DANFENG (DAPHNE) YAO

Professor of Computer Science
Elizabeth and James Turner Fellow and CACI Fellow
IEEE Fellow

danfeng@vt.edu
`https://yaogroup.cs.vt.edu/index.html`

RESEARCH INTERESTS

My goal is to develop deployable and translational solutions for challenging decision-making problems, including data-driven precision medicine and system and software security, with a shared focus on ensuring correctness, enhancing trustworthiness and fairness, and discovering new insights.

EDUCATION

Ph.D., Computer Science, **Brown University**, Providence, RI — 2007
Thesis: *Privacy-aware Authentication and Authorization in Trust Management*
Advisor: *Roberto Tamassia*, Plastech Professor of Computer Science.

M.S., Computer Science, **Indiana University**, Bloomington, IN — 2002

M.A., Chemistry, **Princeton University**, Princeton, NJ — 2000

B.S., Chemistry, **Peking University**, Beijing, China — 1998

EMPLOYMENT

Department of Computer Science, Virginia Tech, Blacksburg VA
Professor — Jun. 2019 – Present
Elizabeth and James E. Turner Jr. '56 Faculty Fellow and CACI Faculty Fellow

Sanghani Center for Artificial Intelligence and Data Analytics — Jan. 2023 – Present
Affiliated Member

Mayo Clinic, Rochester MN — Sep. 2023 – Present
Research Collaborator

Department of Computer Science, Virginia Tech, Blacksburg VA — Jun. 2014 – Jun. 2019
Associate Professor

Department of Computer Science and Engineering, — Jan. 2016 – Jul. 2016
University of California, San Diego
Visiting Scholar

Department of Computer Science, Virginia Tech, Blacksburg VA — Jan. 2010 – May 2014
Assistant Professor

Department of Computer Science, Rutgers University, New Brunswick, NJ — Jan. 2008 – Dec. 2009
Assistant Professor

Department of Computer Science, Brown University — Aug. 2002 – Dec. 2007
Research assistant (with Roberto Tamassia, Plastech Professor)

CERIAS, Purdue University, West Lafayette IN — Sep. 2006 – Dec. 2007
Visiting scholar (with Professor Elisa Bertino and Mikhail J. Atallah)

HP Systems Security Lab, Princeton, NJ — May 2006 – Aug. 2006
Research intern (with Dr. Stuart Haber)

IAM Technology Inc., Providence, RI — Apr. 2005 – May. 2007
Consultant (with David Croston, CEO)

Center of Genomics and Bioinformatics, Indiana University, Bloomington — May 2001 - Aug. 2002
Research assistant (with Dr. Donald Gilbert)

Department of Chemistry, Princeton University — Aug. 1998 - Dec. 2000

Research assistant (with Professor Daniel Kahne)

HONORS AND AWARDS

Dean's List of Teaching Excellence for 2023-2024, College of Engineering	2024
Nominated for National Academy of Inventors Senior Member	2024
IEEE Fellow	2022
For contributions to enterprise data security and high-precision vulnerability screening	
Dean's Award for Research Excellence, VT College of Engineering	May 2022
Inspiring Innovator Award, Virginia Tech	Apr. 2022
ACM CODASPY Lasting Research Award	Apr. 2021
For pioneering research contributions in enterprise data exposure detection, high-precision vulnerability screening, and anomaly detection	
ACM Distinguished Member for Outstanding Scientific Contributions to Computing	Nov. 2018
Top downloaded article for WIREs Data Mining and Knowledge Discovery in 2019, 2021, and 2022	
A top 25 most downloaded article of the IEEE Signal Processing Society in 2016	
IEEE Excellence in Service Award by Computer Society's TC on Security & Privacy	Oct. 2018
Dean's Faculty Fellow, Virginia Tech CoE	Dec. 2017 – 2022
Elizabeth and James E. Turner Jr. '56 Faculty Fellowship, Virginia Tech CoE	2016 – Present
CACI Faculty Fellow	2014 – Present
Young Investigator Award, Army Research Office (ARO)	Aug. 2014
Outstanding New Assistant Professor Award, Virginia Tech College of Engineering	Feb. 2012
CAREER Award, National Science Foundation	Jan. 2010
Best Paper Awards	*ICNP* '12, *CollaborateCom* '10, *ICICS* '06
Best Poster Awards	*CCI Student Researcher Showcase '23*, *ACM CODASPY* '15, *WOCC* '09
Award for Technological Innovation, Brown University	Apr. 2006
University Fellowship, Brown University	Sep. 2002
Graduate with the Highest Honors, Peking University	Jul. 1998
SONY, IEC and Outstanding Student Fellowships, Peking University	1996-1995

PATENTS

1. Stuart Haber, William Horne, Tomas Sander, and Danfeng Yao. Integrity Verification of Pseudonymized Documents. Sep. 2012. U.S. Patent No. 8,266,439. **(Cited by many data security and blockchain patents from Amazon, Intel, Fujitsu, Salesforce, Texas Instruments.)**

2. Danfeng Yao, Deian Stefan, and Chehai Wu. Systems and Methods for Malware Detection. U.S. Patent No. 8,763,127. Jun. 2014. **(Highly cited, including by cybersecurity patents from FireEye, Qualcomm, Cisco, Microsoft, IBM, Boeing, SAP, Palo Alto Networks, and Bank of America.)**

3. Danfeng Yao and Hao Zhang. Detection of Stealthy Malware Activities with Traffic Causality and Scalable Triggering Relation Discovery. Continuation-in-Part (CIP) Patent. U.S. Patent No. 9,888,030. Feb. 2018. **(Cited by patents from Symantec, IBM, and Nippon Japan.)**

4. Danfeng Yao, Salman Ahmed, and Ya Xiao. Probabilistic Evidence-Based Insider Threat Detection and Reasoning. US patent filed No. PCT/US21/37240. June 14, 2021.

5. Danfeng Yao and Wenjia Song. Systems and Methods for Continuous Cybersecurity Monitoring to Detect Advanced Persistent Threats. Provisional patent being filed. Aug. 2024.

SELECT KEYNOTES AND INVITED TALKS

1. Deployable Security Beyond Detection Accuracy: Gaps, Successes, and Opportunities. EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (SmartSP 2024). New Orleans, LA. Nov. 2024. *Keynote forthcoming*

2. Measurable and Deployable Security: Gaps, Successes, and Opportunities. DC, Maryland, Virginia Security Day. Charlottesville, VA. Mar. 2024. **Keynote.**
3. One-model-predicts-all No More: Training Specialized Models for Minority Patient Groups. *Mayo Clinic Annual Individualizing Medicine Conference.* Ponte Vedra Beach, FL. 2023.
4. Anomaly Detection for System Security: History, Capabilities, and Research Opportunities. NIO Academy. 2023. **Distinguished Lecture Series** (Virtual).
5. Measurable and Deployable Security: Gaps, Successes, and Opportunities. ACNS Workshop on Secure Cryptographic Implementation (SCI). Kyoto, Japan. Jun. 2023. **Keynote.**
6. One-model-predicts-all No More: Training Specialized Models for Minority Patient Groups. Integrated Translational Health Research Institute of Virginia (iTHRIV) Webinar. Mar. 2023.
7. Data Breach, Pegasus, and Ransomware: Making Sense of Cybersecurity Risks. Department of Computer Science, Indiana University Bloomington. Apr. 2022. **Distinguished Lecture.**
8. Data Breaches and Multiple Points to Stop Them. University of Waterloo Cybersecurity and Privacy Institute. Public outreach talk series. Dec. 2021. **Invited talk.**
9. Measurable and Deployable Security: Gaps, Successes, and Opportunities. ACM Conference on Data and Application Security and Privacy (CODASPY). Apr. 2021. **Keynote.**
10. To Be Software Developers' Friends: Tool Development for Cryptographic Coding. International Conference on Information Security and Cryptology (INSCRYPT). Dec. 2020. **Keynote.**
11. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. PrivacyCon 2020. Federal Trade Commission (FTC). July, 2020.
12. Defense in Depth for CPS Security: What Does It Take and How Can Researchers Help? IEEE Workshop on Cyber-Physical Systems Security (CPS-Sec), co-located with IEEE CNS. July 2020. **Keynote.**
13. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. Financial Inclusion Global Initiative (FIGI) Security, Infrastructure and Trust Working Group e-Meeting (affiliated with the World Bank Group and Gates Foundation). April 2020.
14. Data Breaches and Multiple Points to Stop Them. Brown University, Executive Masters Program in Cybersecurity (EMCS). Providence, RI. Oct. 2019. **Keynote.**
15. Data Breaches and Multiple Points to Stop Them. IEEE Signal Processing Society Webinar. Sept. 2019.
16. Measurable Security in Software and Systems. ACM Turing Celebration SIGSAC China. Chengdu, China. May 2019. **Keynote**.
17. Data Breach and Multiple Points to Stop It. ACM Symposium on Access Control Models and Technologies (SACMAT). Indianapolis, IN. **Keynote**. Jun. 2018.
18. Democratize Anomaly Detection Technologies: Challenges, Advances, and Opportunities. Cyber Security & Information Systems Information Analysis Center (CSIAC). **Invited Webinar.** May 2017.
19. Democratize Anomaly Detection Technologies: Challenges, Advances, and Opportunities. INRIA Rennes, France. Apr. 2017. **Invited Talk.**
20. Democratize Anomaly Detection Technologies: Challenges, Advances, and Opportunities. **Departmental Seminar.** University of Virginia, Department of Computer Science. Apr. 2017.

21. Cloud Data Analytics for Security: Applications, Challenges, and Opportunities. **Keynote Speech** at ASIACCS Security in Cloud Computing (SCC) Workshop. Abu Dhabi, UAE. Apr. 2017.

TEACHING

Virginia Tech CS/ECE Departments

CS/ECE 5590 System and Software Security	Spring 2024, Spring 2022, Spring 2020, Spring 2017
CS/ECE 5984 System and Application Security	Spring 2015
CS5984 Theory and Practice of Web Security and Privacy.	Spring 2011

Note: I created and taught CS/ECE 5590 and its previous editions, the only graduate-level system and application security course at VT. In the most recent Spring '24 offering, 55 graduate students across CS and ECE departments enrolled and my teaching evaluation score is **5.6** out of 6.

CS/ECE 4264 Principles of Computer Security	Fall 2020, Fall 2015, 2014, 2013
CS4984 Introduction to Computer Security.	Fall 2012, 2011, 2010

Note: I created CS/ECE 4264, which is a core course of the popular College of Engineering's Cybersecurity minor. The course is now being offered each semester to 80-90 CS and ECE juniors/seniors.

Virginia Tech CS Department

CS6804 Advanced Topics in Intelligent Systems	Fall 2023
CS6804 AI Techniques for Cybersecurity Defenses	Spring 2021
CS5024 Ethics and Professionalism in Computer Science	Fall 2022, 2021

Note: I created most of the CS5024 course materials from scratch by incorporating many real-world examples intersecting technology and society and AI fairness research. The most recent Fall 2022 offering had 57 graduate students and my teaching evaluation score is **5.67** out of 6. CS5024 is a required graduate class.

CS6204 Cyber-physical Systems (CPS) Security	Spring 2019
CS6204 Program Anomaly Detection with Learning	Fall 2016
CS6204 Recent Advances in System and Application Security	Spring 2014
CS3114 Data Structures and Algorithms	Spring 2012
CS6204 Recent Advances in Cyber Security	Spring 2012
CS6204 Advanced Computer Security and Privacy	Spring 2010

Virginia Tech CS/PSCI/BIT Departments

CS/PSCI/BIT 2984 Foundations of Security Environments	Spring 2020 and 2018, Fall 2019 and 2018

Note: I was instrumental in creating and co-teaching this non-major undergraduate security course, part of minor programs in non-CS departments.

Rutgers University CS Department

CS673 Recent Advances in Computer Security	Fall 2009
CS672 Information Security	Fall 2008
CS352 Internet Technology	Spring 2008, Spring 2009
CS500:04 Light Seminar: Secure Information Sharing	Spring 2008

EXTERNAL FEDERAL/INDUSTRY GRANTS

Total External Grants: $13 million. Personal Share: $5.89 million.

1. National Science Foundation (**NSF**) SaTC program. SaTC: TTP: Small: Deployable Behavior-driven Crypto-ransomware Detection Enabled by Practical Logging Strategies. $600,000. 07/15/2024 - 06/30/2027. PI: Danfeng Yao.

