DANFENG (DAPHNE) YAO

RESEARCH INTERESTS

Software and system security, including deployable security, security measurement, secure coding, anomaly detection in systems and programs;

All aspects of enterprise-grade data loss prevention;

Data science and machine learning in biology, medicine, and medical information.

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 Jun. 2019 – Present
Professor
Elizabeth and James E. Turner Jr. '56 Faculty Fellow and CACI Faculty Fellow

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

No. 1 most downloaded article for WIREs Data Mining and Knowledge Discovery in 2019
Nominated for the NSA Best Scientific Cybersecurity Paper Competition Apr. 2020
ACM Distinguished Member for Outstanding Scientific Contributions to Computing Nov. 2018
IEEE Excellence in Service Award by Computer Society's TC on Security & Privacy Oct. 2018
Top 25 most downloaded article of the IEEE Signal Processing Society in 2018
Dean's Faculty Fellow, Virginia Tech CoE Dec. 2017

Elizabeth and James E. Turner Jr. '56 Faculty Fellowship, Virginia Tech CoE	Apr. 2016
CACI Faculty Fellow	Oct. 2014
Young Investigator Award, Army Research Office	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	*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. (Filed by HP Labs.)

2. Danfeng Yao, Deian Stefan, and Chehai Wu. Systems and Methods for Malware Detection. U.S. Patent No. 8,763,127. Jun. 2014. (Filed by Rutgers University.)

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. (Filed by Virginia Tech.)

4. Danfeng Yao and Salman Ahmed. Probabilistic Evidence Based Insider Threat Detection and Reasoning. Provisional Patent Application No. 63/038,308. June 12, 2020.

INVITED TALKS/TUTORIALS/PANELS

1. 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. **Tutorial.**

2. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. PrivacyCon 2020. Federal Trade Commission (FTC). July, 2020.

3. 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.**

4. 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.

5. Impostor Syndrome and What Researchers Need to Know. Research Methods in Chemical Engineering. Virginia Tech. Apr. 2020. **Invited guest lecture.** Video available: `https://youtu.be/JqFKv9Rg0k8`

6. Data Breaches and Multiple Points to Stop Them. Brown University, Executive Masters Program in Cybersecurity (EMCS). Providence, RI. Oct. 2019. **Keynote.**

7. Data Breaches and Multiple Points to Stop Them. IEEE Signal Processing Society Webinar. Sept. 2019.

8. Measurable Security in Software and Systems. ACM Turing Celebration SIGSAC China. Chengdu, China. May 2019. **Keynote**.

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

10. Data Breach and Multiple Points to Stop It. ACM Symposium on Access Control Models and Technologies (SACMAT). Indianapolis, IN. **Keynote**. Jun. 2018.

11. How to efficiently and effectively bring safety and security into software and system development? *International Conference on Software and System Processes (ICSSP), co-located with ICSE.* **Panelist**. Gothenburg, Sweden. May 2018.

12. Human Element in Security. ISDA/Hume colloquium. **Panelist**. Apr., 2018.

13. Small Mistakes in Code, Giant Vulnerabilities in Society: Gaps and Some Solutions for Secure Software Development. City University of Hong Kong. Tsinghua University, Shenzhen. **Invited Seminars**. Dec. 2017.

14. Democratize Anomaly Detection Technologies: Challenges, Advances, and Opportunities. Cyber Security & Information Systems Information Analysis Center (CSIAC). **Invited Webinar.** May 2017.

15. Democratize Anomaly Detection Technologies: Challenges, Advances, and Opportunities. INRIA Rennes, France. Apr., 2017. **Invited Talk.**

16. Democratize Anomaly Detection Technologies: Challenges, Advances, and Opportunities. **Departmental Seminar.** University of Virginia, Department of Computer Science. Apr., 2017.

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

18. Program Anomaly Detection: Methodology and Practices. Xiaokui Shu and Danfeng Yao. Vienna, Austria. Oct. 2016. **ACM CCS Tutorials.**

19. Program Anomaly Detection with Near-zero False Alarms. Penn State University Computer Science and Engineering. State College, PA. **Departmental Seminar**. Sept. 2016.

20. Precise Modeling of Benign Program Behaviors for Proactive System Defense. Apr. 2014. Texas A&M University. College Station, TX. **Departmental Seminar.**

21. User-Intention Based Anomaly Detection. Department of Computer Science. Kansas State University. Apr. 2013. **Departmental Seminar.**

22. User-Intention Based Anomaly Detection. Department of Computer Science. University of California, Irvine. Feb. 2013. **Departmental Seminar.**

23. User-Intention Based Anomaly Detection. Tianjin University, Tianjin China. College of Computing. Jun. 2012. **Invited Talk.**

24. User-Intention Based Anomaly Detection and Malware Analysis. Verisign Labs. Reston, VA. Jul. 2012.

25. Fuzzy Fingerprinting for Privacy-Aware Data-Loss Prevention. Huawei America Research Center. Santa Clara, CA. Jul. 2011.

26. Scalable Data-Loss Prevention Techniques. RackSpace Hosting Inc. Blacksburg VA. Mar. 2011.

27. Host-Based Anomaly Detection Based on User Activities. Georgia Tech Information Security Center (GTISC), UNC Chapel-Hill Department of Computer Science. Apr. 2010.

