Last Updated: May 30, 2023

Hongxin Hu

Associate Professor
Department of Computer Science and Engineering
University at Buffalo

Work Address:
311 Davis Hall
University at Buffalo
Buffalo, New York 14260
hongxinh@buffalo.edu

EDUCATION

Ph.D., Computer Science, Arizona State University, July 2012
M.S., Computer Science, China University of Geosciences, July 2002
B.S., Computer Science, China University of Geosciences, July 1997

PROFESSIONAL EXPERIENCE

Associate Professor, Dept. of Computer Science and Engineering Jan 2021– present
University at Buffalo, Buffalo, NY

Director of Cybersecurity Center Aug 2020 – Jan 2021
Associate Professor, School of Computing Aug 2019 – Jan 2021
Assistant Professor, School of Computing Jul 2014 – Aug 2019
Dean's Faculty Fellow of Computer Science Jan 2017 – Jan 2021
Clemson University, Clemson, SC

Assistant Professor, Dept. of Computer and Information Sciences Aug 2012 – Jun 2014 Delaware State University, Dover, DE

Graduate Student Researcher & Lead Graduate Student, Laboratory of Security Engineering for Future Computing (SEFCOM) Aug 2008 – Jul 2012 Arizona State University, Tempe, AZ

Graduate Student Researcher, Laboratory of Information Integration, Security and Privacy (LIISP) Jan 2006 – Jul 2008
University of North Carolina at Charlotte, Charlotte, NC

Visiting Scholar, Laboratory of Information Integration, Security and Privacy (LIISP) Jan 2005 – Dec 2005 University of North Carolina at Charlotte, Charlotte, NC

Lecturer, College of Computing Aug 2002 – Dec 2004 China University of Geosciences, Wuhan, China

HONORS AND AWARDS

- Outstanding Research Award, UB CSE Department, 2022
- Best Paper Award, ACM ASIA Conference on Computer and Communications Security (ASIACCS), 2022
- Amazon Faculty Research Award, 2022
- Distinguished Paper Award, Annual Computer Security Applications Conference (ACSAC), 2020
- Best Paper Award, IEEE International Conference on Communications (ICC), 2020
- NSF CAREER Award, National Science Foundation (NSF), 2019
- First Place Award, Student Research Competition (SRC) in ACM SIGCOMM, 2018
- Best Paper Award, ACM Technical Symposium on Computer Science Education (SIGCSE), 2018
- Dean's Faculty Fellows Award, College of Engineering, Computing and Applied Sciences, Clemson University, 2017
- Best Paper Honorable Mention Award, ACM Symposium on Access Control Models and Technologies (SACMAT), 2016
- Best Paper Award Nominee, IEEE International Conference on Network Protocols (ICNP), 2015
- Top-10 Finalist for Best Applied Security Paper Award, New York University Cyber Security Awareness Week (CSAW), 2015
- Spotlight Paper, IEEE Transactions on Dependable and Secure Computing (TDSC), 2015
- Front Page News, Post and Courier, 2015
- Third Place Award, Extreme SDN Innovation Challenge, 2015
- Best Paper Award, ACM Conference on Data and Application Security and Privacy (CODASPY), 2014
- Spotlight Paper, IEEE Transactions on Dependable and Secure Computing (TDSC), 2014
- Featured Research Paper, IEEE Special Technical Community on Social Networking (STCSN), 2013
- First Place Award, Delaware U.S. Cyber Challenge Competition, “My Little Pwnies” (60% of female students), 2013
- Applied Security Research Best Paper Award Nominee, New York University Cyber Security Awareness Week (CSAW), 2013
- Outstanding Ph.D. Student Finalist in Computer Science, Arizona State University, 2012
- Best Paper Award Nominee, ACM Symposium on Access Control Models and Technologies (SACMAT), 2011
- Best Paper Award Nominee, International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011
- Applied Security Research Best Paper Award Nominee, New York University Cyber Security Awareness Week (CSAW), 2011
- NSF Travel Grant, NSF CAREER Proposal Writing Workshop, 2013
- ACSAC Conferenceship Award, Annual Computer Security Applications Conference (ACSAC), 2011
- NSF Travel Grant, ACM Conference on Computer and Communications Security (CCS), 2010

- IBM PhD Fellowship Nominee, UNCC, 2008
- Outstanding Teaching Award, China University of Geosciences, 2004

GRANTS AND CONTRACTS

Summary of Research Funding:

Funding Category	Total	Candidate's Share
External sources	$23,368,105	$3,872,583
Internal sources	$88,513	$29,180
Total Funded Research	$23,456,618	$3,901,763

- Received **15** NSF awards (9 as PI and 6 as Co-PI) including an NSF CAREER award, a $10M large-size NSF grant, a $3M large-size NSF grant, a $1.3M medium-size NSF grant, and a $1M medium-size NSF grant.
- Secured grants from NSF (SaTC, CNS, IIS, OAC, SOC, DGE, etc.), NSA, USDOT, U.S. Army, VMware, Google, Amazon, Dell, etc.

Current / Prior Funding:

External (**23** Awards):

1. "Collaborative Research: SAI-R: Integrative Cyberinfrastructure for Enhancing and Accelerating Online Abuse Research", **PI: Hongxin Hu**, Co-PIs: Siwei Lyu, Ziming Zhao, Yini Zhang, Maria Y. Rodriguez, 12/1/2022 - 11/30/2025, **NSF**, **$375,000** (total: $750,000) (35% share).
2. "HAC: Building High Assurance Containers Using FPGA", PI: Ziming Zhao, **Co-PI: Hongxin Hu**, Shambhu Upadhyaya, 10/1/2022- 9/30/2025, **NSA**, **$750,000** (33% share).
3. "NSF Convergence Accelerator Track G: PETS: Programmable Zero-Trust Security for Operating Through 5G Infrastructure", PI: Guofei Gu, Co-PI: Hongxin Hu, 07/15/2022 - 06/30/2023, **NSF**, **Subcontract: University at Buffalo** (**PI: Hongxin Hu**), Subcontract Amount: **$90,000** (total: $750,000) (100% share).
4. "Explaining Learning-based Intrusion Detection Systems for Active Intrusion Responses", **PI: Hongxin Hu**, Co-PI: Ziming Zhao, 06/01/2022 - 05/31/2023, **Amazon Research Award**, **$100,000** (50% share).
5. "Collaborative Research: CCRI: New: Medium: A Development and Experimental Environment for Privacy-preserving and Secure (DEEPSECURE) Machine Learning", PI: Chunming Qiao, **Co-PI: Hongxin Hu**, 10/01/2021 - 09/30/2024, **NSF**, **$520,000** (total: $1.3M) (30% share).
6. "Collaborative Research: EAGER: SaTC-EDU: Learning Platform and Education Curriculum for Artificial Intelligence-Driven Socially-Relevant Cybersecurity", **PI: Hongxin Hu**, 06/01/2021 - 05/31/2023, **NSF**, **$70,000** (total: $300,000) (100% share).
7. "RAPID: Cyber-Hostility and COVID-19", PI: Matthew Costello, **Co-PIs: Hongxin Hu**, Feng Luo, Yin Yang, Long Cheng, 06/15/2020 - 05/31/2021, **NSF**, **$199,996** (20% share).
8. "CloudLab Phase III: Expanding the Frontiers of Cloud Computing Through World-Class Community Infrastructure", PI: Kuang-Ching Wang, Co-PIs: Hongxin Hu, Amy Apon,

10/01/2020 - 09/30/2024, **NSF**, **Subcontract: University at Buffalo** (**PI: Hongxin Hu**), Subcontract Amount: **$196,074** (total: $10M) (100% share).

9. "Cross Cutting Autonomy Enablers", PI: Richard Brooks, **Co-PIs: Hongxin Hu**, Pierluigi Pisu, Linke Guo, Jerome McLendon, 09/01/2020 - 08/31/2022, **U.S. Army**, **$860,488** (20% share).
10. "CAREER: Towards Elastic Security with Safe and Efficient Network Security Function Virtualization", **PI: Hongxin Hu**, 10/01/2019 - 09/30/2024, **NSF**, **$500,000** (100% share).
11. "SDI-CSCS: Collaborative Research: S^2OS: Enabling Infrastructure-Wide Programmable Security with SDI", **PI: Hongxin Hu**, 09/01/2017 - 08/31/2021, **NSF & VMware**, **$600,000** (total: $3M) (100% share).
12. "Collaborative Research: CICI: Secure and Resilient Architecture: SciGuard: Building a Security Architecture for Science DMZ based on SDN and NFV Technologies", **PI: Hongxin Hu**, Co-PIs: Richard Brooks, Kuang-Ching Wang, 01/01/2017 - 12/31/2020, **NSF**, **$499,805** (total: $1M) (60% share).
13. "SaTC: EDU: Collaborative: Enhancing Security Education through Transiting Research on Security in Emerging Network Technologies", **PI: Hongxin Hu**, 09/01/2017 - 08/31/2020, **NSF**, **$79,999** (total: $299,998) (100% share).
14. "III: Small: Collaborative Research: Privacy-aware Collaborative Data Sharing in Human-centered Social Networks", **PI: Hongxin Hu**, Co-PI: Kelly Caine, 09/01/2015 - 08/31/2019, **NSF**, **$323,767** (total: $523,767) (50% share).
15. "EAGER: Defending Against Visual Cyberbullying Attacks in Emerging Mobile Social Networks", **PI: Hongxin Hu**, Co-PIs: Robin Kowalski, Feng Luo, Joseph Mazer, 09/01/2015 - 08/31/2018, **NSF**, **$255,680** (40% share).
16. "NSF Student Travel Grant for 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDN-NFV Security)", **PI: Hongxin Hu**, 03/01/2018 - 02/28/2020, **NSF**, **$5,600** (100% share).
17. "Collaborative Research: CICI: Regional: SouthEast SciEntific Cybersecurity for University Research (SouthEast SECURE)", PI: Jill Gemmill, **Co-PIs: Hongxin Hu**, Jan Holmevik, Nuyun Zhang, 10/01/2016 - 09/30/2019, **NSF**, **$158,004** (total: $452,464) (20% share).
18. "US Ignite: Track 1: Enabling Connected Vehicle Applications through Advanced Network Technology", PI: James Martin, **Co-PIs: Hongxin Hu**, Mashrur Chowdhury, Kuang-Ching Wang, 09/01/2015 - 08/31/2020, **NSF**, **$714,582** (20% share).
19. "University Transportation Center - Center for Connected Multimodal Mobility (C^2M^2)", PI: Mashrur Chowdhury, **Co-PIs: Hongxin H**u, Amy Apon, Jim Martin, etc., 11/30/2016 - 09/30/2022, **USDOT**, **$1,402,200** (5% share).
20. "Development of a Security Platform for Vehicle to Infrastructure Network", PI: Mashrur Chowdhury, **Co-PI: Hongxin Hu**, 05/02/2016 - 08/31/2017, **USDOT**, **$77,287** (50% share).
21. "Cyber-Hostility and COVID-19", **PI: Hongxin Hu**, 08/27/2020 - 08/26/2021, **Google**, **$13,911** (100% share).
22. "Secure Sharing of Electronic Health Records with AWS", **PI: Hongxin Hu**, 07/07/2015 - 07/06/2016, **Amazon**, **$5,000** (100% share).

