Song Liao

liao5@g.clemson.edu — https://songacademic.github.io — (864) 624-3890 — Clemson, SC

RESEARCH INTERESTS

- IoT Security and Privacy
- Policy and Privacy Compliance on Open Platforms
- Abuse Detection on Online Social Platforms

EDUCATION

Clemson University Clemson, SC
Ph.D. Candidate in Computer Science *August 2019 - Present*

- Advisor: Dr. Long Cheng

Xi'an Jiaotong University Xi'an, China
Master of Engineering in Software Engineering *September 2015 - June 2018*

- Advisor: Dr. Yuehu Liu

Xi'an Jiaotong University Xi'an, China
Bachelor of Engineering in Software Engineering *September 2011 - June 2015*

PUBLICATIONS

[1] **Song Liao**, Long Cheng, Haipeng Cai, Linke Guo, and Hongxin Hu, "SkillScanner: Detecting Policy-Violating Voice Applications Through Static Analysis at the Development Phase", *In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*, 2023, Acceptance rate: 158/795 = 20%.

[2] **Song Liao**, Ebuka Okpala, Long Cheng, Nishant Vishwamitra, Mingqi Li, Hongxin Hu, Feng Luo, and Matthew Costello, "Characterizing Offensive Tweets in the Era of COVID-19", *In Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (**KDD**)*, 2023, Acceptance rate: 184/725 = 25%.

[3] Jeffrey Young*, **Song Liao***, Long Cheng, Hongxin Hu, and Huixing Deng, "SkillDetective: Automated Policy-Violation Detection of Voice Assistant Applications in the Wild", *In 31st USENIX Security Symposium (**USENIX Security**)*, 2022, Acceptance rate: 256/1414 = 18%, (Co-first author).

[4] **Song Liao**, Christin Wilson, Long Cheng, Hongxin Hu, and Huixing Deng, "Problematic Privacy Policies of Voice Assistant Applications", *IEEE Security & Privacy Magazine*, 2021.

[5] **Song Liao***, Christin Wilson*, Long Cheng, Hongxin Hu, and Huixing Deng, "Measuring the effectiveness of privacy policies for voice assistant applications", *In Annual Computer Security Applications Conference (**ACSAC**)*, 2020, Acceptance rate: 70/302 = 23%, Distinguish Paper Award.

[6] Wenbo Ding, **Song Liao**, Long Cheng, Ziming Zhao, Keyan Guo, and Hongxin Hu, "Exploring Vulnerabilities in Voice Command Skills for Connected Vehicles", *EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (**SmartSP**)*, 2023.

[7] Nishant Vishwamitra, Keyan Guo, **Song Liao**, Jaden Mu, Zheyuan Ma, Long Cheng, Ziming Zhao and Hongxin Hu, "Understanding and Analyzing COVID-19-related Online Hate Propagation Through Hateful Memes Shared on Twitter", *The 2023 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (**ASONAM**)*, 2023

[8] Matthew Costello, Nishant Vishwamitra, **Song Liao**, Long Cheng, Feng Luo, and Hongxin Hu, "COVID-19 and Sinophobia: Detecting Warning Signs of Radicalization on Twitter and Reddit", *Cyberpsychology, Behavior, and Social Networking*, 2023.

[9] Mingqi Li, **Song Liao**, Ebuka Okpala, Max Tong, Matthew Costello, Long Cheng, Hongxin Hu, and Feng Luo, "COVID-HateBERT: a Pre-trained Language Model for COVID-19 related Hate Speech Detection", *In 2021 20th IEEE International Conference on Machine Learning and Applications (**ICMLA**), IEEE*, 2021.

[10] Matthew Costello, Long Cheng, Feng Luo, Hongxin Hu, **Song Liao**, Nishant Vishwamitra, Mingqi Li, and Ebuka Okpala, "COVID-19: a pandemic of Anti-Asian cyberhate", *Journal of Hate Studies, 17(1)*, 2021.

[11] Long Cheng, Christin Wilson, **Song Liao**, Jeffrey Young, Daniel Dong, and Hongxin Hu, "Dangerous skills got certified: Measuring the trust-worthiness of skill certification in voice personal assistant platforms", *In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*, 2020, Acceptance rate: 121/715 = 17%.