28. Keystroke Dynamic Authentication with Trusted User Inputs for Human-Behavior Driven Bot Detection. Purdue University Computer Science, West Lafayette, IN. Mar. 2009. **Departmental Seminar**.

TEACHING

Virginia Tech Computer Science Department

CS/ECE 4264 Principles of Computer Security. Fall 2020, Fall 2015, 2014, 2013

CS/ECE 5590 System and Application Security. Spring 2020, Spring 2017

CS/PSCI/BIT 2984 Foundations of Security Environments, co-teach) Spring 2020, Fall 2019, Spring 2018, Fall 2018

I am instrumental in creating and co-teaching this integrated security destination area (ISDA) gateway course, as well as a new ISDA capstone course and a new pathway minor (approved).

CS 6204 Cyber-physical Systems (CPS) Security, Spring 2019

CS 6204 Program Anomaly Detection with Learning. Fall 2016

CS/ECE 5984 System and Application Security. Spring 2015

I created CS/ECE 5984 (permanent course number CS/ECE 5590), which is the first graduate-level system and application security course at VT.

CS6204 Recent Advances in System and Application Security. Spring 2014

I created CS/ECE 4264, which is a core course of the College of Engineerings Cybersecurity minor.

CS4984 Introduction to Computer Security. Fall 2012, 2011, 2010

CS3114 Data Structures and Algorithms. Spring 2012

CS6204 Recent Advances in Cyber Security. Spring 2012

CS5984 Theory and Practice of Web Security and Privacy. Spring 2011

CS6204 Advanced Computer Security and Privacy Spring 2010

Rutgers University Computer Science 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

Total funding amount: $9.63 million. Total personal share: $4.33 million.

EXTERNAL GRANTS

1. 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.

2. *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.

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

4. 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.

5. *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 - Present. Awarded amount: $973,500 (as of May 2017).

6. *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.

7. *National Science Foundation (NSF).* REU Supplemental Fund. $16,000. PI: Danfeng Yao. $16,000. Apr. 2012 - Mar. 2013. Personal share: $16,000.

8. 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.

9. *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.

10. *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.

11. *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.

12. 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.

13. 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.

14. National Science Foundation CRISP program. CRISP Type 2: Collaborative Research: Towards Resilient Smart Cities. Walid Saad (PI) (VT ECE), Danfeng Yao is among the VT co-PIs. $1,100,000. Personal share: $206,347. Jan. 2016 - Dec. 2019.

15. *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.

16. National Science Foundation (NSF). CSR:Large:VarSys:Managing variability in high-performance computing systems. PI: Kirk Cameron. Danfeng Yao is among the co-PIs. $2,379,556. 09/01/2016 - 09/30/2020. Personal share: $390,000.

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

18. Office of Naval Research (ONR). Data-driven Vulnerability Repair in Programs with a Cloud Analytics Architecture for Practical Deployment. $1,200,000. PI: Danfeng Yao, co-PI: Trent Jaeger (PSU) and Na Meng (VT). 07/01/2017 – 06/30/2020. Personal share: $612,838.

19. 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.

20. 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.

21. 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. Personal share: $0.

22. 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 – 09/30/2023. Personal share: $500,000.

23. Office of Naval Research (ONR). Supplement to Support IEEE Secure Development Conference. $5,000 in 2020 and $5,000 in 2018. Personal share: $0.

24. National Science Foundation (NSF) SaTC program. iMentor Workshop at the ACM CCS. $15,000. PI: Danfeng Yao. 01/01/2020 - 12/31/2022. Personal share: $0.

INTERNAL FUNDS AND GIFTS

1. *Rutgers University Pervasive Computing Initiative.* Secure and Flexible Information Sharing for Crisis Communication in Pervasive Computing Environments. PI: Danfeng Yao. Co-PI: James Garnett. $50,000. Mar. 2008 - Feb. 2009. Personal share: $40,000.

2. *Rutgers University Academic Excellence Fund.* The Rutgers University Research Initiative on Cybersecurity Economics (RICE). PI: Rebecca Wright. Co-PIs: Vijay Atluri, Richard McLean, and Danfeng Yao. $60,000. Jun. 2009 - May 2010. Personal share: $15,000.

3. *Virginia Tech.* College of Engineering CAREER Incentive Grant. PI: Danfeng Yao. $16,000. Apr. 2010 - 2015.

4. *Virginia Tech ICTAS.* Novel Games for Analyzing Cyber-Security Behaviors: An Interdisciplinary Approach. $60,000. PI: Danfeng Yao. Co-PI: Scott Geller and Manuel Perez-Quinones. Jul. 2011 - Jun. 2012. Personal share: $45,000.

5. *Virginia Tech.* Department of Computer Science Incentive Program. PI: Danfeng Yao. $3,000. 2013.

6. *L-3 Communications via HUME Center.* Causality-Based Traffic Reasoning Methodology for Proactive Network Defense and Mission Assurance. PI: Danfeng Yao. $40,900. Apr. 2014.

7. *Virginia Tech.* Eminent Scholar Supplement through CACI Faculty Fellowship. PI: Danfeng Yao. $5,000 per year. Sep. 2014 - present.

