苏莉娅丨个人简历

学历：博士在读　　就读院校：中国科学院信息工程研究所
主页：https://serea.github.io　　联系方式: +8613041130588/suliya@iie.ac.cn

教育经历

2012年9月 至 2016年6月	中国科学技术大学，信息科学技术学院英才班，学士（保研）
2016年9月 至今	中国科学院信息工程研究所，网络空间安全，博士（在读）

国际合作

2020年1月 至今	德国CISPA Helmholtz Center for Information Security，访问学者。与Yang Zhang（张阳）博士合作研究图分类场景中对图神经网络的成员推理攻击问题。
2019年5月 至 2019年6月	美国Indiana University Bloomington，访问学者。与XiaoFeng Wang（王晓峰）教授和Xiaojing Liao（廖晓静）副教授合作研究区块链场景中的复杂攻击行为的理解与发现。

研究方向

研究兴趣包括大型网络中的复杂恶意行为分析和人工智能算法本身的安全问题。借助行为分析、机器学习和图神经网络方法，分析测量新型攻击活动（例如面向区块链的攻击和面向深度神经网络的攻击），构建更安全的大规模网络系统。

发表论文

[1] **Liya Su**, Zhikun Zhang, Yang Zhang, XiaoFeng Wang, Baoxu Liu. Information Leakage of Graph Level Classifications[C]. USENIX Security. 2021 **(CCF A类会议，**待投稿)

[2] **Liya Su**, Xinyue Shen, Xiangyu Du, Xiaojing Liao, XiaoFeng Wang, Luyi Xing, Baoxu Liu. Evil Under the Sun: Understanding and Discovering Attacks on Ethereum Decentralized Applications[C]. USENIX Security. 2021 **(CCF A类会议，已接收)**

[3] **Liya Su,** Yepeng Yao, Chen Zhang, Zhigang Lu, Baoxu Liu. Marrying Graph Kernel with Deep Neural Network: A Case Study for Network Anomaly Detection[C]. The International Conference on Computational Science (ICCS). 2019: 102-115.) **(IIE B类会议)**

[4] **Liya Su**, Yepeng Yao, Zhigang Lu, Baoxu Liu. Understanding the Influence of Graph Kernels on Deep Learning Architecture: A Case Study of Flow-Based Network Attack Detection[C]. International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2019: 312-318. **(CCF C类会议)**

[5] **Liya Su**, Yepeng Yao, et al. Hierarchical Clustering Based Network Traffic Data Reduction for Improving Suspicious Flow Detection[C]. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2018: 744-753. **(CCF C类会议)**

[6] Yepeng Yao, **Liya Su**, Zhigang Lu, Baoxu Liu. STDeepGraph:Spatial-Temporal Deep Learning on Communication Graphs for Long-Term Network Attack Detection[C]. International

Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2019: 120-127. **(CCF C类会议)**

[7] Yepeng Yao, **Liya Su**, Zhigang Lu. DeepGFL: Deep Feature Learning via Graph for Attack Detection on Flow-based Network Traffic[C]. IEEE Military Communications Conference (MILCOM). IEEE, 2018: 579-584. **(IIE B类会议)**

[8] Mingyi Chen, Yepeng Yao, Junrong Liu, Bo Jiang, **Liya Su**, Zhigang Lu. A Novel Approach for Identifying Lateral Movement Attacks Based on Network Embedding[C]. International Symposium on Parallel Architectures, Algorithms and Networks (ISPA). 2018: 708-715. **(CCF C类会议)**

[9] Qiang Li, Yunan Zhang, **Liya Su**, et al. "An improved method to unveil malware's hidden behavior" [C] 2017 International Conference on Information Security and Cryptology. Springer, Cham, 2017: 362-382. **(IIE C类会议)**

项目经历

2016年3月 至 2017年1月：**国家网络空间威胁情报共享开放平台（2.37亿元）**。独自开始并完成整个项目的调研工作以及数据存储的构建与共享数据字段规划。合作完成威胁情报数据的导入（**7类数据，总计数亿条数据**），数据库构建，以及情报分析的可视化展示。此平台是国家级网络空间威胁情报共享开放平台，提供威胁情报给各级部委和合作公司使用，同时为信工所前场安全分析人员提供服务，借助此平台分析的安全线索支撑了若干起安全事件的发现。其中主要负责的**网络安全可视化展示项目获得中科院大学生奖学金**。同时合作创建并推广**威胁情报安全周报**。

2017年2月 至 2017年12月：**国家某部委重点项目（约1000万元）**。参与撰写威胁情报子系统部分相关材料，主要参与态势感知子系统相关研究，其中**关键技术**源自本人发表的全流量分析论文“Hierarchical Clustering Based Network Traffic Data Reduction for Improving Suspicious Flow Detection”，对采集流量进行约减，可**筛选40%以上**的正常流量，提高异常流量发现效率。

2018年1月 至 2018年6月：**国家某部委重点项目（约2.3亿元）**。参与安全监测平台中网络安全态势感知子系统和内部威胁检测子系统的可研报告撰写。其中**关键技术**源自本人发表的基于深度图的流量分析论文“Marrying Graph Kernel with Deep Neural Network: A Case Study for Network Anomaly Detection”，并且合作发表针对内网横向移动检测的论文“A Novel Approach for Identifying Lateral Movement Attacks Based on Network Embedding”。论文算法集合到态势感知分析平台的**Seckit算法库**中，供实际业务中的高级威胁分析使用。

2018年2月 至 2019年1月：**国家自然科学基金“威胁情报可靠性验证和质量评估方法研究”（25万元）**，参与申请书撰写和威胁情报真值发现方法的提出与论证。编写代码并实现关键解决方案，并实际应用在威胁情报共享开放平台上，**代码量约2500行**，验证和评估情报数据**千万条**。

2019年1月 至 2019年4月：参与撰写**“网络攻击溯源取证”教材（预计2020年11月出版）、“网络安全态势感知”教材（预计2021年11月出版），梳理书稿逻辑结构，编写与校对相关章节**。

曾获荣誉

2018年，中国科学院信息工程研究所，所长优秀奖。
2016年，2017年，中国科学院大学三好学生，优秀干部。
2017年，CCF大数据与计算智能大赛获得复赛11名成绩（用户异常行为分析）。
2016年，阿里云安全算法挑战赛，成绩第二赛季27/936（钓鱼网站检测，WebShell检测）。
2016年，中科院大学生奖学金。
2016年，中国科学技术大学信息科技英才奖学金。
2015年，北美建模大赛Honorable Mention奖。

学术服务与社团工作

External Reviewer: S&P 2021，CCS 2020, HPCC 2019
2016年3月 至 2018年6月：**担任信工所六室第一届学生会主席**。在研究室帮助下，组织人员构建第一届学生会，通过各种行动丰富学生生活，协调各部门的运行。组织了20次"学术分享"、10余次"电影周"、2次"毕业生开题服务"等，协助工会举办"爬行西山"等活动，极大的丰富了研究室师生的课余生活。

编程能力

机器学习与深度学习：Python（包括Pandas，Sklearn，NexworkX，PyTorch，Keras）
图像处理与算法：Matlab，C/C++