Ziming Zhao

Assistant Professor
Department of Computer Science and Engineering
University at Buffalo
Phone: (480) 332-7221
Email: zimingzh@buffalo.edu, ziming.zhao@gmail.com
CactiLab webpage: https://cactilab.github.io/
Personal webpage: https://zzm7000.github.io/

CURRENT RESEARCH INTERESTS

- System and Software Security of IoT and Embedded Platforms (Cortex-M, Cortex-A, TrustZone, etc.)

EDUCATION

Ph.D. in Computer Science	Arizona State University, Tempe, USA	2014
M.S. in Cryptography	Beijing University of Posts and Telecommunications, China	2009
B.E. in Automation	Beijing University of Posts and Telecommunications, China	2006

PROFESSIONAL EXPERIENCE

- Assistant Professor (directing CactiLab), University at Buffalo, July 2020 - Present
- Volunteer Faculty Member, Rochester Institute of Technology, July 2020 - Present
- Assistant Professor (directing CactiLab), Rochester Institute of Technology, Aug 2018 - Jun 2020
- Visiting Faculty Research Program, US Air Force Research Laboratory, May 2020 - July 2020
- Assistant Research Professor (codirecting SEFCOM), Arizona State University, Sep 2015 - Aug 2018
- Postdoctoral Scholar, Arizona State University, Sep 2014 - Aug 2015
- Research Assistant, Arizona State University, Aug 2009 - Sep 2014
- Teaching Assistant, Arizona State University, Aug 2009 - May 2010
- Intern, Microsoft Research Asia, 2008 - 2009

ACHIEVEMENT HIGHLIGHTS and HONORS

- NSF CRII award; received another **2** grants from NSF and DoD
- **8** papers in big 4 security conferences (1 Oakland, 3 USENIX Security, 2 CCS, 1 NDSS); **20+** papers in other security conferences and journals (1 **MobiSys**, 3 ACSAC, 1 ESORICS, 3 CODASPY, 4 SACMAT, 2 CNS, 2 SAC, 1 DFRWS, 1 eCrime, 1 TISSEC, 2 TDSC, 1 TIFS, etc.)
- **3** best or distinguished paper awards (**USENIX Security** 2019, ACM CODASPY 2014, ITU Kaleidoscope 2016); 1 outstanding poster award (ACM CODASPY 2018)
- Over 60 publications (citations=1,500+, h-index=19) in **security**, **system** and **networking**
- Served in TPC at CODASPY, SACMAT, DFRWS, SAC, HotEdge, etc.
- Served as a general co-chair of CODASPY 2018 and the local chair of CODASPY 2017
- Founded ACM Workshop on Automotive and Aerial Vehicle Security (AutoSec)
- Founded *Cacti* and *TigerBytes* hacking teams at RIT (3rd place MITRE Collegiate Embedded CTF 2019)
- Top-10 finalist of best applied security paper award, NYU CSAW 2015; 3rd place Extreme Networks SDN Innovation Challenge 2015
- University Graduate Fellowship, ASU 2009; Star of Future, Microsoft Research Asia 2009

RESEARCH SPECIALTIES

I am interested in security and privacy related problems in computer and communications systems. My current research focus is on **system and software security of IoT and embedded platforms**, e.g., utilizing hardware primitives to design and implement secure systems for attack mitigation.

I also work on **network and web security**, e.g., designing novel firewall and intrusion response systems for the emerging software-defined network and mobile ad-hoc network; **cybercrime and threat intelligence analysis**, e.g., understanding the structure of underground communities and the economy and ecosystem of cybercrime; **user-centric security and human factors in cybersecurity**, e.g., finding vulnerabilities in authentication and payment systems; designing novel access control models and techniques.

- System and software security: ARM Cortex-A, Cortex-M, TrustZone, etc. [MobiSys20, SAC19, ACSAC18a, CODASPY18b, ASHES18]; Android system [JCS16, ACSAC14]; program analysis for security [CODASPY20, TDSC19, TIFS18, CODASPY17, ICST17, ICWS16, TDSC15, CODASPY14, CNS13, WCRE11].
- Network and web security: software-defined networking [COSE19, CCS18, NDSS17, CNS17, SACMAT16]; web security [SAC18, AAMAS17, ITIT17]; other network security [ACSAC18b, TDSC13].
- Analysis of cybercrime, economy and ecosystem: spam and scam [Oakland16, SECURITY19]; underground social dynamics [CODASPY19, ESORICS12]; underground economy [eCrime16, S&PM16].
- User-centric security and human factors in cybersecurity: security operation center [SECURITY19, CCS19]; authentication [SECURITY13, TISSEC15]; access control in online social networks [SACMAT14].

GRANTS

External grants:

- PI. **NSF**. CRII: SaTC: Securing Internet of Things Against Cache-based Attacks. Award Number: 1948175. $172,235, 2020 - 2022.
- Co-PI, **DoD**: VSER - Vehicle Security Education and Research. $149,931.00. DoD, 2019 - 2020. PIs: Hanif Rahbari, and Ziming Zhao.
- Co-PI, **NSF-SFS**: Arizona Cyber Defense Scholarship. Award Number: 1663651. $4,998,009. NSF, 2017 - 2023. PIs: Gail-Joon Ahn, Co-PI: Stephen Yau, Dijiang Huang, Adam Doupé, and Ziming Zhao.

Internal grants:

- PI, RIT BootCamp 2019. Enabling Trusted Computing on Industrial IoT Devices: Software-only TPM on Microcontrollers. $5,000.