8. *Virginia Tech.* College of Engineering YIP Incentive Grant. PI: Danfeng Yao. $6,000. Jan. 2015 - Jan. 2017.

9. *Virginia Tech.* College of Engineering Incentive Grant for Expanding Graduate Enrollment. PI: Danfeng Yao. $34,000. Sep. 2014 - May 2015.

10. *Virginia Tech.* Department of Computer Science Incentive Program. PI: Danfeng Yao. $3,000. 2015.

11. *Virginia Tech.* Eminent Scholar Supplement through Turner Faculty Fellowship. PI: Danfeng Yao. $5,000 per year. Apr. 2016 - present.

12. *Virginia Tech.* Department of Computer Science Incentive Program. PI: Danfeng Yao. $50,000. Aug. 2016 - Present.

13. *Virginia Tech.* Department of Computer Science Incentive Program. PI: Danfeng Yao. $7,000. 2017.

14. *Virginia Tech.* College of Engineering's Dean's Faculty Fellowship. PI: Danfeng Yao. $5,000 per year. May 2018 - April 2021.

15. From *Northrop Grumman* to support undergraduate research in cyber security. PI: Danfeng Yao. $10,000 in 2010, $10,000 in 2011, $5,000 in 2012, 2013, 2014. Personal share: $35,000.

16. *Virginia Tech.* College of Agriculture and Life Sciences (CALS). Establishment of SmartFarm Innovation Network Nodes at Middleburg and Shenandoah Valley Agricultural Research and Extension Centers. PIs: Robin White (Animal and Poultry Sciences) and Vitor Mercadante (Animal and Poultry Sciences). Danfeng Yao is among the Co-PIs. $350,000. Personal share: $40,000. Sept. 2019 – Aug. 2021.

17. *Virginia Tech.* Provost's Office. Democratization of Data Breach and Data Loss Prevention Technologies and Knowledge. PI: Danfeng Yao. Co-PI: Tabitha James (BIT), Tanu Mitra, Bimal Viswanath, and Idris Adjerid (BIT). $20,000. Personal Share: $10,000. Nov. 2019 – Jun. 2020.

18. *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. Personal Share: $12,500. Jun. 2020 – Dec. 2020.

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

SELECT LEADERSHIP ACTIVITIES

1. **Lead program chair of *Annual Computer Security Applications Conference (ACSAC)* 2020 and program co-chair of ACSAC 2019.** I was instrumental in choosing the "Deployable and Impactful Security" hard topic theme for ACSAC '19 and '20, as well as substantially increasing the number of female PC members. I am also on the steering committee of ACSAC (2019 – present).

2. **Steering Committee Chair of IEEE Secure Development Conference (SecDev), Nov. 2019 – Present.** *IEEE SecDev* is organized by IEEE Computer Society's Technical Committee on Security and Privacy (TCSP).

   Lead program chair of *IEEE SecDev* 2018. As the lead PC chair I started a new *Practitioners Session* in SecDev '18 – the first such call in IEEE or ACM security conferences – to bridge the gap between academic research and practical needs in the government and industry. The practitioner session program committee consisted of 20 security experts, mostly from the industry and government sectors. I expanded the size of the regular research program committee from 27 to 40 members. I was instrumental in inviting two female keynote speakers.

3. **Founder of an NSF-sponsored iMentor Workshop aiming to nurture the long-term research interest and commitment in young underrepresented researchers.** The Individualized Cybersecurity Research Mentoring (iMentor) Workshop co-locates with the ACM CCS Conference starting from 2020.

4. **Founder of the *Women in Cybersecurity Research (CyberW) Workshop*, co-located with *ACM CCS* 2017 and *ACM CODASPY* 2020.** CyberW was the first research-oriented venue to promote female cybersecurity research leaders and call for advancing females to senior and leadership positions.

   In CyberW '17, I raised $65,000 to cover for the travel grants of the participants. A total of 51 people received travel grants. There were 70 workshop attendees. I invited 7 top security experts to give keynote speeches.

   CyberW '20 starts a new Early Career award for recognizing early career female cybersecurity researchers (5 years post Ph.D. graduation).

5. **ACM SIGSAC Secretary/Treasurer, 2017 – Present.**

   ACM SIGSAC Executive Committee Member, 2017 – Present.

   My SIGSAC leadership vision is to help encourage and advance female researchers and others from underrepresented groups in cybersecurity, which has been traditionally a male-dominated field. In addition, my goal is to ensure SIGSAC gives back to the community by generously supporting the ACM SIGSAC sponsored conferences, awards, and other outreach and inclusive excellence causes.

   Some of the inclusive excellence initiatives that I started in SIGSAC include: CyberW workshops (at CCS '17 and CODASPY '20), CCS women's networking reception, and iMentor workshops (to kick off in ACM CCS 2020).

   Chair of ACM SIGSAC Committee for the Best Dissertation Awards 2019.

6. **University-wide Stakeholder Committee and Curriculum Development Committee**, Virginia Tech Integrated Security Destination Area (ISDA) 2016 - Present

   ISDA is a large university-wide interdisciplinary initiative. I closely work with a diverse group of faculty from multiple colleges and coordinate with stakeholder departments to create new non-major courses and multiple minor programs, as well as DA-related faculty hiring.