23. "Dasein Connector - NFV Extensions", PI: Amy Apon, **Co-PI: Hongxin Hu**, 09/01/2014 - 12/31/2015, **Dell**, **$107,843** (50% share).

Internal (**5** Awards):

1. "Understanding and Combatting Cyberhate on Social Media", PI: Matthew Costello, **Co-PIs: Hongxin Hu**, Joseph P Maer, Feng Luo, Long Cheng, 09/01/2019 - 08/30/2020, **Clemson University CBSHS/IMPACT grant**, **$20,000** (20% share).
2. "Next Generation IoT Hardware Security for Resilient Smart Grid and ICT Infrastructures", PI: Kumar Venayagamoorthy, **Co-PIs: Hongxin Hu**, Yingjie Lao, Kuang-Ching Wang, Michal Jermanowski, 07/01/2018 - 06/30/2019, **Clemson University SUCCEEDS**, **$37,036** (10% share).
3. "Alleviating the Negative Consequences of Habitual Trust on Collaborative Privacy Control in Online Social Networks", PI: Heshan Sun, **Co-PI: Hongxin Hu**, 09/01/2016 - 08/31/2018, **Clemson University/One-Year Accelerate (OYA) Grant**, **$20,000** (50% share).
4. "Security-Enhanced Mobile Platforms", **PI: Hongxin Hu**, 09/01/2013 - 06/30/2014, **NSF-funded HBCU-UP SMILE Minigrant**, **$5,487** (100% share).
5. "Secure Data Sharing in Online Social Networks", **PI: Hongxin Hu**, 12/15/2012 - 06/15/2013, **DSU/Academic Enrichment Program Award**, **$5,990** (100% share).

Pending Funding

1. "NSF Convergence Accelerator Track G: Zeta Security: Programmable Zero-Trust Security for Operating Through 5G Infrastructure", PI: Guofei Gu, Co-PI: Hongxin Hu, 10/1/2023-9/30/2025, **NSF**, **Subcontract: University at Buffalo** (**PI: Hongxin Hu**), Subcontract Amount: **$400,000** (total: $5,000,000) (100% share).
2. "Collaborative Research: SaTC: CORE: Small: U.S.-Ireland R&D Partnership: Robust Classification of Malware on IoT Systems with DANGER-IoT", PI: Ziming Zhao, **Co-PI: Hongxin Hu**, 09/1/2023-08/31/2026, **NSF**, **$231,490** (50% share).
3. "Collaborative Research: SaTC: EDU: PWNIOT.ACADEMY: Enhancing IoT Software and System Security Education with Student-centered Pedagogy and Next Generation CTF Platform", PI: Ziming Zhao, **Co-PIs: Hongxin Hu**, Matilde Sanchez-Pena, Jinjun Xiong, 11/1/2023-10/31/2026, **NSF**, **$450,000** (total: $500,000) (20% share).

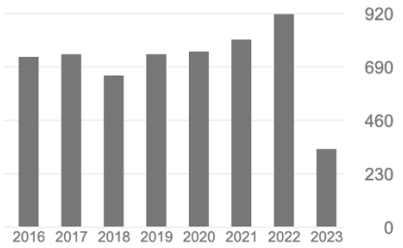
PUBLICATIONS

Publication Summary:

Type of Publication	**Book Chapters**	**Journal Articles** *Published (or accepted / in production)*	**Peer-reviewed Conference Proceedings Articles**
Total No. of Articles	3	47	107

- My work has been cited a total of **7,668** times with an h-index of **45** and an i10-index of **114** (according to Google Scholar as of May 30, 2023).
- Google Scholar: https://scholar.google.com/citations?user=fQQXj1oAAAAJ&hl=en

Cited by		VIEW ALL
	All	Since 2018
Citations	7668	4227
h-index	45	34
i10-index	114	99



Books Chapters

3. Sifa Zhang, Junqin Fan, Hongxin Hu, "Computer Graphics & Image Processing", *Higher Education Press*, Beijing, 2004.
2. Junqin Fan, Hongxin Hu, Sifa Zhang, "Guide on Computer Organization and Assembly Language", *Higher Education Press*, Beijing, 2003.
1. Hongxin Hu, Sifa Zhang, Juan Yang, Junqin Fan, "Internet and Its Applications", *Press of China University of Geosciences*, Wuhan, 2001.

Refereed Journal Articles *(*denotes graduate student; +denotes undergraduate student)*

Published

47. Sungmin Hong*, Lei Xu*, Jianwei Huang*, Hongda Li*, Hongxin Hu and Guofei Gu, "SysFlow: Towards a Programmable Zero Trust Framework for System Security", *IEEE Transactions on Information Forensics and Security (TIFS)*, Accepted for publication, 2023.
46. Matthew John Costello, Nishant Vishwamitra*, Song Liao*, Long Cheng, Feng Luo, Hongxin Hu, "COVID-19 and Sinophobia: Detecting Warning Signs of Radicalization on Twitter and Reddit", *Cyberpsychology, Behavior, and Social Networking*, Accepted for publication, 2023.
45. Fei Ding*, Yin Yang, Hongxin Hu, Venkat Krovi and Feng Luo, "Dual-Level Knowledge Distillation via Knowledge Alignment and Correlation", *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)*, July 2022.
44. Juan Wang, Shirong Hao*, Hongxin Hu, Hongda Li, Wenhui Zhang, Jun Xu and Peng Liu, "S-Blocks: Lightweight and Trusted Virtual Security Function with SGX", *IEEE Transactions on Cloud Computing (TCC)*, 10(2): 1082-1099, 2022.
43. Matthew Costello, Long Cheng, Feng Luo, Hongxin Hu, Song Liao*, Nishant Vishwamitra*, Mingqi Li*, and Ebuka Okpala*, "COVID-19: A Pandemic of Anti-Asian Cyberhate", *Journal of Hate Studies*, 17(1), 2021.
42. Song Liao*, Christin Wilson*, Long Cheng, Hongxin Hu and Huixing Deng*, "Problematic Privacy Policies of Voice Assistant Applications", *IEEE Security & Privacy (S&P)*, June 2021.

41. Guanyu Li*, Menghao Zhang*, Shicheng Wang, Chang Liu, Mingwei Xu, Ang Chen, Hongxin Hu, Guofei Gu, Qi Li, Jianping Wu, "Enabling Performant, Flexible and Cost-Efficient DDoS Defense with Programmable Switches", *IEEE/ACM Transactions on Networking (ToN)*, March 2021.
40. Heng Yu*, Zhilong Zheng*, Junxian Shen*, Congcong Miao*, Chen Sun*, Hongxin Hu, Jun Bi, Jianping Wu, Jilong Wang, "Octans: Optimal Placement of Service Function Chains in Many-Core Systems", *IEEE Transactions Parallel and Distributed Systems (TPDS)*, 32(9), 2202-2215, 2021.
39. Zili Meng*, Yaning Guo, Yixin Shen, Jing Chen, Chao Zhou, Minhu Wang, Jia Zhang, Mingwei Xu, Chen Sun*, Hongxin Hu, "Practically Deploying Heavyweight Adaptive Bitrate Algorithms With Teacher-Student Learning", *IEEE/ACM Transactions on Networking (ToN)*, 29(2):723-736, 2021.
38. Yuan Luo*, Long Cheng, Hongxin Hu, Guojun Peng and Danfeng Yao, "Context-rich Privacy Leakage Analysis through Inferring Apps in Smart Home IoT", *IEEE Internet of Things Journal (IoTJ)*, 8(4), 2736 - 2750, 2021.
37. Juan Wang, Shirong Hao*, Ru Wen, Boxian Zhang, Hongxin Hu and Rongxin Lu, "IoT-Praetor: Undesired Behaviors Detection for IoT Devices", *IEEE Internet of Things Journal (IoTJ)*, 8(2), 927 - 940, 2021.
36. Xincai Fei*, Fangming Liu, Qixia Zhang, Hai Jin and Hongxin Hu, "Paving the Way for NFV Acceleration: A Taxonomy, Survey and Future Directions", *ACM Computing Surveys (CSUR)*, 53(4), 1-42, 2020.
35. Zili Meng*, Jun Bi, Haiping Wang, Chen Sun* and Hongxin Hu, "MicroNF: An Efficient Framework for Enabling Modularized Service Chains in NFV", *IEEE Journal of Selected Areas in Communications (JSAC)*, 37(8), 1851 - 1865, 2019.
34. Menghao Zhang*, Jun Bi, Kai Gao, Yi Qiao, Guanyu Li, Xiao Kong, Zhaogeng Li and Hongxin Hu, "Tripod: Towards a Scalable, Efficient and Resilient Cloud Gateway", *IEEE Journal of Selected Areas in Communications (JSAC)*, 37(3), 570 - 585, 2019.
33. Mhafuzul Islam, Mashrur Chowdhury, Hongda Li* and Hongxin Hu, "Vision-Based Navigation of Autonomous Vehicle in Roadway Environments with Unexpected Hazards", *Journal of the Transportation Research Board (TRB)*, 2673(12), 494-507, 2019.
32. Hongxin Hu, Wonkyu Han*, Sukwha Kyung, Juan Wang, Gail-Joon Ahn, Ziming Zhao and Hongda Li*, "Towards a Reliable Firewall for Software-Defined Networks", *Computers & Security (COSE)*, 87:101597, 2019.
31. Chen Sun*, Jun Bi, Zili Meng*, Tong Yang, Xiao Zhang and Hongxin Hu, "Enabling NFV Elasticity Control with Optimized Flow Migration", *IEEE Journal of Selected Areas in Communications (JSAC)*, 36(10), 2288 - 2303, 2018.
30. Mhafuzul Islam, Mashrur Chowdhury, Hongda Li* and Hongxin Hu, "Cybersecurity Attacks in Vehicle-to-Infrastructure (V2I) Applications and Their Prevention", *Journal of the Transportation Research Board (TRB)*, 2672(19), 66-78, 2018.
29. Chen Sun*, Jun Bi, Zhilong Zheng and Hongxin Hu, "HYPER: A Hybrid High-Performance Framework for Network Function Virtualization", *IEEE Journal of Selected Areas in Communications (JSAC)*, 35(11), 2288 - 2303, 2017.

