XiaoFeng Wang

Curriculum Vitae

email: xiaofeng.wang@ntu.edu.sg web: https://wangxiaofeng7.github.io

EDUCATION

2004	Ph.D. Electrical and Computer Engineering Carnegie Mellon University
1996	M.E. Computer Science and Engineering Shanghai Jiao Tong University
1993	B.E. Computer Science and Engineering Nanjing University of Aeronautics and Astronautics

PROFESSIONAL EXPERIENCE

1/2026 —	President's Chair Professor
7/2025 —	Professor, College of Computing and Data Science, Nanyang Technological University
11/2017— 3/2025	Rudy Professor of Computer Science, Engineering and Informatics
7/2015 — 3/2025	Professor
7/2010 — 6/2015	Associate Professor
8/2004 — 6/2010	Assistant Professor School of Informatics, Computing and Engineering Indiana University at Bloomington
1/1997 — 8/1997	IT Specialist Hewlett-Packard Computer Products (Shanghai) Co.Ltd
3/1996 — 1/1997	Software Engineer Shanghai Venus Software co., LTD

RESEARCH LEADERSHIP & ADMINISTRATIVE EXPERIENCE

- Associate Vice President (Cybersecurity), Nanyang Technological University (NTU), Jan. 1st, 2026 —
- Head of the Division of Computing (HOD), College of Computing and Data Science (CCDS), NTU, Jan. 1st, 2026 —
- Associate Dean of Research, Luddy School of Informatics, Computing, and Engineering, Indiana University at Bloomington, Jan. 1st, 2023 — Dec. 31, 2024
- Director, National Science Foundation, Center for Distributed Confidential Computing (an NSF SaTC Frontiers Project), Oct. 1st, 2022 — Mar. 28th, 2025
  Participants: IU (Lead), CMU, Duke, OSU, Penn State, Purdue, Spelman & Yale
- Chair, ACM Special Interest Group on Security, Audit and Control (SIGSAC): July 1st, 2021 — June 30th, 2025
- Vice Chair, ACM SIGSAC: July 1st, 2017 — June 30th, 2021
- Director, Master of Science in Secure Computing (MSSC) at Indiana University: 2020 — 2022
- Director, Center for System Security and Data Privacy: 2017 — 2025
- Co-Director, Center for Security Informatics: 2010 — 2017

PROFESSIONAL SERVICE

- Program Co-Chair, the ACM Conference on Computer and Communications Security (CCS'18 and CCS'19)
- Member, ACM SIGSAC Executive Committee (July 1st, 2017 —)
- Founding organizer (with my colleagues at IU and UCSD): iDASH Genome Privacy Challenges (www.humangenomeprivacy.org)
- Program Co-Chair, the 11th ACM Asia Conference on Computer and Communications Security (ACM AsiaCCS'16)
- Program Chair, the 11th International Conference on Security and Privacy in Communication Networks (SecureComm'15)
- Workshop Co-Chair, the 22nd ACM Conference on Computer and Communication Security (CCS'15)
- General Chair, the 13th Privacy Enhancing Technologies Symposium (PETS'13)
- Program Chair, the 7th International Workshop on Genome Privacy and Security (GenoPri'20)

- Steering committee member, International Workshop on Genome Privacy and Security (GenoPri)
- Member, PoPETs/PETS Advisory Board
- Associate Editor, ACM Transactions on Privacy and Security (TOPS), since October, 2020
- Associate Editor, IEEE Security and Privacy Magazine, since January, 2019
- Associate Editor, IEEE Transactions on Dependable and Secure Computing (TDSC), December, 2014 to February, 2022
- Area PC Chair, the IEEE Conference on Communications and Network Security (CNS'19)
- Panel Chair, the IEEE Conference on Communications and Network Security (CNS'18)
- Program committee member, the IEEE Symposium on Security and Privacy (S&P'10, 11, 12, 13, 14, 18, 19, 20, 22)
- Panelist, the IEEE Conference on Communications and Network Security (CNS'17)
- Program committee member, the USENIX Security Symposium (Security' 17, 22)
- Invited panelist, Security and Privacy Challenges in Health Informatics, the NSF SaTC PI meeting 2015.
- Program committee member, the 17th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'15)
- Program committee member, the Annual Network and Distributed System Security Symposium (NDSS' 13, 14, 15, 16, 17, 21)
- Program committee member, the International World Wide Web Conference, Security and Privacy Track (WWW'09, 12, 14, 15)
- Program committee member, the ACM Symposium on Information, Computer and Communications Security (ASIACCS'12)
- Member, PET Award 2012 committee
- Program committee member, the International Conference on Distributed Computing Systems (ICDCS'10, 11)
- Chair, Local arrangement committee, CCS'11
  Member, Patron and Industry Outreach, CCS'10
  Chair, Regional arrangement committee, CCS'09
- Program committee member, the Workshop on Security and Privacy in Medical and Home-Care Systems 2009
- Program committee member, the International Conference on Security and Privacy in Communication Networks (SecureComm'08, 09)

- Program committee member, the ACM Conference on Computer and Communication Security (CCS'08, 10, 15, 16, 17, 20, 21, 22)
- Co-Chair, the I3P Workshop on Insider Threats in the Networked World (2008)
- Local arrangement, the 5th Midwest Security Workshop (Spring, 2008), Program chair, the Second MSW (Fall, 2006) and PC members, MSW (2006 – 2008)
- Program committee member, the Fourth International Conference on Information Systems Security (ICISS 2008)
- Program committee member, the Third International Conference on Internet Monitoring and Protection (ICIMP'08)
- Steering committee member, NSF Biomedical Informatics Workshop (2007)
- Program committee member, the Workshop on Privacy in the Electronic Society (WPES'06-08, 12)
- Program committee member, the IEEE International Symposium on Dependable Autonomic and Secure Computing (DASC'06 and '07)
- Program committee member, the 8th International Conference on Information and Communications Security (ICICS '06)
- Program committee member, the 5th International Conference on Cryptology and Network Security (CANS '06)
- Program committee member, the International Workshop on Incentive Based Computing (IBC'05 and '06)
- Program committee member, the 4th International Conference on Applied Cryptography and Network Security (ACNS'06)
- Program committee member, the 16th Annual International Symposium on Algorithms and Computation (ISAAC'05)
- Program committee member, ACM Workshop on Wireless Security 2005 (WiSe'05).
- Program committee member, the International Joint Conference on Autonomous Agents and Multi Agents Systems (AAMAS'04 and 05).
- Panelist: Attacks on and Security Measures for Ad Hoc Wireless Networks, American Association for the Advancement of Science annual Conference 2005.
- Program committee member of IEEE/ACM First International Workshop on Broadband Wireless Services and Applications (BroadWISE 2004)
- Paper reviewer for the IEEE/ACM Transactions on Networking, the ACM Transactions on Information and System Security, the IEEE Transactions on Dependable and Secure Computing, the IEEE Transactions on Parallel and Distributed Systems, International Journal of Knowledge and Information Systems, the IEEE transactions on Knowledge and Data Engineering, Electronic Commerce Research Journal, ACM Conference on Computer and Communication Security, RSA CT, IEEE

INFOCOM, IEEE GLOBECOM, ACM International Conference on Information Security, Workshop on Privacy Enhancing Technologies, Conference on Security and Cryptography for Networks, The IEEE International Conference on Communications, Pacific Rim International Workshop on Multiagent Systems, Pacific Rim International Conference on Artificial Intelligence and IFIP World Computer Congress.

TEACHING EXPERIENCE

Fall 2005- 2025	I430/520 and B649 "Security for Networked Systems" (An upper-level undergraduate and graduate course) Indiana University at Bloomington
Spring 2007- 2025	I521 "Malware: Threat and Defense" (A graduate course) Indiana University at Bloomington
Spring 2006- 2009	I231 "Mathematic Foundations for Cybersecurity" (A second-year undergraduate course) Indiana University at Bloomington
Spring 2005	I400 "Introduction to Information Security" (A third and forth year undergraduate course) Indiana University at Bloomington
Spring 2002	Teaching assistant for 18440 “Internet Security” (An upper-level undergraduate and graduate course) Carnegie Mellon University

INTERNAL SERVICE

1. Facility Committee, Informatics (Fall 2004 – Spring 2006)
2. Faculty Hiring Committee, Informatics (Fall 2004 – Spring 2005, Fall 2008 – Spring 2009, Fall 2011)
3. Admission and Awards Committee, Computer Science (Fall 2004 –)
4. Graduate Admissions and Financial Aid Committee, Informatics (Fall 2006 – Spring 2008, Fall 2014)
5. Graduate Education Committee, Computer Science (Fall, 2010 – 2012, 2014 –)
6. Security Contact for Health Informatics Program (Spring, 2011 –)
7. Chair, Faculty Hiring Committee (security track) (Fall 2013 – Spring 2014)
8. Chair, Admission and Awards Committee, Computer Science (Fall 2014 – 2018)
9. Program Director, Security Informatics Program (2010)
10. Director, Center for Security Informatics (2010 –)

11. Program Director, Secure Computing Program at IU (2020)

IMPACTS OF MY RESEARCH

My research regularly attracts attention from major media outlets, including CNN, The New York Times, MSNBC, PC World, Slashdot, CNet News, and others. Below are links to partial lists of media coverage.