7. **Associate Director of the stack@cs Center for Computer Systems** at Virginia Tech 2017 – Present.

   The stack@cs Center for Computer Systems tackles challenging problems that transcend any single component of the application software and architecture stack. As an associate director, I coordinate and participate in large-scale research and education projects, organize faculty and student events, contribute to the center's personnel and finance management.

8. **Associate editor** for *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Jul. '14 – Aug. '18.

9. **Editorial board member** for *ACM Digital Threats: Research and Practice*, Feb. '18 – Present.

SELECT MEDIA REPORTS

1. CryptoGuard work was featured in Communications of the ACM. Jul. 2020.

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

2. Slashdot, UK's Register, Linux.com and Helpnet Security on our Java secure coding research. Oct. 2017.

   `https://www.theregister.co.uk/2017/09/29/java_security_plagued_stack_overflow/`

   `https://slashdot.org/story/17/10/07/022216`

3. TechXplore on data-oriented attacks and defenses. Mar. 2019.

   `https://techxplore.com/news/2019-03-exploitation-techniques-defenses-dop.html`

4. Wiley's Advanced Science News featured my invited review article on enterprise data breach. `http://www.advancedsciencenews.com/enterprise-data-breach-causes-challenges-prevention-future-directions/` Oct. 2017.

5. New Scientist, ACM Technews, International Business Times, and many others on Android malware collusion work (in ASIACCS '17). Apr. 2017.

6. Featured news in Communications of the ACM on program anomaly detection. Jan. 2016.

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

7. HPC Wire, Government Security News on detecting stealth attacks with program anomaly detection. Oct. 2015.

8. An article from Science on Yao's NSF CAREER Award. Malware and search engines: Lamar Smith goes far afield in his latest hit list of NSF grants. Written by Jeffrey Mervis. Feb., 2015.

   `http://www.sciencemag.org/news/2015/02/malware-and-search-engines-lamar-smith-goes-far-afield-his-latest-hit-list-nsf-grants?rss=1`

9. Computer World, TMC Net, IT Weekly Newsletter on causality-based insider threat detection. Oct. 2014.

10. Data-leak detection research highlight by Software Security Engineering Research Center (S2ERC), an NSF I/UCRC. Aug. 2014.

11. NSF, HPC Wire, Examiner, Federal Computer Week on network traffic causality reasoning for detecting stealthy malware activities. Jun. 2014.

12. Phys.org, and Supercomputing Online on quantitative anomaly detection and award-winning network traffic analysis work. Mar. 2013.

13. International Business Times, Homeland Security News Wires, PHYSORG (United Kingdom) on our award-winning keystroke dynamic security work. Nov. 2010.

14. NSF news, ACM Technews, and many others on our activity-based authentication. Nov. 2009.

GRADUATED STUDENTS AND POSTDOCS

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

   Thesis 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

2. 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

3. Miles Frantz (M.S. '20, continue to pursue Ph.D.)

   Thesis title: Enhancing CryptoGuard's Deployability for Continuous Software Security Scanning

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

   Thesis 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

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

   Thesis title: Program Anomaly Detection Against Data-oriented Attacks

   External committee member: Raheem Beyah, Georgia Tech

6. Haipeng Cai (Postdoc '16, first job as a tenure-track assistant professor at Washington State University, Pullman)

7. Amiangshu Bosu (Postdoc '15, joined Wayne State University as a tenure-track assistant professor)

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

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

   External committee member: Gang Tan, Penn State University

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

   Thesis title: Mining Security Risks from Massive Datasets

   External committee member: Dongyan Xu, Purdue University

10. Xiaokui Shu (Ph.D. '16, first job at IBM Research T. J. Watson Center)

    Thesis title: Threat Detection in Program Execution and Data Movement: Theory and Practice

    External committee member: Trent Jaeger, Penn State University

11. Hao Zhang (Ph.D. '15, first job as a security engineer at the DB security group of Oracle)

    Thesis title: Discovery of Triggering Relations and Its Applications in Network Security and Android Malware Detection

    External committee member: Xinming Ou, Kansas State University

12. Karim Elish (Ph.D. '15, assistant professor at Florida Polytechnic University)

    Thesis title: User-Intention Based Program Analysis for Android Security

    External committee member: Xuxian Jiang, North Carolina State University

13. Kui Xu (Ph.D. '14, security engineer at Google)

    Thesis title: Anomaly Detection Through System and Program Behavior Modeling

    External committee member: David Evans, University of Virginia

14. Hussain Almohri (Ph.D. '13, first job as an assistant professor at Kuwait University)

    Thesis title: High Assurance Models for Secure Systems

    External committee member: Michael Hsiao, VT ECE

15. Huijun Xiong (Ph.D. '13, security engineer at Google)

    Thesis title: Secure Data Service Outsourcing with Untrusted Cloud

    External committee member: Xinwen Zhang, Huawei Research US.

16. Saman Zarandioon (Ph.D. '12 from Rutgers University, coadvised with Vinod Ganapathy, software engineer at Amazon Inc.)