28. Chen Sun*, Jun Bi, Haoxian Chen, Hongxin Hu, Zhilong Zheng, Shuyong Zhu and Chenghui Wu, "SDPA: Towards a Stateful Data Plane in Software-Defined Networking", *IEEE/ACM Transactions on Networking (TON)*, 25(6), 3294 - 3308, 2017.
27. Yuan Shi, Huanguo Zhang, Juan Wang, Feng Xiao, Jianwei Huang, Daochen Zha, Hongxin Hu, Fei Yan and Bo Zhao, "CHAOS: An SDN-Based Moving Target Defense System", *Security and Communication Networks(SCN)*, October, 2017.
26. Yiming Jing, Gail-Joon Ahn, Hongxin Hu, Haehyun Cho, and Ziming Zhao, "TripleMon: A Multi-layer Security Framework for Mediating Inter-Process Communication on Android", *Journal of Computer Security (JCS)*, 24(4), 405 - 426, 2016.
25. Ziming Zhao, Mukund Sankaran, Gail-Joon Ahn, Tom Holt, Yiming Jing and Hongxin Hu, "Mules, Seals, and Attacking Tools: Analyzing Twelve Online Marketplaces", *IEEE Security & Privacy*, 14(3), 32 - 43, 2016.
24. 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)*, 17(4), 1 - 37, 2016.
23. Jun Bi, Shuyong Zhu, Guang Yao, Chen Sun* and Hongxin Hu, "Supporting Virtualized Network Functions with Stateful Data Plane Abstraction", *IEEE Network,* 30(3), 40-45, 2016.
22. Juan Wang, Jiang Wang, Hongyang Jiao, Yong Wang, Shiya Chen, Shihui Liu and Hongxin Hu, "OpenFlow-based Real-Time Conflict Detection and Resolution for SDN Access Control Policies", *Chinese Journal of Computers (CJC)*, 38(4), 2015.
21. Yiming Jing, Gail-Joon Ahn, Ziming Zhao and Hongxin Hu, "Towards Automated Risk Assessment and Mitigation of Mobile Applications", *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 12(5), 571 - 584, 2014.
20. Yan Zhu, Di Ma, Changjun Hu, Gail-Joon Ahn and Hongxin Hu, "Secure and Efficient Random Functions with Variable-Length Output", *Journal of Network and Computer Applications (JNCA)*, 45, 121-133, 2014.
19. Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Changjun Hu and Di Ma, "Role-Based Cryptosystem: A New Cryptographic RBAC System Based on Role-Key Hierarchy", *IEEE Transactions on Information Forensics & Security (TIFS)*, 8(12), 2138-2153, 2013.
18. Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni, "Discovery and Resolution of Anomalies in Web Access Control Policies", *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 10(6), 341-354, 2013.
17. Juan Wang, Hongxin Hu, Bo Zhao, Fei Yan, Huangguo Zhang and Qianhong Wu, "Formal Analysis of Information Card Federated Identity-Management Protocol", *Chinese Journal of Electronics (CJE)*, 22 (1), 2013.
16. Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen[+], "Multiparty Access Control for Online Social Networks: Model and Mechanisms", *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 25(7), 1614-1627, 2012.

15. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Mengyang Yu and Shimin Chen, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 23(12), 2231-2244, 2012.
14. Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni, "Detecting and Resolving Firewall Policy Anomalies", *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 9(3), 318-331, 2012.
13. Ruoyu Wu, Gail-Joon Ahn and Hongxin Hu, "Towards HIPAA-compliant Healthcare Systems in Cloud Computing", *International Journal of Computational Models and Algorithms in Medicine (IJCMAM)*, 3(2), 2012.
12. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Yujing Han and Shimin Chen, "Collaborative Integrity Verification in Hybrid Clouds", *International Journal of Cooperative Information Systems (IJCIS)*, 21(3), 191-200, 2012.
11. Karsten Sohr, Mirco Kuhlmann, Martin Gogolla, Hongxin Hu and Gail-Joon Ahn, "Comprehensive Two-Level Analysis of Role-Based Delegation and Revocation Policies", *Information and Software Technology (IST)*, 54(12), 1396-1417, 2012.
10. Yan Zhu, Hongxin Hu, Gail-Joon Ahn and Stephen S. Yau, "Efficient Audit Service Outsourcing for Data Integrity in Clouds", *Journal of Systems and Software (JSS)*, 85(5), 1083-1095, 2012.
9. Yan Zhu, Mengyang Yu, Hongxin Hu, Gail-Joon Ahn and Hongjia Zhao, "Efficient Constructions of Provably Secure Steganography under Ordinary Covert Channels", *SCIENCE CHINA - Information Sciences*, 55(7), 2012.
8. Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau and Ho G. An, "Dynamic Audit Services for Outsourced Storages in Clouds", *IEEE Transactions on Services Computing (TSC)*, 6(2), 227-238, 2011.
7. Wenjuan Xu, Xinwen Zhang, Hongxin Hu, Gail-Joon Ahn and Jean-Pierre Seifert, "Remote Attestation with Domain-based Integrity Model and Policy Analysis", *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 9(3), 429-442, 2011.
6. Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu, "Risk-Aware Response for Mitigating MANET Routing Attacks", *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 9(2), 250 - 260, 2011.
5. Jing Jin, Gail-Joon Ahn, Hongxin Hu, Michael Covington and Xinwen Zhang, "Patient-centric Authorization Framework for Electronic Healthcare Services", *Computers & Security (COSE)*, 30(2-3), 116-127, 2011.
4. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Huaixi Wang and Shanbiao Wang, "Provably Secure Role-Based Encryption with Revocation Mechanism", *Journal of Computer Science and Technology (JCST)*, 26(4), 697-710, 2011.
3. Yan Zhu, Zexing Hu, Huaixi Wang, Gail-Joon Ahn and Hongxin Hu, "Zero-knowledge Proofs of Retrievability", *SCIENCE CHINA - Information Sciences*, 54(8), 2011.
2. Hongxin Hu and Gail-Joon Ahn, "Constructing Authorization Systems Using Assurance Management Framework", *IEEE Transactions on Systems, Man, and Cybernetics (TSMC)*, 40(4), 396-405, 2010.

1. Gail-Joon Ahn, Hongxin Hu and Jing Jin, "Security-enhanced OSGi Service Environments", *IEEE Transactions on Systems, Man, and Cybernetics (TSMC)*, 39(5), 562-571, 2009.

Refereed Proceedings Articles *(presenter name underlined; *graduate student; +undergraduate students; #high school students)*

107. Song Liao*, Long Cheng, Haipeng Cai, Linke Guo and Hongxin Hu, "SkillScanner: Detecting Policy-Violating Voice Applications Through Static Analysis at the Development Phase", In *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2023)*, Copenhagen, Denmark, November 26-30, 2023.

106. Feng Wei*, Hongda Li*, Ziming Zhao and Hongxin Hu, "xNIDS: Explaining Deep Learning-based Network Intrusion Detection Systems for Active Intrusion Responses", In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 2023)*, Anaheim, CA, USA, August 9-11, 2023.

105. Song Liao*, Ebuka Okpala*, Long Cheng, Mingqi Li*, Nishant Vishwamitra, Hongxin Hu, Feng Luo and Matthew John Costello, "Analysis of COVID-19 Offensive Tweets and Their Targets", In *Proceedings of the 29th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2023)*, Long Beach, CA, USA, August 6-10, 2023. [Acceptance rate: 184/725 = 25.3%]

104. Zili Meng*, Tingfeng Wang, Yixin Shen, Bo Wang, Mingwei Xu, Rui Han, Honghao Liu, Venkat Arun, Hongxin Hu and Xue Wei, "Enabling High Quality Real-Time Communications with Adaptive Frame-Rate", In *Proceedings of the 20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2023)*, Boston, MA, USA, April 17-19, 2023. [Acceptance rate: 50/272 = 18.3%]

103. Zheyuan Ma*, Xi Tan*, Lukasz Ziarek, Ning Zhang, Hongxin Hu and Ziming Zhao, "Return-to-Non-Secure Vulnerabilities on ARM Cortex-M TrustZone: Attack and Defense", In *Proceedings of the 60th ACM/IEEE Design Automation Conference (DAC 2023)*, San Francisco, CA, USA, July 9-13, 2023.

102. Mingqi Li*, Fei Ding*, Dan Zhang*, Long Cheng, Hongxin Hu and Feng Luo, "Multi-level Distillation of Semantic Knowledge for Pre-training Multilingual Language Model", In *Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing (EMNLP 2022)*, Abu Dhabi, Dec 7-11, 2022.

101. Mengda Yang*, Juan Wang, Hongxin Hu, Ao Ren, Ziang Li*, Xiaoyang Xu* and Wenzhe Yi*, "Measuring Data Reconstruction Defenses in Collaborative Inference Systems", In *Proceedings of the 36th Conference on Neural Information Processing Systems (NeurIPS 2022)*, New Orleans, LA, USA, Nov 28 - Dec 9, 2022. [Acceptance rate: 25.6%]

100. Guanyu Li*, Menghao Zhang*, Cheng Guo*, Han Bao*, Mingwei Xu, Hongxin Hu and Fenghua Li, "IMap: Fast and Scalable In-Network Scanning with Programmable Switches", In *Proceedings of the 19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2022)*, Renton, WA, USA, April 4-6, 2022. [Acceptance rate: 50/298 = 16.8%]

99. Jeffrey Young*, Song Liao*, Long Cheng, Hongxin Hu and Huixing Deng*, "SkillDetective: Automated Policy-Violation Detection of Voice Assistant Applications in the Wild", In *Proceedings of the 31st USENIX Security Symposium (USENIX Security 2022)*, August 10–12, 2022. [Acceptance rate: 256/1414= 18.1%]

98. Hongda Li*, Qiqing Huang*, Fei Ding, Hongxin Hu, Long Cheng, Guofei Gu and Ziming Zhao, "Understanding and Detecting Remote Infection on Linux-based IoT Devices", In *Proceedings of the 17th ACM ASIA Conference on Computer and Communications Security (ASIACCS 2022),* May 30 - June 3, 2022. [Acceptance rate: 85/463 = 18.4%] [**Best Paper Award**]

97. Nishant Vishwamitra*, Yifang Li, Hongxin Hu, Kelly Caine, Long Cheng, Ziming Zhao and Gail-Joon Ahn, "Towards Automated Content-based Photo Privacy Control in User-Centered Social Networks", In *Proceedings of the 12th ACM Conference on Data and Application Security and Privacy (CODASPY 2022),* April 24 - 26, 2022.

96. John Anderson*, Qiqing Huang*, Long Cheng and Hongxin Hu, "BYOZ: Protecting BYOD Through Zero Trust Network Security", In *Proceedings of the 16th IEEE International Conference on Networking, Architecture, and Storage (NAS 2022),* Philadelphia, PA, USA, October 3-4, 2022.