Analysis on Underground Markets for Large Language Models:
https://www.techpolicy.press/studying-black-market-for-large-language-models-researchers-find-openai-models-power-malicious-services/
https://www.lemonde.fr/sciences/article/2024/02/13/intelligence-artificielle-les-chatbots-gangrenes-par-les-cybercriminels_6216174_1650684.html
https://www.wsj.com/articles/welcome-to-the-era-of-badgpts-a104afa8
https://www.fastcompany.com/91184474/black-market-ai-chatbots-thriving

Analysis on Information Leaks from Large Language Models:
https://www.nytimes.com/interactive/2023/12/22/technology/openai-chatgpt-privacy-exploit.html

Winning Two Tracks of NeurIPS'22 Trojan Detection Challenge:
https://news.luddy.indiana.edu/story.html?story=Luddy-School-gets-pair-of-wins-in-Trojan-Detection-Challenge

NSF SaTC Frontiers Award for CDCC:
https://news.iu.edu/stories/2022/08/iub/releases/04-nsf-cybersecurity-awards-distributed-data-user-privacy.html
https://beta.nsf.gov/news/nsf-announces-awards-advance-cybersecurity-efforts

Genome Privacy Competition:
https://www.genomeweb.com/informatics/new-community-challenge-seeks-evaluate-methods-computing-encrypted-genomic-data
http://www.nature.com/news/extreme-cryptography-paves-way-to-personalized-medicine-1.17174

MassVet: http://sit.soic.indiana.edu/en/2015/09/06/massvet-usenix/

XARA Threats to Mac OS X and iOS, and also Android Secure Upgrading:
http://sit.soic.indiana.edu/en/2015/09/07/xara-ccs/
https://luyixing.weebly.com/media-coverage.html

Privacy in Dissemination of Human Genomic Data:
News Release by Ontario's Information and Privacy Commissioner and BioSpace

Security Analysis of Cashier-as-a-Service Systems:
http://www.informatics.indiana.edu/xw7/record/impacts/CaaS.htm

Sound Malware for Android Phones
http://www.informatics.indiana.edu/xw7/record/impacts/Soundcomber.htm

Facebook Authorization Flaw
http://www.informatics.indiana.edu/xw7/record/impacts/Facebook.htm

Side-Channel Information Leaks in Web Applications
http://www.informatics.indiana.edu/xw7/record/impacts/SideChannel.htm

Puzzle Auction
http://www.informatics.indiana.edu/xw7/record/impacts/PuzzleAuction.htm

HONORS

2025 Distinguished Paper Award: the 32nd ACM Conference on Computer and Communications Security (CCS): for research on compliance implications of web scraping for LLM services

2024 ACM Fellow (Class 2023): for contributions to systems security and privacy

2023 Stanford List of World's Top Scientists

2023 AMiner AI 2000 Most Influential Security and Privacy Scholars List (21st between 2013 and 2022)

2023 AAAS Fellow (Class 2022): for distinguished contributions to the field of systems security and data privacy, particularly for security analysis and protection of computing systems and protection of human genomic data

2022 Winning Team: NeurIPS'22 Trojan Detection Challenge (Final Round and Evasive Trojans Track)

2022 Best Paper Honorable Mention: the 29th ACM Conference on Computer and Communications Security (CCS): for research on imitation adversary attacks on neural ranking models

2021 ACM Distinguished Member: for contributions to systems security and genomic privacy

2020 AMiner AI 2000 Most Influential Security and Privacy Scholars List (20th between 2010 and 2019)

2019 CSAW'19 US-Canada Applied Research Competition Winner (3rd place): for research on the security risks of voice-controlled third-party functions for virtual personal assistant systems (Google Assistant, Amazon Alexa, etc.)

2019 Distinguished Paper Award, the 26th Network and Distributed System Security Symposium (NDSS): for research on cybercrime analysis

2019 Distinguished Paper Award, the 26th Network and Distributed System Security Symposium (NDSS): for research on Genomic Privacy

2019 IEEE Fellow (Computer Society): for contributions to system security and genomic privacy

2018 CSAW'18 US-Canada Applied Research Finalist: for the research on iOS side-channel analysis (which led to the change of the iOS kernel)

2017 James H. Rudy Professorship, Indiana University

2016 Best Paper Award in Applied Cyber Security Research, 3rd Place, CSAW'16 (NYU-Poly Cyber Security Awareness Week): for research on cyber threat intelligence gathering

2014 Best Paper Award in Applied Cyber Security Research, 3rd Place, CSAW'14 (NYU-Poly Cyber Security Awareness Week): for research on security risks in Android customization

2014 Third place in National Security Innovation Competition: for the work on Android secure upgrading

2013 Finalist for the Best Applied Security Paper Award, CSAW'13 (NYU-Poly Cyber Security Awareness Week): for research on dedicated hosts on malicious web infrastructures

2011 Award for Outstanding Research in Privacy Enhancing Technologies (the PET Award): for research on Genomic Privacy

2011 PET Award runner-up: for research on side-channel information leaks in web applications

2011 Best Practical Paper Award, the 32nd IEEE Symposium on Security and Privacy: for research on logic flaws in hybrid web applications

2006 Fast-track submission to the ACM Transactions on Information System Security as one of the best papers of the ACM Conference on Computer and Communications Security 2006: for research on malware detection

SELECTED INVITED TALKS

2024 Keynote for the 11th ACM Workshop on Adaptive and Autonomous Cyber Defense (AACD 2024)

2024 Keynote for the 17th Central Area Networking and Security Workshop (CANSec)

2024 Keynote for the 19th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS)

2024 Invited Seminar for Cybersecurity and Privacy (CySeP) Summer School, an ACM Europe Summer School organized by KTH Royal Institute of Technology in Stockholm, Sweden

2021 Invited Talk at the UK Security and Privacy Seminar

2021 Invited Talk at Institute for Assured Autonomy at Johns Hopkins University

2021 Distinguished Cybersecurity Lecture, Computer Science and Engineering, Ohio State University

2020 Keynote for 14th International Conference on Network and System Security, Melbourne, Australia

2019 Keynote for SIGSAC at ACM Turing Celebration Conference, China

2018 Keynote at the 3rd Singapore Cybersecurity R&D Conference (SG-CRC'18)

2018 Keynote at the 6th Midwest Security Workshop

2018 Keynote at the 1st Riverside Security and Privacy Workshop

2018 Keynote at the SRC Forum on Smart City

2018 Invited Talk at the 13th ACM Asia Conference on Computer and Communications Security (AsiaCCS'18)

2016 Keynote at the 10th Central Area networking and Security Workshop (CANSec'16).

2016 Invited seminar, Chinese University of Hong Kong

2016 Seminar talk, Northwestern University

2016 Seminar talk, University of Southern California

2015 Seminar, Northeastern University

2014 TRUST Security Seminar, University of California, Berkeley

2014 Invited talk. Narus Inc.

2014 Seminar talk. Purdue University

2013 Seminar talk. University of Maryland at College Park

2013 Seminar talk. University of Texas at Austin

2013 Invited talk. Chinese Academy of Sciences, China

2012 Invited talk. Microsoft Faculty Summit

2012 Invited talk. Computer Science Center, Shangdong Academy of Sciences, China

2012 Invited talk. Computer Science, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland

2012 Seminar talk. Computer Science, University of Illinois at Urbana-Champaign

2011 Invited talk. IBM T. J. Watson Research Center

2011 Seminar talk. CyLab, Carnegie Mellon University

2011 Seminar talk. Computer Science Department, North Carolina State University

2010 CERIAS seminar talk, Purdue University.

2010 IPAM Workshop on Statistical and Learning- Theoretic Challenges in Data Privacy

2009 Invited talk. Microsoft Research Asia.

2009 CERIAS seminar, Purdue University.

2008 Seminar talk. Computer Science Department, North Carolina State University.

2008 Seminar talk. Computer Science Department, Indiana University and Purdue University at Indianapolis.

2005 Panel: Attacks on and Security Measures for Ad Hoc Wireless Networks, American Association for the Advancement of Science annual Conference.

2002 Invited talk. Workshop on Multi-Agent Learning: Theory and Practice.

CURRENT AND PAST GRANTS

PI (Lead PI of multi-institutional projects + IU PI): $22.85 million
Total (Excluding internal grant total): $37.35 million
Personal Share: around $10 million

- Intel Trustworthy Data Center of the Future (TDCoF): Enabling Open, Privacy-Preserving FaaS based Distributed Confidential Computing for Trusted Data Center"
  Role: Lead PI
  Amount: $150,000 (IU share: $120,000)
  Time: Intel's gift fund, expected to be allocated in 2024, 2025 and 2026

- NSF-CNS-2207231: "Collaborative Proposals: SaTC: Frontiers: Center for Distributed Confidential Computing (CDCC)"
  Role: Lead PI
  Amount: $9,000,000 (IU share: $3,080,174)
  Time: From 10/01/2022 to 9/31/2027

- NSF-CNS-2154199: “Collaborative Research: SaTC: CORE: Medium: Audacity of Exploration: Toward Automated Discovery of Security Flaws in Networked Systems through Intelligent Documentation Analysis”
  Role: Lead PI
  Amount: $1,200,000 (IU share: $550,000)
  Time: From 7/01/2022 to 6/30/2026

- ARO-IARPA TrojAI (Competing Renewal), part of the project led by Peraton Labs
  Role: IU PI (with Haixu Tang)
  Amount: $1,133, 213 (IU share)
  Time: From 10/31/22 – 10/30/24

- NIH CEGS: “Genetic & Social Determinants of Health: Center for Admixture Science and Technology”
  Role: Co-PI of IU Subcontract
  Amount: $11,700,000 (IU Subcontract share: $415,850)
  Time: 2021- 2026

- NSF-CCF-2124225: “FMitF: Track II: Usability, Scalability, and Deployment Improvement of VerioT”,
  Role: Co-PI
  Amount: $99,983
  Time: From 7/01/2021 to 12/31/2022

- ONR Navy ROTC Cybersecurity Training Program
  Role: Co-PI
  Amount: $250,000
  Time: From 8/01/2020 to 7/31/2021

- ARO-IARPA TrojAI: “Statistical Methods for Backdoor Detection in Deep Neural Networks”, part of the Project Illiad of Perspecta Labs
  Role: PI (with Haixu Tang)
  Amount: $704,980 (IU share)
  Time: From 7/30/20 to 10/31/22

- NIH R01 (R01HG010798): “Secure and Privacy-preserving Genome-wide and Phenome-wide Association Studies via Intel Software Guard Extensions (SGX)”
  Role: Lead PI
  Amount: $1,493,069
  Time: From 08/09/2019 to 05/31/2023
  (Subcontract to CMU: $327,610)

- NSF-CNS-1801432: “SaTC: CORE: Medium: Collaborative: Understanding and Discovering Illicit Online Business Through Automatic Analysis of Online Text Traces”
  Role: Lead PI

Amount: $1,200,000 (IU share: $900,000)
Time: From 9/01/2018 to 8/31/2023

- NSF-CNS-1838083: “BIGDATA: IA: Enabling Large-Scale, Privacy-Preserving Genomic Computing with a Hardware-Assisted Secure Big-Data Analytics Framework”
  Role: Lead PI
  Amount: $1,000,000
  Time: From 1/01/2019 to 12/31/2022