2. National Science Foundation (**NSF**) SaTC program. Conference: 2024 Secure and Trustworthy Cyberspace PI Meeting. PI: Danfeng Yao. $50,000. 05/01/2024 - 04/30/2025.

3. National Science Foundation (**NSF**) SaTC program. SaTC: CORE: Small: Systematic Threat Characterization and Prevention in Open-Domain Dialog Systems. PI: Bimal Viswanath. Co-PI: Danfeng Yao. $600,000. 02/01/2023 - 01/31/2026. Personal share: $181,173.

4. Office of Naval Research (**ONR**). Soft Auditing on Trust for Detecting Clandestine Executions with Maximum Deployability. PI: Danfeng Yao, co-PI: Na Meng (VT) and Nathan Dautenhahn. $900,000. 01/01/2022 - 05/31/2025. Personal share: $570,000.

5. National Science Foundation (**NSF**) SaTC program. iMentor Workshop at the ACM CCS. $150,000. PI: Danfeng Yao. 01/01/2020 - 12/31/2023.

6. National Science Foundation (**NSF**) SaTC program. SaTC:TTP:Medium:Collaborative: Deployment-quality and Accessible Solutions for Cryptography Code Development. PI: Daphne Yao (VT), co-PIs: Barton Miller (UW-Madison) and Na Meng (VT). $1.2 million. 10/01/2019 – 08/31/2024. Personal share: $500,000.

7. National Science Foundation (**NSF**). Planning Grant: Engineering Research Center for Computer And Network RESIliency and Security for Transportation (CAN-RESIST). Daphne Yao is among the Co-PIs. $100K. 09/01/2019 – 08/31/2020.

8. Office of Naval Research (**ONR**). Data-driven Vulnerability Repair in Programs with a Cloud Analytics Architecture for Practical Deployment. $1.2 million. PI: Danfeng Yao, co-PI: Trent Jaeger (PSU) and Na Meng (VT). 07/01/2017 – 06/30/2020. Personal share: $612,838.

   Supplement to Support IEEE Secure Development Conference. $5,000 in 2020 and $5,000 in 2018.

9. National Science Foundation (**NSF**). SaTC: CORE: Small: Securing Web-to-Mobile Interface Through Characterization and Detection of Malicious Deep Links. $500,000. PI: Gang Wang, co-PI: Danfeng Yao. 09/01/2017 - 08/31/2020. Personal share: $235,000.

10. Defense Advanced Research Projects Agency (**DARPA**) CASE Program. Automatic Generation of Anti-Specifications from Exploits for Scalable Program Hardening. $400,000. PI: Danfeng Yao, co-PI: Gang Tan (PSU). 10/01/2017 – 09/30/2018. Personal share: $210,000.

11. National Science Foundation (**NSF**) CRISP program. CRISP Type 2: Collaborative Research: Towards Resilient Smart Cities. Walid Saad (PI) (VT ECE), Danfeng Yao is among the VT co-PIs. $1.1 million. Personal share: $206,347. Jan. 2016 - Dec. 2019.

12. NSF I/UCRC Security and Software Engineering Research Center (**S2ERC**). Event-driven Probabilistic Anomaly Detection for UAV Security. Danfeng Yao (PI). $40,000. 05/01/2016 - 04/30/2017.

13. National Science Foundation (**NSF**) CSR Program. CSR: Large: VarSys: Managing variability in high-performance computing systems. PI: Kirk Cameron (Virginia Tech). Danfeng Yao is among the co-PIs. $2.38 million. 09/01/2016 - 09/30/2020. Personal share: $390,000.

14. National Science Foundation (**NSF**) CBET Division. EAGER: Privacy-enhancing CrowdPCR for Early Epidemic Detection. $100,000. PIs: Danfeng Yao and Victor Ugaz at Texas A&M Chemical Engineering. Sep., 2016 – Aug., 2017. Personal share: $50,000.

15. Defense Advanced Research Projects Agency (**DARPA**). Detection of Malware Collusion with Static Dependence Analysis on Inter-App Communication. PI: Danfeng Yao, Co-PI: Barbara Ryder. $430,000. Personal share: $400,000. Mar. 2015 - May 2016.

16. Army Research Office Young Investigator Program (**ARO YIP**). Causality-Based Traffic Reasoning for Securing Large-Scale Networks. PI: Danfeng Yao. $150,000. Aug. 2014 - Aug. 2017.

17. NSF I/UCRC Security and Software Engineering Research Center (**S2ERC**). Cloud-based Screening of Massive Data for Security Leaks in Enterprise Environments. $40,000. PI: Danfeng Yao. Aug. 2014 - Jul. 2016.

18. Office of Naval Research (**ONR**). Real-Time Anomaly Detection and Quantitative Assurance for Securing Systems. PI: Danfeng Yao. $450,000. Jan. 2013 - Aug. 2016. Personal share: $450,000.

19. NSF I/UCRC Security and Software Engineering Research Center (**S2ERC**). Detection of Data Exfiltration in Enterprise Environments. $38,643. PI: Danfeng Yao. May 2013 - May 2014. Personal share: $38,643.

20. NSF I/UCRC Security and Software Engineering Research Center (**S2ERC**). Advanced Dependence Analysis for Android Malware Classification. $30,000. PI: Danfeng Yao. Co-PI: Barbara G. Ryder. Jul. 2013 - Jun. 2014. Personal share: $26,632.

21. NSF I/UCRC Security and Software Engineering Research Center (**S2ERC**). User-Centric Dependency Analysis in Programs for Identifying Malware. $40,000. PI: Danfeng Yao. Jan. 2012 - Dec. 2012. Personal share: $40,000.

22. Army Research Office (**ARO**). Exploring Personalized Security with Novel Learning Techniques for Host-Based Anomaly Detection. PI: Danfeng Yao. $50,000. May 2011 - April 2012. Personal share: $50,000.

23. National Science Foundation (**NSF**). Cyber Security Industry/University Cooperative Research Center. PI: T. Charles Clancy. Co-PIs: Danfeng Yao, Joseph Tront, Michael Hsiao, and Jung-Min Park. Aug. 2011 - Jul. 2017. Awarded amount: $973,500.

24. National Science Foundation (**NSF**) **CAREER** Program. CAREER: Human-Behavior Driven Malware Detection. PI: Danfeng Yao. $530,000. Feb. 2010 - Mar. 2016. Personal share: $530,000.

    REU Supplemental Fund. $16,000. PI: Danfeng Yao. $16,000. Apr. 2012 - Mar. 2013. Personal share: $16,000.

25. Department of Homeland Security (**DHS**). Center of Excellence for Command, Control, and Interoperability. PI: Fred Roberts. Danfeng Yao is among the Rutgers researchers. Aug. 2009 - Jul. 2015. Personal share: $40,000.

26. National Science Foundation (**NSF**). CT - ISG: ROME: Robust Measurement in Sensor Networks. PI: Yanyong Zhang. Co-PI: Danfeng Yao and Hui Xiong. $400,000. Sep. 2008 - Aug. 2011. Personal share: $133,000.

MAJOR PENDING PROPOSALS

- National Institutes of Health (**NIH**) NLM. Systematic Methods for Patient Deep Subtyping and Individualized Prognosis for Complex Diseases. Lead PI: Danfeng Yao. PI: Shulan Tian (Mayo). Co-I: Eric Klee (Mayo Clinic). *Pending, R01 proposal.* $1,530,745.
- Office of Naval Research (**ONR**). Mitigating Supply Chain Attacks Using Large Language Models. PI: Na Meng. Co-PI: Danfeng Yao. *Pending.* $726,476.

GRANTS FROM VA

1. Commonwealth Cyber Initiative (CCI). Southwest Virginia Node. System-wide Measurement of Defense-in-depth Readiness of Medical CPS Devices. PI: Danfeng Yao. Co-PI: Homa Alemzadeh (UVa) and Bimal Viswanath (VT). $20,000. Jun. 2020 – Dec. 2020. Personal Share: $12,500.

2. Commonwealth Cyber Initiative (CCI). Southwest Virginia Node. Probabilistic and Evidence-based Insider Threat Reasoning and Detection for Critical Infrastructures. PI: Danfeng Yao. $20,000. Jun. 2020 – Dec. 2020.

3. Commonwealth Cyber Initiative (CCI). Enhancing the Privacy and Reliability of Massive-scale Bluetooth Low Energy Contact Tracing. $200,000. PI: Danfeng Yao, co-PI: Tijay Chung (VT) and Carol Fung (VCU). 01/01/2021 - 12/31/2021. Personal share: $140,000.

4. Commonwealth Cyber Initiative (CCI). High-precision Insider Threat Detection and Reasoning with Probabilistic Evidence. PI: Danfeng (Daphne) Yao. $50,000. 06/15/2021 - 06/14/2022.

5. Commonwealth Cyber Initiative (CCI). Market Research for No-train AI in Enterprise Defense-in-depth Applications. PI: Danfeng Yao. $30,000. 04/01/2022 – 12/31/2022.

6. Commonwealth Cyber Initiative (CCI). Scalable Continuous Monitoring Solutions for Enterprise Security. PI: Danfeng Yao. $50,000. 03/01/2023 – 02/29/2024.

7. Commonwealth Cyber Initiative (CCI). An Empirical Evaluation of Large Language Models (LLMs) in Generating Security Tests to Mitigate Supply Chain Attacks. PI: Na Meng. Co-PI: Danfeng Yao. $50,000. 01/01/2024 - 12/31/2024. Personal share: $10,000.

8. 4-VA Collaborative Program. Enforcing Safe Product Software Updates with Proactive Runtime Checking. PI: Chang Lou (University of Virginia). Co-PI: Danfeng Yao. $30,000. Personal share: $5,000.

9. Commonwealth Cyber Initiative (CCI). Addressing Software Defects and Security Vulnerabilities in Smart Home Automation. PI: Xinghua Gao. Co-PI: Na Meng and Danfeng Yao. $35,000. 08/01/2024 - 08/31/2025. Personal share: $5,000.

SELECT MEDIA REPORTS

1. The Scientist, ScienMag, MedicalXpress, and VT News on our spatial profiling approach to map out discoveries for future brain research (work in *Cell Reports Methods* 2024 led by Dr. Chang Lu in VT Chemical Engineering).

2. NPR With Good Reason and VT News on our AI fairness technique and its significant lifesaving implications (work in *Communications Medicine* 2022 led by Yao).

3. WSLS News and VT News on the privacy guarantees of contact tracing apps (work in *IEEE Computer* 2022 led by Yao).

4. Communications of the ACM (Jul. 2020) featured CryptoGuard (work in *ACM CCS '19, IEEE SecDev '19, IEEE TSE '22, ACM DTRAP '22, IEEE S&P '23* led by Yao).

   `https://cacm.acm.org/news/246385-a-tool-for-hardening-java-crypto/fulltext`

5. Slashdot, UK's Register, Linux.com and Helpnet Security on our Java secure coding research (work in *ICSE* 2018 led by Dr. Meng Na).

6. Wiley's Advanced Science News featured a review article on enterprise data breaches (in *WIREs Data Mining and Knowledge Discovery* 2017, led by Yao). `http://www.advancedsciencenews.com/enterprise-data-breach-causes-challenges-prevention-future-directions/`

7. New Scientist, ACM Technews, and International Business Times on Android malware collusion (work in *ASIACCS* 2017 led by Yao).

8. Communications of the ACM, HPC Wire, and Government Security News on our program anomaly detection algorithms (work in *ACM CCS* 2015 led by Yao).

   `http://cacm.acm.org/news/196663-anomaly-detectors-catch-zero-day-hackers/fulltext`

9. Computer World, TMC Net, IT Weekly Newsletter on causality-based threat detection and receiving the 2014 ARO YIP Award.

10. Software Security Engineering Research Center (S2ERC), an NSF I/UCRC, highlighted our data-leak detection research in 2014 (work in *SecureComm 2012 and IEEE TIFS 2015* led by Yao).

11. NSF, HPC Wire, Examiner, Federal Computer Week on network traffic causality reasoning for detecting stealthy malware activities (work in *ACM ASIACCS* 2014 led by Yao).

12. International Business Times, Homeland Security News Wires, PHYSORG (United Kingdom) on our award-winning keystroke dynamic security work (in *CollaborateCom* 2010 led by Yao).

13. NSF news, ACM Technews, and many others on our activity-based authentication (work in *ACM CCS SafeConfig* 2009 led by Yao).

