XIALI HEI

OFFICE: 301 E. Lewis Street, Lafayette, LA 70503, USA, Office: 1-337-482-1037

EMAIL: xiali.hei@louisiana.edu **HOMEPAGE:** https://www.xialihei.com

RESEARCH INTEREST

Cyber-Physical System Security, Hardware Security, Artificial Intelligence (AI) Security, Captcha Attacks and Design, Privacy-Preserving Learning

EDUCATION

Temple University Sep. 2009 - May 2014
Ph.D. of Computer Science *Advisor: Dr. Xiaojiang Du and Dr. Shan Lin*

Tsinghua University Sep. 2002 - Jul. 2005
M.S. of Software Engineering *Advisor: Dr. Kwok-Yan Lam*

Xi'an Jiaotong University Sep. 1998 - Jul. 2002
B.S. of Electronic Engineering *Advisor: Dr. Jianyi Liu*

WORKING EXPERIENCE

University of Pennsylvania Sep. 2023 - present
Visiting *Visiting Associate Professor*

University of Louisiana at Lafayette Aug. 16th 2023 - present
Sabbatical leave, Tenure-track *Associate Professor*

University of Louisiana at Lafayette Aug. 2017 - Aug. 15th 2023
Tenure-track *Assistant Professor*

Delaware State University Aug. 2015 - Jul. 2017
Tenure-track *Assistant Professor*

Frostburg State University Aug. 2014 - Jul. 2015
Tenure-track *Assistant Professor*

HONORS AND AWARDS

08/2023 NSF CVDI Center Award

06/2023 NSF SaTC Core Small Award

11/2022 NSF RII Track 4 Faculty Fellowship

07/2022-06/2025 Alfred and Helen M. Lamson Endowed Professorship Award

09/2021 Facebook Award

09/2021 NSF MRI Award

07/2021 LA Broad Regents CEMC Award

07/2021 Two LA Broad Regents SURE Awards

06/2021 NSF CVDI Center Award

12/2020 LA Broad Regents LAMDA coopertation program Award

06/2019 NSF RII Track-1 Award

06/2016 NSF CRII Award

11/2015 Delaware Economic Development Office Award

08/2014 ACM 2014 MobiHoc Best Poster Runner-up Award

12/2013 Dissertation Completion Fellowship

04/2013 The Bronze Award Best Graduate Project in Future of Computing Competition

04/2013 IEEE INFOCOM student travel grant

12/2010 IEEE GLOBECOM student travel grant

GRANTS: 15 AWARDED, PERSONAL SHARING: 3M, TOTAL AMOUNT: 24 M

[G16] Project Title: CAREER: SaTC: CPS: EPSCoR: Secure Tele-surgical Robots Under Emerging Attacks. Total amount: $574,978. 6/1/2024-5/30/2029, **NSF**, **Role: PI, Pending**.

[G15] Project Title: Deep Learning Based Image Segmentation Methods to Identify Grain Characteristics for Rock Drilling, Renewed. Total amount: $50,000. 10/1/2023-9/30/2024, **NSF Center for Visual and Decision Informatics (CVDI)**, **Role: PI**.

[G14] Project Title: SaTC: CORE: Small: Mitigating Threats of Physical-Domain Signal Injections on Security, Reliability, and Safety of Sensing and Control Systems. Total amount: $599,984. 7/1/2023-6/30/2026, **NSF**, **Role: PI**.

[G13] Project Title: RII Track-4:NSF: Fundamentals of Creating Trustworthy Medical Cyber-Physical Systems Under EMI Attacks. Total amount: $286,453. 1/1/2023-12/31/2024, **NSF**, **Role: single-PI**.

[G12] Project Title: Deep Learning Based Image Segmentation Methods to Identify Grain Characteristics for Rock Drilling. Total amount: $50,000. 10/1/2022-9/30/2023, **NSF Center for Visual and Decision Informatics (CVDI)**, **Role: PI**.

[G11] Privacy-Preserving Federated Learning for Minimized fNIRS Data. Total amount: $149,180. 10/1/2021-9/30/2022, **Facebook**, **Role: Single PI**.

[G10] Project Title: MRI: Development of High-Confidence Medical Cyber-Physical System Research Instrument with Benchmark Security Software. Total amount: $1,134,297. 10/1/2021-9/30/2024, **NSF**, **Role: PI**.