PUBLICATIONS

- **8** papers in big 4 security conferences (1 Oakland, 3 USENIX Security, 2 CCS, 1 NDSS); **20+** papers in other security conferences and journals (1 **MobiSys**, 3 ACSAC, 1 ESORICS, 3 CODASPY, 4 SACMAT, 2 CNS, 2 SAC, 1 DFRWS, 1 eCrime, 1 TISSEC, 2 TDSC, 1 TIFS, etc.)
- **3** best or distinguished paper awards (**USENIX Security**, CODASPY, ITU Kaleidoscope)
- My work has been cited **1,500+** times with an h-index of 19 and an i10-index of 28 (according to Google Scholar as of September, 2020).

Conference Papers

MobiSys20 Haehyun Cho, Jinbum Park, Donguk Kim, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, Gail-Joon Ahn. SmokeBomb: Effective Mitigation Method against Cache Side-channel Attacks on the ARM Architecture. In *Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services* (**MobiSys**), Toronto, Canada, 2020. (34/175 = 19.4% acceptance rate)

SECURITY20 Cong Wu, Kun He, Jing Chen, Ziming Zhao, Ruiying Du. Users Really Do Answer Telephone Scams. In *Proceedings of the USENIX Security* (**SECURITY**), Boston, USA, 2020. (?% acceptance rate)

CODASPY20 Stuart Millar, Niall McLaughlin, Jesus Martinez del Rincon, Paul Miller and Ziming Zhao. DANdroid: A Multi-View Discriminative Adversarial Network for Obfuscated Android Malware Detection. In *Proceedings of the ACM Conference on Data and Application Security and Privacy* (**CODASPY**), New Orleans, LA, USA, March, 2020. (20.0% acceptance rate)

CCS19 Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In *Proceedings of the ACM Conference on Computer and Communications Security* (**CCS**), London, UK, 2019.

SECURITY19 Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. Users Really Do Answer Telephone Scams. In *Proceedings of the USENIX Security* (**SECURITY**), Santa Clara, USA, 2019. (16.2% acceptance rate, **Distinguished Paper Award**)

SACMAT19 Carlos Rubio Medrano, Shaishavkumar Jogani, Maria Leitner, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. Effectively Enforcing Authorization Constraints for Emerging Space-Sensitive Technologies. In *Proceedings of the ACM Symposium on Access Control Models and Technologies* (**SACMAT**), Toronto, Canada, 2019.

SAC19 Penghui Zhang, Haehyun Cho, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. iCORE: Continuous and Proactive Extrospection on Multi-core IoT Devices. In *Proceedings of the ACM/SIGAPP Symposium On Applied Computing* (**SAC**), Limassol, Cyprus, 2019. (24% acceptance rate)

CODASPY19 Zhibo Sun, Carlos E. Rubio-Medrano, Ziming Zhao, Tiffany Bao, Adam Doupé and Gail-Joon Ahn. Understanding and Predicting Private Interactions in Underground Forums. In *Proceedings of the ACM Conference on Data and Application Security and Privacy* (**CODASPY**), Dallas, TX, USA, March, 2019. (23.5% acceptance rate)

ACSAC18a Haehyun Cho, Penghui Zhang, Donguk Kim, Jinbum Park, Choonghoon Lee, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. Prime+Count: Novel Cross-world Covert Channels on ARM TrustZone. In *Proceedings of the Annual Computer Security Applications Conference* (**ACSAC**), San Juan, Puerto Rico, USA, December, 2018. (20.1% acceptance rate)

ACSAC18b Jaejong Baek, Sukwha Kyung, Haehyun Cho, Ziming Zhao, Adam Doupé, Yan Shoshitaishvili and Gail-Joon Ahn. Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling. In *Proceedings of the Annual Computer Security Applications Conference* (**ACSAC**), San Juan, Puerto Rico, USA, December, 2018. (20.1% acceptance rate)

SmartGridComm18 Vu Coughlin, Carlos Rubio-Medrano, Ziming Zhao and Gail-Joon Ahn. EDSGuard: Enforcing Network Security Requirements for Energy Delivery Systems. In *Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids* (**SmartGridComm**), Aalborg, Denmark, October, 2018

CHASE18 Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao and Gail-Joon Ahn. The Danger of Missing Instructions: A Systematic Analysis of Security Requirements for MCPS. In *Proceedings of the IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies* (**CHASE**), Washington, DC, USA, 2018

CCS18 Vaibhav Hemant Dixit, Adam Doupé, Yan Shoshitaishvili, Ziming Zhao and Gail-Joon Ahn. AIM-SDN: Attacking Information Mismanagement in SDN-datastores. In *Proceedings of the ACM Conference on Computer and Communications Security* (**CCS**), Toronto, Canada, October, 2018. (16.6% acceptance rate)

SAC18 Sai Prashanth Chandramouli, Pierre-Marie Bajan, Christopher Kruegel, Giovanni Vigna, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. Measuring E-Mail Header Injections on the World Wide Web. In *Proceedings of the ACM/SIGAPP Symposium On Applied Computing* (**SAC**), Pau, France, April, 2018

DF18 Mike Mabey, Adam Doupé, Ziming Zhao and Gail-Joon Ahn. Challenges, Opportunities, and a Framework for Web Environment Forensics. In *Proceedings of the IFIP Working Group 11.9 Digital Forensics* (**DF**), New Delhi, India, January, 2018

CIC17 Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao and Gail-Joon Ahn. OntoEDS: Protecting Energy Delivery Systems by Collaboratively Analyzing Security Requirements. In *Proceedings of the IEEE International Conference on Collaboration and Internet Computing* (**CIC**), San Jose, CA, USA, October, 2017

CNS17 Sukwha Kyung, Wonkyu Han, Naveen Tiwari, Vaibhav Dixit, Lakshmi Srinivas, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. HoneyProxy: Design and Implementation of Next-Generation Honeynet via SDN. In *Proceedings of the IEEE Conference on Communications and Network Security* (**CNS**), Las Vegas, October, 2017. (29.9% acceptance rate)

