Dave (Jing) Tian

Curriculum Vitae (2024-05-27)

Interests

Embedded Systems Security, Operating Systems Security, Trusted and Confidential Computing, Hardware Security and Trust

Work

2019.08– **Assistant Professor**, *Purdue University*, West Lafayette, IN, Department of Computer Science.
Systems Security

2018.05–2018.08 **Security Research Engineer Intern**, *Fortanix*, Mountain View, CA, Runtime Encryption.
Intel SGX for Containers

2017.05–2017.08 **Security Research Engineer Intern**, *Samsung Research America (SRA)*, Mountain View, CA, Android Security.
Android USB Security

2009.07–2012.08 **Software Engineer**, *Nokia R&D*, Qingdao, China, Linux Control Platform (LCP).
Software Development for Linux

2008.12–2009.06 **Software Engineer Intern**, *Nokia R&D*, Qingdao, China, Linux Control Platform (LCP).
Software Development for Linux

2006.03–2006.04 **POS Tester Intern**, *Hisense R&D*, Qingdao, China, POS Testing.
POS Testing

Education

2015.01–2019.08 **Ph.D.**, *University of Florida*, Gainesville, FL, Computer & Information Science & Engineering.
Systems Security and Trusted Computing

2012.08–2014.07 **Ph.D. student**, *University of Oregon*, Eugene, OR, Computer & Information Science.
Machine Learning and Systems Security

2006.08–2009.06 **ME**, *Ocean University of China*, Qingdao, China, Electrical Engineering.
Digital Signal Processing and Machine Learning

2002.08–2006.06 **BS**, *Qingdao University of Technology*, Qingdao, China, Electrical & Information Science.
Electrical Engineering

Publications

Journals:

7 **Security Challenges of Intent-Based Network**; Jiwon Kim, Dave (Jing) Tian, Hamed Okhravi, Benjamin E. Ujcich; Communications of the ACM (CACM), 2024.

6 **ENCIDER: Detecting Timing and Cache Side Channels in SGX Enclaves and Cryptographic APIs**; Tuba Yavuz, Farhaan Fowze, Ken (Yihang) Bai, Grant Hernandez, Kevin Butler, Dave (Jing) Tian; IEEE Transactions on Dependable and Secure Computing (TDSC'22); Intel Security Conference (iSecCon'22), 2022

5 **ProXray: Protocol Model Learning and Guided Firmware Analysis**; Farhaan Fowze, Dave (Jing) Tian, Grant Hernandez, Kevin Butler, Tuba Yavuz; IEEE Transactions on Software Engineering (TSE'19), 2019; International Conference on Software Engineering (ICSE'20, Journal First), 2020; Selected for Journal-First presentation at ICSE'20

4 **Towards Automated Firmware Analysis in the IoT Era**; Grant Hernandez, Dave (Jing) Tian, Farhaan Fowze, Tuba Yavuz, Patrick Traynor, Kevin Butler; IEEE Security & Privacy, 2019

3 **Characterizing the Security of the SMS Ecosystem with Public Gateways**; Bradly Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, Kevin Butler; ACM Transactions on Privacy and Security (TOPS), 2018

Purdue University, Department of Computer Science
305 N. University Street, West Lafayette, IN 47907
☎ *(765) 496 6544* • ✉ *root@davejingtian.org* • *davejingtian.org*

2 **Securing ARP/NDP From the Ground Up**; Dave (Jing) Tian, Kevin R. B. Butler, Joseph I. Choi, Patrick D. McDaniel, Padma Krishnaswamy; IEEE Transactions on Information Forensics and Security (TIFS), 2017

1 **Taming the Costs of Trustworthy Provenance through Policy Reduction**; Adam Bates, Dave (Jing) Tian, Grant Hernandez, Thomas Moyer, Kevin R. B. Butler, Trent Jaeger; ACM Transactions on Internet Technology (TOIT), 2017

Conferences:

49 **Exploiting Temporal Vulnerabilities for Unauthorized Access in Intent-based Networking**; Ben Weintraub, Jiwon Kim, Ran Tao, Cristina Nita-Rotaru, Hamed Okhravi, Dave (Jing) Tian, Benjamin E. Ujcich; ACM Conference on Computer and Communications Security (CCS'24), 2024; Acceptance Rate=TBD%

48 **Securing Deep Neural Networks on Edge from Membership Inference Attacks Using Trusted Execution Environments**; Cheng-Yun Yang, Gowri Ramshankar, Nicholas Eliopoulos, Purvish Jajal, Sudarshan Nambiar, Evan Miller, Xun Zhang, Dave (Jing) Tian, Shuo-Han Chen, Chiy-Ferng Perng, Yung-Hsiang Lu; ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED'24), 2024; Acceptance Rate=TBD%

47 **Minding the Semantic Gap for Effective Storage-Based Ransomware Defense**; Weidong Zhu, Grant Hernandez, Washington Garcia, Dave (Jing) Tian, Sara Rampazzi, Kevin Butler; International Conference on Massive Storage Systems and Technology (MSST'24), 2024; Acceptance Rate=TBD%