[G9] Project Title: Development of Two VR-assisted low-cost Online Courses Leading to Security Certificates. Total amount: $116,101. 5/1/2021-5/1/2022, **LA Broad Regents**, **Role: PI**.

[G8] Project Title: Decentralized and Distributed Deep Learning for Industrial IoT Devices. Total amount: $75,000. 8/1/2021-7/31/2022, **NSF Center for Visual and Decision Informatics (CVDI)**, **Role: PI**.

[G7] Project Title: Digital Image Correlation Method (DIC) for AM Process Evaluation and Monitoring. Total amount: $5,000. 5/1/2021-4/30/2022, **LA Broad Regents Supervised Undergraduate Research Experiences program** , **Role: PI**.

[G6] Project Title: Non-invasive Monitor and Attack Detection for Additive Manufacturing. Total amount: $5,000. 5/1/2021-4/30/2022, **LA Broad Regents Supervised Undergraduate Research Experiences program** , **Role: PI**.

[G5] Project Title: Digital Image Correlation Method (DIC) for AM Process Evaluation and Monitoring. Total amount: $39,400. 1/1/2021-12/31/2021, **LA Broad Regents**, **Role: co-PI**.

[G4] Project Title: RII Track-1: Louisiana Materials Design Alliance (LAMDA). Total amount: $20M. 07/1/2020-6/30/2025, **NSF** OIA-1946231, Yearly renewed, **Role: substituted co-PI, personal share: 840,000**.

[G3] Project Title: CRII: SaTC: CPS: RUI: Cyber-Physical System Security in Implantable Insulin Injection Systems. Amount: $174,995. 06/1/2016-12/31/2019, **NSF** CNS-1566166, CNS-1812553, **Role: Single PI**.

[G2] Project Title: A Human-Aware Energy-efficient Security Framework for Memory-restrained Internet of Everything Devices. State of Delaware Federal Research and Development Matching Grant Program. Amount: $99,997. 11/1/2015-10/31/2017. **Role: Single PI**.

[G1] Professional Development Fund, $3,500. 04/1/2016-05/30/2016, **Role: Single PI**.

NEWS

Report about our hCaptcha paper by **The Record** [Link], by **Slashdot** [Link], by **Hacker News** [Link].

Report about our Captcha paper by **The Register**, [Link], by **RECLAIM THE NET**, [Link].

Report about our CCS paper by **Control Engineering**, [Link], by **Control** [Link].

Report about our USENIX Security paper **The Register**. [Link]

PEER-REVIEWED PUBLICATIONS

CONFERENCE

59. **[SmartSP2023-1]** Diba Afroze, Yazhou Tu, and **Xiali Hei**. "Securing the Future: Exploring Privacy Risks and Security Questions in Robotic Systems." *Submitted to SmartSP'23* , 2023.

58. **[HICSS-57-2]** Sai Venkatesh Chilukoti, Md Imran Hossen, Liqun Shan, Vijay Srinivas Tida, and **Xiali Hei**. "Privacy Enhanced Training of EfficientNet-B1 Model to Predict Gastrointestinal Cancer Status." *Submitted to HICSS-57: Hawaii International Conference on System Sciences*, 2024.

57. **[HICSS-57-1]** Vijay Srinivas Tida, Md Imran Hossen, Liqun Shan, Sai Venkatesh Chilukoti, Sonya Hsu, and **Xiali Hei**. "Unified Kernel-Segregated Transpose Convolution Operation." *Submitted to HICSS-57: Hawaii International Conference on System Sciences*, 2024.

56. **[NeurIPS2023]** Sai Venkatesh Chilukoti, Md Imran Hossen, Liqun Shan, Vijay Srinivas Tida, **Xiali Hei** . "No More DP-SGD Fine-Tuning? Simple heuristic-based strategies provide the best balance between accuracy and privacy." *Manuscript being submitted to NeurIPS2023*, May 2023.

55. **[USENIX2023]** Yazhou Tu, Liqun Shan, Md Imran Hossen, Sara Rampazzi, Kevin Butler, and **Xiali Hei**. "Auditory Eyesight: Demystifying Microsecond-Precision Keystroke Tracking Attacks On Arbitrary Unrefined Keyboard Inputs." *Accepted by USENIX Security, Acceptance rate: **1.24** % (acceptance without major revision).*, 2023.