- The Precision Health Initiative. Indiana University Grant Challenges Initiative
  Role: Participant
  Amount for the project involved: $200,000
  Time: From 9/01/16 to 9/30/22

- NIH U01 (1U01EB023685): “Encryption Methods and Software for Privacy-Preserving Analysis of Biomedical Data”
  Role: MPI (one of the two PIs on the project)
  Amount: $1,395,515
  Time: From 9/30/2016 to 6/30/2020
  (Subcontract to UCSD: $453,137)

- NSF-CNS-1618493: “TWC: Small: Safeguarding Mobile Cloud Services: New Challenges and Solutions”
  Role: Sole PI
  Amount: $499,968
  Time: From 9/01/2016 to 8/31/2019

- Army Research Office: “How to Compose Security Protection for Third-Party Applications”
  Role: PI
  Amount: $550,000
  Time: From 3/01/2016 to 2/28/2019
  (Subcontract to Purdue: $252,999)

- Gift Grant from Samsung Research
  Role: Sole PI
  Amount: $50,000

- NSF-CNS-1527141: “TWC: Small: Understanding and Mitigating the Security Hazards of Mobile Fragmentation”
  Role: Sole PI
  Amount: $498,897
  Time: From 10/01/2015 to 9/30/2018

- NSF-CNS-1408874: “TWC: Medium: Collaborative: Broker Leads for Privacy-Preserving Discovery in Health Information Exchange”
  Role: IU PI (the project is led by UIUC)
  Amount: $360,000 (total $1.05 million)
  Time: From 9/01/2014 to 8/31/2018

- NIH R01 (1R01HG007078): “Privacy Preserving Technologies for Human Genome Data Analysis and Dissemination”
  Role: Lead PI
  Amount: $900,000
  Time: From 9/23/2013 to 6/30/2016
  (Subcontract to UCSD: $272,025)

- NSF-CNS-1223495: “TWC: Small: Secure Data-Intensive Computing on Hybrid Clouds”
  Role: PI
  Amount: $500,000
  Time: From 9/01/2012 to 8/31/2015

- NSF-CNS-1223477: “TWC: Small: Knowing Your Enemy: Understanding and Counteracting Web Malvertising”
  Role: Sole PI
  Amount: $478,160
  Time: From 9/01/2012 to 8/31/2015

- NSF-CNS-1117106: "TC: Small: Plugging Logic Loopholes in Hybrid Web Applications to Secure Web Commerce"
  Role: Sole PI
  Amount: $499,987
  Time: From 9/01/2011 to 8/31/2014

- NSF-CNS-1017782: “TC: Small: Reining in Side-Channel Information Leaks in the Software-as-a-Service Era”
  Role: Sole PI
  Amount: $494,110
  Time: From 9/01/2010 to 8/31/2014

- Gift Grant from Microsoft Research
  Role: Sole PI
  Amount: $10,000

- NSF-CNS-0716292: “CT-ISG: Automatic Generation of Vaccine Exploits to Protect Commodity Software”
  Role: Sole PI
  Amount: $320,000
  REU Supplemental Award: $19,200

Time: From 9/01/2007 to 8/31/2011

- AFRL SBIR Phase III, Net-Centric Sensor Grids, FA8650-09-D-1639: “Advanced Cloud Computing Technology for Sensor Grids”
  Role: Co-PI
  Amount: $726,000
  Time: From 7/1/2009 to 6/30/2010

- CACR Internal Grant (Gift from the Lilly Endowment Inc.) “Evaluation and Mitigation of Privacy Risks in Human Genome Research”
  Role: PI
  Amount: $49,901.40
  Time: From 7/01/2009 to 6/30/2010

- I3P/DHS: “Mitigating Insider Threat with Incentives” (IU part of the project "Human Behavior, Insider Threat and Awareness")
  Role: PI
  Amount: $370,233.63
  Time: From 4/01/2007 to 7/31/2009

- NSF-IIS-064621:"NSF Frontiers in Health Information Delivery Workshop"
  Role: Co-PI
  Amount: $99,920
  Time: From 10/01/2006 to 10/31/2007

- NSF-IIS-0549313: "A Test-bed for Personalized, Privacy-preserving and High Quality Health Information Delivery"
  Role: Co-PI
  Amount: $100,000
  Time: From 09/15/2005 to 08/31/2007

PRESENTATIONS AT INDUSTRY CONFERENCES

2016 “Discovering and Exploiting Novel Security Vulnerabilities in Apple Zeroconf”. Black Hat USA (Presented by L. Xing and X. Bai)

2016 “Dangerous Hare: Hanging Attribute References Hazards Due to Vendor Customization”. Black Hat USA (Presented by N. Zhang)

PATENTS

1. Y. Huang, X. Wang, H. Tang and X. Wang, "Privacy-Preserving Similar Patient Query Systems and Methods". US15682240
2. X. Wang, K. Yuan, X. Liao and R. Beyah, "Systems and Methods for Detection of Infected Websites". US10880330
3. X. Wang, K. Yuan, X. Zhou, M. Naveed, S. Demetriou, C. Gunter. "External Resource Control of Mobile Devices". US10685142
4. L. Xing and X. Wang, "Detection of Pileup Vulnerabilities in Mobile Operating Systems". US9386027 B2
5. X. Wang, H. Tang, Y. Chen and B. Peng, "Secure and Scalable Mapping of Human Sequencing Reads on Hybrid Clouds". US9276911
6. Y. Xie, F. Yu, Z. Li and X. Wang, "Determining Legitimate and Malicious Advertisements Using Advertising Delivery Sequences". US20130339158 A1

RESEARCH INTERESTS

Confidential Computing, Trustworthy AI, AI-Powered Security Analysis, Carrier Network Security, Cybercrimes, IoT and Mobile Security, Healthcare Security and Privacy, Cloud and Web Security, Game-Theoretic Incentive Engineering

PUBLICATIONS

I am considered to be a top author in systems security during the past 21 years according to system security circus (Eurecom), an overview of system circus (EPFL) and CSRankings

1. H. Chen, Y. Zhang, X. Han, T. Mao, H. Rong, Y. Zhang, H. Zhang, X. Wang, L. Xing and X. Chen, 2025: "LineBreaker: Finding Token-Inconsistency Bugs using Large Language Models". In Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE)
2. H. Chen, Q. Zhou, S. Yang, S. Dang, X. Han, D. Zhang, F. Zhang and X. Wang, 2025: "Agora: Trust Less and Open More in Verification for Confidential Computing". In Proceedings of the 39th ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Language and Applications (OOPSLA)
3. Y. Guo, H. Chen, H. Chen, Y. Luo, X. Wang and C. Wang, 2025: "BOLT: Bandwidth-Optimized Lightning-Fast Oblivious Map powered by Secure HBM Accelerators". In Proceedings of the 32nd ACM Conference on Computer and Communications Security (CCS)
4. J. Cui, M. Zha, X. Wang and X. Liao, 2025: "The Odyssey of robots.txt Governance: Measuring Convention Implications of Web Bots in Large Language Model Services". In Proceedings of the 32nd ACM Conference on Computer and Communications Security (CCS)

5. P. Lv, M. Sun, H. Wang, X. Wang, S. Zhang, Y. Chen, K. Chen and L. Sun, 2025: “RAG-WM: An Efficient Black-Box Watermarking Approach for Retrieval-Augmented Generation of Large Language Models”. In Proceedings of the 32nd ACM Conference on Computer and Communications Security (CCS)

6. X. Yuan, J. Zhang, F. Guo, K. Chen, X. Wang, S. Zhang, Y. Chen, D. Liu, P. Liu, Z. Wang and R. Zhu, 2025: “EvilHarmony: Stealthy Adversarial Attacks against Black-box Speech Recognition Systems”. In Proceedings of the 46th IEEE Symposium on Security and Privacy (S&P)

7. Z. Wang, R. Zhu, Z. Zhang, H. Tang and X. Wang, 2025: “Rigging the Foundation: Manipulating Pre-training for Advanced Membership Inference Attacks”. In Proceedings of the 46th IEEE Symposium on Security and Privacy (S&P)

8. Y. Gong, Z. Chen, J. Liu, M. Chen, F. Yu, W. Lu, X. Wang and X. Liu, 2025: “Topic-FlipRAG: Topic-Orientated Adversarial Opinion Manipulation Attacks to Retrieval-Augmented Generation Models”. In Proceedings of the 34th USENIX Security Symposium (Security)

9. H. Chen, H. Chen, M. Sun, C. Wang and X. Wang, 2025: “PICACHV: Formally Verified Data Use Policy Enforcement for Secure Data Analytics”. In Proceedings of the 34th USENIX Security Symposium (Security)

10. Z. Wang, R. Zhu, D. Zhou, Z. Zhang, X. Wang and H. Tang, 2025: “Sharpness-Aware Initialization: Improving Differentially Private Machine Learning from First Principles”. In Proceedings of the 34th USENIX Security Symposium (Security)

11. W. Wang, L. Song, B. Mei, S. Liu, S. zhao, S. Yan, X. Wang, D. Meng, R. Hou, 2025: “The Road to Trust: Building Enclave within Confidential VMs”. In Proceedings of the 32nd Annual Network and Distributed System Security Symposium (NDSS)

12. M. Zheng, J. Xue, Z. Wang, X. Chen, Q. Lou, L. Jiang and X. Wang, 2024: “SSL-Cleanse: Trojan Detection and Mitigation in Self-Supervised Learning”. In Proceedings of the 18th European Conference on Computer Vision (ECCV)

13. T. Le, D. Zhao, Z. Wang, X. Wang and Y. Tian, 2024: “Alexa, is the skill always safe? Uncover Lenient Skill Vetting Process and Protect User Privacy at Run Time”. In Proceedings of the 46th International Conference on Software Engineering: Software Engineering in Society Track (ICSE-SEIS)

14. Y. Zhang, Y. Ma, J. Liu, X. Liu, X. Wang and W. Lu, 2024: “Detection Vs. Anti-detection: Is Text Generated by AI Detectable?”. In Proceedings of the 19th iConference

15. Y. Zhang, L. Zhao, C. Che, X. Wang, D. Meng and R. Hou, 2024: “SpecFL: An Efficient Speculative Federated Learning System for Tree-based Model Training”. In Proceedings of the 30th IEEE International Symposium on High-Performance Computer Architecture (HPCA)