PUBLICATIONS

I am the lead author in most papers that have my student (indicated by *) as the first author, regardless of my position.

Google Scholar: `https://scholar.google.com/citations?user=_JLQTKwAAAAJ`
NCBI Bibliography: `https://www.ncbi.nlm.nih.gov/myncbi/1rKaDs5Qtp8Mil/bibliography/public/`
ORCID ID: 0000-0001-8969-2792

BOOK

1. Danfeng Yao, Xiaokui Shu*, Long Cheng*, and Salvatore J. Stolfo. Anomaly Detection as a Service: Challenges, Advances, and Opportunities. In *Synthesis Lectures on Information Security, Privacy, and Trust.* Editors: Elisa Bertino and Ravi Sandhu. Morgan & Claypool. Oct. 2017. `https://doi.org/10.2200/S00800ED1V01Y201709SPT022` **First book synthesizing multi-decade-long anomaly detection research for cybersecurity; downloaded 500 times.**

PEER-REVIEWED MAGAZINES

1. Danfeng (Daphne) Yao. Rebuttal How-to: Strategies, Tactics, and the Big Picture in Research. *Communications of the ACM.* 67(1). Jan. 2024. **High-impact article.**

   (Talk video: https://www.youtube.com/watch?v=5dBdXYr9ltw)

2. Salman Ahmed*, Ya Xiao*, Taejoong (Tijay) Chung, Carol Fung, Moti Yung, and Danfeng (Daphne) Yao. Privacy Guarantees of BLE Contact Tracing: A Case Study on COVIDWISE. *IEEE Computer.* Feb. 2022. **News Media Reports.**

3. Danfeng (Daphne) Yao, Sazzadur Rahaman, Ya Xiao*, Sharmin Afrose*, Miles Frantz*, Ke Tian, Na Meng, Cristina Cifuentes, Yang Zhao, Nicholas Allen, Nathan Keynes, Barton P. Miller, Elisa Heymann, Murat Kantarcioglu, and Fahad Shaon. Being the Developers' Friend: Our Experience Developing a High Precision Tool for Secure Coding. *IEEE Security & Privacy.* Mar. 2022.

4. Danfeng (Daphne) Yao. Depth and Persistence: What Researchers Need to Know About Impostor Syndrome. *Communications of the ACM.* 64(6). Jun. 2021. **High-impact article.** (Talk video: https://www.youtube.com/watch?v=JqFKv9Rg0k8)

JOURNALS

5. Zhengzhi Liu, Chengyu Deng, Zirui Zhou, Ya Xiao*, Shan Jiang, Bohan Zhu, Lynette B. Naler, Xiaoting Jia, Danfeng (Daphne) Yao, and Chang Lu. Epigenomic tomography for probing spatially-defined chromatin state in the brain. *Cell Reports Methods.* 4(3):100738. Mar. 2024. **Featured in The Scientist.**

6. Miles Frantz*, Ya Xiao*, Tanmoy Sarkar Pias*, Na Meng, and Danfeng (Daphne) Yao. Methods and Benchmark for Detecting Cryptographic API Misuses in Python. *IEEE Transactions on Software Engineering (TSE).* 50(5). May 2024.

7. Ya Xiao*, Wenjia Song*, Salman Ahmed*, Xinyang Ge, Bimal Viswanath, Na Meng, and Danfeng (Daphne) Yao. Measurement of Embedding Choices on Cryptographic API Completion Tasks. *ACM Transactions on Software Engineering and Methodology (TOSEM).* 33(3). Pages 1–30. 2024.

8. Ya Xiao*, Wenjia Song*, Jingyuan Qi*, Bimal Viswanath, Patrick McDaniel, and Danfeng (Daphne) Yao. Specializing Neural Networks for Cryptographic Code Completion Applications. *IEEE Transactions on Software Engineering (TSE).* Jul. 2023

9. Edward Jacobs, IV, Sabrina Campelo, Kenneth Aycock, Danfeng (Daphne) Yao, and Rafael V. Davalos. Spatiotemporal Estimations of Temperature Rise During Electroporation Treatments using a Deep Neural Network. *Computers in Biology and Medicine.* 2023. 10.1016/j.compbiomed.2023.107019

10. Sharmin Afrose*+, Wenjia Song*+, Charles B. Nemeroff, Chang Lu, and Danfeng (Daphne) Yao. Subpopulation-specific Machine Learning Prognosis for Underrepresented Patients with Double Prioritized Bias Correction. *Communications Medicine.* 2022. $^{+}$: equal contributions. **Featured in NPR News.**

11. Ya Xiao*, Yang Zhao, Nicholas Allen, Nathan Keynes, Danfeng (Daphne) Yao, and Cristina Cifuentes. Industrial Experience of Finding Cryptographic Vulnerabilities in Large-scale Codebases. *ACM Digital Threats: Research and Practice (DTRAP).* Mar. 2022. **Featured in Communications of the ACM.**

12. Sharmin Afrose*, Ya Xiao*, Sazzadur Rahaman, Barton P. Miller, and Danfeng (Daphne) Yao. Evaluation of Static Vulnerability Detection Tools with Java Cryptographic API Benchmarks. *IEEE Transactions on Software Engineering (TSE).* Feb. 2022. **Benchmarks used across the world.**

13. Ying Zhang, Mahir Kabir, Ya Xiao*, Danfeng (Daphne) Yao, and Na Meng. Automatic Detection of Java Cryptographic API Misuses: Are We There Yet? *IEEE Transactions on Software Engineering (TSE).* Feb. 2022.

14. Yuan Luo*, Ya Xiao*, Long Cheng, Guojun Peng, and Danfeng (Daphne) Yao. Deep Learning-Based Anomaly Detection in Cyber-Physical Systems: Progress and Opportunities. *ACM Computing Surveys.* 2021. (Impact Factor: 10.3)

15. Sazzadur Rahaman*, Haipeng Cai*, Omar Chowdhury, and Danfeng (Daphne) Yao. From Theory to Code: Identifying Logical Flaws in Cryptographic Implementations in C/C++. *IEEE Transactions on Dependable and Secure Computing (TDSC).* 2021. (Impact factor: 6.40)

16. Long Cheng*, Salman Ahmed*, Hans Liljestrand, Thomas Nyman, Haipeng Cai, Trent Jaeger, N. Asokan, and Danfeng (Daphne) Yao. Exploitation Techniques for Data-Oriented Attacks with Existing and Potential Defense Approaches. In *the ACM Transactions on Privacy and Security (TOPS)*, April 2021.

17. Yuan Luo*, Long Cheng, Hongxin Hu, Guojun Peng, and Danfeng (Daphne) Yao. Context-rich Privacy Leakage Analysis through Inferring Apps in Smart Home IoT. *IEEE Internet of Things Journal.* 8(4). 2736-2750. Feb. 2021. (Impact factor: 11.70)

18. Long Cheng*, Ke Tian*, Danfeng Yao, Lui Sha, and Raheem Beyah. Checking is Believing: Event-aware Program Anomaly Detection in Cyber-physical Systems. *IEEE Transactions on Dependable and Secure Computing (TDSC).* 18(2). 2021. (Impact factor: 6.40)

19. Ke Tian*, Gang Tan, Barbara G. Ryder, and Danfeng (Daphne) Yao. Prioritizing Data Flows and Sinks for App Security Transformation. *Computers & Security.* Feb. 2020. (Impact factor: 3.58)

20. Ke Tian*, Danfeng Yao, Barbara Ryder, Gang Tan, and Guojun Peng. Code-heterogeneity Aware Detection for Repackaged Malware. *IEEE Transactions on Dependable and Secure Computing (TDSC).* 17(1), Jan./Feb. 2020. (Impact factor: 6.40)

21. Karim Elish*, Haipeng Cai*, Daniel Barton*, Danfeng Yao, and Barbara Ryder. Identifying Mobile Inter-App Communication Risks. *IEEE Transactions on Mobile Computing (TMC).* 19(1). 90-102. Jan. 2020. (Impact factor: 4.47)

22. Haipeng Cai*, Na Meng, Barbara Ryder, and Danfeng Yao. DroidCat: Effective Android Malware Detection and Categorization via App-Level Profiling. *IEEE Transactions on Information Forensics & Security (TIFS).* 14(6). 1455-1470. Jun. 2019. (Impact factor: 5.82)

23. Xiaokui Shu*, Danfeng Yao, Naren Ramakrishnan, and Trent Jaeger Long-Span Program Behavior Modeling and Attack Detection. *ACM Transactions on Privacy and Security (TOPS).* 20(4). Oct. 2017.

24. Long Cheng*, Fang Liu*, and Danfeng Yao. Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions *WIREs Data Mining and Knowledge Discovery (DMKD).* 7(5). Wiley. Sep/Oct, 2017. **Invited review paper, featured by Wiley's Advanced Science News.** (Impact factor: 1.94) **No. 1 most downloaded in 2019; No. 3 most downloaded in 2021 and 2022 for WIREs DMKD.** `http://wires.wiley.com/WileyCDA/WiresCollection/id-49.html`

25. Hao Zhang*, Danfeng Yao, Naren Ramakrishnan, and Zhibin Zhang. Causality Reasoning about Network Events for Detecting Stealthy Malware Activities. *Computers & Security.* 58: 180-198. Elsevier. 2016. **Patented technology.** (Impact factor: 2.65)

26. Hussain Almohri*, Layne T. Watson, Danfeng Yao, and Xinming Ou. Security Optimization of Dynamic Networks with Probabilistic Graph Modeling and Linear Programming. *IEEE Transactions on Secure and Dependable Computing (TDSC).* 13(4): 474-487. 2016. (Impact factor: 6.40)

27. Xiaokui Shu*, Jing Zhang, Danfeng Yao, and Wu-Chun Feng. Fast Detection of Transformed Data Leaks. *IEEE Transactions on Information Forensics & Security (TIFS).* 11(3): 528-542. 2016. (Impact factor: 5.82; **article viewed 11K+ times**.) Shorter version received **Best Poster Award at ACM CODASPY '15.**

28. Xiaokui Shu*, Danfeng Yao, and Elisa Bertino. Privacy-Preserving Detection of Sensitive Data Exposure with Applications to Data-Leak Detection as a Service. *IEEE Transactions on Information Forensics & Security (TIFS).* 10(5). 1092-1103. May 2015. (Impact factor: 5.82) **Top 25 most downloaded article of the IEEE Signal Processing Society in 2016; viewed 18K+ times.**

29. Karim O. Elish*, Xiaokui Shu*, Danfeng Yao, Barbara Ryder, and Xuxian Jiang. Dependency-Based Static Program Profiling for Android Malware Detection. *Computers & Security.* 49, 255–273. March, 2015. (Impact factor: 2.65)

30. Hussain Almohri*, Danfeng Yao, and Dennis Kafura. Process Authentication for High System Assurance. *IEEE Transactions on Dependable and Secure Computing (TDSC).* 11(2), 168-180. March/April 2014. (Impact factor: 6.40)

31. Kui Xu*, Patrick Butler*, Sudip Saha*, and Danfeng Yao. DNS for Massive-Scale Command and Control. *IEEE Transactions on Dependable and Secure Computing (TDSC).* 10(3), 143-153. May/June 2013. (Impact factor: 6.40)

32. Kui Xu*, Huijun Xiong*, Chehai Wu*, Deian Stefan*, and Danfeng Yao. Data-Provenance Verification for Secure Hosts. *IEEE Transactions on Dependable and Secure Computing (TDSC).* 9(2), 173-183. March/April 2012. **Patented technology.** (Impact factor: 6.40)

33. Deian Stefan*, Xiaokui Shu*, and Danfeng Yao. Robustness of Keystroke-Dynamics Based Biometrics Against Synthetic Forgeries. *Computers & Security.* 31(1), 109-121. 2012. Elsevier. (Impact factor: 2.65)

34. Jerry Rick Ramstetter*, Yaling Yang, and Danfeng Yao. Applications and Security of Next-Generation User-Centric Wireless Systems. *Future Internet, Special Issue on Security for Next Generation Wireless and Decentralized Systems.* Editors: Ralf Steinmetz and André Koenig. Jun. 2010. **Invited paper.**

35. Qian Yang*, Danfeng Yao, Kaitlyn Muller, and James Garnett. Using a Trust Inference Model for Flexible and Controlled Information Sharing During Crises. *Journal of Contingencies and Crisis Management.* 18(4), 231-241. Dec. 2010. Wiley-Blackwell. (Impact factor: 1.07)

36. Roberto Tamassia, Danfeng Yao, and William H. Winsborough. Independently-Verifiable Decentralized Role-Based Delegation. *IEEE Transactions on Systems, Man, and Cybernetics, Part A.* 40(6), 1206-1219. Nov. 2010. (Impact factor: 5.13)

37. Danfeng Yao and Roberto Tamassia. Compact and Anonymous Role-Based Authorization Chain. *ACM Transactions on Information and System Security (TISSEC).* 12(3). 1-27. 2009.