54. **[SmartSP2023]** Jianyi Zhang, Yuchen Wang, Yazhou Tu, Sara Rampazzi, Zhiqiang Lin, Insup Lee, and **Xiali Hei**. "ADC-Bank: Detecting and Filtering Acoustic Out-of-Band Signal Injection on Inertial Sensors." *Accepted to SmartSP'23* , 2023.

53. **[CPSIoTSec2023]** Yazhou Tu, Sara Rampazzi, and **Xiali Hei**. "Towards Adversarial Process Control on Inertial Sensor Systems with Physical Feedback Side Channels." *Submitted to CPSIoTSec'23*, 2023.

52. **[Arxiv2022]** Yazhou Tu, Sara Rampazzi, and **Xiali Hei**. "Towards Adversarial Control Loops in Sensor Attacks: A Case Study to Control the Kinematics and Actuation of Embedded Systems." *preprint arXiv:2203.07670*, 2022. [paper]

51. **[AAAI2024]** Jianyi Zhang, Qichao Jin, Fangjiao Zhang, Md Imran Hossen, Zhi Sun and **Xiali Hei**. "FL-PLAS: Backdoor-resistant Federated Learning based on Partial Layer Aggregation Strategy." *Submitted to AAAI*, 2024.

50. **[COMPSAC2023]** Jianyi Zhang, Leixin Yang, Yuyang Han, Zixiao Xiang, and **Xiali Hei**. "A Small Leak Will Sink Many Ships: Vulnerabilities Related to Mini Programs Permissions." *Accepted by the 2023 IEEE Computer*

Society Signature Conference on Computers, Software, and Applications (COMPSAC 2023), 2023.

49. **[SecTL2023]** Md Imran Hossen, Yazhou Tu, and **Xiali Hei**. "A First Look at the Security of EEG-based Systems and Intelligent Algorithms under Physical Signal injection." *Accepted by The inaugural AsiaCCS 2023 Workshop on Secure and Trustworthy Deep Learning Systems (SecTL 2023)*, 2023. [paper]

48. **[HICSS-56-1]** Vijay Srinivas Tida, Sai Venkatesh Chilukoti, Sonya Hsu, and **Xiali Hei**. "Kernel-Segregated Transpose Convolution Operation." *Accepted by HICSS-56: Hawaii International Conference on System Sciences*, 2023. [paper]

47. **[HICSS-56-2]** Vijay Srinivas Tida, Sonya Hsu, and **Xiali Hei**. "Privacy-Preserving Deep Learning Model for Covid-19 Disease Detection." *Accepted by HICSS-56: Hawaii International Conference on System Sciences*, 2023. [paper]

46. **[EuroSP2022]** Md Imran Hossen, and **Xiali Hei**. "aaeCAPTCHA: The Design and Implementation of Audio Adversarial CAPTCHA." *Published by IEEE Euro S&P*, 2022. [paper]

45. **[WOOT2021]** MD Imran Hossen and **Xiali Hei**. "A Low-Cost Attack against the hCaptcha System ." *WOOT*, 2021. [paper]

44. **[ASIACCS2021]** Yazhou Tu, Vijay Srinivas Tida , Zhongqi Pan, and **Xiali Hei**. "Transduction Shield: A Low-Complexity Method to Detect and Correct the Effects of EMI Injection Attacks on Sensors." *ACM ASIACCS*, 2021. [paper]

43. **[RAID2020]** MD Imran Hossen, Yazhou Tu, Md Fazle Rabby, Md Nazmul Islam, Hui Cao, and **Xiali Hei**. "An Object Detection based Solver for Googles Image reCAPTCHA v2." *USENIX RAID*, 2020. [paper]

42. **[CCS2019]** Yazhou Tu, Sara Rampazzi, Bin Hao, Angel Rodriguez, Kevin Fu, and **Xiali Hei**. "Trick or Heat? Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks." *ACM CCS*, 2019. [paper]

41. **[DSN2019]** Pingchuan Ma, Zhiqiang Wang, **Xiali Hei**, Xiaoxiang Zou, Jianyi Zhang, Qixu Liu, Xin Lyu, and Zihan Zhuo. "A Quantitative Approach for Medical Imaging Device Security Assessment." *The 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, 2019. [paper]