16. D. Xu, K. Chen, M. Lin, C. Lin and X. Wang, 2024: “AutoPwn: Artifact-Assisted Heap Exploit Generation for CTF PWN Competitions”. IEEE Transactions on Information Forensics and Security (TIFS), Vol. 19: 293-306

17. M. Zha, Z. Lin, S. Tang, X. Liao, Y. Nan and X. Wang, 2024: “Understanding Cross-Platform Referral Traffic for Illicit Drug Promotion”. In Proceedings of the 31st ACM Conference on Computer and Communications Security (CCS)

18. X. Chen, S. Tang, R. Zhu, S. Yan, L. Jin, Z. Wang, L. Su, Z. Zhang, X. Wang and H. Tang, 2024: “The Janus Interface: How Fine-Tuning in Large Language Models Amplifies the

Privacy Risks". In Proceedings of the 31st ACM Conference on Computer and Communications Security (CCS)

19. Y. Zhang, Z. Hu, X. Wang, Y. Hong, Y. Nan, X. Wang, J. Cheng and L. Xing, 2024: "Navigating the Privacy Compliance Maze: Understanding Risks with Privacy-Configurable Mobile SDKs". In Proceedings of the 33rd USENIX Security Symposium (Security)
20. Z. Lin, J. Cui, X. Liao and X. Wang, 2024: "Malla: Demystifying Real-world Large Language Model Integrated Malicious Services". In Proceedings of the 33rd USENIX Security Symposium (Security)
21. H. Rong, W. You, X. Wang, T. Mao, 2024: "Toward Unbiased Multiple-Target Fuzzing with Path Diversity". In Proceedings of the 33rd USENIX Security Symposium (Security)
22. Z. Wang, R. Zhu, D. Zhou, Z. Zhang, J. Mitchell, H. Tang and X. Wang, 2024: "DPAdapter: Improving Differentially Private Deep Learning through Noise Tolerance Pre-training". In Proceedings of the 33rd USENIX Security Symposium (Security)
23. Z. Wang, D. Tang, X. Wang, W. He, Z. Geng and W. Wang, 2024: "Tossing in the Dark: Practical Bit-Flipping on Gray-box Deep Neural Networks for Runtime Trojan Injection". In Proceedings of the 33rd USENIX Security Symposium (Security)
24. D. Xu, D. Tang, Y. Chen, X. Wang, K. Chen, H. Tang and L. Li, 2024: "Racing on the Negative Force: Efficient Vulnerability Root-Cause Analysis through Reinforcement Learning on Counterexamples". In Proceedings of the 33rd USENIX Security Symposium (Security)
25. Z. Lin, Z. Li, X. Liao, X. Wang and X. Liu, 2024: "MAWSEO: Adversarial Wiki Search Poisoning for Illicit Online Promotion". In Proceedings of the 45th IEEE Symposium on Security and Privacy (S&P)
26. R. Zhu, D. Tang, S. Tang, Z. Wang, G. Tao, S. Ma, X. Wang and H. Tang, 2024: "Gradient Shaping: Enhancing Backdoor Attack Against Reverse Engineering". In Proceedings of the 31st Annual Network and Distributed System Security Symposium (NDSS)
27. Z. Li, W. Liu, X. Wang, B. Yuan, H. Tian, H. Jin and S. Yan, 2023: "Lost along the Way: Understanding and Mitigating Path-Misresolution Threats to Container Isolation". In Proceedings of the 30th ACM Conference on Computer and Communications Security (CCS)
28. Z. Wang, J. Guan, X. Wang, W. Wang, L. Xing and F. Alharbi, 2023: "The Danger of Minimum Exposures: Understanding Cross-App Information Leaks on iOS through Multi-Side-Channel Learning". In Proceedings of the 30th ACM Conference on Computer and Communications Security (CCS)
29. Y. Nan, X. Wang, L. Xing, X. Liao, R. Wu, J. Wu, Y. Zhang and X. Wang, 2023: "Are You Spying on Me? Large-Scale Analysis on IoT Data Exposure through Companion Apps". In Proceedings of the 32nd USENIX Security Symposium (Security)

30. X. Wang, Y. Sun, S. Nanda and X. Wang, 2023: "Credit Karma: Understanding Security Implications of Exposed Cloud Services through Automated Capability Inference". In Proceedings of the 32nd USENIX Security Symposium (Security)
31. H. Chen, H. Chen, M. Sun, K. Li, Z. Chen and X. Wang, 2023: "A Verified Confidential Computing as a Service Framework for Privacy Preservation". In Proceedings of the 32nd USENIX Security Symposium (Security)
32. X. Wang, Y. Zhang, X. Wang, Y. Jia and L. Xing, 2023: "Union under Duress: Understanding Hazards of Duplicate Resource Mismediation in Android Software Supply Chain". In Proceedings of the 32nd USENIX Security Symposium (Security)

33. Z. Yu, Y. Chang, S. Zhai, N. Deily, T. Ju, X. Wang, U. Jammalamadaka and N. Zhang, 2023: “XCheck: Verifying Integrity of 3D Printed Patient-Specific Devices via Computing Tomography”. In Proceedings of the 32nd USENIX Security Symposium (Security)

34. Y. Chen, D. Tang, Y. Yao, M. Zha and X. Wang, 2023: “Sherlock on Specs: Building LTE Conformance Tests through Automated Reasoning”. In Proceedings of the 32nd USENIX Security Symposium (Security)

35. R. Zhu, D. Tang, Siyuan Tang, X. Wang and H. Tang, 2023: “Selective Amnesia: On Efficient, High-Fidelity and Blind Suppression of Backdoor Effects in Trojaned Machine Learning Models”. In Proceedings of the 44th IEEE Symposium on Security and Privacy (S&P)

36. W. Wang, W. Liu, H. Chen, X. Wang, H. Tian, D. Lin, 2023: “Trust Beyond Border: Lightweight, Verifiable User Isolation for Protecting In-Enclave Services”. IEEE Trans. Dependable Secur. Comput. 20(1): 522-538 (2023).

37. Z. Wang, P. Li, R. Hou, Z. Li, J. Cao, X. Wang, D. Meng, 2023: “HE-Booster: An Efficient Polynomial Arithmetic Acceleration on GPUs for Fully Homomorphic Encryption”. IEEE Trans. Parallel Distributed Syst. 34(4): 1067-1081 (2023).

38. J. Chen, Y. Wang, Y. Zhou, W. Ding, Y. Tang, X. Wang and K. Li, 2023: “Understanding the Security Risks of Decentralized Exchanges by Uncovering Unfair Trades in the Wild”. In Proceeding of 8th IEEE European Symposium on Security and Privacy (EuroS&P).

39. S. Tang, X. Mi, Y. Li, X. Wang and K. Chen, 2022: “Clues in Tweets: Twitter-Guided Discovery and Analysis of SMS Spam”. In Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS)

40. H. Liu, Z. Yu, M. Zha, X. Wang, W. Yeoh, Y. Vorobeychik and N. Zhang, 2022: “When Evil Calls: Targeted Adversarial Voice over IP-Telephony Network”. In Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS)

41. J. Liu, Y. Kang, D. Tang, K. Song, C. Sun, X. Wang, W. Lu and X. Liu, 2022: “Order-Disorder: Imitation Adversarial Attacks for Black-box Neural Ranking Models”. In Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS)

42. Y. Chen, D. Tang, Y. Yao, M. Zha, X. Wang and X. Liu, 2022: “Seeing the Forest for the Trees: Understanding Security Hazards in the 3GPP Ecosystem through Intelligent Analysis on Change Requests”. In Proceedings of the 31st USENIX Security Symposium (Security)

43. Z. Li, W. Liu, H. Chen, X. Wang, X. Liao, L. Xing, M. Zha, H. Jin and D. Zou, 2022: “Robbery on DevOps: Understanding and Mitigating Illicit Cryptomining on Continuous Integration Service Platforms”. In Proceedings of the 43rd IEEE Symposium on Security and Privacy (S&P)

44. P. Wang, Z. Lin, X. Liao and X. Wang, 2022: “Demystifying Local Business Search Poisoning for Illicit Drug Promotion”, In Proceedings of the 29th Annual Network and Distributed System Security Symposium (NDSS)

45. M. Zhang, J. Wang, Y. Nan, X. Wang, Y. Zhang and Z. Yang, 2022: “Hazard Integrated: Understanding Security Risks in App Extensions to Team Chat Systems”, In Proceedings of the 29th Annual Network and Distributed System Security Symposium (NDSS)

46. Y. Chen, J. Zhang, X. Yuan, S. Zhang, K. Chen, X. Wang and S. Guo, 2022: “SoK: A Modularized Approach to Study the Security of Automatic Speech Recognition Systems”**.** ACM Transactions on Privacy and Security (TOPS), 25(3): 17:1- 17:31.

47. T. Chen, Z. Li, X. Luo, X. Wang, T. Wang, Z. He, K. Fang, Y. Zhang, H. Zhu, H. Li, Y. Cheng and X. Zhang, 2022: “SigRec: Automatic Recovery of Function Signatures in Smart Contracts”. IEEE Transactions on Software Engineering. 48(8): 3066-3086.

48. T. Kuo, X. Jiang, H. Tang, X. Wang, A. Harmaci, M. Kim, K. Post, D. Bu, T. Bath, J. Kim, W. Liu, H. Chen and L. Ohno-Machado, 2022: “The Evolving Privacy and Security Concerns for Genomic Data Analysis and Sharing as Observed from the iDASH Competition”. Journal of the American Medical Informatics Association (JAMIA).

49. W. Wang, W. Liu, H. Chen, X. Wang, H. Tian and D. Lin, 2021: “Trust Beyond Border: Lightweight, Verifiable User Isolation for Protecting In-Enclave Services”. IEEE Transactions on Dependable and Secure Computing (TDSC).

50. D. Seyler, W. Liu, X. Wang and C. Zhai, 2021: “Towards Dark Jargon Interpretation in Underground Forums”. In Proceedings of the 43rd annual BCS-IRSG European Conference on Information Retrieval (ECIR).