38. Michael T. Goodrich, Roberto Tamassia, and Danfeng Yao. Notarized Federated Identity Management for Increased Trust in Web Services. *Journal of Computer Security*, 16(4): 399-418. 2008.

39. Danfeng Yao, Keith Frikken, Mike Atallah, Roberto Tamassia. Private Information: To Reveal or Not to Reveal. *ACM Transactions on Information and System Security (TISSEC).* 12(1). 1-27. Feb. 2008. **Short version received Best Student Paper Award at ICICS '06.**

40. Yunhua Koglin, Danfeng Yao, and Elisa Bertino. Secure Content Distribution by Parallel Processing from Cooperative Intermediaries. *IEEE Transactions on Parallel and Distributed Systems (TPDS).* 19(5): 615-626. 2008. (Impact factor: 4.18)

MANUSCRIPT UNDER REVIEW

- Tanmoy Sarkar Pias*, Sharmin Afrose*, Moon Das, Ipsita Hamid Trisha, Xinwei Deng, Charles Nemeroff, and Danfeng (Daphne) Yao. Low Responsiveness of Machine Learning Models to Critical or Deteriorating Health Conditions. medRxiv. DOI: 10.1101/2024.09.25.24314400. 2024.

- Tanmoy Sarkar Pias*, Yiqi Su*, Xuxin Tang*, Haohui Wang*, Shahriar Faghani, and Danfeng (Daphne) Yao. Enhancing Fairness and Accuracy in Diagnosing Type 2 Diabetes in Young Population. medRxiv. DOI: 10.1101/2023.05.02.23289405. 2023.

- Wenjia Song*, Sanjula Karanam*, Ya Xiao*, Jingyuan Qi*, Nathan Dautenhahn, Na Meng, Elena Ferrari, and Danfeng (Daphne) Yao. Crypto-Ransomware and Their Defenses: In-depth Behavioral Characterization, Discussion of Deployability, and New Insights. 2024.

BOOK CHAPTERS

41. Xiaokui Shu*, Fang Liu*, and Danfeng Yao. Rapid Screening of Big Data Against Inadvertent Leaks. In *Big Data: Theories, Applications and Concepts.* Editors: Shui Yu and Song Guo. Springer. Pages: 193-236. 2016.

42. Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. Forward-Secure Hierarchical IBE with Applications to Broadcast Encryption Schemes. In *Cryptology and Information Security Series on Identity-Based Cryptography.* Editors: Marc Joye and Gregory Neven. IOS Press. Oct. 2008.

PEER-REVIEWED CONFERENCES/WORKSHOPS

43. Jingwen Yan, Song Liao, Mohammed Aldeen, Luyi Xing, Danfeng (Daphne) Yao, and Long Cheng. SKILLPoV: Towards Accessible and Effective Privacy Notice for Amazon Alexa Skills. In *Proceedings of Network and Distributed System Security (NDSS) Symposium.* San Diego, CA. Feb. 2025.

44. Wenjia Song*, Hailun Ding, Na Meng, Peng Gao, and Danfeng (Daphne) Yao. Madeline: Continuous and Low-cost Monitoring with Graph-free Representations to Combat Cyber Threats. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. Waikiki, Hawaii. Dec. 2024. **Provisional patent being filed.**

45. Ming Zhu*, Mohimenul Karim*, Ismini Lourentzou, and Danfeng (Daphne) Yao. Semi-Supervised Code Translation Overcoming the Scarcity of Parallel Code Data. In *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. Sacramento, CA. Nov. 2024. (Acceptance rate: 27.3%)

46. Song Liao, Long Cheng, Xiapu Luo, Zheng Song, Haipeng Cai, Danfeng (Daphne) Yao, and Hongxin Hu. A First Look at Security and Privacy Risks in the RapidAPI Ecosystem. *ACM Conference on Computer and Communications Security (CCS)*. Salt Lake City, UT. 2024.

47. Alex Kedrowitsch*, Jonathan Black, and Danfeng (Daphne) Yao. Resilient Routing for Low Earth Orbit Mega-Constellation Networks. In *Proceedings of the 2nd Workshop on the Security of Space and Satellite Systems*, co-located with the NDSS Symposium. Mar. 2024.

48. Wyatt Sweat* and Daphne Yao. Cybersecurity Usage in the Wild: A look at Deployment Challenges in Intrusion Detection and Alert Handling. *Workshop on Research for Insider Threats (WRIT)*, co-located with the *Annual Computer Security Applications Conference (ACSAC)*. Austin, TX. Dec. 2023.

49. Tahmina Sultana Priya*, Fan Leng, Anthony C. Luehrs, Eric W. Klee, Alina M. Allen, Konstantinos N. Lazaridis, Danfeng (Daphne) Yao, Shulan Tian. Deep Phenotyping of Non-Alcoholic Fatty Liver Disease Patients with Genetic Factors for Insights into the Complex Disease. *Machine Learning for Health (ML4H) Symposium 2023 (Findings Track)*, Dec. 2023, New Orleans, La.

50. Connor Weeks, Aravind Cheruvu, Sifat Muhammad Abdullah, Shravya Kanchi, Danfeng (Daphne) Yao, and Bimal Viswanath. A First Look at Toxicity Injection Attacks on Open-domain Chatbots. In *Proceedings of Annual Computer Security Applications Conference (ACSAC)*. 2023.

51. Salman Ahmed*, Hans Liljestrand, Hani Jamjoom, Matthew Hicks, N. Asokan, and Danfeng (Daphne) Yao. Not All Data are Created Equal: Data and Pointer Prioritization for Scalable Protection Against Data-Oriented Attacks. In *Proceedings of the USENIX Security Symposium.* Aug. 2023. **Artifacts Available Badge.**

52. Sazzadur Rahaman, Miles Frantz*, Barton Miller and Danfeng Yao. SpanL: Creating Algorithms for Automatic API Misuse Detection with Program Analysis Compositions. *Proceedings of the Workshop on Secure Cryptographic Implementation (SCI)*, co-located with *International Conference on Applied Cryptography and Network Security (ACNS)*. Kyoto, Japan. 2023.

53. Md Mahir Asef Kabir, Ying Wang, Danfeng(Daphne) Yao, and Na Meng. How Do Developers Follow Security-Relevant Best Practices When Using NPM Packages? In *Proceedings of the IEEE Secure Development Conference (SecDev)*. Atlanta, GA. Oct. 2022.

54. Ying Zhang, Ya Xiao*, Md Mahir Asef Kabir, Danfeng (Daphne) Yao, and Na Meng. Example-Based Vulnerability Detection and Repair in Java Code. *ACM/IEEE International Conference on Program Comprehension (ICPC)*, co-located with *ICSE*. May 2022.

55. Sharmin Afrose*, Danfeng (Daphne) Yao, and Olivera Kotevska. Measurement of Local Differential Privacy Techniques for IoT-based Streaming Data. *International Conference on Privacy, Security, and Trust (PST)*. Dec. 2021.

56. Mazharul Islam*, Sazzadur Rahaman*, Na Meng, Behnaz Hassanshahi, Paddy Krishnan, and Danfeng (Daphne) Yao. Coding Practices and Recommendations with Spring Security for Enterprise Applications. In *Proceedings of the IEEE Secure Development Conference (SecDev)*. Sep. 2020.

57. Salman Ahmed*, Ya Xiao*, Gang Tan, Kevin Snow, Fabian Monrose, and Danfeng (Daphne) Yao. Methodologies for Quantifying (Re-)randomization Security and Timing under JIT-ROP. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS).* Nov. 2020.

58. Xiaodong Yu*, Fengguo Wei, Xinming Ou, Michela Becchi, Tekin Bicer, and Danfeng (Daphne) Yao. GPU-Based Static Data-Flow Analysis for Fast and Scalable Android App Vetting. In *Proceedings of the 34th IEEE International Parallel and Distributed Processing Symposium (IPDPS).* New Orleans, LA. May 2020. (Acceptance rate: 25%)

59. Pronnoy Goswami, Saksham Gupta, Zhiyuan Li, Na Meng, and Danfeng (Daphne) Yao. Investigating The Reproducibility of NPM Packages. In *Proceedings of the International Conference on Software Maintenance and Evolution (ICSME).* Oct. 2020.

60. Sazzadur Rahaman*, Ya Xiao*, Sharmin Afrose*, Fahad Shaon, Ke Tian*, Miles Frantz*, Murat Kantarcioglu, and Danfeng (Daphne) Yao. CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS).* London, UK. Nov. 2019. (Acceptance rate: 16%) **Featured in Communications of the ACM.**

61. Sazzadur Rahaman*, Gang Wang, and Daphne Yao. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS).* London, UK. Nov. 2019. (Acceptance rate: 16%) **Invited to present at FTC PrivacyCon 2020.**

62. Ya Xiao*, Qingying Hao*, and Danfeng (Daphne) Yao. Neural Cryptanalysis: Metrics, Methodology, and Applications in CPS Ciphers. In *Proceedings of the IEEE Conference on Dependable and Secure Computing (DSC).* **Invited paper.** Hangzhou, China. Nov. 2019.

63. Xiaodong Yu*, Ya Xiao*, Kirk Cameron, and Danfeng Yao. Comparative Measurement of Cache Configurations' Impacts on Cache Timing Side-Channel Attacks. *USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, co-located with *USENIX Security Symposium.* Santa Clara, CA. Aug. 2019. (Acceptance rate: 31%)

64. Sharmin Afrose*, Sazzadur Rahaman*, and Daphne Yao. CryptoAPI-Bench: A Comprehensive Benchmark on Java Cryptographic API Misuses. *IEEE Secure Development (SecDev) Conference.* Sept. 2019. Tyson Corner, VA. (Acceptance rate: 36%)

65. Long Cheng*, Hans Liljestrand, Salman Ahmed*, Thomas Nyman, Trent Jaeger, N. Asokan, and Daphne Yao. Exploitation Techniques and Defenses for Data-Oriented Attacks. *IEEE Secure Development (SecDev) Conference.* Sept. 2019. Tyson Corner, VA. (Acceptance rate: 36%)

66. Ke Tian*, Jan Steve, Hang Hu, Danfeng Yao, and Gang Wang. Needle in a Haystack: Tracking Down Elite Phishing Domains in the Wild. In *ACM Internet Measurement Conference (IMC).* Boston, MA. Oct. 2018. (Acceptance rate: 25%)

67. Ke Tian*, Zhou Li, Kevin Bowers, and Danfeng Yao. FrameHanger: Evaluating and Classifying Iframe Injection at Large Scale. In *Proceedings of the International Conference on Security and Privacy in Communication Networks (SECURECOMM).* Singapore. Aug. 2018. (Acceptance rate: 30.5%)

68. Na Meng, Stefan Nagy*, Danfeng Yao, Wenjie Zhuang, and Gustavo Argoty. Secure Coding Practices in Java: Challenges and Vulnerabilities. *International Conference on Software Engineering (ICSE).* Gothenburg, Sweden. May, 2018. (Acceptance rate: 20.9%) **Multiple high-profile media reports.**

69. Long Cheng*, Ke Tian*, and Danfeng Yao. Enforcing Cyber-Physical Execution Semantics to Defend Against Data-Oriented Attacks. In *Proceedings of Annual Computer Security Applications Conference (ACSAC).* Orlando, FL. Dec. 2017. (Acceptance rate: 19.7%)

70. Ning Zhang, Ruide Zhang, Qiben Yan, Wenjing Lou, Y. Thomas Hou, and Danfeng Yao. Black Penguin: On the Feasibility of Detecting Intrusion with Homogeneous Memory. *Network and Cloud Forensics Workshop*, co-located with *IEEE Conference on Communications and Network Security (CNS).* Las Vegas, NV.