AAMAS17 Sailik Sengupta, Satya Gautam Vadlamudi, Subbarao Kambhampati, Adam Doupé, Marthony Taguinod, Ziming Zhao and Gail-Joon Ahn. A Game Theoretic Approach in Strategy Generation for Moving Target Defense in Web Applications. In *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems* (**AAMAS**), So Paulo, Brazil, May, 2017. (26.0% acceptance rate)

CODASPY17 Niall McLaughlin, Jesus Martinez del Rincon, BooJoong Kang, Suleiman Yerima, Paul Miller, Sakir Sezer, Yeganeh Safaei, Erik Trickel, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. Deep Android Malware Detection. In *Proceedings of the ACM Conference on Data and Applications Security and Privacy* (**CODASPY**), Scottsdale, Arizona, March, 2017. (short paper)

ICST17 Junjie Tang, Xingmin Cui, Ziming Zhao, Shanqing Guo, Xinshun Xu, Chengyu Hu, Tao Ban and Bing Mao. NIVAnalyzer: a Tool for Automatically Detecting and Verifying Next-Intent Vulnerabilities in Android Apps. In *Proceedings of IEEE International Conference on Software Testing, Verification and Validation* (**ICST**), Tokyo, Japan, March, 2017.

NDSS17 Juan Deng, Hongda Li, Hongxin Hu, Kuang-Ching Wang, Gail-Joon Ahn, Ziming Zhao and Wonkyu Han. On the Safety and Efficiency of Virtual Firewall Elasticity Control. In *Proceedings of the Network and Distributed System Security Symposium* (**NDSS**), San Diego, California, February, 2017. (16.1% acceptance rate)

CIC16 Ajay Modi, Zhibo Sun, Anupam Panwar, Tejas Khairnar, Ziming Zhao, Adam Doupé, Gail-Joon Ahn and Paul Black. Towards Automated Threat Intelligence Fusion. In *Proceedings of IEEE International Conference on Collaboration and Internet Computing*, (**CIC**), 2016.

ITU16 Huahong Tu, Adam Doupé, Ziming Zhao and Gail-Joon Ahn. Toward Authenticated Caller ID Transmission: The Need for a Standardized Authentication Scheme in Q.731.3 Calling Line Identification Presentation. In *Proceedings of ITU Kaleidoscope 2016: ICTs for a Sustainable World*, November 2016, Bangkok, Thailand. (**Best Paper Award**)

ICWS16 Jia Chen, Xingmin Cui, Ziming Zhao, Jie Liang and Shanqing Guo. Toward Discovering and Exploiting Private Server-side Web APIs. In *Proceedings of IEEE International Conference on Web Services* (**ICWS**), June 2016, San Francisco. (26% acceptance rate)

DFRWS16 Mike Mabey, Adam Doupé, Ziming Zhao and Gail-Joon Ahn. dbling: Identifying Extensions Installed on Encrypted Web Thin Clients. In *Proceedings of Digital Forensics Research Conference* (**DFRWS**), August 2016, Seattle, Washington.

SACMAT16 Wonkyu Han, Hongxin Hu, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. State-aware Network Access Management for Software-Defined Networks. In *Proceedings of 21st ACM Symposium on Access Control Models And Technologies* (**SACMAT**), June 2016, Shanghai, China. (33% acceptance rate)

eCrime16 Kevin Liao, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. Behind Closed Doors: Measurement and Analysis of CryptoLocker Ransoms in Bitcoin. In *Proceedings of APWG Symposium on Electronic Crime Research* (**eCrime**), June 2016, Toronto, Canada.

Oakland16 Huahong (Raymond) Tu, Adam Doupé, Ziming Zhao and Gail-Joon Ahn. SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam. In *Proceedings of 37th IEEE Symposium on Security and Privacy* (**Oakland**), May 2016, San Jose. (13.3% acceptance rate)

IRI15 Marthony Taguinod, Adam Doupé, Ziming Zhao and Gail-Joon Ahn. Toward a Moving Target Defense for Web Applications. In *Proceedings of 16th IEEE International Conference on Information Reuse and Integration* (**IRI**), August 2015, San Francisco, California, USA. (invited paper)

SACMAT15 Carlos E. Rubio-Medrano, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. Federated Access Management for Collaborative Network Environments: Framework and Case Study. In *Proceedings of 20th ACM Symposium on Access Control Models and Technologies* (**SACMAT**), June 2015, Vienna, Austria. (28.8% acceptance rate, full paper)

ACSAC14 Yiming Jing, Ziming Zhao, Gail-Joon Ahn and Hongxin Hu. Morpheus: Automatically Generating Heuristics to Detect Android Emulators. In *Proceedings of 30th Annual Computer Security Applications Conference* (**ACSAC**), 2014, New Orleans, USA. (19.9% acceptance rate, finalist for CSAW Best Applied Security Paper Award 2015)

SACMAT14 Hongxin Hu, Gail-Joon Ahn, Ziming Zhao and Dejun Yang. Game Theoretic Analysis of Multiparty Access Control in Online Social Networks. In *Proceedings of 19th ACM Symposium on Access Control Models And Technologies* (**SACMAT**), June 2014, London, Ontario, Canada. (29.8% acceptance rate)

ONS14 Hongxin Hu, Gail-Joon Ahn, Wonkyu Han and Ziming Zhao. Towards a Reliable SDN Firewall. In *Proceedings of the Open Networking Summit* (**ONS**) *Research Track*, March 2014, Santa Clara, California, USA. (28.2% acceptance rate, oral presentation)