95. Keyan Guo*, Wentai Zhao[#], Jaden Mu[#], Nishant Vishwamitra*, Ziming Zhao and Hongxin Hu, "Understanding the Generalizability of Hateful Memes Detection Models Against COVID-19-related Hateful Memes", In *Proceedings of IEEE 2022 International Conference on Machine Learning and Applications (ICMLA 2022),* December 12-14, 2022.

94. Guanyu Li*, Menghao Zhang*, Cheng Guo*, Han Bao*, Mingwei Xu, Hongxin Hu, "Switches are Scanners Too! A Fast and Scalable In-Network Scanner with Programmable Switches", In *Proceedings of the 20th ACM Workshop on Hot Topics in Networks (HotNets 2021)*, November 10-12, 2021.

93. Dian Chen*, Hongxin Hu, Qian Wang, Yinli Li, Cong Wang, Chao Shen and Qi Li, "CARTL: Cooperative Adversarially-Robust Transfer Learning", In *Proceedings of the 38th International Conference on Machine Learning (ICML 2021)*, July 18-24, 2021. [**Long presentation**, top 3% (166/5513)]

92. Nishant Vishwamitra*, Hongxin Hu, Feng Luo and Long Cheng, "Towards Understanding and Detecting Cyberbullying in Real-world Images", In *Proceedings of the 28th Network and Distributed System Security Symposium (NDSS 2021)*, February 21-24, 2021. [Acceptance rate: 87/573 = 15.2%]

91. Wenbo Ding*, Hongxin Hu and Long Cheng, "IoTSafe: Enforcing Safety and Security Policy with Real IoT Physical Interaction Discovery", In *Proceedings of the 28th Network and Distributed System Security Symposium (NDSS 2021)*, February 21-24, 2021. [Acceptance rate: 87/573 = 15.2%]

90. Jing Chen*, Zili Meng*, Yaning Guo*, Mingwei Xu and Hongxin Hu, "HierTopo: Towards High-Performance and Efficient Topology Optimization for Dynamic Networks", In *Proceedings of Proceedings of the 29th IEEE/ACM International Symposium on Quality of Service (IWQoS 2021)*, June 25-28, 2021. [Acceptance rate: 64/256 = 25%]

89. Mingqi Li*, Song Liao*, Ebuka Okpala*, Max Tong[#], Matthew Costello, Long Cheng, Hongxin Hu and Feng Luo, "COVID-HateBERT: a Pre-trained Language Model for COVID-19 related Hate Speech Detection", In *Proceedings of IEEE 2021 International Conference on Machine Learning and Applications (ICMLA 2021)*, December 13-16, 2021.

88. Joseph Clements*, Yuzhe Yang*, Ankur Sharma*, Hongxin Hu and Yingjie Lao, "Rallying Adversarial Techniques against Deep Learning for Network Security", In *Proceedings of 2021 IEEE Symposium Series on Computational Intelligence (SSCI 2021)*, December 4-7, 2021.

87. Long Cheng, Christin Wilson, Song Liao, Jeffrey Young, Daniel Dong[+], Hongxin Hu, "Dangerous Skills Got Certified: Measuring the Trustworthiness of Skill Certification in Voice Personal Assistant Platforms", In *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2020)*, November 9-13, 2020. [Acceptance rate: 121/715 = 16.9%]

86. Song Liao, Christin Wilson, Long Cheng, Hongxin Hu and Huixing Deng, "Dangerous Skills Got Certified: Measuring the Trustworthiness of Skill Certification in Voice Personal Assistant Platforms", In *Proceedings of the 2020 Annual Computer Security Applications Conference (ACSAC 2020)*, December 7-11, 2020. [Acceptance rate: 23%] [**Distinguished Paper Award**]

85. Zili Meng*, Minhu Wang, Jiasong Bai, Mingwei Xu, Hongzi Mao and Hongxin Hu, "Interpreting Deep Learning-Based Networking Systems", In *Proceedings of the ACM SIGCOMM Conference (SIGCOMM 2020)*, August 10-14, 2020. [Acceptance rate: 54/250 = 21.6%]

84. Shuhe Wang, Chen Sun*, Zili Meng, Minhu Wang, Jiamin Cao, Mingwei Xu, Jun Bi, Qun Huang, Masoud Moshref, Tong Yang, Hongxin Hu and Gong Zhang, "Martini: Bridging the Gap between Network Measurement and Control Using Switching ASICs", In *Proceedings of the 26th IEEE International Conference on Network Protocols (ICNP 2020)*, Madrid, Spain, October 13-16, 2020. [Acceptance rate: 16.84%]

83. Jiasong Bai, Menghao Zhang*, Guanyu Li, Chang Liu, Mingwei Xu and Hongxin Hu, "FastFE: Accelerating ML-based Traffic Analysis with Programmable Switches", In *Proceedings of the 1st Workshop on Secure Programmable Network Infrastructure (SPIN2020)*, co-located with SIGCOMM 2020, New York, USA, August 10, 2020.

82. Fei Ding, Hongda Li*, Feng Luo, Hongxin Hu, Long Cheng, Hai Xiao and Rong Ge, "DeepPower: Non-intrusive and Deep Learning-based Detection of IoT Malware Using Power Side Channels", In *Proceedings of 15th ACM ASIA Conference on Computer and Communications Security (ASIACCS 2020)*, Taipei, Taiwan, June 1-5, 2020. [Acceptance rate: 67/308 = 21.7%]

81. Menghao Zhang*, Guanyu Li, Shicheng Wang, Chang Liu, Ang Chen, Hongxin Hu, Guofei Gu, Qi Li, Mingwei Xu and Jianping Wu, "Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches", In *Proceedings of the 27th Network and Distributed System Security Symposium (NDSS 2020)*, San Diego, CA, USA, February 23-26, 2020. [Acceptance rate: 88/506 = 17.4%]

80. Yifang Li, Nishant Vishwamitra*, Hongxin Hu and Kelly Caine, "Towards A Taxonomy of Content Sensitivity and Sharing Preferences for Photos", In *Proceedings of the 2020 ACM Conference on Human Factors in Computing Systems (CHI 2020)*, Honolulu, Hawaii, USA, April 25-30, 2020. [Acceptance rate: 760/3126 = 24.3%]

79. Shuhe Wang, Zili Meng*, Chen Sun, Minhu Wang, Mingwei Xu, Jun Bi, Tong Yang, Qun Huang and Hongxin Hu, "SmartChain: Enabling High-Performance Service Chain Partition between SmartNIC and CPU", In *Proceedings of 2020 IEEE International Conference on Communications (ICC 2020)*, Dublin, Ireland, June 7-11, 2020. [**Best Paper Award**]

78. Zili Meng*, Jing Chen, Yaning Guo, Chen Sun*, Hongxin Hu and Mingwei Xu, "PiTree: Practical Implementation of ABR Algorithms Using Decision Trees", In *Proceedings of the 27th ACM International Conference on Multimedia (MM 2019)*, Nice, France, October 21-25, 2019. [Oral paper acceptance rate: 88/936 = 9.4%]

77. Menghao Zhang*, Jiasong Bai, Guanyu Li, Zili Meng, Hongda Li*, Hongxin Hu and Mingwei Xu, "When NFV Meets ANN: Rethinking Elastic Scaling for ANN-based NFs", In *Proceedings of IEEE ICNP 2019 HDR-Nets Workshop (HDR-Nets 2019)*, Chicago, IL, USA, October 7, 2019.

76. Xiaohong Yuan, Zhipeng Liu, Younghee Park, Hongxin Hu and Hongda Li*, "Teaching SDN Security Using Hands-on Labs in CloudLab", In *Proceedings of the 23nd Colloquium for Information System Security Education (CISSE 2019)*, Las Vegas, Nevada, USA June 10-12, 2019.

75. Hongda Li*, Feng Wei* and Hongxin Hu, "Enabling Dynamic Network Access Control with Anomaly-based IDS and SDN", In *Proceedings of ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDN-NFV Security 2019)*, Richardson, TX, USA, March 27, 2019.

74. Zhilong Zheng, Jun Bi, Heng Yu, Haiping Wang, Chen Sun*, Hongxin Hu and Jianping Wu, "Octans: Optimal Placement of Service Function Chains in Many-Core Systems", In *Proceedings the 37th IEEE International Conference on Computer Communications (INFOCOM 2019)*, Paris, France, April 29-May 2, 2019. [Acceptance rate: 288/1464 = 19.7%]

73. Xiang Zhang, Nishant Vishwamitra*, Hongxin Hu and Feng Luo, "CrescendoNet: A New Deep Convolutional Neural Network with Ensemble Behavior", In *Proceedings of the 17th IEEE International Conference on Machine Learning and Applications (ICMLA 2018)*, Orlando, Florida, USA, December 17-20, 2018.

72. Wenbo Ding* and Hongxin Hu, "On the Safety of IoT Device Physical Interaction Control", In *Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS 2018)*, Toronto, Canada, October 15-19, 2018. [Acceptance rate: 134/809 = 16.6%]

71. Hongda Li*, Hongxin Hu, Guofei Gu, Gail-Joon Ahn and Fuqiang Zhang*, "vNIDS: Towards Elastic Security with Safe and Efficient Virtualization of Network Intrusion Detection Systems", In *Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS 2018)*, Toronto, Canada, October 15-19, 2018. [Acceptance rate: 134/809 = 16.6%]

