会议主题：

* 基于人工智能的恶意软件检测与对抗性学习，以及数据服务平台

会议总结：

1. 从恶意软件检测到对抗性学习—江纬 ：
   1. 主要内容
      * 1. 恶意软件检测(难点，进展，成果)
        2. 对抗性学习（未来研究的重点）
        3. 数据科学团队建设
   2. 讨论
      * 1. 对抗性学习能否与应用结合？
        2. 现有的研究模型（如PE模型，APK模型，PDF模型）能否结合到防火墙，终端安全产品中？
2. 数据服务平台—王木梯：
   1. 主要内容
      * 1. 数据基础架构（CPU:42H；内存：106G； 存储：34T）
        2. 病毒数据样本来源渠道与共享（https://admin.qy.com）
        3. 病毒数据样本信息处理以及现有技术处理方式
        4. 病毒样本数据服务扩展（沙箱分析报告，病毒危害等级分析，逆向分析报告，数据可视化，cert年度报告）
   2. 讨论
      * 1. 都比较同意数据收集的重要性，并鼓励与支持继续做好数据收集的工作
        2. 在数据收集的同时，能否做到数据的关联分析，关联CVE，并且做出报告，提出解决方案，打补丁等等
        3. 数据处理结果能否提供API对其他开发人员调用
3. 深度学习模型的对抗－陈俊航
   1. 主要内容
      * 1. 黑盒攻击与白盒攻击
        2. 防守之健壮性（对抗学习，扰乱梯度，降维）
        3. 检测（Sample Statistic,Training a Detector, Prediction Inconsistency）
   2. 讨论
      * 1. 图片识别在网络安全中的应用
4. 恶意文件检测与对抗性学习 – 王凤娇
   1. 主要内容
      * 1. 黑盒攻击与白盒攻击
        2. 防守之健壮性（对抗学习，扰乱梯度，降维）
        3. 检测（Sample Statistic,Training a Detector, Prediction Inconsistency）
   2. 讨论
      * 1. 图片识别在网络安全中的应用

需求：

1. 产品落实
2. 数据中心的建立

亮点：

1. 数据的重要性，是持久的；是否可以有基因工程的数据

技术分享的方法是可行的，下次继续