71. Ke Tian*, Gang Tan, Danfeng Yao, and Barbara Ryder. ReDroid: Prioritizing Data Flows and Sinks for App Security Transformation. In *Proceedings of workshop on Forming an Ecosystem Around Software Transformation (FEAST).* Collocated with the ACM Conference on Computer and Communications Security (CCS). Dallas, TX. Nov. 2017.

72. Alexander Kedrowitsch*, Danfeng (Daphne) Yao, Gang Wang, and Kirk Cameron. A First Look: Using Linux Containers for Deceptive Honeypots. In *Proceedings of ACM Workshop on Assurable & Usable Security Configuration (SafeConfig).* Collocated with the ACM Conference on Computer and Communications Security (CCS). Dallas, TX. Nov. 2017.

73. Sazzadur Rahaman* and Danfeng Yao. Program Analysis of Cryptography Implementations for Security. In *Proceedings of IEEE Secure Development Conference (SecDev).* Cambridge, MA. Sep., 2017. (Acceptance rate: 32.3%)

74. Fang Liu*, Chun Wang, Andres Pico*, Danfeng Yao, and Gang Wang. Measuring the Insecurity of Mobile Deep Links of Android. In *Proceedings of the 26th USENIX Security Symposium.* Vancouver, Canada. Aug. 2017. (Acceptance rate: 16.3%)

75. Sazzadur Rahaman*, Long Cheng*, Danfeng Yao, He Li, and Jung-Min Park. Provably Secure Anonymous-yet-Accountable Crowdsensing with Scalable Sublinear Revocation. The *17th Privacy Enhancing Technologies Symposium (PETS).* Minneapolis, MN. Jul. 2017. (Acceptance rate: 21.7%)

76. Hussain Almohri, Long Cheng*, Danfeng Yao, and Homa Alemzadeh. On Threat Modeling and Mitigation of Medical Cyber-Physical Systems. In *Proceedings of IEEE International Workshop on Security, Privacy, and Trustworthiness in Medical Cyber-Physical Systems (MedSPT)*, in conjunction with the *IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE).* Philadelphia, PA. Jul. 2017. **Invited paper.**

77. Fang Liu*, Haipeng Cai*, Gang Wang, Danfeng Yao, Karim O. Elish* and Barbara G. Ryder. MR-Droid: A Scalable and Prioritized Analysis of Inter-App Communication Risks. In *Proceedings of Mobile Security Technologies (MoST) Workshop*, in conjunction with the *IEEE Symposium on Security and Privacy.* San Jose, CA. May 2017. (Acceptance rate: 33%)

78. Amiangshu Bosu*, Fang Liu*, Danfeng Yao, and Gang Wang. Collusive Data Leak and More: Large-scale Threat Analysis of Inter-app Communications. In *Proceedings of ACM Symposium on Information, Computer & Communication Security (ASIACCS).* Apr. 2017. (Acceptance rate: 20%) **Numerous media reports.**

79. Ke Tian*, Danfeng Yao, Barbara Ryder and Gang Tan. Analysis of Internal Code Heterogeneity for High-Precision Classification of Repackaged Malware. In *Proceedings of Mobile Security Technologies (MoST) Workshop*, in conjunction with the *IEEE Symposium on Security and Privacy.* San Jose, CA. May 2016. (Acceptance rate: 29%.)

80. Kui Xu*, Ke Tian*, Danfeng Yao, and Barbara Ryder. A Sharper Sense of Self: Probabilistic Reasoning of Program Behaviors for Anomaly Detection with Context Sensitivity. In *Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).* Toulouse, France. Jun., 2016.(Acceptance rate: 22%)

81. Xiaodong Yu, Wu-chun Feng, Danfeng Yao, and Michela Becchi. O3FA: A Scalable, Finite Automata-based, Pattern-Matching Engine for Out-of-Order Packet Inspection in IDS. In *Proceedings of the 12th ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS '16).* Santa Clara, CA. Mar. 2016. (Acceptance rate: 21%).

82. Xiaokui Shu, Nikolay Laptev, and Danfeng Yao. DECT: Distributed Evolving Context Tree for Understanding User Behavior Pattern Evolution. In *Proceedings of 19th International Conference on Extending Database Technology (EDBT)*, co-located with *International Conference on Database Theory (ICDT)*. Mar., 2016. Bordeaux, France. **Selected for demo at AAAI '16.**

83. Xiaokui Shu*, Danfeng Yao, and Barbara Ryder. A Formal Framework for Program Anomaly Detection. In *Proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*. Kyoto, Japan. Nov. 2015. (Acceptance rate: 23.5%.)

84. Xiaokui Shu*, Danfeng Yao, and Naren Ramakrishnan. Unearthing Stealthy Program Attacks Buried in Extremely Long Execution Paths. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Denver, Colorado. Oct. 2015. (Acceptance rate: 19.8%.) **Featured in Communications of the ACM. Topic selected for ACM CCS'16 tutorial.**

85. Kui Xu*, Danfeng Yao, Barbara Ryder, and Ke Tian. Probabilistic Program Modeling for High-Precision Anomaly Classification. In *Proceedings of the 2015 IEEE Computer Security Foundations Symposium (CSF)*. Verona, Italy. Jul. 2015. (Acceptance rate: 35%.)

86. Karim Elish*, Danfeng Yao, and Barbara Ryder. Static Characterization of Pairwise Android Inter-Component Communications for Collusion Detection. In *Proceedings of Mobile Security Technologies (MoST)*, in conjunction with the *IEEE Symposium on Security and Privacy*. San Jose, CA. May 2015. (Acceptance rate: 30%)

87. Xiaokui Shu*, Jing Zhang, Danfeng Yao, and Wu-Chun Feng. Rapid and Parallel Content Screening for Detecting Transformed Data Exposure. In *Proceedings of the International Workshop on Security and Privacy in Big Data (BigSecurity)*, co-located with *IEEE INFOCOM*. Hong Kong. April, 2015. (Acceptance rate: 26%)

88. Hao Zhang*, Maoyuan Sun, Danfeng Yao, and Chris North. Visualizing Traffic Causality for Analyzing Network Anomalies. In *Proceedings of International Workshop on Security and Privacy Analytics (SPA)*, co-located with *ACM CODASPY*. San Antonio, TX. Mar. 2015.

89. Fang Liu*, Xiaokui Shu*, Danfeng Yao, and Ali Butt. Privacy-Preserving Scanning of Big Content for Sensitive Data Exposure with MapReduce. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*. San Antonio, TX. Mar. 2015. (Acceptance rate: 21%) **Featured by NSF I/UCRC S2ERC research highlight.**

90. Yanzhi Dou, Kexiong (Curtis) Zeng, Yaling Yang, and Danfeng Yao. MadeCR: Correlation-based Malware Detection for Cognitive Radio. In *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*. Hong Kong. Apr. 2015. (Acceptance rate: 19%)

91. Britton Wolfe, Karim Elish*, and Danfeng Yao. High Precision Screening for Android Malware with Dimensionality Reduction. In *Proceedings of the 13th International Conference on Machine Learning and Applications (ICMLA'14)*. Detroit, MI. Dec. 2014. (Acceptance rate: 35%)

92. Kui Xu*, Danfeng Yao, Manuel A. Perez-Quinones, Casey Link*, and E. Scott Geller. Role-Playing Games for Security Evaluation: A Case Study on Email Secrecy. In *Proceedings of 10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2014)*. Miami, FL. Oct. 2014. (Acceptance rate: 20%).

93. Britton Wolfe, Karim Elish*, and Danfeng Yao. Comprehensive Behavior Profiling for Proactive Android Malware Detection. In *Proceedings of the 7th International Conference on Information Security (ISC)*. Hong Kong. Oct. 2014. *Lecture Notes in Computer Science (LNCS)* 8783, 328-344. (Acceptance rate: 19%).

94. Hao Zhang*, Danfeng Yao and Naren Ramakrishnan. Detection of Stealthy Malware Activities with Traffic Causality and Scalable Triggering Relation Discovery. In *Proceedings of the 9th ACM*

Symposium on Information, Computer and Communications Security (ASIACCS). Kyoto, Japan. Jun. 2014. (Acceptance rate: 20%). **U.S. Patent Granted.**

95. Hussain Almohri*, Danfeng Yao, and Dennis Kafura. DroidBarrier: Know What is Executing on Your Android. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY).* San Antonio, TX. Mar. 2014. (Acceptance rate: 23.5%).

96. Xiaokui Shu*, John Smiy*, Danfeng Yao, and Heshan Lin. Massive Distributed and Parallel Log Analysis for Organizational Security. In *Proceedings of the International Workshop on Security and Privacy in Big Data (BigSecurity)*, in conjunct with Globecom. Atlanta, GA. Dec. 2013. (Acceptance rate: 35%).

97. Huijun Xiong*, Qingji Zheng, Xinwen Zhang, and Danfeng Yao. CloudSafe: Securing Data Processing within Vulnerable Virtualization Environment in Cloud. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS).* Washington, D.C. Oct. 2013. (Acceptance rate: 28%)

98. Karim Elish*, Yipan Deng*, Danfeng Yao and Dennis Kafura. Device-Based Isolation for Securing Cryptographic Keys. In *Proceedings of the 3rd International Symposium on Internet of Ubiquitous and Pervasive Things (IUPT).* Halifax, Canada. Jun. 2013.

99. Yipeng Wang, Xiaochun Yun, M. Zubair Shafiq, Alex X. Liu, Zhibin Zhang, Liyan Wang, Danfeng Yao, Yongzheng Zhang, and Li Guo. A Semantics Aware Approach to Automated Reverse Engineering Unknown Protocols. In *Proceedings of 20th IEEE International Conference on Network Protocols (ICNP).* Austin, TX. Oct. 2012. **Best Paper Award**. (Acceptance rate: 23%).

100. Xiaokui Shu* and Danfeng Yao. Data Leak Detection as a Service. In *Proceedings of the 8th International Conference on Security and Privacy in Communication Networks (SECURECOMM).* Padua, Italy. Sep. 2012. (Acceptance rate: 29%).

101. Hao Zhang*, William Banick*, Danfeng Yao and Naren Ramakrishnan. User Intention-Based Traffic Dependence Analysis For Anomaly Detection. In *Proceedings of Workshop on Semantics and Security*, in conjunction with the *IEEE Symposium on Security and Privacy.* 2012.

102. Karim O. Elish*, Danfeng Yao, and Barbara G. Ryder. User-Centric Dependence Analysis for Identifying Malicious Mobile Apps. In *Proceedings of the Workshop on Mobile Security Technologies (MoST)*, in conjunction with the *IEEE Symposium on Security and Privacy.* 2012.

103. Hussain Almohri*, Danfeng Yao, and Dennis Kafura. Identifying Native Applications with High Assurance. In *Proceedings of the Second ACM Conference on Data and Application Security and Privacy (CODASPY).* 2012. (Acceptance rate: 25%).

104. Huijun Xiong*, Xinwen Zhang, Wei Zhu, and Danfeng Yao. Towards End-to-End Secure Content Storage and Delivery with Public Cloud. In *Proceedings of the Second ACM Conference on Data and Application Security and Privacy (CODASPY).* 2012. (Acceptance rate: 25%).

105. Kui Xu*, Danfeng Yao, Qiang Ma*, and Alex Crowell*. Detecting Infection Onset with Behavior-Based Policies. In *Proceedings of the International Conference on Network and System Security (NSS).* Pages 57 - 64. Milan, Italy. Sep. 2011 (Acceptance rate: 22%).

106. Saman Zarandioon*, Danfeng Yao, and Vinod Ganapathy. K2C: Cryptographic Cloud Storage with Lazy Revocation and Anonymous Access. In *Proceedings of the 7th International ICST Conference on Security and Privacy in Communication Networks (SecureComm).* Sep. 2011. London, UK. (Acceptance rate: 24%).

107. Huijun Xiong*, Xinwen Zhang, Wei Zhu and Danfeng Yao. CloudSeal: End-to-End Content Protection in Cloud-based Storage and Delivery Services. In *Proceedings of the 7th International ICST Conference on Security and Privacy in Communication Networks (SecureComm).* Lecture Notes in Computer Science (LNCS). Sep. 2011. London, UK.