40. **[USENIX2018]** Yazhou Tu, Zhiqiang Lin, Insup Lee, and **Xiali Hei**. "Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors." *USENIX SECURITY Symp. 2018*, 2018. [paper]

39. **[MASS2018]** Bin Hao, **Xiali Hei**, Yazhou Tu, Xiaojiang Du, and Jie Wu. "Voiceprint-Based Access Control for Wireless Insulin Pump Systems." *IEEE MASS 2018*, 2018. [paper]

38. **[ICC2018-1]** Jian Zhao, Kam Kong, **Xiali Hei**, Yazhou Tu and Xiaojiang Du. "A Visible Light Channel based Access Control Scheme for Wireless Insulin Pump Systems." *IEEE ICC 2018*, 2018. [paper]

37. **[ICC2018-2]** Kuo Chi, Longfei Wu, Xiaojiang Du, Guisheng Yin, Jie Wu, Bo Ji, and **Xiali Hei**. "Enabling Fair Spectrum Sharing between Wi-Fi and LTE-Unlicensed." *IEEE ICC 2018*, 2018. [paper]

36. **[ICC2017-SHIPHER]** **Xiali Hei**, Binheng Song, and Caijin Ling. "SHipher: Families of Block Ciphers based on customized operator." *IEEE ICC 2017*, 2017. [paper]

35. **[ICC2017-2]** Kam Kong, **Xiali Hei**, Caijin Ling, Mohsen Guizani, and Hui Cao. "A Countermeasure Against Face-Spoofing Attacks Using Interaction Video Framework." *IEEE ICC 2017*, 2017. [paper]

34. **[GLOBECOM2016]** Caijin Ling, **Xiali Hei**, Kam Kong, Michael Peays, and Mohsen Guizani. "You Cannot Sense My PINs: A Side Channel Attack Deterrent Solution for Touch-enabled Devices." *IEEE GLOBECOM 2016*, 2016. [paper]

33. **[CISS2015]** Gang Wang, Wenming Li, and **Xiali Hei**. "Energy-aware real-time scheduling on Heterogeneous

Multi-Processor." *In Proc. of the 49th Information Sciences and Systems (CISS)*, 2015. [paper]

32. [**EIISOP2015**] Xunyu Pan, Timothy J Cross, Liangliang Xiao, and **Xiali Hei**. "Musical examination to bridge audio data and sheet music." *T/SPIE Electronic Imaging. International Society for Optics and Photonics*, 2015. [paper]
31. [**MOBILEHEALTH2014**] **Xiali Hei** and Shan Lin. "Multi-part file encryption for electronic health records cloud." *In the Proceedings of the 4th ACM MobiHoc Workshop on Pervasive wireless healthcare*, 2014. [paper]
30. [**MOBIHOC2014**] **Xiali Hei**, Xiaojiang Du, and Shan Lin. "Near field communication based access control for wireless medical devices." *In the Proceedings of the 15th ACM international symposium on Mobile ad hoc networking and computing*, 2014. **Best Poster Runner-up Award!** [paper]
29. [**INFOCOM2013**] **Xiali Hei**, Xiaojiang Du, Shan Lin, and Insup Lee. "PIPAC: Patient Infusion Pattern based Access Control Scheme for Wireless Insulin Pump System." *In Proc. of IEEE INFOCOM 2013*, 2013. [paper]
28. [**ICC2013**] **Xiali Hei**, Xiaojiang Du, and Shan Lin. "Two Vulnerabilities in Android OS Kernel." *In Proc. of IEEE ICC 2013*, 2013. [paper]
27. [**ICC2012-1**] **Xiali Hei**, Xiaojiang Du, and Shan Lin. "Two Matrices for Blakleys Secret Sharing Scheme." *In Proc. of IEEE ICC 2012*, 2012. [paper]
26. [**ICC2012-2**] **Xiali Hei**, Xiaojiang Du, and Shan Lin. "A Distributed Login Framework for Semi-structured Peer-to-Peer Networks." *In Proc. of IEEE ICC 2012*, 2012. [paper]
25. [**INFOCOM2011**] **Xiali Hei**, Xiaojiang Du. "Biometric-based Two-level Secure Access Control for Implantable Medical Devices during Emergencies." *In Proc. of IEEE INFOCOM (mini-conference)*, 2011.2011 [paper]
24. [**GLOBECOM2010**] **Xiali Hei**, Xiaojiang Du, Jie Wu, Fei Hu. "Defending Resource Depletion Attacks on Implantable Medical Devices." *In Proc. of IEEE GLOBECOM 2010*, 2010. [paper]