46 **D-Helix: A Generic Decompiler Testing Framework Using Symbolic Differentiation**; Muqi Zou, Arslan Khan, Ruoyu Wu, Han Gao, Antonio Bianchi, Dave (Jing) Tian; USENIX Security Symposium (Security'24), 2024; Acceptance Rate=TBD%

45 **Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations**; Jianliang Xu, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, Antonio Bianchi; USENIX Security Symposium (Security'24), 2024; Acceptance Rate=TBD%

44 **Building GPU TEEs using CPU Secure Enclaves with GEVisor**; Xiaolong Wu, Dave (Jing) Tian, Chung Hwan Kim; ACM Symposium on Cloud Computing 2023 (SoCC'23), 2020; Acceptance Rate = TBD%

43 **SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth**; Jianliang Xu, Ruoyu Wu, Dongyan Xu, Dave (Jing) Tian, Antonio Bianchi; IEEE Symposium on Security and Privacy (Oakland'24), 2024; Acceptance Rate=TBD%

42 **Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery**; Kyungtae Kim, Sungwoo Kim, Kevin Butler, Antonio Bianchi, Rick Kennell, Dave (Jing) Tian, USENIX Security Symposium (Security'23), 2023; Acceptance Rate=TBD%

41 **Fuzzing SGX Enclaves via Host Program Mutations**; Arslan Khan, Muqi Zou, Kyungtae Kim, Dongyan Xu, Antonio Bianchi, Dave (Jing) Tian; IEEE European Symposium on Security and Privacy (EuroS&P'23), 2023; Acceptance Rate=TBD%

40 **EC: Embedded Systems Compartmentalization via Intra-Kernel Isolation**; Arslan Khan, Dongyan Xu, Dave (Jing) Tian; IEEE Symposium on Security and Privacy (Oakland'23), 2023; Acceptance Rate=TBD%

39 **Low-Cost Privilege Separation with Compile Time Compartmentalization for Embedded Systems**; Arslan Khan, Dongyan Xu, Dave (Jing) Tian; IEEE Symposium on Security and Privacy (Oakland'23), 2023; Acceptance Rate=TBD%

38 **Fuzzing Intent-Based Networking with Intent-State Transition Guidance**; Jiwon Kim, Benjamin E. Ujcich, Dave (Jing) Tian; USENIX Security Symposium (Security'23), 2023; Acceptance Rate=TBD%

37 **DnD: Decompiling Deep Neural Network Compiled Binary**; Ruoyu Wu, Taegyu Kim, Dave (Jing) Tian, Antonio Bianchi, Dongyan Xu; Black Hat Europe (BH-EU'22), 2022; Acceptance Rate=TBD%

36 **GLeeFuzz: Fuzzing WebGL Through Error Message Guided Mutation**; Hui Peng, Zhihao Yao, Ardalan Amiri Sani, Dave (Jing) Tian, Mathias Payer; USENIX Security Symposium (Security'23), 2023; Acceptance Rate=TBD%

35 **TruEMU: An Extensible, Open-Source, Whole-System iOS Emulator**; Trung Nguyen, Kyungtae Kim, Antonio Bianchi, Dave (Jing) Tian; Black Hat USA (BH-USA'22), 2022; Acceptance Rate=TBD%

34 **DnD: A Cross-Architecture Deep Neural Network Decompiler**; Ruoyu Wu, Taegyu Kim, Dave (Jing) Tian, Antonio Bianchi, Dongyan Xu; USENIX Security Symposium (Security'22), 2022; Acceptance Rate=17.2%

33 **Reverse Engineering and Retrofitting Robotic Aerial Vehicle Control Firmware using DisPatch**; Taegyu Kim, Aolin Ding, Sriharsha Etigowni, Pengfei Sun, Jizhou Chen, Luis Garcia, Saman Zonouz, Dongyan Xu, Dave (Jing) Tian; ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'22), 2022; Acceptance Rate=21.6%

32 **ShadowAuth: Backward-Compatible Automatic CAN Authentication for Legacy ECUs**; Sungwoo Kim, Gisu Yeo, Taegyu Kim, Junghwan "John" Rhee, Yuseok Jeon, Antonio Bianchi, Dongyan Xu, Dave (Jing) Tian; ACM ASIA Conference on Computer and Communications Security (ASIACCS'22), 2022; Acceptance Rate=18.4%

31 **Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities**; Jianliang Wu, Ruoyu Wu, Dongyan Xu, Dave (Jing) Tian, Antonio Bianchi; IEEE Symposium on Security and Privacy (Oakland'22), 2022; Acceptance Rate=14.5%

30 **FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks**; Kyungtae Kim, Taegyu Kim, Ertza Warraich, Byoungyoung Lee, Kevin Butler, Antonio Bianchi, Dave (Jing) Tian; IEEE Symposium on Security and Privacy (Oakland'22), 2022; Acceptance Rate=14.5%

29 **Privacy-Preserving Localization Using Enclaves**; Arslan Khan, Joseph I.Choi, Dave (Jing) Tian, Tyler Ward, Kevin Butler; Patrick Traynor, John Shea, Tan Wong; IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON'21), 2021; Acceptance Rate=TBD%, Best Presentation Award

28 **Towards Improving Container Security by Preventing Runtime Escapes**; Michael Reeves, Dave (Jing) Tian, Antonio Bianchi, Berkay Celik; IEEE Secure Development Conference (SecDev'21), 2021; Acceptance Rate=TBD%