    Thesis title: Improving the Security and Usability of Cloud Services with User-Centric Security Models

17. Hannah Roth (M.S. '17, first position after graduation: MITRE Corp)

    Thesis title: Smartphone Privacy in Citizen Science

18. 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

19. Daniel Barton (M.S. '16, first job at Lockheed Martin)

    Thesis title: Usable Post-classification Visualization for Android Collusion Detection and Inspection

20. Yipan Deng (M.S. '11, first job as an engineer at Intel)

    Thesis title: DeviceGuard: External Device-Assisted System and Data Security

21. 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

CURRENT PH.D. AND M.S. STUDENTS

- Ya Xiao (Ph.D., joined VT in 2017)

  Tentative thesis title: *Automatic Secure Code Generation with Reusable Representation Learning*

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

- Salman Ahmed (Ph.D., joined VT in 2017)

  Tentative thesis title: *Quantitative Measurements and Methodologies for Attack Surface Reduction*

  External committee member: Fabian Monrose, University of North Carolina at Chapel Hill

- Sharmin Afrose (Ph.D., joined VT in 2018)
- Miles Frantz (Ph.D., joined VT in 2018)
- Wenjia Song (Ph.D., joined VT in 2019)
- Emma Meno (M.S., joined VT in 2019)

PUBLICATIONS

* indicates Yao's student or postdoc.
Google Scholar: `http://scholar.google.com/citations?user=v0bzUvMAAAAJ&hl=en`

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`

JOURNALS

2. Yuan Luo, Long Cheng, Hongxin Hu, Guojun Peng, and Danfeng Yao. Context-rich Privacy Leakage Analysis through Inferring Apps in Smart Home IoT. *IEEE Internet of Things Journal*. Aug. 2020. (Impact factor: 11.70)
3. 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)
4. 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)
5. 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)
6. 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)*. 2019. (Impact factor: 6.40)
7. 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)*. 2019. (Impact factor: 6.40)
8. 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)
9. 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.
10. 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 article of 2019 for WIREs DMKD.** `http://wires.wiley.com/WileyCDA/WiresCollection/id-49.html`

11. 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)

12. 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)

13. 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) Shorter version received **Best Poster Award at ACM CODASPY '15.**

14. 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 2018.**

15. 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)

16. 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)

17. 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)

18. 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)

19. 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)

20. 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.**

21. 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)

22. 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)

23. 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.

24. 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.

25. 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.**

26. 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)

BOOK CHAPTERS

27. 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.

28. 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 MAGAZINES

29. Danfeng Yao. Impostor Syndrome and What Researchers Need to Know. *Communications of the ACM (CACM).* Under Review. Jul. 2020.

PEER-REVIEWED CONFERENCES/WORKSHOPS

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

31. 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.

32. 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.

33. 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.

34. 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. Jul. 2020.**

35. 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.**

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

37. 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%)

38. 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%)

39. 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%)

40. 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%)

41. 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%)

42. 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.**

43. 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%)

44. 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.

45. 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.

46. 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.

47. 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%)

48. 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%)

49. 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%)

50. 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.**

51. 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%)

52. 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. Invited for Best Paper Competition at Cyber Security Awareness Week (CSAW).**

53. 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%.)

54. 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%)

55. 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%).

56. 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.**

57. 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%.)

58. 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.**

59. 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%.)

60. 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%)

61. 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%)

62. 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.

63. 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.**

64. 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%)

65. 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%)

66. 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%).

67. 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%).

68. 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%). **Patent Granted.**

69. 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%).

70. 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%).

71. 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%)

72. 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.

73. 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%).

74. 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%).

75. 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.* San Francisco, CA. May 2012.

76. 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*. San Francisco, CA. May 2012.

77. 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)*. San Antonio, TX. Feb. 2012. (Acceptance rate: 25%).

78. 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)*. San Antonio, TX. Feb. 2012. (Acceptance rate: 25%).

79. 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%).

80. 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%).

81. 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.

82. 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%)

83. 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%).

84. 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)*. Chicago, IL. Nov. 2010. **Best Paper Award.** (Acceptance rate: 38%).

85. 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.**

86. 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)*. 24-35. Apr. 2010. Beijing, China. (Acceptance rate: 23%).

87. 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%).

88. 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%).

89. 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.**

90. 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.

91. 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%).

92. 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.

93. 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%).

94. 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.**

95. 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%).

96. 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.

97. 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.

98. 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)*. Pages 353-362. Mar. 2008. (Acceptance rate: 25.2%).

Below are publications from Ph.D.

99. 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.* Moncton, New Brunswick, Canada. Jul. 2007.

100. 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 '07)*. 93-94. Redondo Beach, CA. Jul. 2007.

101. 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 '07)*, Special Track on Web Technologies. 1654-1661. ACM Press. Seoul, Korea. Mar. 2007.

102. 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 '06)*. LNCS 4307, pages 190-209. Springer. Raleigh, NC. Dec. 2006. **Best Student Paper Award**. (Acceptance rate: 32%).

103. 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 '06)*. West Point, NY. Jun. 2006.

104. 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 '06)*. LNCS 4127, pages 133-147. Springer. Sophia Antipolis, France. Jul. 2006.

105. 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 '05) in Conjunction with Vis 2005 and InfoVis 2005*. Pages 65-74. IEEE Press. Minneapolis, MN. Oct. 2005.

106. 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 '05)*. Pages 157-168. IEEE Press. Athens, Greece. Sep. 2005. (Acceptance rate: 25%).

