# 苏莉娅 | 个人简历

主页：https://serea.github.io　　联系方式：sereat@163.com

## 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 2021年6月 | 中国科学院信息工程研究所，网络空间安全，博士（硕转博） |
| 2021年7月 至今 | 京东集团博士管培生（暂未定岗） |

## 国际合作

| | |
|---|---|
| 2020年1月 2021年2月 | 德国CISPA Helmholtz Center for Information Security (CS Rankings Top 1)，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 (CS Rankings Top 11)，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。

## 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**。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**。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**。**关键技术**源自本人发表的全流量分析论文，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**。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，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”。

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）**，提出和论证威胁情报真值发现的方法。

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）**。

## 发表论文

[1] **Liya Su**, Zhikun Zhang, Yang Zhang, XiaoFeng Wang, Baoxu Liu. Information Leakage of Graph Level Classifications[C]. **(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)**

[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)

## 曾获荣誉

2021年，国家奖学金。

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，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。

## 社团工作

2016年3月 至 2018年6月：**担任信工所六室第一届学生会主席**。