JOURNAL

23. [**DCNS2023**] Jianyi Zhang, Fengjiao Zhang, Qichao Jin, Zhiqiang Wang, Kang Xie, and **Xiali Hei**. "XMAM:X-raying Models with A Matrix to Reveal Backdoor Attacks for Federated Learning." *Published, Digital Communications and Networks*, 2023. [paper]
22. [**BigData2023**] Vijay Srinivas Tida, Sonya Hsu, and **Xiali Hei**. "A Unified Training Process for Fake News Detection based on Fine-Tuned BERT Model." *Big Data*, Accepted, Impact Factor 4.426.
21. [**AGER2023**] Liqun Shan, Chengqian Liu, Yanchang Liu, Yazhou Tu, Linyu Deng, and **Xiali Hei**. "Physics-informed Neural Networks Based on Long Short-term Memory and Attention Mechanism for Solving Partial Differential Equations in Porous Media." *Advances in Geo-Energy Research*, Accepted, Impact Factor 6.96.
20. [**Energies2022**] Liqun Shan, Chengqian Liu, Yanchang Liu, Weifang Kong, and **Xiali Hei**. "Rock CT Image Super-Resolution Using Residual Dual-Channel Attention Generative Adversarial Network." *MDPI Energies*, Published, Impact Factor 3.004.
19. [**BMC2021**] Md Fazle Rabby, Yazhou Tu, Md Imran Hossen, Insup Lee, Anthony S Maida, and **Xiali Hei**. "Stacked LSTM Based Deep Recurrent Neural Network with Kalman Smoothing for Blood Glucose Prediction." *BMC Medical Informatics and Decision Making*, 2021. [pdf]
18. [**Electronics-2020**] Yuan Ping, Bin Hao, **Xiali Hei**, Jie Wu, and Baocang Wang. "Maximized Privacy-Preserving Outsourcing on Support Vector Clustering." *Electronics*, 2020. Impact factor: 2.110
17. [**ACCESS2019-1**] Yuan Ping, Bin Hao, **Xiali Hei**, Yazhou Tu, Xiaojiang Du, and Jie Wu. "Feature Fusion and Voiceprint Based Access Control for Wireless Insulin Pump Systems." *IEEE ACCESS*, 2019. [pdf]
16. [**ACCESS2019-2**] Yuan Ping, Bin Hao, Huina Li, Yuping Lai, Chun Guo, Hui Ma, Baocang Wang, and **Xiali Hei**. "Efficient Training Support Vector Clustering with Appropriate Boundary Informations." *IEEE AC-*

CESS, 2019. [pdf]

15. [**JCSSC2019**] Shiliang Zhang, Hui Cao, Zonglin Ye, Yanbin Zhang, and **Xiali Hei**. "An outlier detection scheme for dynamical sequential datasets." *Journal Communications in Statistics-Simulation and Computation*, 2019. [pdf]

14. [**TNNLS2018**] Shiliang Zhang, Hui Cao, Shuo Yang, Yanbin Zhang, and **Xiali Hei**. "Sequential Outlier Criterion for Sparsification of Online Adaptive Filtering." *IEEE Transactions on Neural Networks and Learning Systems*, 2018.Impact factor: 6.08 [pdf]

13. [**MPE2017**] Shiliang Zhang, Hui Cao, Yanbin Zhang, Lixin Jia, Zonglin Ye, and **Xiali Hei**. "Data-Driven Optimization Framework for Nonlinear Model Predictive Control." *Mathematical Problems in Engineering*, 2017. [pdf]

12. [**CILS2017**] Hui Cao, Yajie Yu, Yanbin Zhou, and **Xiali Hei**. "Double outlyingness analysis in quantitative spectral calibration: Implicit detection and intuitive categorization of outliers." *Chemometrics and Intelligent Laboratory Systems*, 2017. [pdf]

11. [**TPDS2014**] **Xiali Hei**, Xiali Hei, Xiaojiang Du, Shan Lin, Insup Lee, and Oleg Sokolsky. "Patient Infusion Pattern based Access Control Schemes for Wireless Insulin Pump System." *IEEE Transactions on Parallel and Distributed Systems*, 2014. [pdf]

Pre-Print

10. [**Archive2023-1**] Jianyi Zhang, Xu Ji, Zhangchi Zhao, **Xiali Hei**, and Kim-Kwang Raymond Choo. "Ethical Considerations and Policy Implications for Large Language Models: Guiding Responsible Development and Deployment." *Arxiv*, 2023.