70. Yifang Li, Nishant Vishwamitra*, Bart P. Knijnenburg, Hongxin Hu and Kelly Caine, "Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos", In *Proceedings of the 21st ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2018)*, Jersey City, NJ, USA, November 3-7, 2018. [Acceptance rate: 105/384 = 27.3%]
69. Zhilong Zheng, Jun Bi, Haiping Wang, Chen Sun*, Heng Yu, Hongxin Hu, Kai Gao and Jianping Wu, "Grus: Enabling Latency SLOs for GPU-Accelerated NFV Systems", In *Proceedings of the 26th IEEE International Conference on Network Protocols (ICNP 2018)*, Jersey City, NJ, USA, November 3-7, 2018. [Acceptance rate: 35/196 = 17.9%]
68. Zhilong Zheng, Jun Bi, Chen Sun*, Heng Yu, Hongxin Hu, Zili Meng*, Shuhe Wang, Kai Gao and Jianping Wu, "A GPU-Accelerated Elastic Framework for NFV", In *Proceedings of the 2nd Asia-Pacific Workshop on Networking (APNet 2018)*, Beijing, China, August 2-3, 2018.
67. Kang Chen, Jianwei Liu, James Martin, Kuang-Ching Wang and Hongxin Hu, "Improving Integrated LTE-WiFi Network Performance with SDN based Flow Scheduling", In *Proceedings of the 27th IEEE International Conference on Computer Communications and Networks (ICCCN 2018)*, Hangzhou, China, July 30-August 2, 2018. [Acceptance rate: 29.5%]
66. Chen Sun*, Jun Bi, Zili Meng*, Xiao Zhang and Hongxin Hu, "OFM: Optimized Flow Migration for NFV Elasticity Control", In *Proceedings of the 26th IEEE/ACM International Symposium on Quality of Service (IWQoS 2018)*, Banff, Alberta, Canada, June 4-6, 2018. [Acceptance rate: 26/125 = 20.8%]
65. Zili Meng, Jun Bi, Haiping Wang, Chen Sun* and Hongxin Hu, "CoCo: Compact and Optimized Consolidation of Modularized Service Function Chains in NFV", In *Proceedings of the 53rd IEEE International Conference on Communications (ICC 2018)*, Kansas City, Missouri, USA, May 20-24, 2018.
64. Hongda Li*, Fuqiang Zhang*, Lu Yu, Jon Oakley, Hongxin Hu and Richard Brooks, "Towards Efficient Traffic Monitoring for Science DMZ with Side-channel Based Traffic Winnowing", In *Proceedings of ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDN-NFV Security 2018)*, Tempe, Arizona, USA, March 21, 2018.
63. Juan Wang, Chengyang Fan, Jie Wang, Shirong hao, Yi li and Hongxin Hu, "Challenges Towards Protecting VNF with SGX", In *Proceedings of ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDN-NFV Security 2018)*, Tempe, Arizona, USA, March 21, 2018.
62. Younghee Park, Hongxin Hu, Xiaohong Yuan and Hongda Li*, "Enhancing Security Education Through Designing SDN Security Labs in CloudLab", In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE 2018)*, Baltimore, Maryland, USA, February 21-24, 2018. [**Best Paper Award**]
61. Guofei Gu, Hongxin Hu, Eric Keller, Zhiqiang Lin and Donald Porter, "Building a Security OS with Software Defined Infrastructure", In *Proceedings of the 8th ACM*

SIGOPS Asia-Pacific Workshop on Systems (APSys 2017), IIT, Bombay, Indian, September 2-3, 2017.

60. Yifang Li, Nishant Vishwamitra*, Hongxin Hu, Bart Knijnenburg and Kelly Caine, "Effectiveness and Users' Experience of Face Blurring as a Privacy Protection for Sharing Photos via Online Social Networks", In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting (HFES 2017)*, Austin, Texas, USA, October 9-13, 2017.
59. Yifang Li, Nishant Vishwamitra*, Bart Knijnenburg, Hongxin Hu and Kelly Caine, "Effectiveness and Users' Experience of Face Blurring as a Privacy Protection for Sharing Photos via Online Social Networks", In *Proceedings of the 1st International Workshop on The Bright and Dark Sides of Computer Vision: Challenges and Opportunities for Privacy and Security (CV-COPS 2017)*, Honolulu, Hawaii, USA, July 21, 2017.
58. Chen Sun*, Jun Bi, Zhilong Zheng, Heng Yu and Hongxin Hu, "NFP: Enabling Network Function Parallelism in NFV", In *Proceedings of the ACM SIGCOMM Conference (SIGCOMM 2017)*, Los Angeles, CA, USA, August 21-25, 2017. [Acceptance rate: 36/250 = 14.4%]
57. Nishant Vishwamitra*, Yifang Li, Kevin Wang+, Hongxin Hu, Kelly Caine and Gail-Joon Ahn, "Towards PII-based Multiparty Access Control for Photo Sharing in Online Social Networks", In *Proceedings of the 22nd ACM Symposium on Access Control Models And Technologies (SACMAT 2017)*, Indianapolis, IN, USA, June 21-23, 2017. [Acceptance rate: 14/50 = 28.0%]
56. Anjan Rayamajhi, Mizanur Rahman, Manveen Kaur, Jianwei Liu, Mashrur Chowdhury, Hongxin Hu, Jerome McClendon, Kuang-Ching Wang, Abhimanyu Gosain and Jim Martin, "ThinGs In a Fog: System Illustration with Connected Vehicles", In *Proceedings of the IEEE 85th Vehicular Technology Conference (VTC 2017)*, Sydney, NSW, Australia, June 4-7, 2017.
55. Nuyun Zhang, Hongda Li*, Hongxin Hu and Younghee Park, "Towards Effective Virtualization of Intrusion Detection Systems", In *Proceedings of ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDN-NFV Security 2017)*, Scottsdale, Arizona, USA, March 24, 2017.
54. Younghee Park, Pritesh Chandaliya, Akshaya Muralidharan, Nikash Kumar and Hongxin Hu, "Dynamic Defense Provision via Network Functions Virtualization", In *Proceedings of ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDN-NFV Security 2017)*, Scottsdale, Arizona, USA, March 24, 2017.
53. Nishant Vishwamitra*, Xiang Zhang, Jonathan Tong[#], Hongxin Hu, Feng Luo, Robin Kowalski and Joseph Mazer, "MCDefender: Toward Effective Cyberbullying Defense in Mobile Online Social Networks", In *Proceedings of the 3rd International Workshop on Security and Privacy Analytics (IWSPA 2017)*, Scottsdale, Arizona, USA, March 24, 2017.
52. 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 24th Network and Distributed System Security*

Symposium (NDSS 2017), San Diego, CA, USA, February 26 - March 1, 2017. [Acceptance rate: 68/423 = 16.1%]

51. Jinwei Liu, Haiying Shen and Hongxin Hu, "Load-aware and Congestion-free State Management in Network Function Virtualization", In *Proceedings of International Conference on Computing, Networking and Communications (ICNC 2017)*, Silicon Valley, USA, January 26-29, 2017.
50. Xiang Zhang, Jonathan Tong[#], Nishant Vishwamitra*, Joseph P. Mazer, Robin Kowalski, Elizabeth Whittake, Hongxin Hu, Feng Luo, Jamie Macbeth and Edward Dillon, "Cyberbullying Detection with a Pronunciation Based Convolutional Neural Network", In *Proceedings of the 15th IEEE International Conference on Machine Learning and Applications (ICMLA 2016)*, Anaheim, California, USA, December 18-20, 2016.
49. Chen Sun*, Jun Bi and Hongxin Hu, "NeSMA: Enabling Network-Level State-Aware Applications in SDN", In *Proceedings of the 24th IEEE International Conference on Network Protocols (ICNP 2016)*, CoolSDN Workshop, Singapore, November 8-11, 2016.
48. Manveen Kaur, James Martin and Hongxin Hu, "Comprehensive View of Security Practices in Vehicular Networks", In *Proceedings of the 5th International Conference on Connected Vehicles & Expo (ICCVE 2016)*, Seattle, USA, September 12-16, 2016.
47. Kang Chen, Ryan Izard, Hongxin Hu, Kuangching Wang and James Martin, "HetSDN: Exploiting SDN for Intelligent Network Usage in Heterogeneous Wireless Networks", In *Proceedings of 2016 IEEE/ACM International Symposium on Quality of Service (IWQoS 2016)*, Beijing, China, June 20-21, 2016.
46. Hitesh Padekar, Younghee Park, Hongxin Hu and Sang-Yoon Chang, "Enabling Dynamic Access Control for Controller Applications in Software-Defined Networks", In *Proceedings of the 21st ACM Symposium on Access Control Models And Technologies (SACMAT 2016)*, Shanghai, China, June 5-8, 2016. [**Best Paper Honorable Mention**]
45. Wonkyu Han, Hongxin Hu, Ziming Zhao, Adam Doupé, Gail-Joon Ahn, Kuang-Ching Wang and Juan Deng, "State-aware Network Access Management for Software-Defined Networks", In *Proceedings of the 21st ACM Symposium on Access Control Models And Technologies (SACMAT 2016)*, Shanghai, China, June 5-8, 2016.
44. Jason Anderson, Udit Agarwal, Hongda Li*, Hongxin Hu, Craig Lowery and Amy Apon, "Performance Considerations of Network Functions Virtualization using Containers", In *Proceedings of International Conference on Computing, Networking and Communications (ICNC 2016)*, Kauai, Hawaii, USA, February 15-18, 2016.
43. Juan Deng, Hongxin Hu, Hongda Li*, Zhizhong Pan, Kuang-Ching Wang, Gail-Joon Ahn, Jun Bi and Younghee Park, "VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls", In *Proceedings of IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN 2015)*, San Francisco, USA, November 18-21, 2015.
42. Shuyong Zhu, Jun Bi, Chen Sun*, Chenghui Wu and Hongxin Hu, "SDPA: Enhancing Stateful Forwarding for Software-Defined Networking", In *Proceedings of the 23rd IEEE International Conference on Network Protocols (ICNP 2015)*, San Francisco,

USA, November 10-13, 2015. [Acceptance rate: 38/187 = 20.3%] [**Best Paper Nominee**]

41. Khaled Riad, Yan Zhu, Hongxin Hu and Gail-Joon Ahn, "AR-ABAC: A New Attribute Based Access Control Model Supporting Attribute-Rules for Cloud Computing", In *Proceedings of the 1st IEEE International Conference on Collaboration and Internet Computing (CIC 2015)*, Hangzhou, China, October 27-30, 2015.
40. Yiming Jing, Ziming Zhao, Gail-Joon Ahn and Hongxin Hu, "Morpheus: Automatically Generating Heuristics to Detect Android Emulators", In *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC 2014)*, New Orleans, LA, USA, December 8-12, 2014. [Acceptance rate: 47/236 = 19.9%] [Finalist for CSAW 2015 Best Applied Security Paper Award]
39. WC Moody, Hongxin Hu and Amy W. Apon, "Defensive Maneuver Cyber Platform Modeling with Stochastic Petri Nets", In *Proceedings of the 10th International Conference on Collaborative Computing (CollaborateCom 2014)*, Miami, Florida, USA, October 22-25, 2014.
38. Hongxin Hu, Wonkyu Han*, Gail-Joon Ahn, "FlowGuard: Building Robust Firewalls for Software-Defined Networks", In *Proceedings of ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN 2014)*, Chicago, IL, USA, August 22, 2014. [Acceptance rate: 16/114 = 14.0%]
37. Wonkyu Han*, Hongxin Hu and Gail-Joon Ahn, "LPM: Layered Policy Management for Software-Defined Networks", In *Proceedings of the 28th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2014)*, Vienna, Austria. July 14-16, 2014.
36. Hongxin Hu, Gail-Joon Ahn, Ziming Zhao and Dejun Yang, "Game Theoretic Analysis of Multiparty Access Control in Online Social Networks", In *Proceedings of the 19th ACM Symposium on Access Control Models And Technologies (SACMAT 2014)*, London, Ontario, Canada, June 25-27, 2014. [Acceptance rate: 17/59 = 29.3%]
35. Hongxin Hu, Gail-Joon Ahn, Wonkyu Han and Ziming Zhao, "Towards a Reliable SDN Firewall", In *Proceedings of the Open Networking Summit 2014 (ONS 2014)*, Research Track, Santa Clara, California, USA, March 3-5, 2014. [Acceptance rate: 28.2%]
34. 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 2014)*, San Antonio, Texas, USA, March 3-5, 2014. [Acceptance rate: 19/119 = 16.0%] [**Best Paper Award**]
33. Juan Wang, Yong Wang, Hongxin Hu, Qingxin Sun, He Shi and Longjie Zeng, "Towards a Security-Enhanced Firewall Application for OpenFlow Networks", In *Proceedings of the 5th International Symposium on Cyberspace Safety and Security (CSS 2014)*, November 13-15, 2013.
32. Juan Wang, Xuhui Xie and Hongxin Hu, "Towards a Trusted Launch Mechanism for Virtual Machines in Cloud Computing", In *Proceedings of the 4th International Conference on Cloud Computing (CLOUDCOMP 2014)*, October 17–19, 2013.