107. 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 '05)*. Stanford University, CA. Jul. 2005. **Received Brown University's Award for Technological Innovation.**

108. 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 '04)*. Pages 354-363. ACM Press. Washington, DC, Oct. 2004. (Acceptance rate: 18%).

109. 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 '04)*. Pages 146-155. ACM Press. Yorktown Heights, NY, Jun. 2004. (Acceptance rate: 27%).

NON-PEER-REVIEWED PUBLICATIONS

1. Ya Xiao, Yang Zhao, Nicholas Allen, Nathan Keynes, Danfeng Yao, and Cristina Cifuentes. Industrial Experience of Finding Cryptographic Vulnerabilities in Large-scale Codebases. CoRR abs/2007.06122. 2020.

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.

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`

- **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.

OTHER PROFESSIONAL ACTIVITIES

1. NSF panelist (multiple times, including CAREER panels)
2. Proposal-review Panelist for VT Computer Science in '17, '15 and VCU CAREER Academy in '16
3. Served as a proposal reviewer for

   American Association for the Advancement of Science (AAAS) International Grant Review Program, '19

   University of Toledo, '18,

   Research Grants Council (RGC) of Hong Kong, '20, '19, '18, '17,

   Israeli Ministry of Science, Technology and Space, '17,

   American Association for the Advancement of Science (AAAS) Research Competitiveness Program, '17,

   Department of Mathematics of the University of Padova, Italy, '16.
4. **Technical Program Committee member for numerous top security conferences**, including:

   NDSS '21, *ICSE '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. Editorial board member for *International Journal of Security and Networks*, Jan. '11 – Mar. '15.
6. Serving as a session chair in numerous conferences, including ACM CCS '19, ACSAC '19, ACM SACMAT '18, IEEE SecDev '17, ACM CCS '16, '15, '14 and ASIACCS '17, '14.

7. Panel co-chair for the *12th EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2016.

8. Program co-chair for the *Third International Workshop on Security in Cloud Computing (SCC)*, held in conjunction with *ASIACCS*. 2015.

9. Moderator for the Special Interest Panel in S2ERC Showcase (NSF I/UCRC), Nov. 2013

10. Co-organizer of Northeast Security and Privacy Day at Rutgers University, May 2009.

11. Reviewer for

    ACM Transactions on Embedded Computing Systems, *Proceedings of IEEE*, *Computers & Security*, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information, Forensics and Security*, *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*.

12. Book chapter review for *Algorithm Design and Applications*. Wiley. Jun. 2014.

OTHER PRESENTATIONS

1. Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations. IEEE ICDE Workshop on Women in Data Science (WiDS). April 2020.

2. Data-driven Vulnerability Repair in Programs with Cloud Analytics for Practical Deployment. ONR TPCP PI Meetings. Jun. 2019. May 2018.

3. Enterprise Data Breach and Multiple Points to Stop it. National Center for Women & Information Technology (NCWIT) Virginia Aspirations in Computing. Mar. 2019.

4. Automatic Generation of Anti-Specifications from Exploits for Scalable Program Hardening. DARPA CASE Kickoff Meeting. Arlington, VA. Feb. 2018.

5. Cybersecurity: What, Why, How? Sophomore Seminar. Virginia Tech Computer Science Department. Oct. 2016.

6. 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.

7. Overview of VT CS/ECE Education and Research Activities. *University-Wide Cybersecurity Workshop*. Blacksburg, VA. Aug. 2016.

8. Program Anomaly Detection with Near-zero False Alarms. Missouri University of Science and Technology (MST). Departmental Seminar. Rolla, MO. Apr. 2016.

9. Detection of Malware Collusion with Static Dependence Analysis on Inter-App Communication. *DARPA APAC PI Meeting*. Tampa, FL. Oct. 2015.

10. Probabilistic Program Modeling for High-Precision Anomaly Classification. *IEEE CSF*. Verona, Italy. Jul. 2015.

11. Precise Modeling of Benign Program Behaviors for Proactive System Defense. Brown University Computer Science Department Systems Reading Group. Providence, RI. Nov. 2014.

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

13. Inter-Component and Inter-App Communication Analysis in Android for Advanced Malware Detection. NSF I/UCRC S2ERC Showcase. May. 2014. Washington D.C.

14. User-Intention Based Anomaly Detection for Cyber Security. *37th annual meeting of the SIAM Southeastern Atlantic Section.* Oak Ridge National Lab. Mar. 2013.

15. Distributed Detection of Data Exfiltration in Enterprise Environments. Security Software and Engineering Research Center Showcase. Arlington, VA. May 2012.

16. User-Centric Dependence Analysis in Programs for Identifying Malware. Security Software and Engineering Research Center Showcase. Ames, IA. Nov. 2011.

17. Data Leak Detection in Enterprise Environments. NSF I/UCRC S2ERC Showcase. Nov. 2013. Pensacola, FL.

18. Advanced Program Analysis for Android App Classification. NSF I/UCRC S2ERC Showcase. Nov. 2013. Pensacola, FL.

19. Probabilistic Program Modeling for Anomaly Detection. IEEE Security & Privacy Symposium. Short talk. San Francisco. May 2013.