CODASPY14 Yiming Jing, Gail-Joon Ahn, Ziming Zhao and Hongxin Hu. RiskMon: Continuous and Automated Risk Assessment of Mobile Applications. In *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy* (**CODASPY**), March 2014, San Antonio, Texas, USA. (16.0% acceptance rate, **Best Paper Award**)

CNS13 Ziming Zhao and Gail-Joon Ahn. Using Instruction Sequence Abstraction for Shellcode Detection and Attribution. In *Proceedings of the 1st IEEE Conference on Communications and Network Security* (**CNS**), Oct 2013, Washington DC, USA. (28.3% acceptance rate)

SECURITY13 Ziming Zhao, Gail-Joon Ahn, Jeong-Jin Seo and Hongxin Hu. On the Security of Picture Gesture Authentication. In *Proceedings of the 22nd USENIX Security Symposium* (**SECURITY**), Aug 2013, Washington DC, USA. (15.9% acceptance rate)

ESORICS12 Ziming Zhao, Gail-Joon Ahn, Hongxin Hu and Deepinder Mahi. SocialImpact: Systematic Analysis of Underground Social Dynamics. In *Proceedings of the 17th European Symposium on Research in Computer Security* (**ESORICS**), Sep 2012, Pisa, Italy. (20.1% acceptance rate)

GLOBECOM11 Ziming Zhao, Gail-Joon Ahn and Hongxin Hu. Examining Social Dynamics for Countering Botnet Attacks. In *Proceedings of the 54th IEEE Global Communications Conference* (**GLOBECOM**), Dec 2011, Houston, USA.

WCRE11 Ziming Zhao, Gail-Joon Ahn and Hongxin Hu. Automatic Extraction of Secrets from Malware. In *Proceedings of the 18th Working Conference on Reverse Engineering* (**WCRE**), Oct 2011, Limerick, Ireland. (25.9% acceptance rate, full paper)

GLOBECOM10 Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu. Risk-Aware Response for Mitigating MANET Routing Attacks. In *Proceedings of the 53th IEEE Global Communications Conference* (**GLOBECOM**), Dec 2010, Miami, USA.

ICINIS08 Ziming Zhao, Yanfei Liu, Hui Li and Yixian Yang. An Efficient User-to-User Authentication Scheme in Peer-to-Peer System. In *Proceedings of the International Conference on Intelligent Networks and Intelligent Systems* (**ICINIS**), Nov 2008, Wuhan, China.

CW08 Yanfei Liu, Ziming Zhao, Hui Li, Qun Luo and Yixian Yang. An Efficient Remote User Authentication Scheme with Strong Anonymity. In *Proceedings of International Conference on Cyberworlds* (**CW**), Sep 2008, Hangzhou, China.

Journal Papers

COSE19 Hongxin Hu, Wonkyu Han, Sukwha Kyung, Gail-Joon Ahn, Ziming Zhao, Hongda Li and Juan Wang. Towards a Reliable Firewall for Software-Defined Networks. *Computers & Security* (**COSE**), 2019.

TDSC19 Jing Chen, Chiheng Wang, Ziming Zhao, Min Chen, Ruiying Du, and Gail-Joon Ahn. Semantics-Aware Privacy Risk Assessment Using Self-Learning Weight Assignment for Mobile Apps. *IEEE Transactions on Dependable & Secure Computing* (**TDSC**), 2019.

TIFS18 Jing Chen, Chiheng Wang, Ziming Zhao, Kai Chen, Ruiying Du, and Gail-Joon Ahn. Uncovering the Face of Android Ransomware: Characterization and Real-time Detection. *IEEE Transactions on Information Forensics & Security* (**TIFS**), 2018.

CSM17 Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. Toward Standardization of Authenticated Caller ID Transmission. *IEEE Communications Standards Magazine* (**CSM**), 2017.

ITIT17 Sai Prashanth Chandramouli, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. E-mail Header Injection Vulnerabilities. *it - Information Technology* (**ITIT**), 2017.

JCS16 Yiming Jing, Gail-Joon Ahn, Hongxin Hu, Haehyun Cho and Ziming Zhao. TRIPLEMON: A Multilayer Security Framework for Mediating Inter-Process Communication on Android. *Journal of Computer Security* (**JCS**), Vol. 24, no. 4, pp. 405-426, 2016.

S&PM16 Ziming Zhao, Mukund Sankaran, Gail-Joon Ahn, Thomas J. Holt, Yiming Jing and Hongxin Hu. Mules, Seals, and Attacking Tools: Analyzing Twelve Online Marketplaces. *IEEE Security & Privacy Magazine. Special Issue: What's New in the Economics of Cybersecurity?* (**S&PM**), Vol. 14, Issue 1, 2016.

TISSEC15 Ziming Zhao, Gail-Joon Ahn and Hongxin Hu. Picture Gesture Authentication: Empirical Analysis, Automated Attacks, and Scheme Evaluation. *ACM Transactions on Information and System Security* (**TISSEC**), Vol. 17, Issue 4, 2015.

TDSC15 Yiming Jing, Gail-Joon Ahn, Ziming Zhao and Hongxin Hu. Towards Automated Risk Assessment and Mitigation of Mobile Application. *IEEE Transactions on Dependable and Secure Computing* (**TDSC**), Vol. 12, Issue 5, 2015.

TDSC13 Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu. Risk-Aware Mitigation for MANET Routing Attacks. *IEEE Transactions on Dependable and Secure Computing* (**TDSC**), Vol. 9, Issue. 2, 2012.

Workshop Papers

MSCPES19 Josephine Lamp, Carlos Rubio Medrano, Ziming Zhao, and Gail-Joon Ahn. ExSol: Collaboratively Assessing Cybersecurity Risks for Protecting Energy Delivery Systems. In *Proceedings of Workshop on Modeling and Simulation of Cyber-Physical Energy Systems* (**MSCPES**), April 2019, Montreal, Canada.