27 **LIGHTBLUE: Automatic Profile-Aware Debloating of Bluetooth Stacks**; Jianliang Wu, Ruoyu Wu, Daniele Antonioli, Mathias Payer, Nils Ole Tippenhauer, Dongyan Xu, Dave (Jing) Tian, Antonio Bianchi; USENIX Security Symposium, 2021; Acceptance Rate = 18.8%

26 **M2MON: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles**; Arslan Khan, Hyungsub Kim, Byoungyoung Lee, Dongyan Xu, Antonio Bianchi, Dave (Jing) Tian; USENIX Security Symposium, 2021; Acceptance Rate = 18.8%

25 **PASAN: Detecting Peripheral Access Concurrency Bugs within Bare-metal Embedded Applications**; Taegyu Kim, Vireshwar Kumar, Junghwan Rhee, Jizhou Chen, Kyungtae Kim, Chung Hwan Kim, Dongyan Xu, Dave (Jing) Tian; USENIX Security Symposium, 2021; Acceptance Rate = 18.8%

24 **Generic, Sparse Tensor Core for Neural Networks**; Xiaolong Wu, Yang Yi, Dave Tian, Jiajia Li; International Workshop on Machine Learning for Software Hardware Co-Design (MLSH'20), 2020; Acceptance Rate = TBD%

23 **Vessels: Efficient and Scalable Deep Learning Prediction on Trusted Processors**; Kyungtae Kim, Chung Hwan Kim, Junghwan Rhee, Xiao Yu, Haifeng Chen, Dave Tian, Byoungyoung Lee; ACM Symposium on Cloud Computing 2020 (SoCC'20), 2020; Acceptance Rate = 24.5%

22 **Logging to the Danger Zone: Race Condition Attacks and Defenses on System Audit Frameworks**; Riccardo Paccagnella, Kevin Liao, Dave Tian, Adam Bates; ACM Conference on Computer and Communications Security (CCS'20), 2020; Acceptance Rate = 16.9%

21 **BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy**; Jianliang Wu, Yuhong Nan, Vireshwar Kumar, Dave (Jing) Tian, Antonio Bianchi, Mathias Payer, Dongyan Xu; USENIX Workshop on Offensive Technologies (WOOT'20), 2020; Acceptance Rate = 33.3%, Best Paper Award

20 **From Control Model to Program: Investigating Robotic Aerial Vehicle Accidents with MAYDAY**; Taegyu Kim, Chung Hwan Kim, Altay Ozen, Fan Fei, Zhan Tu, Xiangyu Zhang, Xinyan Deng, Dave (Jing) Tian, Dongyan Xu; USENIX Security Symposium, 2020; Acceptance Rate = 16.3%

19 **Custos: Practical Tamper-Evident Auditing of Operating Systems Using Trusted Execution**; Riccardo Paccagnella, Pubali Datta, Wajih Ul Hassan, Adam Bates, Christopher Fletcher, Andrew Miller, Dave (Jing) Tian; The Network and Distributed System Security Symposium (NDSS'20), 2020; Acceptance Rate = 17.4%

18 **BigMAC: Fine-Grained Policy Analysis of Android Firmware**; Grant Hernandez, Dave (Jing) Tian, Anurag Swarnim Yadav, Byron J. Williams, Kevin Butler; USENIX Security Symposium, 2020; Acceptance Rate = 16.3%

17 **Examining DES-based Cipher Suite Support within the TLS Ecosystem**; Vanessa Frost, Dave Tian, Christie Ruales, Vijay Prakash, Kevin Butler, Patrick Traynor; ACM ASIA Conference on Computer and Communications Security (ASIACCS'19), 2019; Acceptance Rate = 22% short paper

16 **A Hybrid Approach to Secure Function Evaluation using SGX**; Joseph Choi, Dave Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Kevin Butler, Patrick Traynor; ACM ASIA Conference on Computer and Communications Security (ASIACCS'19), 2019; Acceptance Rate = 17%

15 **A Practical Intel SGX Setting for Linux Containers in the Cloud**; Dave (Jing) Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, Kevin Butler; ACM Conference on Data and Application Security and Privacy (CODASPY'19), 2019; Acceptance Rate = 23.5%, Distinguished Poster Award (for poster accompanying the full paper)

14 **LBM: A Security Framework for Peripherals within the Linux Kernel**; Dave (Jing) Tian, Grant Hernandez, Joesph Choi, Vanessa Frost, Peter Johnson, Kevin Butler; IEEE Symposium on Security and Privacy (S&P'19), 2019; Acceptance Rate = 12.5%

13 **ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem**; Dave (Jing) Tian, Grant Hernandez, Joesph Choi, Vanessa Frost, Christie Ruales, Patrick Traynor, Hayawardh Vijaykumar, Lee Harrison, Amir Rahmati, Mike Grace, Kevin Butler; USENIX Security Symposium, 2018; Acceptance Rate = 19.1%

12 **SoK: "Plug & Pray" Today – Understanding USB Insecurity in Versions 1 through C**; Dave (Jing) Tian, Nolen Scaife, Deepak Kumar, Michael Bailey, Adam Bates, Kevin Butler; IEEE Symposium on Security and Privacy (S&P'18), 2018; Acceptance Rate = 11.5%