UNDER REVIEW

[1] **Song Liao**, Long Cheng, Xiapu Luo, Zheng Song, Haipeng Cai, and Hongxin Hu, "Uncovering and Exploiting Security Risks in the RapidAPI Ecosystem", ***Usenix Security 2024***.

[2] **Song Liao**, Mohammed Aldeen, Jingwen Yan, Long Cheng, Xiapu Luo, Haipeng Cai, Hongxin Hu, “Understanding GDPR Non-Compliance in Privacy Policies of Alexa Skills in European Marketplaces”, ***Web Conference 2024***.

[3] Wenbo Ding, **Song Liao**, Long Cheng, Ziming Zhao, and Hongxin Hu, “Command Hijacking on Voice-Controlled IoT in Amazon Alexa Platform”, ***Usenix Security 2024***.

[4] Mohammed Aldeen, Jeffery Young, **Song Liao**, Tsu-Yao Chang, Long Cheng, Haipeng Cai, Xiapu Luo, Hongxin Hu, “End-Users Know Best: Identifying Undesired Behavior of Alexa Skills Through User Review Analysis”, ***Web Conference 2024***.

POSTERS

[1] **Song Liao**, Mohammed Aldeen, Jingwen Yan and Long Cheng, “Poster: On GDPR Compliance of Amazon Alexa's Privacy Policies in European Marketplaces”, *IEEE Secure Development Conference (**SecDev**)*, 2023

[2] **Song Liao**, Long Cheng, “Poster: Understanding the Policy-Compliance Practices of Voice Application Developers”, *IEEE Secure Development Conference (**SecDev**)*, 2022

[3] Long Cheng, Ebuka Okpala, **Song Liao**, and Danfeng(Daphne) Yao, “BranchCorr: Detecting Incompatible Branch Behavior by Enforcing Branch Correlation Integrity”, *IEEE Secure Development Conference (**SecDev**)*, 2019.

AWARDS

- Distinguished Paper Award, Annual Computer Security Applications Conference (ACSAC), 2020
- Google awarded us $5,000 bug bounty for discovering vulnerabilities in Google Actions.
- Travel grant from CCS (2023), SmartSP (2023), IEEE SecDev (2022)
- Talford Endowed Fellowship Award, 2023
- Talford Endowed Fellowship Award, 2022

MEDIA AND NEWS

- We presented our work on Policy Violation Detection of Voice Assistant Applications at the FTC's PrivacyCon 2021.
- Google awarded us two bug bounties for reporting various policy-violating Google Actions (2021).
- We presented our work on Trustworthiness of Skill Certification in Voice Personal Assistant Platforms at the FTC's PrivacyCon 2020.
- The Register, Washington Internet Daily, ZDNet and some other media reported our work on measuring the trustworthiness of Alexa's skills certification (2020).
- The Register and VentureBeat reported our work on Alexa skill privacy policy analysis (2020).

GRANT PROPOSAL CONTRIBUTION

I contributed to the following proposals, which are led by my Ph.D. advisor:

CAREER: Ensuring Privacy, Inclusiveness, and Policy Compliance in the Era of Voice Personal Assistants

Sponsoring Agency: NSF 2023 - 2028

- Status: Granted
- Award Amount: $502,505.00
- In this project, we will design new techniques and mechanisms to ensure privacy, inclusiveness, and policy compliance in voice personal assistant systems. I contributed to the project by providing insights into the preliminary results and developing tools for future endeavors.

RAPID: Cyber-Hostility and COVID-19

Sponsoring Agency: NSF 2020 - 2022

- Status: Granted
- Award Amount: $199,996.00
- In this project, we examine the new wave of cyber-hostility encountered during the COVID-19 pandemic by studying data collected from major social media websites. I am the primary contributor to the project. I contributed to the proposal writing, data collection, data analysis, paper publication and support for others.

Collaborative Research: EAGER: SaTC-EDU: Learning Platform and Education Curriculum for Artificial Intelligence-Driven Socially-Relevant Cybersecurity

Sponsoring Agency: NSF 2021 - 2023

- Status: Granted
- Award Amount: $316,000.00
- In this project, we develop curricular modules and hands-on labs to educate both CS and non-CS students on AI-driven cyberharassment detection, related attacks against AI models, and social issues in AI models for cyberharassment detection. I contributed to the proposal writing and several lab implementations in this project.