ASHES18 Mauricio Gutierrez, Ziming Zhao, Adam Doupé, Yan Shoshitaishvili and Gail-Joon Ahn. CacheLight: Defeating the CacheKit Attack. In *Proceedings of the Workshop on Attacks and Solutions in Hardware Security* (**ASHES**), October, 2018, Toronto, Canada.

MedSPT18 Josephine Lamp, Carlos Rubio Medrano, Ziming Zhao, and Gail-Joon Ahn. The Danger of Missing Instructions: A Systematic Analysis of Security Requirements for MCPS. In *Proceedings of the International Workshop on Security, Privacy, and Trustworthiness in Medical Cyber-Physical Systems* (**MedSPT**), September, 2018, Washington D.C., USA.

ABAC18 Carlos Rubio Medrano, Ziming Zhao and Gail-Joon Ahn. RiskPol: A Risk Assessment Framework for Preventing Attribute-Forgery Attacks to ABAC Policies. In *Proceedings of ACM Workshop on Attribute Based Access Control* (**ABAC**), March 2018, Tempe, Arizona, USA.

SDNNFV18 Vaibhav Hemant Dixit, Sukwha Kyung, Ziming Zhao, Adam Doupé, Yan Shoshitaishvili and Gail-Joon Ahn. Challenges and Preparedness of SDN-based Firewalls. In *Proceedings of ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (**SDNNFVSec**), March 2018, Tempe, Arizona, USA.

MTD17 Josephine Lamp, Carlos E. Rubio-Medrano, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. Mutated Policies: Towards Proactive Attribute-based Defenses for Access Control. In *Proceedings of ACM Workshop on Moving Target Defense* (**MTD**), Nov 2017, Dallas, Texas, USA.

MSCPES17 Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao, and Gail-Joon Ahn. Towards Adaptive and Proactive Security Assessment for Energy Delivery Systems. In *Proceedings of Workshop on Modeling and Simulation of Cyber-Physical Energy Systems* (**MSCPES**), April 2017, Pittsburgh, PA, USA.

SDNNFV16 Wonkyu Han, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. HoneyMix: Toward SDN-based Intelligent Honeynet. In *Proceedings of ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (**SDNNFVSec**), March 2016, New Orleans, LA, USA.

ABAC16 Carlos M. Rubio, Josephine Lamp, Marthony Taguinod, Adam Doupé, Ziming Zhao and Gail-Joon Ahn. Position Paper: Towards a Moving Target Defense Approach for Attribute-based Access Control. In *Proceedings of ACM Workshop on Attribute Based Access Control* (**ABAC**), March 2016, New Orleans, LA, USA.

HotSDN14 Hongxin Hu, Wonkyu Han, Gail-Joon Ahn and Ziming Zhao. FlowGuard: Building Robust Firewalls for Software-Defined Networks. In *Proceedings of ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking* (**HotSDN**), August 2014, Chicago, Illinois, USA. (14.0% acceptance rate, full paper with long presentation)

Extended Abstracts/Posters

CODASPY18a Penghui Zhang, Bernard Ngabonziza, Haehyun Cho, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. SeCore: Continuous Extrospection with High Visibility on Multi-core ARM Platforms. In *Proceedings of the 8th ACM Conference on Data and Application Security and Privacy* (**CODASPY**), March 2018. (**Outstanding Poster Award**)

CODASPY18b Yongxian Zhang, Xinluo Wang, Ziming Zhao and Hui Li. Secure Display for FIDO Transaction Confirmation. In *Proceedings of the 8th ACM Conference on Data and Application Security and Privacy* (**CODASPY**), March 2018.

SACMAT17 Hongda Li, Juan Deng, Hongxin Hu, Kuang-Ching Wang, Gail-Joon Ahn, Ziming Zhao and Wonkyu Han. Poster: On the Safety and Efficiency of Virtual Firewall Elasticity Control. In *Proceedings of 22st ACM Symposium on Access Control Models And Technologies* (**SACMAT**), June 2017.

AAMAS16 Satya Gautam Vadlamudi, Sailik Sengupta, Subbarao Kambhampati, Marthony Taguinod, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. Moving Target Defense For Web Applications Using Bayesian Stackelberg Games. In *Proceedings of International Conference on Autonomous Agents and Multiagent Systems* (**AAMAS**), May 2016, Singapore.

Books

B1 *P2P Technology Principle and C++ Development*. Editors: Wen Zhang and Ziming Zhao. Posts and Telecom Press, China, 2008. ISBN: 978-7-115-18105-3/TP.

Book Chapters

BC1 Mauricio Gutierrez, Ziming Zhao, Adam Doupé, Yan Shoshitaishvili and Gail-Joon Ahn. Mitigating the CacheKit Attack in *Frontiers in Hardware Security and Trust*. Editors: Chang Chip Hong, Yuan Cao. IET.

BC2 Kevin Liao, Ziming Zhao, Adam Doupé and Gail-Joon Ahn. Ransomware and Cryptocurrency: Partners in Crime in *Cybercrime Through an Interdisciplinary Lens*. Editors: Thomas J. Holt. Routledge.

BC3 Ziming Zhao and Gail-Joon Ahn. Examining Social Dynamics and Malware Secrets to Mitigate Net-centric Attacks in *Hackers and Hacking: A Reference Handbook*. Editors: Thomas J. Holt and Bernadette H. Schell. ABC-CLIO, LLC. ISBN: 978-1-61069-276-2.

BC4 Ziming Zhao. Key Management in *Symmetric Cryptography and Its Applications*. Editors: Hui Li, Lixiang Li and Shuai Shao. Beijing University of Posts and Telecommunications Press, China, 2009. ISBN: 978-7-56351-717-6.