51. W. Liu, W. Wang, H. Chen, X. Wang, Y. Liu, K. Chen, X. Wang, Q. Shen, Y. Chen and H. Tang, 2021: “Practical and Efficient in-Enclave Verification of Privacy Compliance”. In Proceedings of the 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).

52. D. Seyler, W. Liu, Y. Zhang, X. Wang, C. Zhai, 2021: “DarkJargon.net: A Platform for Understanding Underground Conversation with Latent Meaning”. In Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR).

53. Y. Jia, B. Yuan, L. Xing, D. Zhao, Y. Zhang, X. Wang, Y. Liu, K. Zheng, P. Crnjak, Y. Zhang, D. Zou and H. Jin, 2021: “Who's In Control? On Security Risks of Disjointed IoT Device Management Channels”. In Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS)

54. C. Widanage, W. Liu, J. Li, H. Chen, X. Wang, H. Tang and J. Fox, 2021: “HySec-Flow: Privacy-Preserving Genomic Computing with SGX-based Big-Data Analytics Framework”. In Proceedings of the 14th IEEE International Conference on Cloud Computing (CLOUD).

55. Y. Lee, X. Wang, X. Liao and X. Wang, 2021: “Understanding Illicit UI in iOS Apps Through Hidden UI Analysis”. IEEE Transactions on Dependable and Secure Computing (TDSC), 18(5): 2390-2402.

56. J. Wang, Y. Xiao, X. Wang, Y. Nan, L. Xing, X. Liao, J. Dong, N. Serrano, H. Lu, X. Wang, Y. Zhang, 2021: “Understanding Malicious Cross-library Data Harvesting on Android”. In Proceedings of the 30th USENIX Security Symposium (Security)

57. B. Liang, H. Li, M. Su, X. Li, W. Shi and X. Wang, 2021: “Detecting Adversarial Image Examples in Deep Neural Networks with Adaptive Noise Reduction”. IEEE Transactions on Dependable and Secure Computing (TDSC), 18(1): 72-85.

58. D. Bu, X. Wang and H. Tang, 2021: “Haplotype-based membership inference from summary genomic data”. Bioinformatics, Volume 37, Issue Supplement_1, July 2021.

59. Y. Chen, Y. Yao, X. Wang, D. Xu, C. Yue, X. Liu, K. Chen, H. Tang and B. Liu, 2021 "Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis". In Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P)

60. L. Su, X. Shen, X. Du, X. Liao, X. Wang, L. Xing and B. Liu, 2021 “Evil Under the Sun: Understanding and Discovering Attacks on Ethereum Decentralized Applications”, In Proceedings of the 30th USENIX Security Symposium (Security)

61. X. Mi, S. Tang, Z. Li, X. Liao, F. Qian and X. Wang, 2021 “Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks”, In Proceedings of the 28th Annual Network and Distributed System Security Symposium (NDSS)

62. K. Li, J. Chen, X. Liu, Y Tang, X. Wang and X. Luo, 2021 “As Strong As Its Weakest Link: How to Break Blockchain DApps at RPC Service”, In Proceedings of the 28th Annual Network and Distributed System Security Symposium (NDSS)

63. N. Dokmai, C. Kockan, K. Zhu, X. Wang, C. Sahinalp and H. Cho, 2021 “Privacy-Preserving Genotype Imputation in a Trusted Execution Environment”, In Proceedings of the 25th International Conference on Research in Computational Molecular Biology (RECOMB)

64. D. Tang, X. Wang, H. Tang and K. Zhang, 2021 “Demon in the Variant: Statistical Analysis of DNNs for Robust Backdoor Contamination Detection”, In Proceedings of the 30th USENIX Security Symposium (Security)

65. R. Zhu, C. Jiang, X. Wang, S. Wang, H. Zheng and H. Tang, 2020 “Privacy-preserving construction of generalized linear mixed model for biomedical computation”, Bioinformatics, Vol. 36, Supplement 1, the 28th Conference on Intelligent Systems for Molecular Biology (ISMB)

66. Y. Long, L. Wang, D. Bu, V. Bindschaedler, X. Wang, H. Tang, C. Gunter, K. Chen, 2020 “A Pragmatic Approach to Membership Inferences on Machine Learning Models”, In Proceedings of the 5th IEEE European Symposium on Security and Privacy (EuroS&P)

67. H. Lu, L. Xing, Y. Xiao, Y. Zhang, X. Liao, X. Wang and X. Wang, 2020 “Demystifying Resource Management Risks in Emerging Mobile App-in-App Ecosystems”, In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)

68. E. Alowaisheq, S. Tang, Z. Wang, F. Alharbi, X. Liao and X. Wang, 2020 “Zombie Awakening: Stealthy Hijacking of Active Domains Through DNS Hosting Referral”, In Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS)

69. T. Lv, R. Li, Y. Yang, K. Chen, X. Liao, X. Wang, P. Hu and L. Xing, 2020 “RTFM! Automatic Assumption Discovery and Verification Derivation from Library Document for API Misuse Detection”, In Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS)

70. Y. Chen, X. Yuan, J. Zhang, Y. Zhao, S. Zhang, K. Chen and X. Wang, 2020 “Devil's Whisper: A General Approach for Physical Adversarial Attacks against Commercial Black-box Speech Recognition Devices”, In Proceedings of the 29th USENIX Security Symposium (Security)

71. B. Yuan, Y. Jia, L. Xing, D. Zhao, X. Wang, D. Zou, H. Jin and Y. Zhang, 2020 “Shattered Chain of Trust: Understanding Security Risks in Cross-Cloud IoT Access Delegation”, In Proceedings of the 29th USENIX Security Symposium (Security)

72. J. Zhu, R. Hou, X. Wang, W. Wang, J. Cao, B. Zhao, Z. Wang, Y. Zhang, J. Ying, L. Zhang and D. Meng, 2020 “Enabling Rack-scale Confidential Computing using Heterogeneous Trusted Execution Environment”, In Proceedings of the 41th IEEE Symposium on Security and Privacy (IEEE S&P)

73. Y. Jia, L. Xing, Y. Mao, D. Zhao, X. Wang, S. Zhao and Y. Zhang, 2020 “Burglars' IoT Paradise: Understanding and Mitigating Security Risks of General Messaging Protocols on IoT Clouds”, In Proceedings of the 41th IEEE Symposium on Security and Privacy (IEEE S&P)

74. P. Wang, X. Liao, Y. Qin and X. Wang, 2020 “Into the Deep Web: Understanding E-commerce Fraud from Autonomous Chat with Cybercriminals”, In Proceedings of the 27th Annual Network and Distributed System Security Symposium (NDSS)

75. Y. Lee, Y. Zhao, J.Zeng, K. Lee,N. Zhang, F. H. Zhezan, Y. Tian, K. Chen and X. Wang, 2020 “Using Sonar for Liveness Detection to Protect Smart Speakers against Remote Attackers”, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)

76. Z. Mi, H. Chen, Y. Zhang, S. Peng, X. Wang and M. Reiter, 2020 “CPU Elasticity to Mitigate Cross-VM Runtime Monitoring”, IEEE Transactions on Dependable and Secure Computing, 17(5): 1094-1108

77. Y. Chen, L. Xing, Y. Qin, X. Liao and X. Wang, 2019 “Devils in the Guidance: Predicting Logic Vulnerabilities in Payment Syndication Services through Automated Documentation Analysis”, In Proceedings of the 28th USENIX Security Symposium (Security)

78. Y. Lee, X. Wang, K. Lee, X. Liao and X. Wang, 2019 “Understanding iOS-based Crowdturfing Through Hidden UI Analysis”, In Proceedings of the 28th USENIX Security Symposium (Security)

79. X. Feng, X. Liao, X. Wang, H. Wang, Q. Li, K. Yang, H. Zhu and L. Sun, 2019 “Understanding and Securing Device Vulnerabilities through Automated Bug Report Analysis”, In Proceedings of the 28th USENIX Security Symposium (Security)

80. X. Wang, Y. Sun, S. Nanda and X. Wang, 2019 “Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps”, In Proceedings of the 28th USENIX Security Symposium (Security)

81. K. Yuan, D. Tang, X. Liao, X. Wang, X. Feng, Y. Chen, M. Sun, H. Lu, K. Zhang, 2019 “Stealthy Porn: Understanding Real-World Adversarial Images for Illicit Online Promotion”, In Proceedings of the 40th IEEE Symposium on Security and Privacy (IEEE S&P)

82. Y. Chen, M. Zhang, N. Zhang, D. Xu, Q. Zhao, X. Feng, K. Yuan, Y. Su, Y. Tian, K. Chen X. Wang and W. Zou, 2019 “Demystifying Hidden Privacy Settings in Mobile Apps”, In Proceedings of the 40th IEEE Symposium on Security and Privacy (IEEE S&P)

83. W. You, X. Wang, S. Ma, J. Huang, X. Zhang, X. Wang, B. Liang, 2019 “On-the-fly Input Type Probing for Better Zero-day Vulnerability Discovery”, In Proceedings of the 40th IEEE Symposium on Security and Privacy (IEEE S&P)

84. E. Alowaisheq, P. Wang, S. Alrwais, X. Liao, X. Wang, T. Alowaisheq, X. Mi, S. Tang, B. Liu, 2019 “Cracking Wall of Confinement: Understanding and Analyzing Malicious Domain Takedowns”, In Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS)

85. I. Hagestedt, Y. Zhang, M. Humbert, P. Berrang, H. Tang, X. Wang, M. Backes, 2019 “MBeacon: Privacy-Preserving Beacons for DNA Methylation Data”. In Proceedings of the Annual Network and Distributed System Security Symposium (NDSS)

86. N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian and F. Qian, 2019 “Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems”. In Proceedings of the 40th IEEE Symposium on Security and Privacy (IEEE S&P)

87. X. Mi, X. Feng, X. Liao, B. Liu, X. Wang, F. Qian, Z. Li, S. Alrwais, L. Sun, Y. Liu, 2019 “Residential Evil: Understanding Residential IP Proxy as a Dark Service”. In Proceedings of 40th IEEE Symposium on Security and Privacy (IEEE S&P)

88. X. Zhang, Y. Zhang, Q. Mo, H. Xia, Z. Yang, M. Yang, X. Wang, L Lu, H. Duan, 2018 “An Empirical Study of Web Resource Manipulation in Real-World Mobile Applications”. In the Proceedings of the 27th USENIX Security Symposium (Security).