Collaborative Research: SAI-R: Integrative Cyberinfrastructure for Enhancing and Accelerating Online Abuse Research

Sponsoring Agency: NSF 2022 - 2025

- Status: Granted

- Award Amount: $750,000.00
- This project will develop the first scalable, sustainable, customizable, extendable, portable, and user-friendly Integrative Cyberinfrastructure for Online Abuse Research (ICOAR), which fills a much-needed gap and advances research capability for researchers in both CISE and SBE communities to apply advanced ML methods for online abuse research. I contributed to the layer design and proposal writing for the project.

TEACHING

Graduate Teaching Assistant (TA)

- CPSC-6200/4200 Computer Security Principles, Fall 2023
- CPSC-8570 Network Technologies Security, Spring 2023
- CPSC-6200/4200 Computer Security Principles, Fall 2022
- CPSC-6200/4200 Computer Security Principles, Summer 2022
- CPSC-6200/4200 Computer Security Principles, Spring 2021

Guest Lectures

- I gave several guest lectures on the CPSC 6200/4200 class

MENTORING EXPERIENCE

As part of my Ph.D. studies, I mentored multiple students.

- Provide guidance to Jingwen Yan (Clemson, Ph.D., 2023) in the analysis of Alexa skill privacy notice generation.
- Mentored Kevius Tribble (South Carolina Governor's School for Science and Mathematics, high school, 2022) in COVID-related rumor detection using deep learning.
- Mentored Joshua Williams (D.W. Daniel High School, 2022) in user review analysis in voice assistant applications.
- Mentored Rahul Solleti (Green Level High School, 2022) in the privacy policy analysis of voice assistants and Zoom marketplace.
- Mentored Ethan Michael Anderson, Preethika Yetukuri, and Taran Prasad Kavuru (Clemson, undergraduate, 2022) in voice assistant application review analysis using NLP methods.
- Mentored Aidan Mcpherson (Clemson, undergraduate, 2021) in privacy policy analysis using existing tools.
- Provide guidance to Huixing Deng (Clemson, MS, 2019) in privacy policy analysis and policy violation detection in Alexa skills.

PAPER REVIEW

- The Web Conference (WWW), 2024
- IEEE Transactions on Dependable and Secure Computing (TDSC), 2023
- IEEE/ACM International Conference on Automated Software Engineering (ASE), 2023
- International Journal of Human-Computer Interaction (IJHCI), 2023
- Annual Computer Security Applications Conference (ACSAC), 2020, 2021,2022, 2023
- International Conference on Distributed Computing Systems (ICDCS), 2023
- International Conference on Computer Communications and Networks (ICCCN), 2023
- International Conference on Information and Communications Security (ICICS), 2023
- Internation Conference on Security and Privacy in Communication Networks (SecureComm), 2023
- IEEE International Conference on Computer Communications (INFOCOM), 2021, 2022
- IEEE International Conference on Parallel and Distributed Systems (ICPADS), 2022
- IEEE Conference on Communications and Network Security (CNS), 2020, 2021
- International Performance Computing and Communications Conference (IPCCC), 2020, 2021
- IEEE Global Communications Conference (GLOBECOM), 2019, 2020
- IEEE International Conference on Internet of Things (iThings), 2019

TALKS

- "SkillScanner: Detecting Policy-Violating Voice Applications Through Static Analysis at the Development Phase", CCS, Copenhagen, Denmark, 2023
- "Exploring Vulnerabilities in Voice Command Skills for Connected Vehicles", SmartSP, Chicago, 2023
- "Measuring the effectiveness of privacy policies for voice assistant applications", ACSAC, Virtual, 2020

COLLABORATORS

- Hongxin Hu, Associate Professor at the University at Buffalo
- Haipeng Cai, Associate Professor at Washington State University
- Xiapu Luo, Professor at The Hong Kong Polytechnic University
- Feng Luo, Professor at Clemson University
- Nishant Vishwamitra, Assistant Professor at the University of Texas at San Antonio
- Matthew Costello, Associate Professor at Clemson University