11 **FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution**; Grant Hernandez, Farhaan Fowze, Dave Tian, Tuba Yavuz, Kevin Butler; ACM Conference on Computer and Communications Security (CCS'17), 2017; Acceptance Rate = 18.1%

10 **CPAC: Securing Critical Infrastructure with Cyber-Physical Access Control**; Sriharsha Etigowni, Dave Tian, Grant Hernandez, Kevin Butler, Saman Zonouz; Annual Computer Security Applications Conference (ACSAC'16), 2016; Acceptance Rate = 22.8%

9 **ProvUSB: Block-level Provenance-Based Data Protection for USB Storage Devices**; Dave (Jing) Tian, Adam Bates, Kevin Butler, Raju Rangaswami; ACM Conference on Computer and Communications Security (CCS'16), 2016; Acceptance Rate = 16.5%

8 **Making USB Great Again with USBFILTER**; Dave (Jing) Tian, Nolen Scaife, Adam Bates, Kevin Butler, Patrick Traynor; USENIX Security Symposium, 2016; Acceptance Rate = 15.5%

7 **Detecting SMS Spam in the Age of Legitimate Bulk Messaging**; Bradley Reaves, Logan Blue, Dave Tian, Patrick Traynor, Kevin Butler; ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'16), 2016; Acceptance Rate = 35.0%

6 **Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways**; Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, Kevin Butler; IEEE Symposium on Security and Privacy (S&P'16), 2016; Acceptance Rate = 13.3%

5 **Defending Against Malicious USB Firmware with GoodUSB**; Dave (Jing) Tian, Adam Bates, Kevin Butler; Annual Computer Security Applications Conference (ACSAC'15), 2015; Acceptance Rate = 24.3%

4 **Trustworthy Whole-System Provenance for the Linux Kernel**; Adam Bates, Dave Tian, Kevin Butler, Thomas Moyer; USENIX Security Symposium, 2015; Acceptance Rate = 15.7%

3 **More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations**; Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, Kevin Butler; International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA'15), 2015; Acceptance Rate = 22.7%

2 **Securing ARP from the Ground Up**; Jing (Dave) Tian, Kevin R.B. Butler, Patrick D. McDaniel, Padma Krishnaswamy; ACM Conference on Data and Application Security and Privacy (CODASPY'15), 2015; Acceptance Rate = 33.3%

1 **Securing SSL Certificate Validation through Dynamic Linking**; Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, Jing (Dave) Tian, Abdulrahman Alkhelaifi, Kevin R. B. Butler; ACM Conference on Computer and Communications Security (CCS'14), 2014; Acceptance Rate = 19.5%

Patents:

2 **Protocol Model Learning and Guided Firmware Analysis**; US 11640464

1 **Method and Apparatus For Vetting Universal Serial Bus Device Firmware**; US 11568044B2

Service

Organizing Committee

- Midwest Security Workshop (MSW): '20
- EAI SecureComm: '20 (Poster Chair)
- ACSA ACSAC: '21 (Student Conferenceship Coordinator)
- USENIX Security: '21 (Session Co-chair)
- IEEE SafeThings: '22 (TPC Co-chair), '23 (General Co-Chair)
- IEEE SecDev: '24 (Vice General Chair), '25 (General Chair)

Technical Program Committee
- USENIX Security: ’19, ’21, ’22
- USENIX RAID: ’20
- USENIX WOOT: ’23, ’24
- ISOC NDSS: ’21, ’24
- ISOC NDSS BAR: ’20, ’22, ’23, ’24
- ISOC NDSS AutoSec: ’22
- ISOC NDSS VehicleSec: ’23, ’24
- ESORICS: ’20, ’21, ’22
- EAI SecureComm: ’20
- ACM AsiaCCS: ’21, ’22, ’24
- ACM CODASPY: ’24
- ACSA ACSAC: ’21, ’22, ’23, ’24
- IEEE Security & Privacy (Oakland): ’23, ’24
- IEEE CNS: ’21
- IEEE SafeThings: ’22 (co-chair)
- IEEE SecDev: ’22, ’23
- IEEE DSN: ’25

Conference External Review
- IEEE S&P: ’16, ’17, ’18, ’20
- USENIX Security: ’14, ’15, ’17, ’18, ’20, ’23
- ISOC NDSS: ’16, ’17, ’18, ’19
- ACM CCS: ’14, ’15, ’16
- USENIX OSDI: ’16
- ACM AsiaCCS: ’15, ’17, ’18
- USENIX WOOT: ’16
- ACSAC: ’16
- PETS: ’15
- IEEE MOST: ’15
- IEEE CNS: ’17

Journal Review
- Security and Communication Networks (SCN): ’17
- Journal of Network and Systems Management (JONS): ’17, ’21
- Journal of Information Security and Applications (JISA): ’20, ’22
- Journal of Information Science and Engineering (JISE): ’20
- Journal of Computer & Security (JCS): ’20
- IEEE Internet of Things Journal (IoT): ’19
- IEEE Transactions on Dependable and Secure Computing (TDSC): ’20, ’21, ’22, ’23
- IEEE Embedded Systems Letters (ESL): ’24
- Journal of Purdue Undergrad Research (JPUR): ’22
- International Journal of Information Security: ’23

