

王凤娇

Email: 634272867@qq.com

WeChat: wfjyouyoude

Cell: 15602209397

Github:<https://yonahwang.github.io>



求职意向: 算法工程师

自我简述

我是王凤娇，2016年毕业于西南林业大学，4年制本科，计算机技术与科学学院，信息工程。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。

职能技能

深入研究人工智能相关模型（如回归，决策树，分类等）

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

工作经历

公司： 蓝盾信息安全技术股份有限公司

时间： 2016 年 10 月 - 2018 年 10 月

职位： 信息安全研究员

部门： 前沿部门

目标职责 1： 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。

关键成果：

1. 发表学术论文一篇，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. 构建(训练)基于有监督学习的机器学习(随机森林)模型 3 个以上。

目标职责 2： 研究对抗性机器学习(adversarial machine learning)的应用，及 针对 对抗性机器学习在 AI 模型中遇到问题提出解决方案。

关键成果：

1. 对抗性机器学习与特征融合(feature fusion)的研究，并投稿英文论文一篇。
2. 成功使用自己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。
3. 使用 cuckoo 沙箱进行恶意文件验证，来验证病毒变异后是否保持有恶意代码。
4. 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。

目标职责 2:漏洞扫描 SQL 库维护，主要负责蓝盾漏洞扫描库的 waf、ips 等相关规则编写，规则更新与漏扫库的维护分类，及漏洞验证。

关键成果:

1. 使用 Openvas 漏洞评估系统的一个数据库，漏洞扫描库进行每周更新，半年内更新最新漏洞达到上万条，包括勒索病毒的漏洞。
2. 漏洞验证。搭建有漏洞的数据库系统，包括有 SQLserver,mysql,BD 等数据库漏洞环境，然后对其有漏洞的环境进行漏洞验证。
3. 漏扫库维护。对于漏扫 SQL 库的日常管理（SQL 增，删，查，改），更新，分类，以及漏扫产品解决方案优化。

主要论文

- [1]. 王凤娇, 江纬, 杨育斌, 柯宗贵. 基于机器学习的恶意文件检测与分类器对抗性学习研究[J]. 在第 33 次全国计算机安全学术交流会. 2018 (accepted) ;
- [2]. Yubin Yang, Wei Jiang, Fengjiao Wang, Shumin Wei. Malicious Document Detection and Robust ML Model Construction. 2018; (under submission)

教育背景

西南林业大学 计算机与信息学院 信息工程

本科 信息工程 2012 年 9 月 - 2016 年 7 月, 昆明, 云南

主要课程: 数据结构, 机器学习, Linux 系统应用, 面向对象 Java, 计算机图像数字处理