Dissertation

D1 Ziming Zhao. Discovering and Using Patterns for Countering Security Challenges. Doctoral Dissertation, Computer Sciences, Arizona State University, 2014.

TEACHING EXPERIENCE

Classes at University at Buffalo:

- CSE 610 Special Topics: Software Security - Attack and Defense for Binaries.

Classes at Rochester Institute of Technology:

- CSEC 741 Sensor and SCADA Security. Spring 2020. Effective Teacher: **4.45**
- CSEC 659/459 Trusted Computing and Trusted Execution. Fall 2019. Effective Teacher: **4.5/5**
- CSEC 741 Sensor and SCADA Security. Spring 2019. Effective Teacher: **4.62/5**, Overall: **4.38/5**
- CSEC 750 Covert Communications. Fall 2018 Effective Teacher: **3.75/5**, Overall: **3.88/5**

Classes at Arizona State University:

- CSE 469 Computer and Network Forensics. Spring 2017 and Spring 2018
  An undergraduate/graduate computer science class with 69+ students. This class focuses on hands-on practices. Evaluation of the Course **4.42/5**, Evaluation of Instructor **4.49/5**, Overall: **4.33/5**
- CSE 468 Computer Network Security. Fall 2016
  An undergraduate/graduate computer science class with 107 students. I developed the syllabus based on the previous CSE 468 class by adding many new materials about attack and defense on network and transport layer protocols. I also introduced 4 more lab assignments to help students get hands-on experience. Evaluation of the Course **4.47/5**, Evaluation of Instructor **4.49/5**, Overall: **4.24/5**

Guest lectures at Arizona State University:

- CSE 465 Information Assurance (Instructor: Gail-Joon Ahn). Trust in Mobile Computing, 2015
- CSE 494/598 Forensic Computing: Computer and Network Forensics (Instructor: Gail-Joon Ahn). Malware Forensics, 2013 - 2016
- CSE 465 Introduction to Information Assurance (Instructor: Gail-Joon Ahn). Cracking Picture Password for Fun and Profit, 2013
- CSE 430 Operating Systems (Instructor: Violet Syrotiuk). Automatic Extraction of Secrets from Malware, 2011

Teaching assistant at Arizona State University:

- CSE 494/598 Computer and Network Forensics (Instructor: Gail-Joon Ahn), Arizona State University, Spring 2010
- CSE 340 Principles of Programming Languages (Instructor: Rida Bazzi), Arizona State University, Fall 2009

STUDENT ADVISING and MENTORING

- Current Ph.D. Students:
  - Xi Tan (Female). University at Buffalo.
  - Md. Tomal Armanuzzaman. University at Buffalo.
  - Wenlin Yang. University at Buffalo.
  - Wei Wang. University at Buffalo.
- Ph.D. Advisee Completed:
  - Wonkyu Han. Policy-driven Network Defense for Software-defined Networks. Co-chaired with Gail-Joon Ahn. Dissertation Committee: Adam Doupé, Dijiang Huang, Yanchao Zhang. Arizona State University, November 2016
- Ph.D. Supervisory Committee Completed:
  - Carlos E. Rubio Medrano (Hispanics). Federated Access Management For Collaborative Environments. Dissertation Committee: Gail-Joon Ahn (Chair), Adam Doupé, Raghu T. Santanam, Dijiang Huang. Arizona State University, November 2016

- Mike Kent Mabey. Forensic Methods and Tools for Web Environments. Dissertation Committee: Gail-Joon Ahn, Adam Doupé, Joohyung Lee. Arizona State University, November 2017
- Huahong Tu. From Understanding Telephone Scams to Implementing Authenticated Caller ID Transmission. Dissertation Committee: Adam Doupé (Co-Chair), Gail-Joon Ahn (Co-Chair), Yanchao Zhang, Dijiang Huang. Arizona State University, November 2017

◦ Ph.D. Supervisory Committee:

- Mohammad Saidur Rahman. Dissertation Committee: Matthew Wright (Chair), Raymond Ptucha, Yu Kong. Rochester Institute of Technology
- Zhuojia Shen. Dissertation Committee: John Criswell (Chair), Michael Scott, Sandhya Dwarkadas. University of Rochester

◦ M.S Thesis Advisor Completed:

- Mauricio Gutierrez Barnett (Hispanics). CacheLight: A Lightweight Approach for Preventing Malicious Use of Cache Locking Mechanisms. Thesis Committee: Adam Doupé, Yan Shoshitaishvili. Arizona State University, May 2018

◦ M.S Thesis Committee:

- Matthew Millar. RIT.

◦ M.S Thesis Committee Completed:

- Abhijeet Srivastava. Data Protection over Cloud. Thesis Committee: Gail-Joon Ahn, Adam Doupé. Arizona State University, April 2016
- Sai Prashanth Chandramouli. E-mail Header Injections. Thesis Committee: Adam Doupé, Gail-Joon Ahn. Arizona State University, April 2016
- Bhakti Bohara. Moving Target Defense Using Live Migration of Docker Containers. Thesis Committee: Dijiang Huang, Adam Doupé. Arizona State University, June 2017
- Tejas Khairnar. Next Generation Black-Box Web Application Vulnerability Analysis Framework. Thesis Committee: Adam Doupé, Gail-Joon Ahn. Arizona State University, April 2017
- Gerard Lawrence Pinto. Shadow Phone and Ghost SIM: A Step toward Geo-Location Anonymous Calling in GSM. Thesis Committee: Adam Doupé, Gail-Joon Ahn. Arizona State University, April 2017
- Anupam Panwar. iGen: Toward Automatic Generation and Analysis of Indicators of Compromise (IOCs) using Convolutional Neural Network. Thesis Committee: Gail-Joon Ahn, Adam Doupé. Arizona State University, April 2017
- Ajay Modi. CSM: Automated Confidence Score Measurement of Threat Indicators. Thesis Committee: Gail-Joon Ahn, Adam Doupé. Arizona State University, April 2017
- Sukwha Kyung. Framework for Evaluating Hardware-assisted Security Function and Its Performance. Thesis Committee: Gail-Joon Ahn, Adam Doupé. Arizona State University, May 2017
- Bhuvana Namasivayam (Female). On Categorization of Phishing Detection Website Features And Using the Feature Vectors to Classify Phishing Websites. Thesis Committee: Rida Bazzi, Huan Liu. Arizona State University, May 2017
- James Keith Hutchins. FrozenNode: Static Linking of Node.js Applications. Thesis Committee: Adam Doupé, Yan Shoshitaishvili. Arizona State University, April 2018