20. User-Intention Based Program Analysis for Security. IEEE Security & Privacy Symposium. Short talk. San Francisco. May 2013.

21. User-Intention Based Anomaly Detection. Virginia Tech, Department of Electrical and Computer Engineering, Center for Embedded Systems for Critical Applications (CESCA). May 2013.

22. User-Centric Security and Privacy. Virginia Tech College of Engineering Advisory Board Meeting. Oct. 2010.

23. Host-Based and User-Centric Approaches for Detecting Drive-By-Download Attacks. Computer Science Departmental Seminar. New Jersey Institute of Technology. Nov. 2009.

24. Host-Based and User-Centric Detection of Drive-By-Download Attacks. DIMACS Fall Mixer. Rutgers University. Sep. 2009.

25. Cryptographic Provenance Verification Approach in Malware Detection with Trusted User Inputs. *Security and Privacy Day.* Rutgers University. May 2009.

26. Personalized Security with Trusted User Inputs for Botnet Detection. *Virginia Tech Computer Science Departmental Seminar*, Blacksburg, VA. May 2009.

27. Keystroke Authentication and Human-Behavior Driven Bot Detection. DyDAn Student-organized Seminar Series, Rutgers University. Nov. 2008.

28. Keystroke Dynamics Authentication and Human-Behavior Driven Bot Detection. *Departmental Seminar.* Stevens Institute of Technology, Department of Electrical and Computer Engineering. Hoboken, NJ. Oct. 2008.

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

30. Efficient signature schemes supporting redaction, pseudonymization, and data deidentification. *BSF/DIMACS/DyDAn Workshop on Data Privacy.* Rutgers University, NJ. Jan. 2008.

31. Private Information: To Reveal or Not to Reveal. *Departmental Seminars*. Department of Computer Science at Rutgers University, Texas A&M University, Washington University at St. Louis, and Indiana University - Purdue University at Indianapolis; Department of Electrical and Computer Engineering at Iowa State University and Purdue University. Spring 2007.

32. Trust and Service Negotiations Using WSPL. Sun Microsystems Lab, Burlington MA. Nov. 2003.

STUDENT AWARDS AND HONORS

Salman Ahmed, Nominated for IBM Ph.D. Fellowship Award	Oct. 2019
Ya Xiao, BitShares Fellowship, Computer Science Department	Oct. 2019
Sazzadur Rahaman, BitShares Fellowship, Computer Science Department	Jul. 2018
Long Cheng, Pratt Fellowship, Computer Science Department	Dec. 2017
Xiaokui Shu, Outstanding Ph.D. Student Award, Computer Science Department	Apr. 2016
Xiaokui Shu, Best Poster Award, ACM CODASPY	Mar. 2015
Karim Elish, First Place in VT Computer Science Graduate Research Poster Competition	Apr. 2014
Karim Elish, Finalist for VT COE Torgersen Graduate Research Award	Apr. 2014
Hussain Almohri, Finalist for VT COE Torgersen Graduate Research Award	Apr. 2013
Joshua Martin, Nominated for CRA Outstanding Undergrad Researchers Award by VT CS	Mar. 2013
Hussain Almohri, Kuwait Government Scholarship	2007-2013
Karim Elish, 1st Place in VT Graduate Research Competition	Mar. 2012
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

1. Zishuai Li ('20, undergraduate at VT CS) on CryptoGuard deployment
2. Chengkai Yao ('20, undergraduate at VT CS) on autonomous drones for smart farms
3. Deepti Suresh ('19-'20, undergraduate at VT CS) on AI ethics and fairness
4. Aparna Ganesh ('20, undergraduate at VT CS) on the history of trusted execution
5. Zachary Burch ('15, undergraduate at VT CS) on proof-of-concept collusion malware in Android
6. Adrianne Williams (NSF REU '15, undergraduate at VT CS) on accuracy comparison of anti-virus tools
7. Allison Hatch (NSF REU '15, undergraduate at VT CS) on the usability evaluation of intrusion detection tools
8. Lance Chao ('14, '15, CyberCorp BS/MS student at VT CS) on Java string analysis for Android collusion detection
9. Hannah Roth ('14 – '16, CyberCorp BS/MS student at VT CS) on improving the usability of program anomaly detection in IoT
10. Andrew Ciambrone (NSF REU '14, undergraduate at VT CS) on big data analysis for early network detection
11. Zack Morris ('14, undergraduate at VT CS) on repackaged Android malware analysis
12. Joshua Martin ('13, undergraduate at VT CS) on Android rootkits and their defenses
13. Samantha Puckett ('13, undergrad at VT CS) on data leak protection in Android

14. Antuan Byalik ('12, undergrad at VT CS) on a cyber game system for user authentication and behavior study.
15. Laurel Schaefer (NSF REU '12, undergrad at VT CS) on social science and cyber security
16. Brendan Avent ('11, '12, undergraduate at VT CS) on a low-cost DNS-tunneling-based location tracking
17. Scott Luxenberg ('11, undergraduate at VT CS) on a low-cost DNS-tunneling-based location tracking system
18. Casey Link ('11, undergraduate at VT CS) on development of a game system for security education
19. William Matt Banick ('10, undergraduate at VT CS/Psychology) on user-intention based traffic dependency study
20. Alexander Crowell (DIMACS REU '09, joined University Michigan CS for PhD) on detection of drive-by-download attacks
21. Anitra Babic (DIMACS REU '09, undergraduate at Chestnut Hill College) on email-activity based authentication
22. Prateek Malhotra ('08, undergraduate at Rutgers CS) on parallel universe design of network traffic prediction for anomaly detection
23. Deian Stefan (DIMACS REU '08, joined UCSD as an assistant professor) on keystroke dynamic authentication