[pdf]

BOOK CHAPTER

9. [**CRC2023-1**] Joseph Layton, Fei Hu, and **Xiali Hei**. "Survey of Machine Learning Defense Strategies." *CRC*, 2023.

[pdf]

8. [**CRC2023-2**] Jiamiao Zhao, Fei Hu, and **Xiali Hei**. "Defensive Schemes for Cyber Security of Deep Reinforcement Learning." *CRC*, 2023.

[pdf]

7. [**CRC2023-3**] Jiamiao Zhao, Fei Hu, and **Xiali Hei**. " 4 Attack Models for Collaborative Deep Learning." *CRC*, 2023.

[pdf]

6. [**IGI2022-1**] Md Imran Hossen, Md Abdullah Al Momin, and **Xiali Hei**. "Generating Device Fingerprints for Smart Device Pairing Using the Unique Spectrum Characteristic From LEDs." *IGI*, 2022.

[pdf]

5. [**IGI2022-2**] Md Imran Hossen, Md Abdullah Al Momin, and **Xiali Hei**. "Handwritten Signature Spoofing With Conditional Generative Adversarial Nets." *IGI*, 2022. [pdf]

4. [**IGI2022-3**] Vijay Srinivas Srinivas Tida, Raghabendra Shah, and **Xiali Hei**. "Deep Learning Approach for Protecting Voice-Controllable Devices From Laser Attacks." *IGI*, 2022. [pdf]

3. [**IGI2019**] Bin Hao and **Xiali Hei**. "Voice Liveness Detection for Medical Devices." *IGI*, 2019. [pdf]

BOOK

2. [**Book1**] **Xiali Hei**, Xiaojiang Du. "Emerging Security Issues in Wireless Implantable Medical Devices." *Springer*, . 2013 [pdf]

DISSERTATION

1. **[DISS2014] Xiali Hei**. "Security issues and defense methods for wireless medical devices." *Temple University*, 2014. [pdf]

TEACHING

Spring 2023: CSCE 512 Computer Network Security

Fall 2022: INFX 499 Ethical Hacking

Spring 2022: CSCE 512 Computer Network Security

Fall 2021: INFX 455 Cyber-physical System Security & CSCE 598 Special Topics

Spring 2021: CSCE 512 Computer Network Security

Fall 2020: INFX 455 Cyber-physical System Security & CSCE 598 Special Topics

Spring 2020: CSCE 512 Computer Network Security

Fall 2019: INFX 455 Cyber-physical System Security & CSCE 598 Special Topics

Fall 2018: CSCE 512 Computer Network Security

Spring 2018: CSCE 512 Computer Network Security

Spring 2017: Advanced Computer Network

Spring 2017: Computer Network

Fall 2016: Advanced Operating system

Fall 2016: Operating system

Spring 2016: Topics in Ethical Hacking (tons of hands-on various hacking methods)

Spring 2016: Advanced Computer Network (tons of new technology)

Fall 2015: Advanced operating system

Fall 2015: Operating system

Spring 2015: Computer Forensics

Spring 2015: Ethical Hacking

Spring 2015: Computer Science Basics

Fall 2014: Database Security

Fall 2014: Software Engineering Security

Fall 2014: Cloud Security

Fall 2014: Computer Science Basics

ACADEMIC SERVICES

Panelist:

1) NSF Cyber-Physical System

2) NSF Secure and Trustworthy Cyberspace

3) NSF Major Research Instrument

Session Chair:

1) USENIX Security Symp. 2020 & 2021 & 2022

2) The Third International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021

3) IEEE Workshop on the Internet of Safe Things 2021

Publicity and Social Media Chair:

1) EAI SmartSP 2023 - EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles

Program Committee Member:

1) The 8th IEEE European Symposium on Security and Privacy, 2023

2) The 1st Workshop on Vehicle Security and Privacy (VehicleSec), co-located with NDSS 2023