◦ M.S Capstone Committee Completed:

- Weeam Alshangiti (Female). Detecting Rogue Controllers in Software Defined Networks Using Anomaly Detection. Rochester Institute of Technology, May 2019

◦ Honors Thesis Advisor Completed:

- Paulina Davison (Female). The Security of Smart Cars. Thesis Committee: Gail-Joon Ahn, Adam Doupé, Yan Shoshitaishvili. Arizona State University, April 2018
- Kaiyi Huang. Security Analysis of IoT Media Broadcast Devices. Thesis Committee: Gail-Joon Ahn. Arizona State University, April 2017
- Mauricio Gutierrez Barnett (Hispanics). Memory Inspection Resistant Rootkit: An Implementation and Analysis. Thesis Committee: Adam Doupé. Arizona State University, April 2017

◦ Honors Thesis Committee Completed:

- James Hutchins. FrozenNode: Static Linking of Node.js Applications. Thesis Committee: Adam Doupé, Yan Shoshitaishvili. Arizona State University, April 2018
- Jonathan Wasserman. TSCAN: Toward Static and Customizable Analysis for Node.js. Thesis Committee: Adam Doupé, Gail-Joon Ahn. Arizona State University, May 2017
- Joshua Smith. On the Application of Malware Clustering for Threat Intelligence Synthesis. Thesis Committee: Gail-Joon Ahn. Arizona State University, April 2017
- Omri Mor. Filesystem I/O Tracing and Replaying. Thesis Committee: Ming Zhao. Arizona State University, April 2017
- Kevin Liao. Toward Inductive Reverse Engineering of Web Applications. Thesis Committee: Adam Doupé, Gail-Joon Ahn. Arizona State University, November 2016
- Tsz Chan. Malware Analysis Framework. Thesis Committee: Gail-Joon Ahn. Arizona State University, April 2016
- Sajid Anwar. Malware Analysis Framework. Thesis Committee: Gail-Joon Ahn. Arizona State University, April 2016

INTERNAL SERVICES

◦ Colloquium + UpBeat Committee, UB, 2020

◦ GCCIS PhD Admission Policies and Procedures Committee, RIT, 2019

◦ GCCIS Foundational Computing Committee (Foundations of Security), RIT, 2019

◦ CSEC Tenure Track Faculty Hiring Committee, Department of Computing Security, RIT, 2019

◦ CSEC Curriculum Committee, Department of Computing Security, RIT, 2018 -

◦ CSEC Ad hoc Committee on Vision, Mission and 5-year plan, 2018 - 2019

PROFESSIONAL ACTIVITIES

◦ Technical Program Co-chair:

- ACM Workshop on Automotive and Aerial Vehicle Cybersecurity (AutoSec), 2019, 2020
- Great Lakes Security Day (GLSD), 2019

◦ Editor:

- Frontiors IoT Security and Privacy, 2018 -

◦ Technical Program Committee:

- USENIX Workshop on Hot Topics in Edge Computing (HotEdge), 2020
- ACM Conference on Data and Applications Security and Privacy (CODASPY), 2020, 2021
- IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGrid), 2020
- Embedded Operating Systems Workshop (EWiLi), 2019
- Digital Forensics Research Conference USA (DFRWS), 2019, 2020
- ACM Symposium on Access Control Models and Technologies (SACMAT), 2018

- ACM Symposium on Applied Computing, Special Track on Internet of Things (SAC IoT), 2018 - 2020
- ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Security), 2018 - 2020
- Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 2019, 2020
- The Secure Knowledge Management Workshop (SKM), 2017
- Guide to Security in SDN and NFV - Challenges, Opportunities, and Applications (GSSNOA), 2016
- Annual International Conference on Information Security Conference (ISC), 2016
- IEEE International Workshop on Trusted Collaboration (TrustCol), 2014 - 2016
- International Symposium on Mobile Security (MSEC), 2015

◦ Organizing Committee:

- General Co-Chair, ACM Conference on Data and Applications Security and Privacy (CODASPY), 2018
- Local Chair, ACM Conference on Data and Applications Security and Privacy (CODASPY), 2017

◦ Session Chair:

- Edge Infrastructure, USENIX Workshop on Hot Topics in Edge Computing (HotEdge), 2020
- Keynote II: Code Obfuscation - Why is this Still a Thing? ACM Conference on Data and Applications Security and Privacy (CODASPY), 2018
- Systems: Attacks and Security, ACM Conference on Computer and Communications Security (CCS), 2014

◦ Conference Reviewer:

- ACM Conference on Computer and Communications Security (CCS), 2013, 2017 - 2019
- ACM Symposium on Access Control Models and Technologies (SACMAT), 2014 - 2015
- ACM Conference on Data and Application Security and Privacy (CODASPY), 2012 - 2015
- ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014
- European Symposium on Research in Computer Security (ESORICS), 2018
- IEEE Global Communications Conference (GLOBECOM), 2014
- International Conference on Computing, Networking and Communications (ICNC), 2014
- International Conference on Computer Communications and Networks (ICCCN), 2014
- International Conference on Information Security Practice and Experience (ISPEC), 2014
- Asia-Pacific Conference on Communications (APCC), 2013