108. Patrick Butler*, Kui Xu*, and Danfeng Yao. Quantitatively Analyzing Stealthy Communication Channels. In *Proceedings of International Conference on Applied Cryptography and Network Security (ACNS).* Lecture Notes in Computer Science. Jun. 2011. Nerja, Spain. (Acceptance rate: 18%)

109. Yipeng Wang, Zhibin Zhang, Danfeng Yao, Buyun Qu, and Li Guo. Inferring Protocol-State Machine from Network Traces: A Probabilistic Description Method. In *Proceedings of International Conference on Applied Cryptography and Network Security (ACNS).* Lecture Notes in Computer Science. Jun. 2011. (Acceptance rate: 18%).

110. Deian Stefan* and Danfeng Yao. Keystroke-Dynamics Authentication Against Synthetic Forgeries. In *Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom).* 2010. **Best Paper Award.** (Acceptance rate: 38%).

111. Deian Stefan*, Chehai Wu*, Danfeng Yao, and Gang Xu. Knowing Where Your Input is from: Kernel-Level Data-Provenance Verification. In *Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS).* Pages 71-87. Beijing China. Jun., 2010. (Acceptance rate: 23%). **Patented technology.**

112. Chih-Cheng Chang*, Brian Thompson*, Hui Wang, Danfeng Yao. Towards Publishing Recommendation Data with Predictive Anonymization. In *Proceedings of ACM Symposium on Information, Computer & Communication Security (ASIACCS).* 2010. (Acceptance rate: 23%).

113. Huijun Xiong*, Prateek Malhotra*, Deian Stefan*, Chehai Wu*, and Danfeng Yao. User-Assisted Host-Based Detection of Outbound Malware Traffic. In *Proceedings of International Conference on Information and Communications Security (ICICS '09).* Pages 293-307. Beijing, China. Dec. 2009. Lecture Notes in Computer Science 5927. Springer. (Acceptance rate 19%).

114. Nitya H. Vyas*, Anna Squicciarini, Chih-Cheng Chang*, and Danfeng Yao. Towards Automatic Privacy Management in Web 2.0 with Semantic Analysis on Annotations. In *Proceedings of International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom).* Washington DC. Nov. 2009. (Acceptance rate: 34.6%).

115. Anitra Babic*, Huijun Xiong*, Danfeng Yao, and Liviu Iftode. Building Robust Authentication Systems with Activity-Based Personal Questions. In *Proceedings of ACM Workshop on Assurable & Usable Security Configuration (SafeConfig).* Collocated with the ACM Conference on Computer and Communications Security. Chicago, IL. Nov. 2009. **Featured on NSF.gov front page.**

116. Saman Zarandioon*, Danfeng Yao, and Vinod Ganapathy. Privacy-aware Identity Management for Client-side Mashup Applications. In *Proceedings of the Fifth ACM Workshop on Digital Identity Management (DIM).* Collocated with the ACM Conference on Computer and Communications Security. Chicago, IL. Nov. 2009. Pages 21-30.

117. Brian Thompson*, Danfeng Yao, Stuart Haber, William G. Horne, and Tomas Sander. Privacy-Preserving Computation and Verification of Aggregate Queries on Outsourced Databases. In *Proceedings of the 9th Privacy Enhancing Technologies Symposium (PETS).* Seattle, WA. Aug. 2009. Lecture Notes in Computer Science 5672. Pages 185-201. (Acceptance rate: 25.6%).

118. Tzvika Chumash* and Danfeng Yao. Detection and Prevention of Insider Threats in Database Driven Web Services In *Proceedings of the Third IFIP WG 11.11 International Conference on Trust Management (IFIPTM).* Pages 117-132. Jun. 2009. West Lafayette, IN.

119. Brian Thompson* and Danfeng Yao. Union-Split Clustering Algorithm and Social Network Anonymization. In *Proceedings of ACM Symposium on Information, Computer & Communication Security (ASIACCS).* Pages 218-227. Mar. 2009. Sydney, Australia. (Acceptance rate: 27%).

120. Tuan Phan* and Danfeng Yao. *SelectAudit*: A Secure and Efficient Audit Framework for Networked Virtual Environments. In *Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom).* Nov., 2008. Orlando, FL. (Acceptance rate: 37%). **Invited paper.**

121. Saman Zarandioon*, Danfeng Yao, and Vinod Ganapathy. Design and Implementation of an Open Framework for Secure Communication in Mashup Applications. In *Proceedings of Annual Computer Security Applications Conference (ACSAC).* Dec. 8-12, 2008, Anaheim, CA. Pages 355-364. (Acceptance rate: 24.3%).

122. Vivek Pathak*, Danfeng Yao, and Liviu Iftode. Securing Location Aware Services Over VANET Using Geographical Secure Path Routing. In *Proceedings of International Conference on Vehicular Electronics and Safety (ICVES).* Columbus, Ohio. September 22-24, 2008.

123. Vivek Pathak*, Danfeng Yao, and Liviu Iftode. Improving Email Trustworthiness through Social-Group Key Authentication. *Proceedings of the Fifth Conference on Email and Anti-Spam (CEAS).* Mountain View, CA. Aug 21-22, 2008.

124. Stuart Haber, Yasuo Hatano, Yoshinori Honda, William Horne, Kunihiko Miyazaki, Tomas Sander, Satoru Tezuka, and Danfeng Yao. Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. In *Proceedings of ACM Symposium on Information, Computer & Communication Security (ASIACCS).* 2008. (Acceptance rate: 25.2%).

Below are publications from Ph.D.

125. Danfeng Yao, Roberto Tamassia, and Seth Proctor. Private Distributed Scalar Product Protocol with Application to Privacy-Preserving Computation of Trust. In *Proceedings of IFIPTM – Joint iTrust and PST Conferences on Privacy, Trust Management and Security.* 2007.

126. Isabel F. Cruz, Roberto Tamassia, and Danfeng Yao. Privacy-Preserving Schema Matching Using Mutual Information. In *Proceedings of the 21th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec).* 2007.

127. Danfeng Yao, Yunhua Koglin, Elisa Bertino, and Roberto Tamassia. Decentralized Authorization and Data Security in Web Content Delivery. In *Proceedings of the 22nd ACM Symposium on Applied Computing (SAC)*, Special Track on Web Technologies. 2007.

128. Danfeng Yao, Keith B. Frikken, Mikhail J. Atallah, and Roberto Tamassia. Point-Based Trust: Define How Much Privacy Is Worth. In *Proceedings of the Eighth International Conference on Information and Communications Security (ICICS).* 2006. **Best Student Paper Award**. (Acceptance rate: 32%).

129. Danfeng Yao and Roberto Tamassia. Cascaded Authorization with Anonymous-Signer Aggregate Signatures. In *Proceedings of the Seventh Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop (IAW).* 2006.

130. Michael T. Goodrich, Roberto Tamassia, and Danfeng Yao. Notarized Federated Identity Management for Increased Trust in Web Services. In *Proceedings of the 20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec).* 2006.

131. Danfeng Yao, Michael Shin, Roberto Tamassia, and William H. Winsborough. Visualization of Automated Trust Negotiation. In *Proceedings of the Workshop on Visualization for Computer Security (VizSEC)*, in Conjunction with Vis and InfoVis. 2005.

132. Danfeng Yao, Roberto Tamassia, and Seth Proctor. On Improving the Performance of Role-Based Cascaded Delegation in Ubiquitous Computing. In *Proceedings of the IEEE/CreateNet Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm).* 2005. (Acceptance rate: 25%).

133. Michael T. Goodrich, Roberto Tamassia, and Danfeng Yao. Accredited DomainKeys: A Service Architecture for Improved Email Validation. In *Proceedings of the Second Conference on Email and Anti-Spam (CEAS).* 2005. **Received Brown University's Award for Technological Innovation.**

134. Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. ID-Based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption. In *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS).* 2004. (Acceptance rate: 18%).

135. Roberto Tamassia, Danfeng Yao, and William H. Winsborough. Role-Based Cascaded Delegation. In *Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT).* 2004. (Acceptance rate: 27%).

NON-PEER-REVIEWED PUBLICATIONS

1. Danfeng Daphne Yao; Terry Benzel. ACSAC 2020: Furthering the Quest to Tackle Hard Problems and Find Practical Solutions. IEEE Security & Privacy 19(6). Nov.-Dec., 2021.

2. Xiaokui Shu*, Ke Tian*, Andrew Ciambrone*, and Danfeng Yao. Breaking the target: An analysis of target data breach and lessons learned. `https://arxiv.org/abs/1701.04940` 2017.

3. Stuart Haber, William G. Horne, Tomas Sander, and Danfeng Yao. Privacy-preserving verification of aggregate queries on outsourced database. *Research Disclosure.* 528: 349-351. Kenneth Mason Publications.

TUTORIALS

1. Tutorial: Investigating Advanced Exploits for System Security Assurance. Salman Ahmed, Long Cheng, Hans Liljestrand, N. Asokan, and Danfeng (Daphne) Yao. *IEEE Secure Development Conference (SecDev).* Oct. 2021.

2. Tutorial: Principles and Practices of Secure Cryptographic Coding in Java. Ya Xiao, Miles Frantz, Sharmin Afrose, and Danfeng (Daphne) Yao. *European Symposium on Research in Computer Security (ESORICS).* 2021. **Invited Tutorial.**

3. Tutorial: Principles and Practices of Secure Crypto Coding in Java. Ya Xiao, Miles Frantz, Sharmin Afrose, Sazzadur Rahaman, and Daphne Yao. *IEEE Secure Development Conference (SecDev).* Sep. 2020.

4. Tutorial: Principles and practices of secure coding. Sazzadur Rahaman, Danfeng Yao, and Na Meng. *IEEE Secure Development Conference (SecDev).* Sep. 2018.

5. Tutorial: Program Anomaly Detection: Methodology and Practices. Xiaokui Shu and Danfeng Yao. *ACM Conference on Computer and Communications Security (CCS).* Oct. 2016.

SOFTWARE AND DATASET

- For Java crypto software security.

  CryptoGuard, a deployment-quality code screening tool for detecting Java crypto misuses (from ACM CCS '19). `https://github.com/CryptoGuardOSS/cryptoguard` Code developed by Sazzadur Rahaman.

  CryptoAPI-Bench, a 171-unit benchmark for evaluating Java crypto API misuse detection tools (from IEEE SecDev '19). `https://github.com/CryptoGuardOSS/cryptoapi-bench` Code developed by Sharmin Afrose.

  Dataset (from ICSE '18) summarizing 500 Java security-related posts from StackOverflow forum. `http://people.cs.vt.edu/nm8247/icse18.xlsx`

- For Python crypto software security.

  Cryptolation, a static code analysis tool for detecting Python cryptographic API misuses (from IEEE TSE '24). `https://github.com/franceme/cryptolation` Code developed by Miles Frantz.

  PyCryptoBench, a large benchmark for evaluating Python crypto API misuse detection tools (from IEEE TSE '24). `https://github.com/franceme/pycryptobench` Benchmark developed by Miles Frantz.

- For web application and payment security.

  PCICheckerLite, a lightweight black-box web scanning tool (from ACM CCS '19). `https://github.com/sazzad114/pci-checker` Code developed by Sazzadur Rahaman.

- For data-oriented programming (DOP) attacks.

  DOP exploit scripts on a vulnerable Proftpd (by Hans Liljestrand) – a version of exploit compatible for Intel PT environments; trace files and analysis tools (by Long Cheng). `https://github.com/doppt/data-oriented-attacks`

- For Android Security.

  1. **DIALDroid Database** with flow-sensitive ICC-related data-flow features extracted from more than 100,000 Android applications. `https://github.com/dialdroid-android/DIALDroid` Code developed by Amiangshu Bosu (former postdoc and collaborator).
  2. **DIALDroid-IC3** for Android ICC Resolution. `https://github.com/dialdroid-android/ic3-dialdroid`. Code developed by Amiangshu Bosu (former postdoc).
  3. **DIALDroid-Bench** for Android Malware Collusion Benchmark. `https://github.com/dialdroid-android/dialdroid-bench`. Code developed by Amiangshu Bosu (former postdoc).
  4. **DR_Droid**: Android repackaged malware detection tools. `https://github.com/ririhedou/dr_droid`. Code developed by Ke Tian (former PhD student).
  5. Linear-programming (LP) based attack graph probabilistic risk propagation. `https://github.com/halmohri/ECSA` Code developed by Hussain Almohri (former PhD student).

- For Program Anomaly Detection, including CPS anomaly detection.

