来，机器学习，特别是深度神经网络已经在图像识别、语音处理、自动驾驶汽车和医学诊断等领域展现出巨大的优势,尤其是图像识别模型已超出人眼识别图像的精确度。然而最近的研究表明深度学习模型容易受到对抗样本的攻击，对抗样本是一类被攻击者精心设计来 fool 深度学习模型的样本，它们与真实样本的区别几乎无法用肉眼分辨，但是却会导致模型进行错误的分类。对抗样本的存在会使得深度学习在安全敏感性领域的应用受到严重威胁。因此，近年对抗样本的构建以及防御成为人工智能安全领域的研究热点。本项目旨在研究新的对抗样本构造方法及其相应的防御技术。

项目 3: 基于机器学习的物理不可克隆函数攻击与防御技术研究

简介:物理不可克隆函数（Physical Unclonable Function，PUF）是一种新的轻量级硬件安全原语。当输入一个激励时，PUF 利用芯片制造过程中难以预测的工艺偏差（Process Variation），输出依赖于芯片的不可克隆的响应，非常适合资源受限环境下的设备认证。然而，攻击者可以收集一定数量的 CRPs 对 PUF 进行建模，因此，PUF 易受基于机器学习的建模攻击。现有的抗机器学习攻击方法可分为结构非线性化和 CR 混淆，但是这些方法很难做到兼具开销小、高稳定和高抗机器学习攻击效果。本项目旨在研究新的机器学习攻击与防御技术。

项目 4: 软件代码重用攻击与防御技术研究

简介:代码复用攻击作为一种全新的攻击手段，不需要注入任何恶意代码，仅利用程序已有的合法代码进行攻击，能成功绕过数据执行保护等多种防御机制，引起学术界和工业界的极大关注和研究。当前代码复用攻击防御技术主要有基于软件的方法和硬件辅助的方法。基于软件的方法性能开销过大，难以部署在实际系统中；硬件辅助的方法虽能减少性能开销，但需要扩展指令集和修改编译器，存在密钥泄露等问题。为解决这些问题，本项目提出一种新的硬件辅助防御技术，主要创新如下：首先，提出一种新的硬件辅助抗代码复用攻击的体系结构，从根源上避免了需要修改指令集和编译器的问题；其次，提出汉明距离匹配和指令级数据隐藏技术，结合物理不可克隆函数，以极低的性能开销和高安全性抵抗代码复用攻击；

最后，提出一种可重构物理不可克隆函数，使产生的密钥可动态更新，以防御高级的全函数复用攻击。本项目的研究对提高系统的安全性具有重要科学意义。

以上课题研究受到国家自然科学基金重点项目、面上项目、青年基金、装备预研、湖南省自然科学基金、湖南省科技计划项目、CCF-IFAA（蚂蚁金服）、CCF-腾讯犀牛鸟基金等项目资助。