**蓝盾前沿技术分享会 会议报告**

会议时间:

* 2018年8月9日 14:00 – 16:00

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

## 会议流程：

|  |  |  |  |
| --- | --- | --- | --- |
|  | 时间 | 演讲主题 | 演讲者 |
| 1 | 14:00 - 14:20 | 从恶意软件检测到对抗性学习 | 江纬 |
| 2 | 14:20 - 14:35 | 数据服务平台 | 王木梯 |
| 3 | 14:35 - 14:50 | 深度学习模型的对抗 | 陈俊航 |
| 4 | 14:50 - 15:05 | 基于人工智能的恶意文档检测与对抗性学习 | 王凤娇 |
| 5 | 15:05 – 15:20 | 双语文档及语料库管理——标准化&内容管理 | 魏舒敏 |
| 6 | 15:20 – 15:40 | 画像的得失 | 刘峰 |
| 7 | 15:40 – 16:00 | 技术讨论与交流 | 全体 |

注：前沿技术分享 每个演讲者大约10分钟，还有5分钟为问答（Q&A）环节。如果您对其中的内容感兴趣，可以直接找对应的小伙伴。所有研究数据及代码都可以共享给大家。

参与互动讨论，请扫描左方二维码

会议内容和讨论：

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. 传统AI模型的建立
        2. 对抗性学习逃逸AI模型
        3. AI模型如何抗逃逸
        4. 模型的应用场景
   2. 讨论
      * 1. 从产品的出发点来看，能否将PDF检测模型放入到出入口检测器
        2. 针对于有恶意性质的，并且具有逃逸性的恶意文件，就标识为有重大危险的标签，这种文件的危害会更大，并且不容易被检测到
5. 双语文档及语料库管理(标准化&内容管理)– 魏舒敏
   1. 主要内容
      * 1. 技术用语标准化管理（产品界面中文用于一致性，建立各产品预料库，语言包）
        2. 英文技术文档阅读支持
   2. 讨论
      * 1. 建立语料库是一个很大又重要，同时需要各产品线的同事相互配合，同时改善工作效率
6. 画像的得失 – 刘峰
   1. 主要内容
      * 1. 基于标签体系实现用户画像
        2. 安全领域画像的问题
        3. 深度学习与经典机器学习（深度学习-必然趋势）
   2. 讨论
      * 1. 结合各自业务场景，选择合适的方法

会议总结：

1. 数据中心的建立，现在各种方法都在兴起，可是所有的方法都依赖于数据之上，各位领导也表示，数据中心的建立与数据处理，是一个长久的战略
2. 前沿技术与产紧密交互，引导与支持产品开发

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