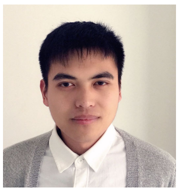


Siyuan Tang
tangsi@iu.edu
(+1) 8122726206

School of Informatics, Computing, and Engineering
Indiana University, Bloomington

Luddy Hall
700 N Woodlawn Ave
Bloomington, IN
47408

Siyuan Tang

Curriculum Vitae

About Me I am a sixth-year Ph.D. student at Indiana University, Bloomington, in the School of Informatics, Computing, and Engineering. I work in the System Security Lab supervised by Prof. XiaoFeng Wang. So far, I have led multiple research projects and published 5 papers at the top 4 security conferences. My research areas include web security, threat intelligence, and AI security. And I expect to graduate in December 2024.

Education

2018 - Now, Indiana University, Bloomington

PhD in Computer Science

2014 - 2017, Nanjing University

MS in Computer Science & Technology

2010 - 2014, Nanjing University

BS in Computer Science & Technology

Internship

2019.06 - 2019.08, Tencent CSIG, Shenzhen

I built a threat intelligence platform at Tencent, CSIG, that automatically identified malicious domains using sinkhole operators. This platform was later integrated into their internal security system.

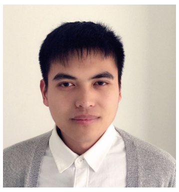
Project Experience

Web Security

My previous research delved into the security concerns of web services including proxy and P2P (peer-to-peer) services. After analyzing over 2 million Android APKs, we found that roughly 1,000 Android apps exhibited insecure behaviors. These apps seamlessly enlisted users into proxy/P2P networks without their consent. Our detailed analysis exposed a new monetization ecosystem where service providers distributed their SDKs to app developers and shared profits after integrating SDKs into the apps. Moreover, we found that some popular Chinese video platforms like Youku and MGTV had set up potentially vulnerable P2P networks among their viewers, without any user consent. One of our papers on this research was published in NDSS 2021, and another is currently under peer review.

Threat Intelligence

Another significant aspect of my research focuses on threat intelligence within social networks. In one study, we analyzed over 50,000 tweets spanning three years and extracted approximately 20,000 unique spam SMS messages reported by genuine Twitter users. We made our automated spam SMS extraction tool, SpamHunter, available to the public, along with a semi-automated framework for evaluating the majority of current anti-spam services. Beyond this, our research has unveiled an emerging drug promotion network on platforms like Instagram and YouTube. Using our drug-referral comment detection pipeline, we identified over 150,000 such comments linked to 3,253 drug dealers. Notably, one of our papers was published in CCS 2022, and another is currently under peer review



Siyuan Tang
tangsi@iu.edu
(+1) 8122726206

School of Informatics,
Computing, and
Engineering
Indiana University,
Bloomington

Luddy Hall
700 N Woodlawn Ave
Bloomington, IN
47408

AI Security

I am also interested in the privacy issues in machine learning models, particularly in the rising Large Language Models (LLMs). In recent research, we assessed potential privacy leakages in GPT models. Contrary to existing beliefs that LLMs only remember a handful of examples from training and often generate hallucinations, we discovered significant privacy breaches when fine-tuning a few real examples. Specifically, our research highlighted how such private data could be easily extracted through fine-tuning, and we demonstrated such privacy leakage through the GPT-3.5 Turbo fine-tuning API. Another our study delved into the well-known trojan backdoors in neural networks, and has been published in S&P (Oakland) 2023.

Skill Experience

Program Analysis

I have expertise in analyzing programs in Java, Javascript, and other foundational languages such as Smali. Throughout our projects, we have developed several detection algorithms for HTML webpages and Android apps, aimed at identifying suspicious proxy and P2P traffic during runtime.

Machine Learning

I have a strong background in risk analysis of neural networks, as well as LLMs like GPT. In our research, I reproduced various attacks and defenses against neural networks and LLMs based on PyTorch and Tensorflow. In the TrojAI competition hosed by NIST, our defense outperformed the state-of-the-art unlearning techniques and ranked in top 10 in Round 5.

Programming Experience

I have proficiency in several programming languages such as C++, Java, and Python, with over 10 years of hands-on experience and more than 300,000 lines of code. You can explore some of my projects on my personal GitHub repository at https://github.com/opmusic..

Selected Publications

"The Janus Interface: How Fine-Tuning in Large Language Models Amplifies the Privacy Risks", *Xiaoyi Chen*, **Siyuan Tang***, Rui Zhu*, Zihao Wang, Shijun Yan, Lei Jin, Liya Su, XiaoFeng Wang, Haixu Tang* , (*equal contribution) **submitted to Usenix 2024**

"Understanding Cross-Platform Referral Traffic for Illicit Drug Promotion", *Mingming Zha, Zilong Lin, **Siyuan Tang**, Xiaojing Liao, Yuhong Nan, XiaoFeng Wang*, **submitted to Usenix 2024**

"Gradient Shaping: Understanding When Backdoor Inversion Fails", *Rui Zhu, Di Tang, **Siyuan Tang**, Yongming Fan, Shiqing Ma, Haixu Tang, XiaoFeng Wang*, **major revision of NDSS 2024**

"Stealthy Peers: Understanding Security Risks of Peer-Assisted Video Streaming", ***Siyuan Tang**, Eihal Alowaisheq, Xianghang Mi, Yi Chen, XiaoFeng Wang, Yanzhi Dou*, **major revision of S&P 2023**

"Selective Amnesia: On Efficient, High-Fidelity and Blind Unlearning of Trojan Backdoors", *Rui Zhu, Di Tang, **Siyuan Tang**, XiaoFeng Wang, Haixu Tang*, **S & P 2023**

"Clues in Tweets: Twitter-Guided Discovery and Analysis of SMS Spam", ***Siyuan Tang**, Xianghang Mi, Ying Li, XiaoFeng Wang, Kai Chen*, **CCS 2022**

"Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks", *Xianghang Mi, **Siyuan Tang**, Zhengyi Li, Xiaojing Liao, Feng Qian, XiaoFeng Wang*, **NDSS 2021**