31. 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 (USENIX Security 2013)*, Washington DC, August 14-16, 2013. [Acceptance rate: 44/277 = 15.9%]
30. Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen, "Enabling Collaborative Data Sharing in Google+", In *Proceedings of the 55th IEEE Global Communications Conference (GLOBECOM 2012)*, Anaheim, California, USA, December 3-7, 2012.
29. Yan Zhu, Shanbiao Wang, Di Ma, Hongxin Hu and Gail-Joon Ahn, "Secure and Efficient Constructions of Hash, MAC and PRF for Mobile Devices", In *Proceedings of the 55th IEEE Global Communications Conference (GLOBECOM 2012)*, Anaheim, California, USA, December 3-7, 2012.
28. Yiming Jing, Gail-Joon Ahn and Hongxin Hu, "Model-based Conformance Testing for Android", In *Proceedings of the 7th International Workshop on Security (IWSEC 2012)*, Fukuoka, Japan, November 7-9, 2012.
27. Ruoyu Wu, Gail-Joon Ahn and Hongxin Hu, "Secure Sharing of Electronic Health Records in Clouds", In *Proceedings of the 8th IEEE International Conference on Collaborative Computing (CollaborateCom 2012)*, Pittsburgh, Pennsylvania, USA, October 14-17, 2012.
26. 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 2013)*, Pisa, Italy, September 10-14, 2012. [Acceptance rate: 50/248 = 20.1%]
25. Yan Zhu, Hongxin Hu, Gail-Joon Ahn and Mengyan Yu, "Comparison-Based Encryption for Fine-grained Access Control in Clouds", In *Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy (CODASPY 2013)*, San Antonio, Texas, USA, February 7-9, 2012. [Acceptance rate: 21/113 = 18.6%]
24. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang and Shanbiao Wang, "Towards Temporal Access Control in Cloud Computing", In *Proceedings of the 31st IEEE International Conference on Computer Communications (INFOCOM 2012)*, Mini-conference, Orlando, Florida, USA, March 25-30, 2012. [Acceptance rate: 378/1547 = 24.4%]
23. Ruoyu Wu, Gail-Joon Ahn and Hongxin Hu, "Towards HIPAA-compliant Healthcare Systems", In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium (IHI 2012)*, Miami, Florida, USA, January 28-30, 2012. [Acceptance rate: 48/269 = 17.8%]
22. Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen, "Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks", In *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC 2011)*, Orlando, Florida, USA, December 5-9, 2011. [Acceptance rate: 39/195 = 20.0%]
21. 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 2011)*, Houston, Texas, USA, December 5-9, 2011.

20. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Yujing Han and Shimin Chen, "Collaborative Integrity Verification in Hybrid Clouds", In *Proceedings of the 7th International Conference on Collaborative Computing (CollaborateCom 2011)*, Orlando, Florida, USA, October 15-18, 2011.
19. Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni, "Ontology-based Policy Anomaly Management for Autonomic Computing", In *Proceedings of the 7th International Conference on Collaborative Computing (CollaborateCom 2011)*, Orlando, Florida, USA, October 15-18, 2011.
18. 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 2011)*, Orlando, Florida, USA, December 5-9, 2011. [Acceptance rate: 39/195 = 20.0%]
17. Hongxin Hu and Gail-Joon Ahn, "Multiparty Authorization Framework for Data Sharing in Online Social Networks", In *Proceedings of the 25th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2011)*, Richmond, Virginia, USA. July 11-13, 2011.
16. Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni, "Anomaly Discovery and Resolution in Web Access Control Policies", In *Proceedings of the 16th ACM Symposium on Access Control Models And Technologies (SACMAT 2011)*, Innsbruck, Austria, June 15-17, 2011. [**Best Paper Nominee**]
15. Yan Zhu, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu and Stephen S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds", In *Proceedings of the 26th ACM Symposium on Applied Computing (SAC 2011)*, Security Track, TaiChung, Taiwan, March 21-25, 2011. [Acceptance rate: 9/41 = 21.9%]
14. Juan Wang and Hongxin Hu, "Security Validation of Information Card Protocol with AVISPA", In *Proceedings of International Conference on Energy Systems and Electrical Power (ESEP 2011)*, Singapore, Dec 9-10, 2011.
13. Yan Zhu, Zexing Hu, Huaixi Wang, Hongxin Hu and Gail-Joon Ahn, "A Collaborative Framework for Privacy Protection in Online Social Networks", In *Proceedings of the 6th International Conference on Collaborative Computing (CollaborateCom 2010)*, Chicago, Illinois, USA, October 9-12, 2010.
12. Ruoyu Wu, Gail-Joon Ahn, Hongxin Hu and Mukesh Singhal, "Information Flow Control in Cloud Computing", In *Proceedings of the 6th International Conference on Collaborative Computing (CollaborateCom 2010)*, Chicago, Illinois, USA, October 9-12, 2010.
11. Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni, "FAME: A Firewall Anomaly Management Environment", In *Proceedings of ACM CCS Workshop on Assurable & Usable Security Configuration (SafeConfig 2010)*, Chicago, IL, USA, October 4, 2010.
10. Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu, "Risk-Aware Response for Mitigating MANET Routing Attacks", In *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM 2010)*, Miami, Florida, USA, December 6-10, 2010.

9. Wenjuan Xu, Gail-Joon Ahn, Hongxin Hu, Xinwen Zhang and Jean-Pierre Seifert, "DR@FT: Efficient Remote Attestation Framework for Dynamic Systems", In *Proceedings of 15th European Symposium on Research in Computer Security (ESORICS 2010)*, Athens, Greece, September 20-22, 2010. [Acceptance rate: 42/201 = 20.8%]
8. Gail-Joon Ahn, Hongxin Hu, Joohyung Lee and Yunsong Meng, "Representing and Reasoning about Web Access Control Policies", In *Proceedings of 34th Annual IEEE International Computer Software and Applications Conference (COMPSAC 2010)*, Seoul, South Korea, July 19-23, 2010. [Acceptance rate: 39/193 = 20%]
7. Gail-Joon Ahn, Hongxin Hu, Joohyung Lee and Yunsong Meng, "Reasoning about XACML Policy Descriptions in Answer Set Programming", In *Proceedings of 13th International Workshop on Nonmonotonic Reasoning (NMR 2010)*, Toronto, Canada, May 14-16, 2010.
6. Yan Zhu, Gail-Joon Ahn, Hongxin Hu and Huaixi Wang, "Cryptographic Role-based Security Mechanisms based on Role-Key Hierarchy", In *Proceedings of 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010)*, Beijing, China, April 13-16, 2010. [Acceptance rate: 35/166 = 21%]
5. Jing Jin, Gail-Joon Ahn, Hongxin Hu, Michael Covington and Xinwen Zhang, "Patient-centric Authorization Framework for Sharing Electronic Health Records", In *Proceedings of the 14th ACM Symposium on Access Control Models And Technologies (SACMAT 2009)*, Stresa, Italy, June 3-5, 2009.
4. Gail-Joon Ahn, Hongxin Hu and Jing Jin, "Towards Role-based Authorization for OSGi Service Environments", In *Proceedings of the 12th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS 2008)*, Kunming, China, October 21-23, 2008.
3. Hongxin Hu and Gail-Joon Ahn, "Enabling Verification and Conformance Testing for Access Control Model", In *Proceedings of the 13th ACM Symposium on Access Control Models And Technologies (SACMAT 2008)*, Estes Park, Colorado, USA, June 11-12, 2008. [Acceptance rate: 20/79 = 25%]
2. Jing Jin, Gail-Joon Ahn, Mohammed Shehab and Hongxin Hu, "Towards Trust-aware Access Management for Ad-hoc Collaborations", In *Proceedings of the 3rd International Conference on Collaborative Computing (CollaborateCom 2007)*, New York, USA, November 12-15, 2007.
1. Gail-Joon Ahn and Hongxin Hu, "Towards Realizing a Formal RBAC Model in Real Systems", In *Proceedings of the 12th ACM Symposium on Access Control Models And Technologies (SACMAT 2006)*, Sophia Antipolis, France, June 20-22, 2007. [Acceptance rate: 19/79 = 24%]

TECHNICAL PRESENTATIONS

Invited Talks

48. "Fast and Scalable In-Network Security with Programmable Switches", the 4th Buffalo Wireless Day, November 2022.
47. "Security in the Emerging Internet of Things (IoT)", Wuhan University, 2022.

46. “Defending Against Cyberharassment in the Age of Machine Learning”, UB Center for Information Integrity Kick-Off Symposium, 2022.
45. “Fast and Scalable In-Network Security with Programmable Switches”, FABRIC Keeping Networks Innovative Together (KNIT) Winter Workshop, November 2021.
44. “Data for Deep Learning-based Network Intrusion Detection Systems”, Workshop on Data for AI in Network Systems, October 2021.
43. “Rethinking Security for the Internet of Things (IoT)”, University of Missouri, 2021.
42. “Security Labs for Software Defined Networks in CloudLab”, Cybersecurity Faculty Development Workshop, the University of Tennessee at Chattanooga, 2021.
41. “Network Security Function Virtualization: Challenges and Solutions”, Keynote Speech, ACM SDN-NFV Sec Workshop, 2021.
40. “AI-based Cyberharassment Detection”, REU Site: Special Topics on Biometrics and Authentication, 2021.
39. “Rethinking Security for the Internet of Things (IoT)”, University of Louisiana at Lafayette, 2021.
38. “Rethinking Security for the Internet of Things (IoT)”, University of North Carolina at Charlotte, 2021.
37. “Rethinking Security for the Internet of Things (IoT)”, University at Buffalo - SUNY, 2020.
36. “Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches”, NDSS 2020.
35. “Rethinking Security for the Internet of Things (IoT)”, University of Delaware, 2020.
34. “Dynamic Defense of IoT Malware”, VMWare, 2019.
33. “Rethinking Security for the Internet of Things (IoT)”, Wuhan University, 2019.
32. “Rethinking Security for the Internet of Things (IoT)”, University of Texas at Dallas, 2019.
31. “vNIDS: Safe and Efficient Virtualization of Network Intrusion Detection Systems”, VMWare, 2018.
30. “Safety Control on IoT Device Physical Interaction”, Tsinghua University, 2018.
29. “Enabling Reliable Access Control in Modern Network and Information Systems”, University of Texas at Arlington, 2018.
28. “Network Security Function Virtualization (NSFV): Challenges and Solutions”, Tsinghua University, 2017.
27. “Network Security Function Virtualization (NSFV): Challenges and Solutions”, Wuhan University, 2017.
26. “Network Security Function Virtualization: Challenges and Solutions”, NFV World Congress, 2017.
25. “Securing Software Defined Networks: From Theory to Practice”, SDN Security panel, IEEE CNS 2016.