Others
- NSF Panel: ’22, ’23

Fundings

ONR Bringing Fuzzing to the Cyber-Physical World; $800K, co-PI

DARPA AMP - DICER: Directed Compilation for Assured Patching; $3.9M, co-PI

DOE CyManII - Discovering Vulnerabilities in IIoT-Enabled Manufacturing Systems; $110M, co-PI

ONR IoT-D: Towards Internets of Dialect-Speaking Things; $6M, Senior Personnel

NSF Faculty Early Career Development Program (CAREER); $520K, sole-PI

ONR An Integrated Toolkit for IoT Protocol Dialecting with Formal Verification; $620K, co-PI

Wistron Securing AI Workload on Edge/IoT Devices; $248K, co-PI

Wistron Securing Hardware and Firmware Supply Chain; $248K, PI

ONR Semantic Decompilation of Deep Neural Network Binaries and Its Adversarial and Defensive Implications; $750K, PI

Rolls-Royce	FailFlow – Tracing the flow of cyber-attacks from one domain to another to motivate the development of a Common Applicability Enumeration; $110K, co-PI
DARPA	FIRE - FIREFLY: A Cyber-Physical Framework for Scalable CPS Modeling and Simulation; $6.5M, co-PI
Lockheed Martin	Towards an End-to-end Pipeline for Lifting and Patching DNN Binaries for Adversarial and Defensive Application; $65K, co-PI
Lockheed Martin	An End-to-end, Automated Pipeline for Lifting and Patching DNN Binaries for Adversarial and Defensive Applications; $120K, co-PI

Invited Talks

Apr 2024	Panel: Where Code Meets Chip, The 25th annual CERIAS Security Symposium, Moderator: Anand Raghunathan
Apr 2024	Fuzzing SGX Enclaves viaHost Program Mutations, Intel Produce Assurance and Security (IPAS) Tech Sharing, Host: Daniel Dinu
Aug 2021	DisPatch: Patching Control-Semantic Bugs in RAV Firmware, DARPA ReMath PI Meeting, Host: Sergey Bratus
Mar 2019	Defending Operating Systems from Malicious Peripherals, Georgetown University, Host: Clay Shields
Mar 2019	Defending Operating Systems from Malicious Peripherals, University of Texas Dallas, Host: Murat Kantarcioglu
Mar 2019	Defending Operating Systems from Malicious Peripherals, University of California Santa Cruz, Host: Owen Arden
Feb 2019	Defending Operating Systems from Malicious Peripherals, Virginia Tech, Host: Matthew Hicks
Feb 2019	Defending Operating Systems from Malicious Peripherals, Purdue University, Host: Dongyan Xu
Feb 2019	Defending Operating Systems from Malicious Peripherals, Duke University, Host: Benjamin Lee
Feb 2019	Defending Operating Systems from Malicious Peripherals, Drexel University, Host: Dario Salvucci
Nov 2018	Defending Operating Systems from Malicious Peripherals, University of Illinois Urbana-Champaign, Host: Adam Bates
Nov 2018	Defending Operating Systems from Malicious Peripherals, Pennsylvania State University, Host: Patrick McDaniel

Awards

2023	Seed for Success Acorn Awards, Purdue University
2022	NSF CAREER Award, NSF
2021	Best Presentation Award, IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference
2020	Cyber Security Awareness Week (CSAW) Applied Research Award, (Top-10) Finalist
2020	Best Paper Award, USENIX Workshop on Offensive Technologies
2019	Student Travel Grant, IEEE Symposium on Security and Privacy
2019	Distinguished Poster Award, ACM Conference on Data and Application Security and Privacy
2018	Second Place Award, SEC Academic Conference (Cybersecurity) Student Poster Presentation
2017	Best Poster Award, FICS Annual Research Conference
2017	Gartner Group Info Tech Scholarship, University of Florida
2016	Best Poster Award, FICS Annual Research Conference
2015	ACSAC Student Conferenceship Award, ACSA
2015	CISE Travel Grant, University of Florida
2015	USENIX Security Student Grant, USENIX
2014	Gartner Group Graduate Fellowship, University of Florida
2011	Alcatel-Lucent R&D Well Done Award, Alcatel-Lucent
2009	Alcatel-Lucent R&D Innovation Award, Alcatel-Lucent
2009	Comprehensive Award of Excellent Graduate Scholarship, Ocean University of China
2009	Excellent Graduate Student Scholarship, Ocean University of China
2006	Full Graduate Scholarship, Ocean University of China
2004	Outstanding Student Cadre Scholarship, Qingdao Technological University

Teaching

2019.08– **Assistant Professor**, *Dept. of Computer Science, Purdue University*, West Lafayette, IN.
- CS59000-OSS Operating System Security (Fall 2019)
- CS52800 Network Security (Spring 2020, Spring 2023, Spring 2024)
- CS59100 CERIAS Security Seminar (Spring 2020)
- CS50300 Operating Systems (Fall 2020)
- CS42600 Computer Security (Spring 2021, Fall 2022)
- CS59200-TCC Trusted and Confidential Computing (Fall 2021)
- CS59200-PES Peripheral and Embedded Security (TBD)
- CS59200-HWS Hardware Security (Spring 2025)

