**王凤娇**

**Email:** [yonahwang@foxmail.cm](mailto:yonahwang@foxmail.cm)

**WeChat:**  wfjyouyoude

**Cell：** 15602209397

**Github :** <https://github.com/Yonahwang>

**求职意向：**AI算法研发工程师 & 数据分析

**自我简述**

**reasum_line7**

我是王凤娇，2016年毕业于西南林业大学，计算机技术与科学学院，信息工程4年制本科学历。毕业后在蓝盾股份前沿部门从事机器学习与信息安全等相关研究工作。

**工作经历**

**reasum_line7**

**公司**： 蓝盾信息安全技术股份有限公司

**时间：** 2016年10月 – 至今

**职位**： 信息安全研究员

**部门**： 前沿部门

**目标**： 为工业界和学术界提供一个基于人工智能的恶意文件检测引擎，通过对领域特征的挖掘，并结合数据科学中的建模，构建基于机器学习的恶意文件分类模型，并将研究成果发表到相关国际会议中。

**工作职责：**

1. 使用机器学习的方法对恶意文件与正常文件进行分类与检测
2. 收集模型训练的数据，并对数据进行分析与合并归类
3. 阅读并收集国内外人工智能前沿技术论文，并做技术分享
4. 将研究成果以论文的形式提交到国际知名会议
5. 针对于目前的检测恶意文件的模型进行优化，主要在特征提取与提高检测率等方面
6. 在PDF文件检测的AI模型中添加对抗性学习与动态分析

**关键成果**:

1. 发表论文一篇，在“第33次全国计算机安全学术交流会”，论文标题为“**基于机器学习的恶意文件检测与分类器对抗性学习研究**”

2. 使用python爬虫收集恶意PDF文档数据集，总样本数201368 个

3. 模型准确率高达99.82%（在二十万数据集中），误报率0.01%，单个文档预测时间维持在毫秒级别

4. 成功使用生成的恶意文档对抗样本（adversarial examples）对分类器发动逃逸攻击，触发分类器根据攻击重新训练，得出一个鲁棒性和抗逃逸能力更强的模型。

5. 针对模型健壮性问题，提出了5种行之有效的抗逃逸模型防御技术

6. 加入对抗性机器学习(adversarial machine learning)与特征融合(feature fusion)的研究，并投稿英文论文一篇。

7. 在公司公众号发表前沿技术相关的文章

**职能技能**

**reasum_line7**

深入研究人工智能相关模型（如回归，决策树，分类，聚类等）

深入研究如何把人工智能技术应用到计算机安全领域

熟悉数据科学工具，如Word & Excel.

熟悉基本算法，数据结构，SQL数据库增删查改等

了解面向对象语言Python，Java, Scala等

了解深度学习TensorFlow框架及使用

了解大数据平台处理工具，如Spark，Hadoop，

良好的沟通协调和团队合作能力，积极乐观，抗压能力强

喜欢学习新的东西，并与团队分享交流

**技能证书**

**reasum_line7**

网络信息安全工程师技术水平

信息安全保障人员认证（CISAW）证书