3) USENIX Security Symp. 2022 & Auto Security Workshop 2022 & SafeThings Workshop 2022 & 22nd Privacy Enhancing Technologies Symposium (PETS 2022)

4) USENIX Security Symp. 2021 & Auto Security Workshop 2021 & SafeThings Workshop 2021

5) USENIX Security Symp. 2020

6) USENIX Security Symp. 2019

7) International Conference on Data Intelligence and Security (ICDIS 2019)

8) IEEE GLOBECOM 2013 & 2014 & 2015 & 2016 & 2017

9) IEEE CyperC 2014 & 2015 & 2016

10) IEEE ICC 2014 & 2015 & 2016 & 2017 & 2018

11) IEEE ICCVE 2013 & 2014 & 2015 & 2016

12) IEEE ICACCI 2014

13) IEEE WASA 2016 & 2017

Editor of journals:

1) Associate editor of IEEE Access (2020-2023)

2) Assistant managing editor of JISTMSR (Journal of Information Systems and Technology Management for Specialized Research);

3) Guest editor of Special Issue Security Analytics and Intelligence for Cyber-Physical Systems for IEEE Access

Reviewer for journals:

1) IEEE Transactions on Wireless Communications

2) IEEE Transactions on Parallel and Distributed Systems

3) IEEE Wireless Communications Letters

4) IEEE Wireless Communications Magazine

5) International Journal of Ad Hoc and Ubiquitous Computing

6) Wiley Journal of Security and Communication Networks

INVITED TALKS

13. "Research on Attacks, Defenses, and Designs of Image and Audio CAPTCHAs", *University of Houston*, USA, 2022.

12. "Investigate and Mitigate the Attacks Caused by Out-of-Band Signals", *University of Pennsylvania*, USA, 2022.
11. "Investigate and Mitigate the Attacks Caused by Out-of-Band Signals", *Stony Brook University*, USA, 2022.
10. "Investigate and Mitigate the Attacks Caused by Out-of-Band Signals", *Saint Josephs University*, USA, 2021.
9. "Security of Wireless Medical Devices", *University of Louisiana at Lafayette*, USA, 2017.
8. "Security of Wireless Medical Devices", *Georgia State University*, USA, 2017.
7. "Security of Wireless Medical Devices", *University of Idaho*, USA, 2017.
6. "Security of Wireless Medical Devices", *Delaware State University* , USA, 2015.
5. "Security of Wireless Medical Devices", *Fairleigh Dickinson University* , USA, 2015.
4. "Security of Wireless Medical Devices", *Frostburg State University* , USA, 2014.
3. "Security of Wireless Medical Devices", *Virginia Commonwealth University* , USA, 2014.
2. "Security of Wireless Medical Devices", *Mary University* , USA, 2014.
1. "Security of Wireless Medical Devices", *McMaster University*, Canana, 2013.

MENTORING, LEADERSHIP & ACTIVITIES

- Current Ph.D. students: Borun Das, Shovon Paul, Sai Venkatesh Chilukoti, Liqun Shan (female), Xingli Zhang (female), Diba Afroze (female).
- Graduated Ph.D Students: Yazhou Tu (will join Auburn University as a tenure-track assistant professor), Vijay Srinivas Tida (Co-advised, will join The College of Saint Benedict and Saint Johns University as a tenure-track assistant professor), Md Imran Hossen (On job market).
- Current M.S. students: Foba Ogunkeye (minority),
- Graduated M.S. students: Md Fazle Rabby, Md Abdullah Al Momin, Yazhou Tu, Jian Zhao, Michael Peays (Minority student)
- Current Undergraduate students: Kristina Khalid-Abasi (female minority), Hien Nguyen (female), Jed R Booth, Mason J Mendoza, Peyton G Shaw
- Previous Undergraduate Students: Roshitha Vallurupalli (female), Ashley Nicole Williams (female minority), Matthew Fillman, Niara Medley (female minority), Michaela Barnett (female minority)
- Current Post-doc: Yazhou Tu, Md Imran Hossen.
- Previous Post-doc: Dr. Bin Hao
- Current Visiting Scholar: N/A.
- Previous Visiting Scholar: Dr. Jianyi Zhang, Dr. Yuan Ping, Mr. Caijin Ling