UNIVERSITY/DEPARTMENT SERVICES

Promotion & Tenure Committee, VT CS 2019-2021
Faculty Search Committee, VT CS 2019-2020
Distinguished Lectures Committee, VT CS 2019-2020
Engineering Faculty Organization (EFO) Executive Committee, VT College of Engineering 2017 - Present
VT Aerospace and Ocean Engineering (AOE) Faculty Search Committee (for an ISDA position) 2018-2019
CAREER Proposal Mentoring, VT CS Summer 2017, 2018
University-wide Clustering Hire Search Committee, Virginia Tech Integrated Security Destination Area (ISDA) 2017-2018
University-wide Stakeholder Committee, Virginia Tech Integrated Security Destination Area (IS DA) 2016 - Present
University-wide Curriculum Development Subcommittee, Virginia Tech Integrated Security Destination Area (IS DA) 2016 - Present
Faculty Design Team, Virginia Tech Integrated Security Destination Area 2016 - 2017
Personnel Committee, Virginia Tech Computer Science 2016 - 2017
Course Certification of NSA's Center of Academic Excellence for Cyber operations Apr. 2016
Department Head Search Committee, Virginia Tech Computer Science 2014-2015
Co-organizer of graduate recruitment weekend 2015
Co-chair of Faculty Search Committee, Virginia Tech Computer Science 2014-2015
Faculty Search Committee, Virginia Tech Computer Science 2016-2017, 2014-2015, 2013-2014, 2012-2013, 2011-2012, 2010-2011
Graduate Program Committee, Virginia Tech Computer Science 2016-2017, 2014-2015
Diversity Committee, Virginia Tech Computer Science 2014-2015
Chair of Computer Science Ph.D. Qualifier Exam Committee 2012-2013
Graduate Admission Committee, Virginia Tech Computer Science 2013-2014, 2012-2013, 2011-2012
CS/ECE joint cyber security curriculum development 2011-2012, 2012-2013, 2013-2014

- This joint effort produced the popular COE Cybersecurity minor degree program.

Qualifier Exam Committee, Virginia Tech Computer Science 2011-2012, 2013-2014
Faculty Search Committee, Virginia Tech Electrical and Computer Engineering 2011-2012
Publicity and Awards Committee, Rutgers Computer Science 2008-2009
Admission Committee, Rutgers Computer Science 2008-2009

OUTREACH AND DIVERSITY

Panelist at the IEEE ICDE Workshop on Women in Data Science (WiDS). 2020
Organizer of ACM SIGSAC Women in Cybersecurity Research (CyberW) Workshop 2020
Organizer of the ACM CCS Women's Networking Reception 2019
Meet and Greet with VT Asian American Student Union 2019
Volunteered at the Women in Computing Day (attended by 80 middle school girls), VT CS 2019
Presented at the Blacksburg ACM local chapter 2018
Saudi Young Leaders Exchange Program (VT CPE) 2017
Founder of Women in Cybersecurity Research (CyberW) Workshop (co-located with ACM CCS) 2017
National Center for Women & IT (NCWIT) reviewer 2016
Co-organizer of the system reading group at VT CS 2015-2017
Advising a local high school student on steganography research 2015
Panelist for Brown University CS Department Career Workshop for Ph.D. students Nov. 2014
Grace Hopper Conference Scholarship Application Committee Member 2014
Advising Roanoke Valley Governor's School students on keystroke dynamics authentication Oct. 2013
Media consultant to Washington Times on cyber security for small businesses May 2014
Women's networking event for recruiting female undergraduates to VT CS major Jan. 2013, 2014
Lectures at Imagination Camps for middle school students, Virginia Tech Jul. 2012
Recruiting underrepresented students into NSF REU programs May 2012
Exhibition at Kids' Tech, Virginia Tech Feb. 2012
Academic career panel, Virginia Tech Computer Science Oct. 2011
Presenter for C-Tech^2 High School Girls Summer School 2011
Presented at Women's Preview Weekend of College of Engineering Mar. 2010, Apr. 2011
Demo at the COE recruiting events for underrepresented high school sophomores Apr. 2011
Presentation and demo for representatives from General Dynamics, Oct. 2010
Panelist on the VT CS Graduate Council Academic Job Search Panel Oct. 2011
Presented in the *Meet the Faculty* event of Computer Science Dept. Jan. 2010, Jan. 2011
Signed up as a mentor in Scieneering mentoring program Mar. 2011
Recruiting a minority Ph.D. student from Georgia Tech for faculty Jan. 2011
Demos and posters at VT CS 40th anniversary weekend Nov. 2010
Serving as an e-mentor in Rutgers University Women in Engineering Leadership League 2008-2009
DIMACS Career Planning Seminar for graduate students and postdocs Oct. 2008