2018.09–2019.07 **Guest Lecturer**, *Dept. of Computer & Information Science & Engineering, University of Florida*, Gainesville, FL.
- CNT 5410 Computer and Network Security (Fall 2018)
- CIS 5370 Computer and Information Security (Spring 2019)

2012.09–2013.06 **Graduate Teaching Fellow**, *Dept. of Computer & Information Science, University of Oregon*, Eugene, OR.
- CIS 122 Intro to Programming & Problem Solving Using Python (Fall 2012, Winter 2013, Lab)
- CIS 415 Operating Systems (Spring 2013, Lab)

Book Review

2013.12–Present **Technical Reviewer**, *Packt Publishing*, Birmingham, UK.
- Mastering Python Regular Expressions
- Python 3 Text Processing with NLTK 3 Cookbook
- Building Probabilistic Graphical Models with Python
- Mastering Probabilistic Graphical Models with Python
- Embedded Linux Projects Using Yocto Project Cookbook
- Yocto for Raspberry Pi
- LLVM Cookbook
- Building Programming Language Interpreters

Certifications

2011 AIX certification (AN10, AN12), IBM

2010 Project Management, ChoiZe Management Consulting

2010 Linux Debugging and Performance, JOHN BRYCE

2008 Sun Certified Java Programmer (SCJP), Sun Microsystems

2008 Solaris OS Architecture, Sun ERI & OpenTech

2008 Solaris 10 Admin Training, Sun Developer Network (China) & Unix-Center

2007 Sun Studio Hands-on Training with Unix/Linux Commands, Sun Developer Network (China) & Unix-Center

2004 National Computer Rank Examination (NCRE), Rank 2, C programming, China Education Ministry

1998 Microcomputer Operation Certification for Adult (DOS, Foxbase), Pute Computer Training Center of Qingdao Technological University

Media Coverage

ReversingLabs "Memory-safe languages and security by design: Key insights, lessons learned", https://www.reversinglabs.com/blog/memory-safe-languages-and-secure-by-design-key-insights-and-lessons-learned

CSO "Google offers free access to fuzzing framework", https://www.csoonline.com/article/1303540/google-offers-free-access-to-fuzzing-framework.html

Slashdot "Billions of Devices Vulnerable To New 'BLESA' Bluetooth Spoofing Attack", https://it.slashdot.org/story/20/09/16/220211/billions-of-devices-vulnerable-to-new-blesa-bluetooth-spoofing-attack

ZDNet "Billions of devices vulnerable to new 'BLESA' Bluetooth security flaw", https://www.zdnet.com/article/billions-of-devices-vulnerable-to-new-blesa-bluetooth-security-flaw/

NetSec.news "Billions of Devices Vulnerable to 'BLESA' Bluetooth Spoofing Vulnerability", https://www.netsec.news/billions-of-devices-vulnerable-to-blesa-bluetooth-spoofing-vulnerability/

ThreatPost "Bluetooth Spoofing Bug Affects Billions of IoT Devices", https://threatpost.com/bluetooth-spoofing-bug-iot-devices/159291/

Tom's Guide "Billions of Android phones and smart devices open to attack – what to do now", https://www.tomsguide.com/news/blesa-bluetooth-attack

SysDVD "Billions of Bluetooth Devices Vulnerable to BLESA Attack – Hacker", http://sysdvd.com/billions-of-bluetooth-devices-vulnerable-to-blesa-attack-hacker/

TechRadar "Critical Bluetooth security vulnerability could affect billions of devices worldwide", https://www.techradar.com/news/critical-bluetooth-security-vulnerability-could-affect-billions-of-devices-worldwide

International Business Times "What Is BLESA? Hackers Can Potentially Target Billions of Devices with Bluetooth Security Flaw", https://www.ibtimes.sg/what-blesa-hackers-can-potentially-target-billions-devices-bluetooth-security-flaw-51582

Silicon Angle "Vulnerability in the Bluetooth software stack opens the door to hackers", https://siliconangle.com/2020/09/16/vulnerability-bluetooth-software-stack-opens-door-hackers/

Sensors Tech Forum "Bluetooth Low Energy Spoofing Attack Endangers Billions of Devices", https://sensorstechforum.com/blesa-attack-endangers-billions-devices/

How To Fix "Experts discovered BLESA attack, to which are vulnerable billions of Bluetooth devices", https://howtofix.guide/experts-discovered-blesa-attack-to-which-are-vulnerable-bluetooth-devices/

Google News Post "Critical Bluetooth safety vulnerability may just have an effect on billions of gadgets international", http://googlenewspost.com/2020/09/16/critical-bluetooth-security-vulnerability-could-affect-billions-of-devices-worldwide/

Cyware "Cyware Daily Threat Intelligence, September 16, 2020", https://cyware.com/daily-threat-briefing/cyware-daily-threat-intelligence-september-16-2020-bc5d

Threats Hub "Billions of devices vulnerable to new 'BLESA' Bluetooth security flaw", https://www.threatshub.org/blog/billions-of-devices-vulnerable-to-new-blesa-bluetooth-security-flaw/