  6. CPS application traces, smart syringe examples, and event dependency functions from our eFSA work (ACSAC '17 and IEEE TDSC '19) https://github.com/cslongc/efsa

     A YouTube video demo of eFSA anomaly detection at `https://youtu.be/-VEjidSgGIc`
  7. Call traces and call tracking tools. `https://github.com/yaoGroupAnomaly/traceCollect.` Organized by Ke Tian and Long Cheng (PhD students).
  8. Labs for n-gram and FSA-based program anomaly detection (Part of our ACM CCS'16 tutorial). `https://github.com/subbyte/padlabs`. Code developed by Xiaokui Shu (former PhD student).

- For attack graphs and probabilistic risk management.

  6. To compute Expected Chance of a Successful Attack (ECSA). `https://github.com/halmohri/ECSA` Developed by Hussain Almohri.

GRADUATED PH.D. STUDENTS

1. Miles Frantz (Ph.D. '24, first job at Peraton) Dissertation title: *Measurement and Development for Automated Secure Coding Solutions*

   External committee member: Dr. Raj Rajagopalan, Director and Fellow of Cyber Security at Resideo

2. Ming Zhu (Ph.D. '23, co-advisor: Ismini Lourentzou, Research Scientist at Salesforce AI Research)

   Dissertation title: *Neural Sequence Modeling for Domain-Specific Language Processing: A Systematic Approach*

   External committee member: Wasi Uddin Ahmad, AWS AI Labs

3. Ya Xiao (Ph.D. '22, first job at TikTok)

   Dissertation title: *Neural Network-based Methodologies for Securing Cryptographic Code*

   External committee member: Patrick McDaniel, Penn State University; Xinyang Ge, Netflix

4. Sharmin Afrose (Ph.D. '22, first job at Oak Ridge National Lab)

   Dissertation title: *Methodology Development for Improving the Performance of Critical Classification Applications*

   External committee member: Sharon Xiaolei Huang, PSU; Aditya Prakash, Georgia Tech

5. Salman Ahmed (Ph.D. '21, first job at IBM Research)

   Dissertation title: *Quantitative Metrics and Measurement Methodologies for System Security Assurance*

   External committee members: Fabian Monrose, University of North Carolina at Chapel Hill; Gang Wang, UIUC; Patrick Schaumont, WPI.

6. Sazzadur Rahaman (Ph.D. '20, first job as a tenure-track assistant professor at University of Arizona.)

   Dissertation title: *From theory to practice: Deployment-grade tools and methodologies for software security*

   External committee member: David Evans, University of Virginia; Patrick Schaumont, Worcester Polytechnic Institute

7. Hang Hu (Ph.D., '20, lead advisor was Gang Wang of UIUC; first job at Google.)

   Thesis title: *Characterizing and Detecting Online Deception via Data-Driven Methods*

   External committee member: Yuan Tian, University of Virginia

8. Xiaodong Yu (Ph.D. '19, first job at Argonne National Laboratory.)

   Dissertation title: *Algorithms and Frameworks for Accelerating Security Applications on HPC Platforms*

   External committee member: Michela Becchi, North Carolina State University; Xinming (Simon) Ou, University of South Florida

9. Long Cheng (Ph.D. '18, first job as a tenure-track assistant professor at Clemson University.)

   Dissertation title: *Program Anomaly Detection Against Data-oriented Attacks*

   External committee member: Raheem Beyah, Georgia Tech

10. Ke Tian (Ph.D. '18, first job at Microsoft security group)

    Dissertation title: *Learning-based Mobile App Analysis and Binary Customization for Security*

    External committee member: Gang Tan, PSU

11. Fang Liu (Ph.D. '17, first job as an Internet security research engineer at Palo Alto Networks)

    Dissertation title: *Mining Security Risks from Massive Datasets*

    External committee member: Dongyan Xu, Purdue University

12. Xiaokui Shu (Ph.D. '16, first job at IBM Research T. J. Watson Center)
    Dissertation title: *Threat Detection in Program Execution and Data Movement: Theory and Practice*
    External committee member: Trent Jaeger, PSU

13. Hao Zhang (Ph.D. '15, first job as a security engineer at the DB security group of Oracle)
    Dissertation title: *Discovery of Triggering Relations and Its Applications in Network Security and Android Malware Detection*
    External committee member: Xinming Ou, Kansas State University

14. Karim Elish (Ph.D. '15, assistant professor at Florida Polytechnic University)
    Dissertation title: *User-Intention Based Program Analysis for Android Security*
    External committee member: Xuxian Jiang, North Carolina State University

15. Kui Xu (Ph.D. '14, security engineer at Google)
    Dissertation title: *Anomaly Detection Through System and Program Behavior Modeling*
    External committee member: David Evans, University of Virginia

16. Hussain Almohri (Ph.D. '13, first job as an assistant professor at Kuwait University)
    Dissertation title: *High Assurance Models for Secure Systems*
    External committee member: Michael Hsiao, VT ECE

17. Huijun Xiong (Ph.D. '13, security engineer at Google)
    Dissertation title: *Secure Data Service Outsourcing with Untrusted Cloud*
    External committee member: Xinwen Zhang, Huawei Research US.

18. Saman Zarandioon (Ph.D. '12 from Rutgers University, Director of Engineering at Truveta, co-advised with Vinod Ganapathy)
    Dissertation title: *Improving the Security and Usability of Cloud Services with User-Centric Security Models*

GRADUATED M.S. STUDENTS

1. Sanjula Karanam (M.S., 2023), co-advised with Professor Haining Wang
   Thesis title: Ransomware Detection Using Windows API Calls & Machine Learning

2. Miles Frantz (M.S. '20, continue to pursue Ph.D.)
   Thesis title: Enhancing CryptoGuard's Deployability for Continuous Software Security Scanning

3. Emma Meno (M.S. '21)
   Thesis title: Neural Cryptanalysis for Cyber-Physical System Ciphers

4. Hannah Roth (M.S. '17, first position after graduation: MITRE Corp)
   Thesis title: Smartphone Privacy in Citizen Science

5. Alexander Kedrowitsch (M.S. '17, first position after graduation: instructor at West Point Academy)
   Thesis title: Deceptive Environments for Cybersecurity Defense on Low-power Devices

6. Daniel Barton (M.S. '16, first job at Lockheed Martin)
   Thesis title: Usable Post-classification Visualization for Android Collusion Detection and Inspection

7. Yipan Deng (M.S. '11, first job as an engineer at Intel)
   Thesis title: DeviceGuard: External Device-Assisted System and Data Security

8. Nitya H. Vyas (M.S., '10 from Rutgers University, first job as an engineer at VMTurbo)

   Thesis title: Usable Web 2.0 Privacy Management and Medical Imaging Search: An Ontology-Based Approach

SUPERVISED POSTDOC RESEARCHERS

1. Haipeng Cai (Postdoc '16, first job as a tenure-track assistant professor at Washington State University, Pullman)
2. Amiangshu Bosu (Postdoc '15, joined Wayne State University as a tenure-track assistant professor)

CURRENT PH.D. AND M.S. STUDENTS

1. Wenjia Song (Ph.D., joined the Ph.D. program in 2019)

   Tentative dissertation title: Deployable Data-driven Algorithms for Critical Detection Problems: From Healthcare to Cybersecurity Defenses

   External committee member: Brendan Saltaformaggio, Georgia Tech

2. Alexander Kedrowitsch (Ph.D., joined VT in 2022)

   Tentative dissertation title: Evolving Security Paradigms for Spacecraft and Networks: Metrics, Testbeds, and Scalable Solutions

   External committee member: Samuel Jero, Technical Staff, MIT Lincoln Laboratory

3. Tanmoy Sarkar Pias (Ph.D., joined VT in 2021)

   External committee member: Pearl Chiu, Fralin Biomedical Research Institute at VTC

   External committee member: Shalmali Joshi, Columbia University

4. Tahmina Sultana Priya (Ph.D., joined VT in 2023)

5. Mohimenul Karim (Ph.D., joined the Ph.D. program in 2021)

PROFESSIONAL LEADERSHIP ACTIVITIES

1. Leadership in supporting deployable and constructive security research:

   Steering Committee Chair of IEEE Secure Development Conference (SecDev), 2019 – 2022

   Steering Committee Member of Annual Computer Security Applications Conference (ACSAC), 2019 – Present

   Major conference organization: Lead Program Chair of *ACSAC* '20, program co-chair of *ACSAC* '19; Lead Program Chair of *IEEE SecDev* '18

   - I started the *Practitioners Session* in IEEE SecDev '18 – the first such call in IEEE or ACM security conferences – to bridge the gap between academic research and practical needs. IEEE SecDev is sponsored by the IEEE Computer Society's Technical Committee on Security and Privacy (TCSP). For ACSAC, I helped create the "Deployable and Impactful Security" hard topic theme, which ran for multiple years. I restarted the *IEEE Cybersecurity Award for Practice* to recognize high-impact contributions to bringing transformative cybersecurity defenses.

2. **Vice Chair** of ACM Special Interest Group on Security, Audit and Control (SIGSAC), 2021 – Present

   Executive Committee Member of ACM SIGSAC, 2017 – Present

   Secretary/Treasurer of ACM SIGSAC, 2017 – 2021

   My contributions as a SIGSAC leader include:

- **Research initiatives: Doctoral Symposium and CACM Highlights**
  I was instrumental in starting the first-ever doctoral symposium in the security research community, co-locating with ACM CCS 2024. I led the discussion at the community-wide SIGSAC business meeting, helped appoint the inaugural program chair, and persuaded SIGSAC executive committee to provide student travel funding. I was instrumental in creating the inaugural committee for selecting SIGSAC-conference papers to be highlighted by the high-impact *Communications of ACM* magazine.
- **Community building: iMentor, CyberW, and Women's Network Receptions**
  I was the founder and lead organizer of the NSF-sponsored Individualized Cybersecurity Research Mentoring (iMentor) Workshop, co-located with ACM CCS Conference 2020, 2021, and 2023. I was also the founder and lead organizer of the Women in Cybersecurity Research (CyberW) Workshop, co-located with ACM CCS 2017 and ACM CODASPY 2020. With my leadership, SIGSAC started regularly sponsoring Women's Networking Receptions at SIGSAC conferences.

3. **Program Co-organizer** of the 2024 NSF Secure and Trustworthy Cyberspace (SaTC) PI meeting, Pittsburgh, PA

   - I was instrumental in creating new types of PI meeting program activities, including dedicated sessions to highlight research and education projects, tutorials, and involving industry speakers.

4. **Steering Committee Member** of Network and Distributed System Security Symposium (NDSS), 2022 – Present

5. **Chair of award committees** for: ACM SIGSAC Outstanding Innovation and Contribution Awards evaluation '21; ACM SIGSAC Best Dissertation Awards evaluation '19

SELECT EDITORSHIPS

1. Associate Editor-in-chief of *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2023 – Present

2. Editorial board member for *ACM Digital Threats: Research and Practice*, 2018 – 2023

   I was instrumental in creating the *ACM DTRAP Special Issue on ACSAC 2019.*

3. Co-Guest Editor. *IEEE Security & Privacy Magazine Special Issue on ACSAC 2020.* Volume 19, Issue 6. Nov.-Dec. 2021.

4. Associate editor for *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2014 – 2018.

OTHER PROFESSIONAL ACTIVITIES

1. Member of award/fellowship committees for: IEEE Innovation in Societal Infrastructure Award Committee '24, IEEE Fellow evaluation '23; *ACM CODASPY* Lasting Research Award evaluation '22-Present; *ACM SIGSAC China* Awards evaluation '19 - '22; ACM SIGSAC Outstanding Innovation and Contribution Awards evaluation '22; NSF/CRA CSGrad4US Fellowship evaluation '24, NCWIT '16, Grace Hopper Conference Scholarship '14

2. Workshop/panel organization: Founder and organizer of ACM SIGSAC Individualized Cybersecurity Research Mentoring (iMentor) Workshop, co-located with ACM CCS Conference '23, '21, and '20; Program co-chair for *ASIACCS Workshop on Security in Cloud Computing (SCC '15)*; Panel co-chair for *SecureComm '16*

3. Served as a panelist/proposal reviewer for: NSF panelist (many times, including SaTC/OAC CAREER panels); Vienna Science and Technology Fund '23; Research Grants Council (RGC) of Hong Kong 2017-2024; AAAS International Grant Review Program '19; University of Toledo '18; Israeli Ministry of Science, Technology and Space '17; AAAS Research Competitiveness Program '17; Department of Mathematics of the University of Padova, Italy '16; VCU CAREER Academy '16