24. “Enabling Reliable Access Control for Emerging Networking Technologies”, Tsinghua University, 2016.
23. “Enabling Reliable Access Control for Emerging Networking Technologies”, University of Science and Technology Beijing, 2016.
22. “Enabling Reliable Access Control for Emerging Networking Technologies”, China University of Geosciences, 2016.
21. “Enabling Reliable Access Control for Emerging Networking Technologies”, Wuhan University, 2016.
20. “HetSDN: Exploiting SDN for Intelligent Network Usage in Heterogeneous Wireless Networks”, IWQoS 2016.
19. “Enabling Dynamic Access Control for Controller Applications in SoftwareDefined Networks”, SACMAT 2016.
18. “Virtualizing and Utilizing Network Security Functions for Securing Software Defined Infrastructure”, NSF SDI/SDX Workshop, 2016.
17. “NFV-enabled Security Mechanism”, NFV World Congress, 2016.
16. “Defending Against Visual Cyberbullying Attacks in Emerging Mobile Social Networks”, NSF SaTC EAGER Workshop, 2016.
15. “VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls”, NFV-SDN 2015.
14. “Building Robust Firewalls for Software-Defined Networks”, CyberDNA Security Seminar, UNC Charlotte, 2015.
13. “Defensive Maneuver Cyber Platform Modeling with Stochastic Petri Nets”, CollaborateCom 2014.
12. “Towards a Reliable SDN Firewall”, 2014 Open Networking Summit (ONS) Research Track.
11. “Securing Software-Defined Networks”, Faculty Workshop on Secure Software Engineering & Computer Science Retention sponsored by the U.S Department of Education, 2013.
10. “Enabling Collaborative Data Sharing in Google+”, GLOBECOM 2012.
9. “Secure and Efficient Constructions of Hash, MAC and PRF for Mobile Devices”, GLOBECOM 2012.
8. “Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks”, ACSAC 2011.
7. “Ontology-based Policy Anomaly Management for Autonomic Computing”, CollaborateCom 2011.
6. “Multiparty Authorization Framework for Data Sharing in Online Social Networks”, DBSec 2011.
5. “Firewall Policy Analysis for Autonomic Computing”, Poster, IARE 2011.
4. “FAME: A Firewall Anomaly Management Environment”, SafeConfig 2010.

3. "Efficient Provable Data Possession for Hybrid Clouds", Poster, CCS 2010.

2. "Assurance Management Framework for Access Control", Poster, IARE 2010.

1. "Enabling Verification and Conformance Testing for Access Control Model", SACMAT 2008.

Abstracts and Other Conference Presentations *(presenter name underlined; * graduate student; +undergraduate student)*

7. Zili Meng*, Jun Bi, Chen Sun*, Shuhe Wang, Minhu Wang and Hongxin Hu, "PAM: When Overloaded, Push Your Neighbor Aside!", In *Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos*, Budapest, Hungary, August 20-25, 2018. [First Place in SIGCOMM 2018 SRC]

6. Zili Meng*, Jun Bi, Chen Sun*, Anmin Xu and Hongxin Hu, "PRAM: Priority-aware Flow Migration Scheme in NFV Networks", In *Proceedings of the ACM Symposium on SDN Research on Posters and Demos*, Santa Clara, CA, USA, April 3-4, 2017.

5. Chen Sun*, Jun Bi, Zhilong Zheng and Hongxin Hu, "SLA-NFV: an SLA-aware High Performance Framework for Network Function Virtualization", In *Proceedings of the ACM SIGCOMM Conference on Posters and Demos*, Florianópolis, Brazil, August 22-26, 2016.

4. Juan Wang, Bo Zhao, Huanguo Zhang, Fei Yan, Liqiang Zhang, Fajiang Yu and Hongxin Hu, "An E2E Trusted Cloud Infrastructure", In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS 2014)*, Poster, Scottsdale, AZ, USA, November 3-7, 2014.

3. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Xiaorui Gong and Shimin Chen, "Temporal Attribute-Based Encryption in Clouds", In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS 2011)*, Poster, Chicago, IL, USA, October 17-21, 2011.

2. Yan Zhu, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu and Stephen S. Yau, "Efficient Provable Data Possession for Hybrid Clouds", In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS 2010)*, Poster, Chicago, IL, USA, October 4-8, 2010.

1. Wenjuan Xu, Gail-Joon Ahn, Hongxin Hu, Xinwen Zhang and Jean-Pierre Seifert, "Building Dynamic Remote Attestation Framework", In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009)*, Poster, Chicago, IL, USA, November 9-13, 2009.

POST-DOCTORAL RESEARCH ASSOCIATES

1. Kang Chen (Computer Engineering, Clemson University, PhD 2014), Postdoctoral Research Associate. Sep 2014 - Aug 2015. First employment: **Assistant Professor**, Southern Illinois University.
2. Juan Deng (Computer Engineering, Clemson University, PhD 2012), Postdoctoral Research Associate. Sep 2014 - Jul 2016. First employment: Senior Researcher, Huawei.

GRADUATE STUDENTS

Dissertations/Theses Directed

Ph.D. degrees

1. Wenbo Ding, PhD, University at Buffalo, SUNY, January 2017-May 2023, "Safe and Secure Physical Interaction Control in IoT Platforms", working at KLA Corporation.
2. Nishant Vishwamitra, PhD, University at Buffalo, SUNY, May 2016-May 2022, "Understanding and Defending Against Cyberharassment in the Era of Machine Learning", working as a tenure-track **Assistant Professor** in the Department of Information Systems and Cyber Security at UT San Antonio.
3. Hongda Li, PhD, Clemson University, May 2015-August 2020, "ProSec: Enabling Programmable Security in Software-Defined Infrastructure", working at Palo Alto Networks.
4. Zili Meng, PhD, Tsinghua University, May 2019-May 2023, co-advised with Mingwei Xu, "Real-time Multimedia Transmission Delay Optimization", working as a tenure-track **Assistant Professor** in the Department of Electronic and Computer Engineering (ECE) at Hong Kong University of Science and Technology (HKUST).
5. Chen Sun, PhD, Tsinghua University, May 2015-May 2019, co-advised with Dr. Jun Bi, "Research on Key Technologies for High Performance Network Function Virtualization Systems", working at Alibaba Inc.
6. Menghao Zhang, PhD, Tsinghua University, May 2018-July 2021, co-advised with Dr. Jianping Wu and Dr. Mingwei Xu, working as Post-Doctoral Researcher at Tsinghua University & Kuaishou Technology.
7. Wonkyu Han, PhD, Arizona State University, May 2013-August 2016, co-advised with Dr. Gail-Joon Ahn, "Policy-driven Network Defense for Software Defined Networks".
8. Shuyong Zhu, PhD, Tsinghua University, May 2015- August 2016, co-advised with Dr. Jun Bi, "Research on Stateful Forwarding in Data Plane for Software-Defined Networking".

Dissertations/Theses in Progress

1. Feng Wei, PhD, May 2018-present, degree expected May 2024
2. Qiqing Huang, PhD, May 2020-present, degree expected May 2025
3. Keyan Guo, PhD, January 2022-present, degree expected May 2027
4. Jonathan Anderson (Clemson University, co-advised), PhD, May 2020-present, degree expected August 2024

Special Achievements of Graduate Students

- Keyan Guo, Recipient of Best Teaching Assistant Award, UB CSE 2022
- Hongda Li & Qiqing Huang, Recipient of ASIACCS'22 Best Paper Award, 2022
- Nishant Vishwamitra, Feng Wei, and Qiqing Huang in the team Cacti, placed 5th in Baidu AutoDriving CTF 2021
- Hongda Li, Recipient of SIGCSE'18 Best Paper Award, 2018

- Hongda Li, Recipient of Outstanding Ph.D. Student Award in Computer Science in the School of Computing at Clemson University, 2019
- Hongda Li, Recipient of Talford Annual Fellowship Award, 2018
- Nishant Vishwamitra, Recipient of Talford Annual Fellowship Award, 2018
- Zili Meng, Recipient of Microsoft Research Asia PhD Fellowship, 2020
- Zili Meng, Recipient of ICC'20 Best Paper Award, 2020
- Zili Meng, Recipient of Gold Medal of SIGCOMM 2018 SRC, 2018
- Chen Sun, Recipient of Google PhD Fellowship, 2018
- Chen Sun, Recipient of CNP'15 Best Paper Nominee, 2015

Dissertation/Thesis Committee Member

1. Yan Ju, University at Buffalo, SUNY, PhD degree expected May 2024
2. Xi Tan, University at Buffalo, SUNY, PhD degree expected May 2025
3. Md. Armanuzzaman Tomal, University at Buffalo, SUNY, PhD degree expected May 2025
4. Jerome Dinal Herath, SUNY Binghamton, PhD Dissertation, April 2022
5. Adil Alsuhaim, School of Computing, Clemson University, PhD degree expected August 2022
6. Jason Anderson, School of Computing, Clemson University, PhD degree expected August 2022
7. Oluwakemi Hambolu, Holcombe Department of Electrical and Computer Engineering, Clemson University, PhD, September 2017
8. William Clay Moody, School of Computing, Clemson University, PhD, May 2016
9. Fan Yang, Holcombe Department of Electrical and Computer Engineering, Clemson University, PhD, May 2015
10. Emmanuel John, School of Computing, Clemson University, MS, May 2016
11. Udit Agarwal, School of Computing, Clemson University, MS, August 2016