89. X. Yuan, Y. Chen, Y. Zhao, Y. Long, X. Liu, K. Chen, S. Zhang, H. Huang, X. Wang, C. Gunter, 2018 "CommanderSong: A Systematic Approach for Practical Adversarial Voice Recognition". In Proceedings of the 27th USENIX Security Symposium (Security).

90. K. Yuan, X. Liao, X. Wang, 2018 "Reading Thieves' Cant: Automatically Identifying and Understanding Dark Jargons from Cybercrime Marketplaces". In Proceedings of the 27th USENIX Security Symposium (Security).

91. G. Chen, W. Wang, T. Chen, S. Chen, Y. Zhang, X. Wang, T. Lai, D. Lin, 2018 "Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races". In Proceedings of the 39th IEEE Symposium on Security and Privacy (IEEE S&P)

92. J. Chen, W. Diao, Q. Zhao, C. Zuo, Z. Lin, X. Wang, W. Lau, M. Sun, R. Yang, K. Zhang, 2018 "IoTFuzzer: Discovering Memory Corruptions in IoT Through App-based Fuzzing". In Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS)

93. X. Zhang, X. Wang, X. Bai, Y. Zhang, X. Wang, 2018 "OS-level Side Channels without Procfs: Exploring Cross-App Information Leakage on iOS". In Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS)

94. Y. Nan, Z. Yang, X. Wang, Y. Zhang, D. Zhu, M. Yang, 2018 "Finding Clues for Your Secrets: Semantics-Driven, Learning-Based Privacy Discovery in Mobile Apps". In Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS)

95. Y. Duan, M. Zhang, A. Bhaskar, H. Yin, X. Pan, T. Li, X. Wang, X. Wang, 2018 "Things You May Not Know About Android (Un)Packers: A Systematic Study based on Whole-System Emulation". In Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS)

96. P. Wang, X. Mi, X. Liao, X. Wang, K. Yuan, F. Qian, R. Beyah, 2018 "Game of Missuggestions: Semantic Analysis of Search-Autocomplete Manipulations". In Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS)

97. J. Tang, A. Korolova, X. Bai, X. Wang, X. Wang, 2017 "Privacy Loss in Apple's Implementation of Differential Privacy on macOS 10.12". Preprint, arXiv: 1709.02753.

98. K. Chen, T. Li, B. Ma, P. Wang, X. Wang, P. Zong, 2017 "Filtering for Malice Through the Data Ocean: Large-Scale PHA Install Detection at the Communication Service Provider Level". In Proceedings of the 20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID).

99. Y. Chen, W. You, Y. Lee, K. Chen, X. Wang, W. Zou, 2017 "Mass Discovery of Android Traffic Imprints through Instantiated Partial Execution". In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)

100. T. Li, X. Wang, M. Zha, K. Chen, X. Wang, L. Xing, X. Bai, N. Zhang, X. Han, 2017 "Unleashing the Walking Dead: Understanding Cross-App Remote Infections on Mobile WebViews". In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)

101. W. You, P. Zong, K. Chen, X. Wang, X. Liao, P. Bian, B. Liang, 2017 "SemFuzz: Semantics-based Automatic Generation of Proof-of-Concept Exploits". In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)

102. W. Wang, G. Chen, X. Pan, Y. Zhang, X. Wang, V. Bindschaedler, H. Tang, C. Gunter, 2017 "Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in

SGX". In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)

103. X. Mi, F. Qian, Y. Zhang, X. Wang, 2017 "An Empirical Characterization of IFTTT: Ecosystem, Usage and Performance". In Proceedings of the 17th ACM Internet Measurement Conference (IMC).

104. X. Bai, Z. Zhou, X. Wang, Z. Li, X. Mi, N. Zhang, T. Li, S. Hu, K. Zhang, 2017 "Picking Up My Tab: Understanding and Mitigating Synchronized Token Lifting and Spending in Mobile Payment". In Proceedings of the 26th USENIX Security Symposium (Security).

105. Y. Tian, N. Zhang, Y. Lin, X. Wang, B. Ur, X. Guo, P. Tague, 2017 "SmarthAuth: User-Centered Authorization for the Internet of Things". In Proceedings of the 26th USENIX Security Symposium (Security)

106. S. Alrwais, X. Liao, X. Mi, P. Wang, X. Wang, F. Qian and R. Beyah, D. McCoy, 2017 "Under the Shadow of Sunshine: Understanding and Detecting BulletPoof Hosting on Legitimate Service Provider Networks". In Proceedings of the 38th IEEE Symposium on Security and Privacy (IEEE S&P)

107. Y. Lee, T. Li, N. Zhang, S. Demetriou, M. Zha, X. Wang, K. Chen, X. Zhou, X. Han, M. Grace, 2017 "Ghost Installer in the Shadow: Security Analysis of App Installation on Android". In Proceedings of the 47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2017)

108. X. Liu, T. Chen, F. Qian, Z. Guo, F. Lin, X. Wang, K. Chen, 2017 "Characterizing Smartwatch Usage in the Wild". In Proceedings of the 15th ACM International Conference on Mobile Systems, Applications, and Services (ACM MobiSys)

109. X. Pan, X. Wang, Y. Duan, X. Wang, H. Ying, 2017 "Dark Hazard: Learning-based, Large-Scale Discovery of Hidden Sensitive Operations in Android Apps". In Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS)

110. Y. Nan, Z. Yang, M. Yang, S. Zhou, Y. Zhang, G. Gu, X. Wang, L. Sun, 2017 "Identifying User-Input Privacy in Mobile Applications at a Large Scale". In the IEEE Transactions on Information Forensics & Security (Extension of 127)

111. X. Mi, F. Qian and X. Wang, 2016 "SMig: Stream Migration Extension for HTTP/2". In Proceedings of the 12th International Conference on Emerging Networking Experiments and Technologies (CoNEXT).

112. S. Alrwais, K. Yuan, E. Alowaisheq, X. Liao, A. Oprea, X. Wang and Z. Li, 2016 "Catching Predators at Watering Holes: Finding and Understanding Strategically Compromised Websites". In Proceedings of the 32nd Annual Computer Security Applications Conference (ACSAC).

113. X. Liao, K.Yuan, X. Wang, Z. Li, L. Xing and R. Beyah, 2016 "Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence". In Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)

114. X. Liao, S. Alrwais, K. Yuan, L. Xing, X. Wang, S. Hao and R. Beyah, 2016 "Lurking Malice in the Cloud: Understanding and Detecting Cloud Repository as a Malicious Service". In Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS)

115. X. Bai, L. Xing, N. Zhang, X. Wang, X. Liao, T. Li and S. Hu, 2016 "Staying Secure and Unprepared: Understanding and Mitigating the Security Risks of Apple ZeroConf". In Proceedings of the 37th IEEE Symposium on Security and Privacy (IEEE S&P)

116. K. Chen, X. Wang, Y. Chen, P. Wang, Y. Lee, X. Wang, B. Ma, A. Wang, Y. Zhang, W. Zou, 2016 "Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS". In Proceedings of the 37th IEEE Symposium on Security and Privacy (IEEE S&P)

117. X. Liao, K. Yuan, X. Wang, Z. Pei, H. Yang, J. Chen, H. Duan, K. Du, E. Alowaisheq, S. Alrwais, L. Xing and R. Beyah, 2016 "Seeking Nonsense, Looking for Trouble: Efficient Promotional-Infection Detection through Semantic Inconsistency Search". In Proceedings of the 37th IEEE Symposium on Security and Privacy (IEEE S&P)

118. S. Li, N. Bandeira, X. Wang and H. Tang, 2016 "On the Privacy Risks of Sharing Clinical Proteomics Data". In Proceedings of AMIA 2016 Joint Summits on Translational Science

119. M. Naveed, E. Ayday, E. Clayton, J. Fellay, C. Gunter, J. Hubaux, B. Malin, X. Wang, 2015 "Privacy in the Genomic Era", in ACM Computing Surveys (CSUR), Vol. 48, Issue 1 p. 1-44

120. V. Bindschaedler, M. Naveed, X. Pan, X. Wang and Y. Huang, 2015 "Practicing Oblivious Access on Cloud Storage: the Gap, the Fallacy and the New Way Forward". In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS).

121. Y. Chen, T. Li, X. Wang, K. Chen and X. Han, 2015 "Perplexed Messengers from the Cloud: Automated Security Analysis of Push-Messaging Integrations". In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)

122. Y. Aafer, N. Zhang, Z. Zhang, X. Zhang, K. Chen, X. Wang, X. Zhou, W. Du and M. Grace, 2015 "Hare Hunting in the Wild Android: A Study on the Threat of Hanging Attribute References". In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)

123. X. Wang, Y. Huang, Y. Zhao, H. Tang, X. Wang and D. Bu, 2015 "Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance". In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)

124. L. Xing, X. Bai, T. Li, X. Wang, K. Chen, X. Liao, S. Hu and X. Han, 2015 "Cracking App Isolation on Apple: Unauthorized Cross-App Resource Access on MAC OS X and iOS". In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)

125. Y. Chen, V. Bindschaedler, X. Wang, S. Berger and D. Pendarakis, 2015, "Elite: Automatic Orchestration of Elastic Detection Services to Secure Cloud Hosting", In Proceedings of the18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID).

126. K. Chen, P. Wang, Y. Lee, X. Wang, N. Zhang, H. Huang, W. Zou and P. Liu, 2015 "Finding Unknown Malice in 10 Seconds: Mass Vetting for New Threats at the Google-Play Scale". In Proceedings of the 24th USENIX Security Symposium (Security).