4. Technical Program Committee member for:

   ACM CCS HealthSec Workshop '24, *ACM WiSec '24*, *ACNS SCI (Secure Cryptographic Implementation) Workshop '23*, *ACM SACMAT '22* Blue-sky/Vision Track (Chair), *ACM CCS '22*, *USENIX Security '22*, *NDSS '21*, *ICSE '21*, *ACM CODASPY '21*, *The Web Conference '21*, *IEEE Security & Privacy Symposium '20*, *ACM CCS '19*, *IEEE Security & Privacy Symposium '19*, *NDSS '19*, *WWW '19*, *ACM WiSec '19*, *IEEE SecDev '19*, *12th USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, *ACM CCS '18*, *ACSAC '18*, *ACM ASIACCS '18*, *IEEE DSN '18* Fast Track, *IEEE Security & Privacy Symposium '18*, *IEEE ICDCS '18*, *HotSoS '18*, *ACM CODASPY '18*, *ACM ASIACCS CPSS Workshop '18*, *SECURECOMM '18*, *SALAD Workshop '18*, *ACM WiSec '18*, *ACSAC '17, ACM WiSec '17, DSN '17, IEEE ICDCS '17, ACM CODASPY '17, ICCCN '17, ACM ASIACCS '17, ACM ASIACCS SCC Workshop '17, ACM CCS MIST Workshop '17, ACM CCS SafeConfig Workshop '17, ACM CCS FEAST Workshop '17, IEEE CNS NCF Workshop '17*, *ACM CCS '16*, *SECURECOMM '16*, *ACSAC '16*, *ACM ASIACCS '16*, *ACM CODASPY '16*, *ACM CCS MIST Workshop '16*, *IEEE CNS '16*, *Smart City Security and Privacy Workshop (SCSP-W '16)*, *IEEE CloudCom '15*, *ACSAC '15*, *ACM CCS '15 IEEE CNS '15*, *Inscrypt '15*, *NSS '15*, *ACM CCS MIST Workshop '15*, *IEEE ICC '15 CISS*, *IEEE CCNS '15*, *ACM ASIACCS '15 ACSAC '14*, *ACM CCS '14*, *Inscrypt '14*, *SecureComm '14*, *ICCCN MobiPST '14*, *GLOBECOM CISS '14*, *ACM SACMAT '14*, *ACM ASIACCS '14*, *ACM CODASPY '14*, *MIST Workshop '14*, *Inscrypt '13*, *IEEE CNS '13, ACNS '13, ACM ASIACCS '13, ACM CODASPY '13, ISC '13, IEEE GLOBECOM '13, SecureComm '13, SESP '13, MIST '13 ACM ASIACCS '12, ACNS '12, SecureComm '12, ICCS '12, SECRYPT '12, ISPEC '12, SecureComm '11, WPES '11, GLOBECOM '11, CollaborateCom '11, IFIPTM '11, CSA '11, IPDPS '11, MobilPST '11, WWW '10, IEEE CANS '10, GLOBECOM '10, CollaborateCom '10, IEEE ICCCN '10, IFIPTM '10, WWW '09, IEEE ICCCN '09, CollaborateCom '08, ACM SAC '07, IEEE PADM '07.*

5. Journal/book chapter reviewer for *Nature Communications* in 2024, *ACM Computing Surveys*, *Computers & Security*, *IEEE Transactions on Software Engineering (TSE)*, *ACM Digital Threats: Research and Practice (DTRAP) ACM Transactions on Embedded Computing Systems*, *Proceedings of IEEE*, *IEEE Transactions on Dependable and Secure Computing* (TDSC), *IEEE Transactions on Information, Forensics and Security (TIFS)*, *ACM Transactions on Information and System Security (TISSEC)* renamed to *ACM Transactions on Privacy and Security (TOPS)*, *IEEE Systems Journal*, *IEEE Access*, *ACM Transactions on Computer-Human Interaction*, *International Journal of Computer Mathematics*, *Journal of Computer Security*, *Computer Communications*, *IEEE Transactions on Knowledge and Data Engineering*, *IET Information Security*, *British Journal of Mathematics & Computer Science*, *Journal of Biomedical Informatics*, *IEEE Transactions on Services Computing*, *Wireless Networks*, *Mobile Networks and Applications*, *Knowledge and Information Systems*, *Data & Knowledge Engineering Journal*, *Journal of Information Processing*, *IEEE Journal on Selected Areas in Communications*, *Journal of Systems and Software*, *IEEE Internet Computing*, Book chapter review for *Algorithm Design and Applications* (Wiley).

OTHER PRESENTATIONS

1. Navigating Early Career Challenges in Academia. Panel moderator. ACM CCS 2024.

2. Data Breach, Pegasus, and Ransomware: Making Sense of Cybersecurity Risks. Qatar Women In Data Science; Zhejiang University. 2021-2022.

3. Be Developers' Friends: Experiences from Deployment-grade Tool Development and AI-based Code Generation. Shandong University College of Computing, UW-Madison. 2021.

4. Security Roundtable Discussion. Semiconductor Research Corporation (SRC) Spring Tech Forum. Panelist. 2021.

5. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. IEEE ICDE WiDS Workshop '20, SKM Panel '21, NCWIT Virginia '19.

6. How to efficiently and effectively bring safety and security into software and system development? ICSSP, co-located with ICSE. Panelist. Gothenburg, Sweden. 2018.

7. Small Mistakes in Code, Giant Vulnerabilities in Society: Gaps and Some Solutions for Secure Software Development. City University of Hong Kong. Tsinghua University. 2017.

8. Program Anomaly Detection with Near-zero False Alarms. Penn State University. 2016.

9. Precise Modeling of Benign Program Behaviors for Proactive System Defense. Texas A&M University. 2014.

10. Storytelling Security: Causal-Analysis for Proactive Defense. Grace Hopper Conference (GHC). 2014. Phoenix, AZ.

11. User-Intention Based Anomaly Detection and Malware Analysis. Verisign Labs, University of California, Irvine, KSU. 2012-2013.

12. Scalable Data-Loss Prevention Techniques. RackSpace. Blacksburg VA. 2011.

13. Host-Based Anomaly Detection Based on User Activities. Georgia Tech, UNC Chapel-Hill. 2010.

14. Host-Based and User-Centric Approaches for Detecting Drive-By-Download Attacks. Computer Science Departmental Seminar. Stevens Institute of Technology, Rutgers DIMACS Fall Mixer, NJIT, VT. 2008 - 2009.

15. Compact and Anonymous Role-Based Authorization Chains. *NIST Workshop on Applications of Pairing Based Cryptography: Identity-Based Encryption and Beyond.* NIST, Gaithersburg, MD. 2008.

16. Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. *DIMACS Workshop on Data Privacy.* Rutgers University. 2008.

STUDENT AWARDS AND HONORS

Alex Kedrowitsch, Walts Fellowship, VT CS	2024
Tahmina Sultana Priya, Pratt Fellowship, VT CS	2024
Miles Frantz, Richard E. Nance Graduate Fellowship '23 and '24, Finalist for the Graduate Education Award '22, VT CS	
Wenjia Song, Dennis G. Kafura Graduate Fellowship, VT CS	2023
Ming Zhu, Best CCI Poster Presentation Award	Apr. 2023
Tanmoy Sarkar Pias, BitShares Fellowship	2021-2022
Ya Xiao, Inaugural Dennis G. Kafura Fellowship '21-'22, Pratt Fellow '21, BitShares Fellowship '19, VT CS	
Emma Meno, New Horizon Scholarship, VT ICTAS	2020
Sazzadur Rahaman, BitShares Fellowship, VT CS	2018
Long Cheng, Pratt Fellowship, VT CS	2017
Xiaokui Shu, Outstanding Ph.D. Student Award, VT CS	2016
Xiaokui Shu, Best Poster Award, ACM CODASPY	Mar. 2015
Karim Elish, First Place in VT CS Graduate Research Competition	2012, 2014
Finalist for VT COE Torgersen Graduate Research Award: Emma Meno '22, Sazzadur Rahaman '21, Karim Elish '14, Hussain Almohri '13	
Casey Link, VTURCS Best Poster Award	Apr. 2011
Brian Thompson, DHS DyDAn Fellowship	Jan. 2009 - Aug. 2011
Deian Stefan, Botnet Biometrics Work Featured in NSF Highlights	Jan. 2009

SELECT UNDERGRADUATE RESEARCH STUDENTS

Lifan Ren ('22) on reverse engineering and analyzing ransomware
Alex Owens ('23) on characterizing and detecting advanced persistent threats (APTs)
Karla Estrada ('22) on developing lightweight plugins for development-time code screening
Punita Verm ('21) on developer friendly solutions for Java cryptographic code screening
Lin Zhang ('20) on developing drone technology for supporting smart farms.
Zishuai Li ('20) on CryptoGuard deployment
Chengkai Yao ('20) on autonomous drones for smart farms
Deepti Suresh ('19-'20) on AI ethics and fairness
Aparna Ganesh ('20) on the history of trusted execution
Zachary Burch ('15) on proof-of-concept collusion malware in Android
Adrianne Williams (NSF REU '15) on accuracy comparison of anti-virus tools
Allison Hatch (NSF REU '15) on the usability evaluation of intrusion detection tools
Lance Chao ('14-'15) on Java string analysis for Android collusion detection
Hannah Roth ('14-'16) on improving the usability of program anomaly detection in IoT
Andrew Ciambrone (NSF REU '14) on big data analysis for early network detection
Zack Morris ('14) on repackaged Android malware analysis
Joshua Martin ('13) on Android rootkits and their defenses
Samantha Puckett ('13) on data leak protection in Android
Antuan Byalik ('12) on a cyber game system for user authentication and behavior study.
Laurel Schaefer (NSF REU '12) on social science and cyber security
Brendan Avent ('11, '12) on a low-cost DNS-tunneling-based location tracking
Scott Luxenberg ('11) on a low-cost DNS-tunneling-based location tracking system
Casey Link ('11) on development of a game system for security education
William Matt Banick ('10) on user-intention based traffic dependency study
Alexander Crowell (DIMACS REU '09) on detection of drive-by-download attacks
Anitra Babic (DIMACS REU '09) on email-activity based authentication
Prateek Malhotra ('08) on parallel universe design of network traffic prediction for anomaly detection
Deian Stefan (DIMACS REU '08) on keystroke dynamic authentication

SELECT UNIVERSITY/DEPARTMENT SERVICES

Chair of Personnel Committee (Promotion & Tenure), VT CS 2022 - Present
Member of Personnel Committee (Promotion & Tenure), VT CS 2019-2022, 2016 - 2017
Board Member, Commonwealth Cyber Initiative (CCI) Southwest VA Stakeholder Board, 2021 – Present
Stakeholder & Curriculum Development Committees, Integrated Security initiative 2016 - 2020
Faculty/Department Head Search Committee, VT CS 2023-2024, 2019-2020, 2018-2019 (VT AOE), 2016-2018, 2010-2015, 2014-2015 (co-chair), 2011-2012 (VT ECE)
ECE/CS Course Certification of NSA's Center of Academic Excellence for Cyber operations 2016
ECE/CS joint cyber security curriculum development 2011-2014
Graduate Program Committee, VT CS 2016-2017, 2014-2015
Graduate Admission Committee, VT CS 2011-2014
Qualifier Exam Committee, VT CS 2013-2014, 2012-2013 (Chair), 2011-2012
Engineering Faculty Organization Executive Committee, VT COE 2017-2019
Publicity and Awards Committee, Rutgers CS 2008-2009
Admission Committee, Rutgers CS 2008-2009

OTHER OUTREACH/DIVERSITY ACTIVITIES

Member, Virginia Tech APIDA Caucus 2021 - Present
Presentation: Career Success, Race Education, and Support Systems. Invited talk. VT Asian Cultural Engagement Center (ACEC), Learning Lunch Series. 2021
Advised high school students on cybersecurity projects 2021, 2015, 2013
Meet and Greet with VT Asian American Student Union 2019
Women in Computing Day (80+ middle school girls), VT CS 2019

Presented at the Blacksburg ACM local chapter	2018
Lectures and activities at Imagination Camps for middle school students, VT	2012
Exhibition at Kids' Tech, VT	2012
Presenter for C-Tech^2 High School Girls Summer School	2011
Presented at recruiting events, Women's Preview Weekend, VT COE	2010-2014
Served as an e-mentor in Rutgers University Women in Engineering Leadership League	2008-2009