刘明烜

学校：清华大学　　学历：硕士研究生
院系：网络科学与网络空间研究院　　方向：网络空间安全
联系电话：+8618800151375　　邮箱：liumx18@mails.tsinghua.edu.cn

教育经历

2018.09	- 至今	清华大学	网络科学与网络空间研究院	网络空间安全	工学硕士
2014.09	- 2018.06	北京邮电大学	国际学院	电信工程及管理	工学学士

成绩

本科平均 GPA 为 91.6，综合排名为 4/296，保研至清华大学网络科学与网络空间研究院。研究生为网络空间安全方向硕士在读，硕士一年级的成绩均为 B 以上

科目及项目经历

2017.12 - 2018.09　基于深度学习的推广感染检测

基于黑灰产页面的文本内容语义以及图像视觉效果，设计了基于深度学习的检测模型，准确率达到95%以上。利用检测系统检出的大量非法页面，进一步对黑灰产页面的生态进行了测量分析。这部分工作成果形成了[1，2]两篇论文，以及一个检测系统，现已部署在清华校园网内以及奇安信集团，持续稳定运行了 500 多天，本人为项目主要合作者。

2018.11 - 2019.08　基于中文文本特征的对抗文本生成

调研英文语境下对抗文本生成方法的基础上，分析中文与英文的语言差异特性，提出基于中文特性的自动化对抗文本生成方法。这个工作形成了一篇本人为共同一作的论文，发表于 IJCAI 2020（CCF A 类推荐会议）[3]。

2019.11 - 至今　　短信诈骗检测和测量分析

为探索打击伪基站地下产业的新思路，本人与其它研究人员一同基于数据驱动安全的思路，与国内知名安全厂商合作，收集大规模伪基站发送垃圾短信，并对其进行测量分析。该工作已形成一篇论文，发表于 CCS 2020（国际网络安全领域四大顶级会议）。

攻击者利用受害者的个人敏感信息作为诱因进行危害性更强的诈骗，这种诈骗方式学术界还没有进行过讨论。针对包含个人敏感信息的诈骗短信进行了检测和测量的工作。该工作预计投稿 WWW 2020。

2019.9 - 至今　　基于深度学习的恶意 CC 通信检测

从流量行为检测恶意软件的话题上，针对明文的 HTTP 以及加密的 HTTPs，都进行了工作调研以及工程实现。针对 HTTP 的 C&C 通信，提出单流和多流结合的检测方案，该检测系统已部署在华为现网，并形成了一项专利。

作为主要评估题目的成员，本人参与了 DataCon 2020 恶意加密流量检测的赛题评估，现在正在继续探索如何更加高效和准确的检测恶意加密流量，并且可以完成工程部署。

获得奖项

竞赛	GeekPwn 极棒，隐身挑战赛	第三名	项目核心成员
	北京邮电大学第九届大学生创新创业实践	一等奖	项目核心成员
奖学金	本科 2014-2015 学年	综合排名全年级第一，获得了国家奖学金	
	本科 2015-2016 学年	综合排名全年级第一，获得了国家奖学金	
	本科 2016-2017 学年	综合排名全年级第四，获得了一等奖学金	

研究方向

结合硕士期间的研究项目，以及在自然语言处理和数据驱动安全问题上的经验积累，博士期间希望以互联 网地下产业文本信息操控的安全问题继续进行探索，所研究问题有：在线知识平台虚假词条问题研究、恶 意短文本消息内容操控问题研究、高对抗性的恶意文本检测方法研究。

文献

[1] Zhang, Zihan*, **Mingxuan Liu***, Chao Zhang, Yiming Zhang, Zhou Li, Qi Li, Haixin Duan, and Donghong Sun. "Argot: Generating Adversarial Readable Chinese Texts", the 聽 25th International Joint Conferences on Artificial Intelligence (IJCAI), 2020. (**Co-first Authors**).

[2] Yiming Zhang, Baojun Liu, Chaoyi Lu, Zhou Li, Haixin Duan, Shuang Hao, **Mingxuan Liu**, Ying Liu, Dong Wang and Qiang Li. "Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China", the 27th ACM Conference on Computer and Communications Security (CCS), 2020.

[3] Yang Hao, Du Kun, Zhang Yubao, Hao Shuang, Zhou Li, **Mingxuan Liu**, Haining Wang, Haixin Duan, Yazhou Shi, Xiaodong Su, Guang Liu, Zhifeng Geng, Jianping Wu. "Casino royale: a deep exploration of illegal online gambling", the 35th Annual Computer Security Applications Conference (ACSAC), 2019.
[4] Kun Du, Hao Yang, Zhou Li, Haixin Duan, Shuang Hao, Baojun Liu, Yuxiao Ye, **Mingxuan Liu**, Xiaodong Su, Guang Liu, Zhifeng Geng, Zaifeng Zhang and Jinjin Liang. "TL;DR Hazard: A Comprehensive Study of Levelsquatting Scams", the 15th International Conference on Security and Privacy On Communication Networks (SecureComm), 2019.