127. Y. Nan, M. Yang, Z. Yang, S. Zhou, G. Gu and X. Wang, 2015 "UIPicker: User-Input Privacy Identification in Mobile Applications". In Proceedings of the 24th USENIX Security Symposium (Security)

128. N. Zhang, K. Yuan, M. Naveed, X. Zhou and X. Wang, 2015 "Leave Me Alone, App-level Protection Against Runtime Information Gathering on Android". In Proceedings of the 36th IEEE Symposium on Security and Privacy (IEEE S&P)

129. S. Demetriou, X. Zhou, M. Naveed, Y. Lee, K. Yuan, X. Wang and C. Gunter, 2015 "What's in Your Dongle and Bank Account? Mandatory and Discretionary Protection of

Android External Resources’’. In Proceedings of the 22nd Annual Network and Distributed System Security Symposium (NDSS)

130. Y. Zhao, X. Wang, X. Jiang, L. Ohno-Machado and H. Tang, 2015 “Choosing Blindly but Wisely: Differentially Private Solicitation of DNA Datasets for Disease Marker Discovery”. Journal of the American Medical Informatics Association (JAMIA)

131. M. Naveed, S. Agrawal, M. Prabhakaran, X. Wang, E. Ayday, J. Hubaux and C. Gunter, 2014 “Controlled Functional Encryption”. In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)

132. T. Li, X. Zhou, L. Xing, Y. Li, M. Naveed, X. Wang and X. Han, 2014 “Mayhem in the Push Clouds: Understanding and Mitigating Security Hazards in Mobile Push-Messaging Services”. In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)

133. S. Alrwais, K. Yuan, E. Alowaisheq, Z. Li and X. Wang, 2014 “Understanding the Dark Side of Domain Parking”. In Proceedings of the 23rd USENIX Security Symposium (Security).

134. L. Xing, X. Pan, R. Wang, K. Yuan and X. Wang, 2014 “Upgrading Your Android, Elevating My Malware: Privilege Escalation Through Mobile OS Updating”. In Proceedings of the 35th IEEE Symposium on Security and Privacy (IEEE S&P).

135. X. Zhou, Y. Lee, N. Zhang, M. Naveed and X. Wang, 2014 “The Peril of Fragmentation: Security Hazards in Android Device Driver Customizations”. In Proceedings of the 35th IEEE Symposium on Security and Privacy (IEEE S&P).

136. Z. Li, S. Alrwais, X. Wang and E. Alowaisheq, 2014 “Hunting the Red Fox Online: Understanding and Detection of Mass Redirect-Script Injections”. In Proceedings of the 35th IEEE Symposium on Security and Privacy (IEEE S&P)

137. A. Zhang, X. Xie, K. Chang, C. Gunter, J. Han, X. Wang, 2014 “Privacy Risk in Anonymized Heterogeneous Information Networks”. In Proceedings of the 16th International Conference on Extending Database Technology (EDBT)

138. C. Lin, H. Li, X. Zhou and X. Wang, 2014 “Screenmilker: How to Milk Your Android Screen for Secrets”. In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS).

139. M. Naveed, X. Zhou, S. Demetriou, X. Wang and C. Gunter, 2014 “Inside Job: Understanding and Mitigating the Threat of External Device Misbonding on Android”. In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS).

140. A. Das, J. Bonneau, M. Caesar, N. Borisov and X. Wang, 2014 “The Tangled Web of Password Reuse”. In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS).

141. F. Zhang, W. He, Y. Chen, Z. Li, X. Wang, S. Chen and X. Liu, 2013 “Thwarting Wi-Fi Side-Channel Analysis through Traffic Demultiplexing”. IEEE Transactions on Wireless Communications, Volume 13, Issue 1.

142. X. Zhou, S. Demetriou, D. He, N. Muhammad, X. Pan, X. Wang, C. Gunter and K. Nahrstedt, 2013 “Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources”. In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS).

143. R. Wang, L. Xing, X. Wang and S. Chen, 2013 "Unauthorized Origin Crossing on Mobile Platforms: Threats and Mitigation". In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS).

144. Z. Li, S. Alrwais, Y. Xie, F. Yu and X. Wang, 2013 "Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures". In Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE S&P).

145. L. Xing, Y. Chen, X. Wang and S. Chen, 2013 "InteGuard: Toward Automatic Protection of Third-Party Web Service Integrations". In Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS).

146. Z. Li, K. Zhang, Y. Xie, F. Yu and X. Wang, 2012 "Knowing Your Enemy: Understanding and Detecting Malicious Web Advertising". In Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS).

147. R. Wang, S. Chen and X. Wang, 2012 "Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services". In Proceedings of the 33rd IEEE Symposium on Security and Privacy (IEEE S&P).

148. Y. Chen, B. Peng, X. Wang and H. Tang, 2012 "Large-Scale Privacy-Preserving Mappings of Human Genomic Sequences on Hybrid Clouds". In Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS).

149. K. Zhang, X. Zhou, Y. Chen, X. Wang and Y. Ruan, 2011 "Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds". In Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS).

150. X. Zhou, B. Peng, Y. Li, Y. Chen, H. Tang and X. Wang, 2011 "To Release or Not to Release: Evaluating Information Leaks in Aggregate Human-Genome Data". In Proceedings of European Symposium on Research in Computer Security (ESORICS).

151. R. Wang, S. Chen, X. Wang, and S. Qadeer, 2011 "How to Shop for Free Online – Security Analysis of Cashier-as-a-Service Based Web Stores". In Proceedings of the 32nd IEEE Symposium on Security and Privacy (IEEE S&P Oakland).

152. D. Liu, N. Li, X. Wang and J. Camp, 2011 "Security Risk Management Using Incentives". IEEE Security & Privacy Magazine, Vol. 9, Num. 6. (Extension of 153)

153. D. Liu, N. Li, X. Wang and J. Camp, 2011 "Beyond Risk-Based Access Control: Towards Incentive-Based Access Control". Short paper. In Proceedings of the 15th International Conference on Financial Cryptography and Data Security (FC).

154. R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia and X. Wang, 2011 "Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones". In Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS).

155. A. Kapadia, S. Myers, X. Wang and G. Fox. 2011 "Toward Securing Sensor Clouds". In Proceedings of the 12th International Symposium on Collaborative Technologies and Systems (CTS).

156. Z. Li and X. Wang, 2010 "FIRM: Capability-based Inline Mediation of Flash Behaviors". In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC).

157. K. Zhang, Z. Li, R. Wang, X. Wang and S. Chen, 2010 "Sidebuster: Automated Detection and Quantification of Side-Channel Leaks in Web Application Development". In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS).

158. Z. Li, K. Zhang and X. Wang, 2010 "Mash-IF: Practical Information-Flow Control within Client-side Mashups". In Proceedings of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).

159. A. Kapadia, S. Myers, X. Wang and G. Fox. 2010 "Secure Cloud Computing with Brokered Trusted Sensor Networks". In Proceedings of the 11th International Symposium on Collaborative Technologies and Systems (CTS).

160. S. Chen, R. Wang, X. Wang and K. Zhang, 2010 "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow". In Proceedings of the 31st IEEE Symposium on Security and Privacy (IEEE S&P Oakland).

161. X. Wang, P. Golle, M. Jakobsson and A. Tsow, 2009 "Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks". The ACM Transactions on Information and System Security (TISSEC). (Extension of 185)

162. R. Wang, X. Wang, Z. Li, H. Tang, M. Reiter and Z. Dong, 2009 "Privacy-Preserving Genomic Computation Through Program Specialization". In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)

163. R. Wang, Y. Li, X. Wang, H. Tang and X. Zhou, 2009 "Learning Your Identity and Disease from Research Papers: Information Leaks in Genome Wide Association Study". In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)

164. K. Zhang and X. Wang, 2009 "Peeping Tom in the Neighborhood: Keystroke Eavesdropping on Multi-user Systems". In Proceedings of the USENIX Security Symposium (Security)

165. C. Kolbitsch, P. Milani, C. Kruegel, E. Kirda, X. Zhou and X. Wang, 2009 "Effective and Efficient Malware Detection at the End Host". In Proceedings of the USENIX Security Symposium (Security)

166. D. Liu, L. J Camp and X. Wang, 2009 "Mitigating Insider Threats with Incentives". In Proceedings of the 13th International Conference on Financial Cryptography and Data Security (FC).

167. X. Wang, Z. Li and R. Wang. 2008 "Leapfrog: Protecting Sensitive Information within Commodity Applications". IU-CS TR670.

168. J. Li, N. Li, X. Wang and T. Yu, 2008 "Denial of Service Attacks and Defenses in Decentralized Trust Management". The International Journal of Information Security (IJIS). (Extension of 183)

169. X. Wang and M. Reiter. 2008 "Using Web-Referral Architecture to Mitigate Denial-of-Service Threats". The IEEE Transactions on Dependable and Secure Computing (TDSC). (Extension of 182)

170. D. Liu, X. Wang and L. J. Camp, 2008 "Game-theoretic Modeling and Analysis of Insider Threats". International Journal of Critical Infrastructure Protection. (Extension of 174)

171. R. Wang, X. Wang, K. Zhang and Z. Li. 2008 "Towards Automatic Reverse Engineering of Security Configurations". In Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS).

172. R. Wang, X. Wang and Z. Li. 2008 "Panalyst: Privacy-Aware Remote Error Analysis". In Proceedings of the 17th USENIX Security Symposium (Security).

173. Z. Li, X. Wang, Z. Liang and M. Reiter. 2008 "AGIS: Automatic Generation of Infection Signatures". In Proceedings of the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).

174. D. Liu, X. Wang and L. J. Camp. 2008 "Game Theoretic Modeling and Analysis of Insider Threats". In Proceedings of IFIP WG 11.10 International Conference on Critical Infrastructure Protection.

175. C. Richard, G. Philippe, M. Jakobsson, L. Wang and X. Wang. 2008 "Making CAPTCHAs Clickable". In Proceedings of Workshop on Mobile Computing Systems and Applications (HotMobile).

176. X. Wang, Z. Li, N. Li and J. Choi. 2008 "PRECIP: Towards Practical and Retrofittable Confidential Information Protection". In Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS).

177. X. Wang. 2008 "Case Study: A Defense-in-Depth Framework Against Spyware". A book chapter in the book "Crimeware", edited by M. Jakobsson and Z. Ramzan, Addison-Wesley Professional.

178. X. Wang, Z. Li, J. Xu, M. Reiter, C. Kil and J. Choi. 2008 "Fast and Black-box Exploit Detection and Signature Generation for Commodity Software". The ACM Transactions on Information and System Security (TISSEC). (Extension of 181)

179. X. Wang and M. Reiter. 2007 "A Multi-layer Framework for Puzzle-based Denial-of-Service Defense". International Journal of Information Security, August 2007. (Extension of 188 and 190)

180. Z. Li, X. Wang and J. Choi. 2007 "Spyshield: Preserving privacy from spyware add-ons". In Proceedings of the Recent Advance in Intrusion Detection (RAID).