UNDERGRADUATE STUDENTS

1. Martha Newton (REU Student), April 2018 – May 2020
2. Tyreek Wilson (REU Student), April 2018 – May 2020
3. Maxwell Harley (REU Student), Aug 2017 - Feb 2018
4. Nick Castro (REU Student), Sep 2017 - Feb 2018
5. Wesley Knight (REU Student), Sep 2017 - Feb 2018
6. Kevin Wang (REU Student), May 2016 - May 2017
    - Co-authored a SACMAT'17 paper
7. Alexander Sferrella (REU Student), May 2016 - Apr 2017
8. Jan Jorgensen (Arizona State University), May 2010 - May 2012

- Co-authored an ACSAC'11 paper and a GLOBECOM'12 paper
- Co-authored an IEEE TKDE paper featured by the IEEE Special Technical Community on Social Networking

HIGH SCHOOL STUDENTS

1. Wentai Zhao (Northville High School, Northville, MI), June 2022 – October 2022
    - Co-authored an ICMLA'22 paper
    - Studying in Computer Science at University of Michigan
2. Wyatt Dorris (D. W. Daniel High School, Central, SC), May 2019 – May 2020
    - Co-authored an ICMLA'20 paper and an IWSPA'20 paper
    - Studying in Computer Science at Clemson University
3. Jonathan Tong (D. W. Daniel High School, Central, SC), May 2016 - Apr 2017
    - Co-authored an IWSPA'17 paper and an ICMLA'17 paper
    - Studying in Computer Science at Cornell University
4. Charlie Cao (Wootton High School, Rockville, MD), May 2017 - Jul 2017
    - Studying in Computer Science at the University of Maryland, College Park
5. Kevin Feng (D. W. Daniel High School, Central, SC), Jun 2017 - Jul 2017
    - Studying in Computer Science at Duke University

PROFESSIONAL ACTIVITIES

Leadership

Associate Editor

- IEEE Transactions on Dependable and Secure Computing (TDSC), 2020-present
- Computers & Security (COSE), 2020-Present
- Cybersecurity & Privacy, *Frontiers in Big Data*, 2018-Present

Guest Editor

- Special Issue of Network Traffic Analytics in the Era of AI and SDN, *Computer Networks*, 2021
- Special Issue of Advances in Steganography and Multimedia Security for Big Data, *International Journal of Distributed Sensor Networks (IJDSN)*, 2019
- Special Issue of Security in Emerging Networking Technologies, *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2017/2018
- Special Issue of Advances in Network Function Virtualization, *China Communications*, 2018
- Special Issue of Adaptive Mobile Crowd Sensing Security for BYOD Convergence in Mobile Creative Research, *Mobile Information System*, 2016
- Special Issue of Security & Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT), *International Journal of Distributed Sensor Networks*, 2015

- Special Issue of TrustCol2014, *EAI Endorsed Transactions on Collaborative Computing*, 2015

Conference/Workshop (Co-)Founder

- ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Security), 2016
- IEEE International Workshop Big Data Security and Services (BigDataService), 2018

Conference Steering Committee

- EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (SmartSP), 2023-present

Program (Co-)Chair

- ACM International Workshop on Security and Privacy Analytics (IWSPA), 2024
- International Conference on Computer Communications and Networks (ICCCN), SDN/NFV Track, 2021
- ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Security), 2016, 2017, 2018, 2019
- IEEE International Workshop Big Data Security and Services (BigDataService), 2017, 2018, 2019
- IEEE International Workshop on Trusted Collaboration (TrustCol), 2014, 2015, 2016

Poster Chair

- ACM Conference on Data and Application Security and Privacy (CODASPY), 2018 – 2022

Proceedings Chair

- ACM Conference on Data and Application Security and Privacy (CODASPY), 2017
- ACM Symposium on Access Control Models and Technologies (SACMAT), 2014, 2016, 2017, 2018, 2019, 2021, 2022, 2023

Workshop Chair

- Annual Computer Security Applications Conference (ACSAC), 2022 – 2023

Publicity Chair

- ACM Symposium on Access Control Models and Technologies (SACMAT), 2015

Session Chair

- ACM Conference on Data and Application Security and Privacy (CODASPY), 2023
- Automotive and Autonomous Vehicle Security (AutoSec) Workshop, 2021
- ACM Conference on Data and Application Security and Privacy (CODASPY), 2018
- ACM Symposium on Access Control Models and Technologies (SACMAT), 2017

- ACM Conference on Computer and Communications Security (CCS), 2014
- IEEE International Workshop on Trusted Collaboration (TrustCol), 2011

Web Chair

- ACM Conference on Computer and Communications Security (CCS), 2014

Other Service

Technical Program Committee

- ACM Conference on Computer and Communications Security (CCS), 2023
- The Web Conference (WWW), 2019, 2021, 2022
- International Conference on Machine Learning (ICML), 2023
- The International Conference on Learning Representations (ICLR), 2022, 2023
- The AAAI Conference on Artificial Intelligence (AAAI), 2021
- Annual Computer Security Applications Conference (ACSAC), 2018, 2019, 2020, 2021, 2021, 2022, 2023
- ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 2018, 2019, 2021, 2022
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2020
- ACM Conference on Data and Application Security and Privacy (CODASPY), 2018, 2021, 2022, 2023
- ACM Symposium on Access Control Models and Technologies (SACMAT), 2013, 2014, 2015, 2018, 2019, 2020, 2021, 2022, 2023
- IEEE International Conference on Distributed Computing Systems (ICDCS), 2022, 2023
- IEEE Conference on Communications and Network Security (CNS), 2017, 2018, 2019, 2020, 2021, 2022, 2023
- IEEE/ACM International Symposium on Quality of Service (IWQoS), 2021, 2023
- IEEE International Conference on Computer Communications and Networks (ICCCN), 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022,2023
- IFIP Networking Conference (NETWORKING), 2019
- ACM SIGCOMM Workshop on Security in Softwarized Networks: Prospects and Challenges (SecSoN), 2018
- ACM SIGCOMM Workshop on Internet of Things Security and Privacy (IoT S&P), 2018
- ACM Symposium on Applied Computing (SAC), Internet of Things (IoT) track, 2018, 2019, 2020
- ACM International Workshop on Multimedia Privacy and Security (MPS), 2017, 2018
- International Conference on Privacy, Security and Trust (PST), 2017, 2018, 2019
- IEEE International Conference on Advanced and Trusted Computing (ATC), 2016, 2017, 2018
- International Conference on Information and Communications Security (ICICS), 2018
- IEEE International Conference on Cloud Networking (CloudNet), 2018, 2019, 2020
- IEEE International Conference on Smart City Innovations (SCI), 2018

- Workshop on Security and Privacy-Enhanced Big Data (SPEBD), 2018
- IEEE INFOCOM CrossCloud Workshop (CrossCloud), 2014, 2016, 2017, 2018
- ACM Workshop on Internet of Things Security and Privacy (IoT S&P), 2017
- IEEE International Conference on Parallel and Distributed Systems (ICPADS), 2016
- IEEE Global Communications Conference (GLOBECOM), 2015
- International Conference on Computing and Network Communications (CoCoNet), 2015
- Workshop on Action Languages, Process Modeling, and Policy Reasoning (ALPP), 2015
- IEEE ICNP CoolSDN Workshop (CoolSDN), 2014, 2015, 2016
- International Workshop on Access Control Policies, Models and Mechanisms (ACPM), 2014
- IEEE International Workshop on Trusted Collaboration (TrustCol), 2013
- International Symposium on Cyberspace Safety and Security (CSS), 2013
- International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC), 2013
- FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA-Summer), 2012

Conference Paper Reviewer

- ACM Conference on Computer and Communications Security (CCS), 2005-2007, 2013, 2016, 2017, 2018, 2019, 2020
- ACM CHI Conference on Human Factors in Computing Systems (CHI), 2018
- European Symposium on Research in Computer Security (ESORICS), 2018
- ACM Symposium on Access Control Models And Technologies (SACMAT), 2005- 2013
- ACM Conference on Data and Application Security and Privacy (CODASPY), 2011 - 2013
- International World Wide Web Conferences (WWW)--Security and Privacy Track, 2009-2011
- ACM Symposium on Applied Computing (SAC)--Computer Security Track. 2006-2011
- ACM Symposium on InformAtion, Computer and Communications Security (AsiaCCS), 2006-2008

Journal Paper Reviewer

- ACM Transactions on Privacy and Security
- ACM Transactions on Information and System Security
- ACM Transactions on Software Engineering and Methodology
- ACM Transactions on Internet Technology
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Knowledge and Data Engineering
- IEEE/ACM Transactions on Networking
- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Services Computing
- IEEE Transactions on Network and Service Management

- IEEE Internet Computing
- Journal of Computer Security
- Computers & Security
- Security and Communication Networks
- IBM Journal of Research and Development
- International Journal of Information Security
- International Journal of Network Management
- Journal of Systems and Software
- Journal of Data & Knowledge Engineering
- Journal of Biomedical Informatics
- Journal of Organizational Computing and Electronic Commerce
- International Journal of Computer Systems Science and Engineering
- Security and Communication Networks
- IET Information Security
- Wireless Networks
- Cluster Computing
- Sensors
- Journal of Network and Computer Applications
- Journal of Computer Science and Technology

Proposal Reviewer

- NSF Review Panel (2015, 2016, 2017, 2018, 2020, 2021, 2022, 2023)
- NIST/BIRD Foundation Proposal Review (2023)
- Dutch Research Council (NWO) Proposal Review (2022)
- Swiss National Science Foundation Proposal Review (2022)
- Army Research Office (ARO) Proposal Review (2019)
- Maryland Industrial Partnerships Program (MIPStrack) Proposal Review (2014)

Membership in Professional and Honor Societies

- Association for Computing Machinery (ACM), Member
- Institute of Electrical and Electronics Engineers (IEEE), Member

UNIVERSITY SERVICE

Department Committees

- Chair, Faculty Searching Committee for CSE, October 2022 - present
- Chair, Comprehensive Program Review Committee for CSE, 2022
- Chair, Grad Program Assessment Committee for CSE, February 2022 - present
- Co-chair, Ad-hoc Committee for Cybersecurity Minor, January 2021 – present
- Member, Student Engagement and Experiential Learning for CSE, September 2021 - present

- Member, Faculty Search Committee for CSE, January 2021 - present
- Member, Grad Admissions Committee for CSE, January 2021 - present
- Member, Grad Program Assessment Committee for CSE, January 2021 - February 2022

School Committees

- Member, Website Committee for School of Computing at Clemson University, September 2017 – December 2020
- Member, Equipment Committee for School of Computing at Clemson University, 2014 – 2015
- Member, Faculty Search Committee for School of Computing at Clemson University, 2015 – 2020
- Chair, CURI/CS Search Committee for School of Computing at Clemson University, 2018

University Committees

- Member, Cybersecurity Research Task Force at Clemson University, 2016 – 2020
- Member, Search Committee for the C. Tycho Howle Endowed Chair of Collaborative Computing at Clemson University, 2015 - 2017