Editorials 360 "Billions of Units Susceptible To New 'BLESA' Bluetooth Spoofing Assault", https://www.editorials360.com/2020/09/17/billions-of-units-susceptible-to-new-blesa-bluetooth-spoofing-assault/

Sec News "BLESA: billions of devices vulnerable to Bluetooth security flaw", https://en.secnews.gr/267536/bluetooth-flash/

Remark Board "Billions of devices vulnerable to new 'BLESA' Bluetooth security flaw", https://remarkboard.com/m/researchers-unveil-a-bluetooth-le-attack-impacting-billions/1eztwiylfko6v

Security Boulevard "Bluetooth Reconnection Flaw Could Lead to Spoofing Attacks", https://securityboulevard.com/2020/07/bluetooth-reconnection-flaw-could-lead-to-spoofing-attacks/

ESET "ESET discovers Attor, a spy platform with curious GSM fingerprinting", https://www.welivesecurity.com/2019/10/10/eset-discovers-attor-spy-platform/

Firmware Security "USB Fuzzing: A USB Perspective", https://firmwaresecurity.com/2019/07/20/usb-fuzzing-a-usb-perspective/

Hacker News "USB Fuzzing: A USB Perspective", https://news.ycombinator.com/item?id=20478548

LWN.net "Revenge of the modems", https://lwn.net/Articles/766766/

Wired "Exploiting Decades-Old Telephone Tech to Break into Android Devices", https://www.wired.com/story/at-commands-android-vulnerability/

Threatpost "AT Command Hitch Leaves Android Phones Open to Attack", https://threatpost.com/at-command-hitch-leaves-android-phones-open-to-attack/136938/

UF News "Smartphone security risk compared to 'having a ghost user on your phone'", http://news.ufl.edu/articles/2018/08/smartphone-security-risk-compared-to-having-a-ghost-user-on-your-phone.php

independent florida alligator "What the hack: UF research reveals smartphones can be hacked via USB", https://www.alligator.org/news/what-the-hack-uf-research-reveals-smartphones-can-be-hacked/article_4480693e-aced-11e8-b68e-675760f71388.html

Bleeping Computer "Smartphones From 11 OEMs Vulnerable to Attacks via Hidden AT Commands", https://www.bleepingcomputer.com/news/security/smartphones-from-11-oems-vulnerable-to-attacks-via-hidden-at-commands/

How-To Geek "How to Protect Yourself From Public USB Charging Ports", https://www.howtogeek.com/364032/how-to-protect-yourself-from-public-usb-charging-ports/

Slashdot "Smartphones from 11 OEMs, Including Google, Samsung, HTC, Lenovo and Sony, Vulnerable to Attacks Via Hidden AT Commands", https://mobile.slashdot.org/story/18/08/26/1910246/smartphones-from-11-oems-including-google-samsung-htc-lenovo-and-sony-vulnerable-to-attacks-via-hidden-at-commands

Hacker News "ATtention Spanned: Comprehensive Android Vulnerability Analysis of AT Commands", https://news.ycombinator.com/item?id=17837035

Security Affairs "Android mobile devices from 11 vendors are exposed to AT Commands attacks", https://securityaffairs.co/wordpress/75683/hacking/at-commands-attacks-android.html

Fudzilla "Android at the mercy of AT Commands", https://www.fudzilla.com/news/mobile/47037-android-at-the-mercy-of-at-commands

Tech Worm "Android smartphones can be hacked with AT commands attacks", https://www.techworm.net/2018/08/android-smartphones-hacked-at-commands-attacks.html

Fossbytes "How These Android Smartphone Can Be Hacked With Simple AT commands", https://fossbytes.com/android-smartphone-can-be-hacked-with-at-commands/

Kim Komando Show "Modern smartphones vulnerable to old-school attack", https://www.komando.com/happening-now/483269/modern-smartphones-vulnerable-to-old-school-attack

Hacker Combat "Open AT Commands: a Huge Loophole Exploit in Android Revealed", https://hackercombat.com/open-at-commands-a-huge-loophole-exploit-in-android-revealed/

SecurePoint "Vulnerability Found in Major Manufacturers of Android Phones", https://www.securepointtech.com/2018/09/07/vulnerability-found-in-major-manufacturers-of-android-phones/

Hybrid Techcar "Smartphones are vulnerable to hacking commands for ancient modems", https://hybridtechcar.com/2018/08/28/smartphones-are-vulnerable-to-hacking-commands-for-ancient-modems/

Android Community "New security risk for smartphones brings you a "ghost user"", https://androidcommunity.com/new-security-risk-for-smartphones-brings-you-a-ghost-user-20180827/

SANS "AT Commands", https://isc.sans.edu/podcastdetail.html?id=6140

golem.de "Android-Smartphones durch Modem-Befehle verwundbar", https://www.golem.de/news/at-commands-android-smartphones-durch-modem-befehle-verwundbar-1808-136205.html

Tproger "11 manufacturers of Android smartphones have discovered a vulnerability to AT-commands", https://tproger.ru/news/at-commands-deface-smartphones/

habr "Attackers can get full remote access to the Android device through a public USB charging port", https://habr.com/company/crossover/blog/421295/

Niebezpiecznik "Miliony smartfonów można zhackować ukrytymi komendami AT", https://niebezpiecznik.pl/post/miliony-smartfonow-mozna-zhackowac-ukrytymi-komendami-at/