181. X. Wang, Z. Li, J. Xu, M. Reiter, C. Kil and J. Choi. 2006 "Packet Vaccine: Black-box Exploit Detection and Signature Generation". In Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS).

182. X. Wang and M. Reiter. 2006 "WRAPS: Denial-of-Service Defense through Web Referrals". In Proceedings of the 25th IEEE Symposium on Reliable Distributed Systems (SRDS).

183. J. Li, N. Li, X. Wang, and T. Yu. 2006 "Denial of Service Attacks and Defenses in Decentralized Trust Management". In Proceedings of the Second International Conference on Security and Privacy in Communication Networks (SecureComm).

184. Y. Li, J. Mostafa and X. Wang. 2006 "A Privacy Enhancing Infomediary for Retrieving Personalized Health Information from Web". SIGIR 2006 Workshop on Personal Information Management.

185. P. Golle, X. Wang, M. Jakobsson and A. Tsow. 2006 "Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks". In Proceedings of IEEE Symposium on Security and Privacy (IEEE S&P Oakland).

186. M. Reiter, X. Wang and M. Wright. 2005 "Building a Reliable Mix Network through Fair Exchange". In Proceedings of the 3th International Conference on Applied Cryptography and Network Security (ACNS2005). LNCS 3531, Springer-Verlag.

187. M. Jakobsson, X. Wang and S. Wetzel. 2004 "Stealth Attacks on Vehicular Wireless Networks". Invited paper. In Proceedings of IEEE Vehicular Technology Conference 2004-Fall "Wireless Technologies for Global Security" (VTC).

188. X. Wang, M. Reiter. 2004 "Mitigating Bandwidth-Exhaustion Attacks using Congestion Puzzles". In Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS).

189. M. Reiter, X. Wang. 2004 "Fragile Mixing". In Proceedings of 11th ACM Conference on Computer and Communications Security (CCS).

190. X. Wang and M. Reiter. 2003. "Defending Against Denial-of-Service Attacks with Puzzle Auctions", In Proceedings of IEEE Symposium on Security and Privacy (IEEE S&P Oakland).

191. X. Wang, T. Sandholm. 2003. "Learning Near-Pareto-Optimal Conventions in Polynomial Time". Proceedings of the 17th Neural Information Processing Systems: Natural and Synthetic conference (NIPS).

192. T. Sandholm and X. Wang. 2002. "(Im)possibility of Safe Exchange Mechanism Design". Proceedings of National Conference on Artificial Intelligence (AAAI). pages: 338-344. Oral presentation track.

193. X. Wang and T. Sandholm. 2002. "Reinforcement Learning to Play An Optimal Nash Equilibrium in Team Markov Games", Proceedings of the 16th Neural Information Processing Systems: Natural and Synthetic conference (NIPS).

194. X. Wang, K. Hosanagar, R. Krishnan and P. Khosla. 2002. "Equilibrium Reputation Mechanism for Mobile Agent based Electronic commerce". Proceedings of ACM International conference on Autonomous Agent and Multi-agent Systems (AAMAS), pages: 308-309, Poster paper.

195. X. Wang, X. Yi, R. Krishnan, C. Siew and P. Khosla. 2002. "Mobile Agent Based Auctionlike Negotiation in Internet Retail Commerce". Book Chapter. J. Segovia, P.S. Szczepaniak, M. Niedzwiedzinski (Eds.) E-Commerce and Intelligent Methods, Studies in Fuzziness and Soft Computing, Vol. 105., pages: 342-362. ISBN 3-7908-1499-7. Published by Springer-Verlag.

196. X. Wang, P. Khosla and R. Krishnan. 2001. "Optimize Security Mechanism for Electronic Commerce". Montreal, Canada. Proceedings of the 4th International Workshop on Deception, Fraud and Trust in Agent Societies, pages: 113-124.

197. X. Wang, S. Zhang, P. Khosla, H. Kiliccote, C. Zhang and K. Lam. 2000. "Anytime Algorithm for Agent-Mediated Merchant Information Gathering". Proceedings of ACM International Conference on Autonomous Agents (ACM AA), pages: 333-340, ACM press.

198. X. Wang, H. Kiliccote and P. Khosla. 2000. "Multiagent Learning to Secure Computing Systems". Proceedings of International Conference on Multiagent System (ICMAS), pages: 459 –460. Poster paper.

199. X. Yi, C. Siew, X. Wang and E. Okamoto. 2000. "A Secure Agent-based Framework for Internet Trading in Mobile Computing Environments". Journal of Distributed and Parallel Databases, 8, pages: 85-119, Kluwer Academic Publishers.

200. X. Wang, X. Yi, K. Lam, C. Zhang and E. Okamoto. 1999. "Secure Agent-Mediated Auctionlike Negotiation Protocol for Internet Retail Commerce". Proceedings of the third International workshop on Cooperative Information Agents (CIA), pages: 291-302. Springer-Verlag, Lecture Notes in Artificial Intelligence, Vol. 1652.

201. X. Wang, K. Lam and X. Yi. 1998. "Secure Agent-Mediated Mobile Payment". Proceeding of the first Pacific Rim International Workshop on Multiagent Systems (PRIMA 1998), pages: 162-173. Lecture Notes in Artificial Intelligence. Vol. 1599, Springer-Verlag.

202. X. Yi, X. Wang, K. Lam, E. Okamoto and D. Hsu. 1998. “A Secure Auctionlike Negotiation Protocol for Agent-based Internet Trading”, Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems (SRDS), pages: 197-203, IEEE press.

203. X. Wang, X. Yi, K. Lam and E. Okamoto. 1998. “Secure Information Gathering Agent for Internet Trading”, proceedings of the 4th Australian Workshop on Distributed Artificial Intelligence in joint with the 8th Australian Joint Conference on Artificial Intelligence (DAI 1998), pages: 183-193. Australia, Lecture Notes in Artificial Intelligence, Springer-Verlag, Vol. 1544.

204. X. Yi, X. Wang and K. Lam. 1998. “A Secure Intelligent Trade Agent System”, Proceedings of Trends in Distributed Systems for Electronic Commerce (International IFIP/GI Working Conference, 1998), pages: 218-228, Hamburg, Germany, Lecture Notes in Computer Science, Vol.1402, Springer-Verlag.

205. X. Yi, X. Wang and K. Lam. 1998. “An Intelligent Agent Architecture for Securing Internet Trading”, Proceedings of the 14th International Information Security Conference (IFIP/SEC).

MENTORING

Since 2004, I have graduated 22 PhD students. Also, I have unofficially advised several students from other institutions, including UIUC, Georgia Tech, and others. Below is information on those who have completed their programs or PostDoc studies.

PHD Students Graduated from IU:

- Debin Liu (co-advised with Jean Camp): graduated in 2011, first job at PayPal, now founder of a Chinese Startup
- Rui Wang: graduated in 2013, first job at Microsoft Research, now with Google
- Kehuan Zhang: graduated in 2012, first job at Chinese University at Hong Kong and now tenured full professor there
- Zhou Li: graduated in 2013, first job at EMC RSA Lab, now tenured associate professor at UC Irvine (**Winner of NSF Career Award**)
- Xiaoyong Zhou: graduated in 2014, first job at Samsung Research America, now with Google
- Yangyi Chen: graduated in 2015, first job at Google
- Yongan Zhao (co-advised with Haixu Tang): graduated at 2016, first job at Seven Bridge Genomics, now with GNS Healthcare
- Luyi Xing: graduated in 2017, first job at Amazon, now tenured associate professor at UIUC (**Winner of NSF Career Award**)
- Sumayah Alrwais: graduated in 2017, first job at King Saudi University (assistant professor)
- Nan Zhang: graduated in 2018, first job at Facebook (Meta)
- Kan Yuan: graduated in 2018, first job at Facebook (Meta)
- Peter Yeonjoon Lee: graduated in 2019, first job at Hanyang University, South Korea (assistant professor)
- Xianghang Mi: graduated in 2020, first job at Facebook, now assistant professor at the University at Buffalo
- Eihal Alowaisheq: graduated in 2020, first job at King Saudi University (assistant professor)
- Peng Wang: graduated in 2020, first job at Microsoft

- Xueqiang Wang: graduated in 2020, first job at Amazon, and now assistant professor at University of Central Florida
- Zhihao Wang: graduated in 2025, first job at NTU as my PostDoc fellow
- Zilong Lin: graduated in 2025, first job at University of Missouri (assistant professor)
- Siyuan Tang: graduated in 2025, first job at Amazon Annarpruna Labs (software development engineer)
- Yifan Zhang: graduated in 2025, first job at San Diego University (assistant professor)
- Hongbo Chen: graduated in 2025, first job at Google DeepMind
- Huanyao Rong: ABD, expected to graduate in 2026, first job at Microsoft

Unofficially Advised PHD Students Graduated from Other Schools:

- Muhammad Naveed (UIUC, advised by Carl Gunter): graduated in 2016, first job at University of Southern California (assistant professor)
- Xiaojing Liao (Georgia Tech, advised by Raheem Beyah): graduated in 2017, first job at William and Mary College (assistant professor), now tenured associate professor at UIUC **(Winner of NSF Career Award)**
- Xiaolong Bai (Tsinghua University): graduated in 2017, first job at Alibaba
- Tongxin Li (Peking University): graduated in 2018, first job at Baidu USA, now with Google

To a lesser extent, I have also advised the following students:

- Vincent Bindschaedler (UIUC, advised by Carl Gunter): graduated in 2018, first job at the University of Florida (assistant professor)
- Soteris Demetriou (UIUC, advised by Carl Gunter): graduated in 2018, first job at Imperial College London (assistant professor)

PAST POSTDOC Fellows:

- Yi Chen: 2021 to 2024, now assistant professor at the University of Hong Kong
- Di Tang: 2021 to 2024, now associate professor at Sun Yat-Sen University
- Weijie Liu: 2016 to 2018, now associate professor at Nankai University
- Wenhao Wang: 2016 to 2018, now associate professor at Chinese Academy of Sciences
- Kai Chen: from 2014 to 2015, now full professor at Chinese Academy of Science
- Zhuowei Li: from 2005 to 2008, now principal software engineering manager at Microsoft