◦ Journal Reviewer:

- IEEE/ACM Transactions on Networking (TON)
- ACM Transactions on Information and System Security (TISSEC)
- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Journal on Selected Areas in Communications (JSAC)
- IEEE Transactions on Cloud Computing (TCC)
- IEEE Transactions on Biometrics, Behavior, and Identity Science (TBIOM)
- IEEE Transactions on Network and Service Management (TNSM)

- IEEE Transactions on Mobile Computing (TMC)
- IEEE Access Journal
- IEEE Internet Computing (IC)
- Computers & Security - Elsevier (COSE)
- Security and Communication Networks - John Wiley & Sons (SCN)
- Journal of Network and Systems Management - Springer (JNSM)
- Computer Communications - Elsevier (COMCOM)
- Journal of Computer and System Sciences - Elsevier (JCSS)
- International Journal of Security and Networks - Inderscience (IJSN)
- Journal of Network and Systems Management - Springer (JONS)
- Journal of Computer Science and Technology - Springer (JCST)
- World Wide Web Journal - Springer (WWW)
- SCIENCE CHINA Information Sciences - Springer
- Mathematical Problems in Engineering - Hindawi Publishing Corporation
- International Journal of Distributed Sensor Networks - Hindawi Publishing Corporation
- PLOS ONE - Public Library of Science

TALKS, PRESENTATIONS, PANELS

I have presented my research outcomes and been invited to give talks.

- Cache-based Attacks and Defense on Internet of Things, invited talk at *University at Buffalo*, *University of Delaware*, *Chinese Academy of Science Microelectronic Institute, Beijing University of Posts and Telecommunications, Beijiao University, University of Electronics and Technology of China, Sichuan University*, 2019-2020.
- Holistic Cybersecurity from System, Human, and Social Perspectives, invited talk at *Iowa State University*, *Arizona State University*, *University of Notre Dame*, *University of Arizona*, *Purdue University*, *Rochester Institute of Technology*, *University of Iowa*, *University of Delaware*, *Auburn University*, *University of Oklahoma*, *University of Michigan Dearborn*, *University of Louisiana at Lafayette*, *University of Arkansas at Little Rock*, 2017-2018.
- Cache Side-Channel Attack and Defense on Mobile and IoT Devices, *Rochester Joint Chapter of the IEEE Computer and Computational Intelligence Societies*, November 2018, Rochester, USA.
- Toward Building Trusted Execution Environment on Commodity Smartphones, invited talk at *International Symposium on Mobile Security*, December 2015, Seoul, South Korea.
- Using Instruction Sequence Abstraction for Shellcode Detection and Attribution, presented at *IEEE Conference on Communications and Network Security*, Oct 2013, Washington DC, USA.
- On the Security of Picture Gesture Authentication, presented at *USENIX Security Symposium*, Aug 2013, Washington DC, USA.
- Examining Social Dynamics for Countering Botnet Attacks, presented at *IEEE Global Communications Conference*, Dec 2011, Houston, USA.
- Risk-Aware Response for Mitigating MANET Routing Attacks, presented at *IEEE Global Communications Conference*, Dec 2010, Miami, USA.

I have served as a panelist in the following events.

- Greater Lakers Security Day, at *University at Buffalo*, 2019
- Information Assurnace Symposium, at *Arizona State University*, 2018

PATENTS

P1 Huahong Tu, Adam Doupé, Gail-Joon Ahn and Ziming Zhao. Systems and methods for authenticating caller identity and call request header information for outbound telephony communications. US 10447481 B2, 2019.

P2 Gail-Joon Ahn and Ziming Zhao. Granted Patent. Method, systems, and media for measuring quality of gesture-based passwords. US 9069948 B2, June 30, 2015.

ENTREPRENEURIAL and CONSULTING CAREER

- iSign International, Inc., 2017 - , member of Advisory Committee
- GFS Technology, Inc., 2012 - 2016, Technical Advisor (Acquired by iSign International Inc. in 2017)

CAPTURE THE FLAG COMPETITIONS

I am the faculty advisor and the founder of the CTF teams *Cacti* (all kinds of CTFs) and *TigerBytes* (hardware CTFs) at RIT.

- 6th place, 2020 MITRE Collegiate Embedded CTF, *Cacti*.
- 68th, 2019 DoE CyberForce Competition
- 3rd place, 2019 MITRE Collegiate Embedded CTF, *TigerBytes*. https://mitrecyberacademy.org/competitions/embedded/

SKILLS

- Systems: Linux kernel, OP-TEE, ARM Trusted Firmware, Android
- Programmings: C, C++, x86 Assembly, ARM Cortex-A and Cortex-M Assembly, and others
- Reverse engineering

SELECTED MEDIA COVERAGE

- Team Flowguard Wins Third Place In National Innovation Challenge. *ASU Full Circle*, Aug 19, 2015. (Link)
- Windows 8 Picture Passwords Easily Cracked. *InformationWeek Dark Reading*, August 29, 2013. (Link)
- Windows 8's Picture Passwords Weaker Than Users Might Hope. *Slashdot*, September 5, 2013. (Link)
- Windows Picture Passwords - are they really as 'easily crackable' as everyone's saying? *NakedSecurity*, September 9, 2013. (Link)
- Windows 8 Picture Passwords Easily Cracked. *Communications of ACM*, September 4, 2013. (Link)

MISCELLANEOUS

- US Permanent Resident

Last update: Monday 21st September, 2020