Trails of Bits "Binary Analysis: Identifying bugs in binary-only USB firmware", https://www.trailofbits.com/expertise/binary-analysis/

Helpnetsecurity "USBFILTER: Packet-level firewall for blocking USB-based threats", https://www.helpnetsecurity.com/2016/08/12/usbfilter-blocking-threats/

ePlace Solutions "USB Related Cyber Attacks and How to Defend Against Them", https://blog.eplaceinc.com/cyber/2016/09/08/usb-devices-exposing-organizations/

BankInfo Security "A New Way to Mitigate USB Risks", https://www.bankinfosecurity.com/make-usb-great-again-a-9350

RedesZone "USBfilter, un concepto de firewall para los puertos USB", https://www.redeszone.net/2016/08/16/usbfilter-concepto-firewall-los-puertos-usb/

Hacker News "No one, not even the Secret Service, should randomly plug in a strange USB stick", https://news.ycombinator.com/item?id=19609239

Serman "La revolución USB contra los malware", https://serman.com/blog-recuperacion-datos/la-revolucion-usb-contra-los-malware/

Students

Ph.D. Students Muqi Zou (CS, Fall 2020 -), Xiaolong Wu (ECE, Fall 2020 -), Jiwon Kim (CS, Fall 2020 -), Zheng Zhong (CS, Spring 2021 -), Sungwoo Kim (CS, Fall 2021 -, co-advised with Prof. Dongyan Xu), Gisu Yeo (CS, Fall 2022 -), Han Gao (CS, Spring 2023 -), Junpeng Wan (CS, Summer 2023 -), Rob Sammelson (CS, Spring 2024 -, co-advised with Dr. Rick Kennell)

Master Students Mukhilan Pari (MS, CS, Spring 2024 -)

Undergrad Students Priyam Gupta (CS, Spring 2024 -)

Committees Jianliang Wu (Ph.D., Fall 2019 - Summer 2023), Le Yu (Ph.D., Fall 2019 -), Rohit Bhatia (Ph.D., Fall 2019 - Spring 2020), Imtiaz Karim (Ph.D., Fall 2020 - Summer 2023), Reham Aburas (MS/Ph.D., Fall 2020 -), Hyungsub Kim (Ph.D., Fall 2020 - Fall 2023), Ruoyu Wu (Ph.D., Fall 2020 - Summer 2024), Arushi Arora (Ph.D., Spring 2022 - Spring 2024), Michael Reeves (MS, Fall 2020 - Spring 2021), Yiqing Zhu (MS, Spring 2022 -), Khaled Serag (Ph.D., Spring 2022 - Fall 2023), Hongwei Wu (Ph.D., Fall 2022 -), Rowan Hart (MS, Fall 2022), Mirza Masfiqur Rahman (Ph.D., Fall 2023 -), Muhammad Ibrahim (Ph.D., Spring 2023 -), Han Dai (Ph.D., Fall 2023 -), Syed Ghazanfar Abbas (Ph.D., Fall 2023 -), Cheng-Yun Yang (Ph.D., Fall 2023 -), Zeyu Lei (Ph.D., Spring 2024 -)

Ph.D. Alumni Arslan Khan (Ph.D., CS, Fall 2019 - Fall 2023, co-advised with Prof. Dongyan Xu, Assistant Professor, Department of Computer Science and Engineering, Pennsylvania State University)

Kyungtae Kim (Ph.D., CS, Fall 2019 - Fall 2022, co-advised with Prof. Byoungyoung Lee, Assistant Professor, Department of Computer Science, Dartmouth College)

Taegyu Kim (Ph.D., ECE, Fall 2019 - Spring 2021, co-advised with Prof. Dongyan Xu, Assistant Professor, College of Information Science and Technology, Pennsylvania State University)

Hui Peng (Ph.D., CS, Fall 2020 - Spring 2021, co-advised with Prof. Mathias Payer, Google)

Alumni Dikaimin Simon (Ph.D. student, CS, Spring 2021 - Fall 2022), Ertza Warraich (Ph.D. student, CS, Spring 2020 - Summer 2021), Benjamin Nwachukwu (Master student, CS, Fall 2019 - Spring 2020), Arushi Arora (Master student, CS, Summer 2020), Steven Dellamore (Undergrad, CS, Fall 2019), Mark Mikhail (Master student, CS, Fall 2020 - Spring 2021), Seunghyun Yeo (Fall 2021 – Spring 2022), Sai Raj Karra (Undergrad, CS, Spring 2022), Jenny Mendez (Undergrad, UC Berkeley, SROP'22), Jazlyn Ilmani (Undergrad, UMBC, SROP'22), Jack Xiang (Undergrad, CS, Spring 2023), Joseph Hsu (Undergrad, CS, Summer 2023 - Spring 2024)

Links

My web	https://davejingtian.org
My code	https://github.com/daveti
AT command	https://atcommands.org/
Provenance	https://linuxprovenance.org/
FW analysis	https://firmware-analysis.org/
OS Sec	https://ossec.home.blog
OS	https://os1.home.blog
Network Sec	https://netsec.travel.blog
PurSec Lab	https://pursec.cs.purdue.edu
Peri Sec	https://perisec.org