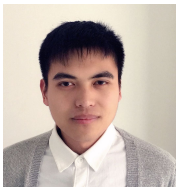


Siyuan Tang
tangsi@iu.edu
(+1) 8122726206

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 in the School of Informatics, Computing, and Engineering at Indiana University, Bloomington. I joined the System Security Lab under the supervision of Prof. XiaoFeng Wang. So far, I have led successfully two research projects and published four papers on top security conferences. My research focuses on web security, threat intelligence and AI security.

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

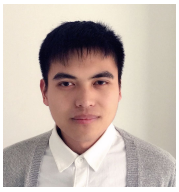
Internship

2019.06 - 2019.08, Tencent CSIG, Shenzhen
I had an internship in Tencent, CSIG to build a threat intelligence platform, which automatically collects the latest sink-holed domains from sinkhole operators. The product was integrated into their internal security system.

Project Experience

Web Security
My previous research projects investigated the security impacts of web domains, proxy and P2P (peer-to-peer) services. Through a large-scale scanning of over 2M Android APKs, we identified 963 Android apps integrated with third-party proxy SDKs, which utilize their customers as proxy peers without proper user consent. In another project, we also identified private P2P services on extremely popular video platforms (e.g., v.qq.com, youtube.com), and 3 public P2P service providers, Peer5 (acquired by Microsoft eCDN), Streamroot, and Viblast, all of which have serious security and privacy concerns, and thus may affect millions of users. One of our work has been published on NDSS 2021 and the other is under peer review.

Threat Intelligence
Another important issue of my research is threat intelligence. Our works shed light on new understanding of the threat intelligence collected from social networks like Twitter, Instagram. In one of our research, we collected over 20K spam SMS from tweets attached with SMS screenshots. We designed a framework, *SpamHunter*, to automatically recognize the reported spam SMS texts and URLs. Such dataset turns out to be more diverse and timely than existing spam SMS collections and threat intelligence engines, i.e., VirusTotal. We also designed an automatic evaluation framework to test the feasibility of these spam SMS texts against the existing anti-spam systems. Our work has been published on CCS 2022. In another recent work, we looked into the cross-platform drug transaction, referring traffic to drug dealers on Instagram through video comments on YouTube or TikTok. Our work revealed new trends on this emerging social-network-based drug ecosystem.



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 security issues in machine learning models, such as backdoor, private information leakage. Our recent project investigated a general defense mechanism against the backdoor in neural networks through the leverage of "catastrophic forgetting". Our findings revealed that it is much easier to forget the backdoor compared with normal tasks (i.e., image recognition). Our work has been published on S&P 2023. We are also working on the privacy issues in the emerging LLMs.

Skill Experience

Program Analysis

I am experienced in program analysis of Java, Javascript codes and other underlying languages like Smali. During our projects, we also designed multiple traffic analysis algorithms to detect the suspicious behavior in the runtime.

Machine Learning

I am also familiar with existing neural network models (e.g., VGG, resNet), and large language models (e.g., GPT-2, llama2). In our works, I performed various evaluation tasks on these machine learning models.

Programming Experience

I am experienced in multiple programming languages, including C++, Java, Python, and also functional programming languages like Racket. My personal github repository is 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* , **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**
"Zombie Awakening: Stealthy Hijacking of Active Domains Through DNS Hosting Referral", *Eihal Alowaisheq, **Siyuan Tang**, Zhihao Wang, Fatemah Alharbi, Xiaojing Liao, XiaoFeng Wang*, **CCS 2020**
"Cracking Wall of Confinement: Understanding and Analyzing Malicious Domain Takedowns", *Eihal Alowaisheq, Peng Wang, Sumayah Alrwais, Xiaojing Liao, XaioFeng Wang, Tasneem Alowaisheq, XiangHang Mi, **Siyuan Tang**, Baojun Liu*, **NDSS 2019 (Distinguished Paper Award)**