Salman Ahmed

Homepage: https://salmanyam.github.io Email: sahmed@ibm.com

Education

Virginia Polytechnic Institute and State University (Virginia Tech) Blacksburg, VA
Ph.D. in Computer Science and Applications Aug. 2017 – Dec. 2021
Advisor: Prof. Daphne Yao
Thesis: Quantitative Metrics and Measurement Methodologies for System Security Assurance

Ph.D. Committee Members
1. Danfeng (Daphne) Yao (Chair), Professor, Turner Fellow, and CACI Fellow, Computer Science, Virginia Tech
2. Gang Wang, Assistant Professor (Ext. Member), Computer Science, University of Illinois at Urbana-Champaign
3. Matthew Hicks, Assistant Professor (Member), Computer Science, Virginia Tech
4. Patrick R. Schaumont (Ext. Member), Professor, Electrical & Computer Engineering, Worcester Polytechnic Institute
5. Fabian Monrose (Ext. Member), Kenan Distinguished Professor, Computer Science, UNC at Chapel Hill

East Tennessee State University Johnson City, TN
Master of Science (MS) in Computer and Information Science Aug. 2015 – May 2017
Advisor: Prof. Asadul Hoque
Thesis: An Investigation into the Performance Evaluation of Connected Vehicle Applications: From Real-World Experiment to Parallel Simulation Paradigm

Bangladesh University of Engineering and Technology Dhaka, Bangladesh
Bachelor of Science (BS) in Computer Science and Engineering Jan 2008 – Feb 2013
Thesis: Audio Steganography with Quantum Key Cryptography
Advisor: Prof. Mohammad Kaykobad

Research Interest

Confidential Computing, Kernel Security, Security Metrics & Methodologies for Security Assurance and Attack Surface Quantification, Measurable Cloud Security, Threat Intelligence Analysis, Insider Threat Detection, and Security of Connected-Vehicle Technology.

Professional Appointments

International Business Machines (IBM) IBM T. J. Watson Research Center, Yorktown Heights, NY
Research Staff Member Jan 2022 – Present
Researching and developing techniques for improving the security, integrity, confidentiality of cloud platforms through specialization and securing communication channels/pipelines.

Virginia Tech Blacksburg, VA
Graduate Research Assistant Aug 2017 – Dec 2021
Developing methodologies and metrics for large-scale security assurance and attack surface quantification

International Business Machines (IBM) IBM T. J. Watson Research Center, Yorktown Heights, NY
Research Intern June 2020 – August 2020

Developed a workload scheduling/placement algorithm for cloud platforms using quantifiable attack surface metrics to improve cloud security through specialization

Banc Intranets Johnson City, TN
Software Developer May 2017 – August 2017
Developed document and ticket management modules in the Banc Intranets' core products

East Tennessee State University Johnson City, TN
Graduate Research Assistant Aug 2015 – May 2017
Developed a smart connected vehicle application that assists drivers for freeway merging

Samsung R&D Suwon, South Korea & Dhaka, Bangladesh
Software Engineer Mar 2013 – Aug 2015
Developed the rotary UI & platform tools such as 15-test, HW-test, Pretest, & Keystring for Samsung smartwatches

Patents

1. Danfeng Yao, Salman Ahmed, and Ya Xiao. Probabilistic Evidence Based Insider Threat Detection and Reasoning. Patent Application No. PCT/US21/37240, Filed on 14 June 2021.
2. Michael Vu Le, Salman Ahmed, and Hani Talal Jamjoom. Security Risk-Aware Scheduling on Container-Based Clouds. U.S. Patent Application No. 17/340,145. File on 07 June 2021.
3. Salman Ahmed, Michael Vu Le, and Hani Talal Jamjoom. Dynamic Quarantining Mechanism (DQM) for Containers in the Cloud. U.S. Patent Application no 18/178508, Filed on 05 Mar 2023.
4. Jinghao Jia, Michael Vu Le, Salman Ahmed, and Hani Talal Jamjoom. Critical-object Guided OS Fuzzing. U.S. Patent Application no 18/121650 Filed on 15 Mar 2023.

Press Coverage and Leadership Activities

- Protection against data-oriented attacks through selective data integrity. Link.
- Are contact tracing apps tracking me? Not at all, say Virginia Tech researchers, VTx (2022). Link
- Alumnus Salman Ahmed receives outstanding thesis award, ETSU News (2018). Link
- Team leader for IEEEXtreme Programming Contest 9.0 and 10.0 (2016 & 2017)

Honors and Awards

- Nominated for the IBM PhD Fellowship Award from CS@VT (2019)
- ETSU School of Graduate Studies Outstanding Thesis Award (2018)
- Tennessee Conference of Graduate Schools Outstanding Master's Thesis (2018)
- Outstanding Computing Graduate Student Award, Department of Computing, ETSU (2017)
- Best Paper Award (3rd Place), Graduate Student Competition of the ACM-Mid Southeast Conference, TN (2016)
- Samsung R&D Icon of the Month Award, Samsung R&D Institute Bangladesh (2015)
- IEEEXtreme Programming Contest 10.0 (18th Place in the USA) (2016)
- Dean's List for outstanding result in the 4th year at BUET (2012)

Publications

Refereed Conference Proceedings

1. Enriquillo Valdez, Salman Ahmed, Zhongshu Gu, Christophe de Dinechin, Pau-Chen Cheng, and Hani Jamjoom. "Confidential Containers Still Leak and How We Fix it". In Proceedings of the 33rd USENIX Security Symposium (under review).
2. Jinghao Jia, Michael V. Le, Salman Ahmed, Dan Williams, and Hani Jamjoom. "eKCFI: Kernel CFI Made Flexible and Easy (to Deploy!) with eBPF." In Proceedings of the EuroSys 2024 (under review).
3. Salman Ahmed, Hans Liljestrand, Hani Jamjoom, Matthew Hicks, N. Asokan, and Danfeng Daphne Yao. Not All Data are Created Equal: Data and Pointer Prioritization for Scalable Protection Against Data-Oriented Attacks. In 32nd USENIX Security Symposium (USENIX Security 23), pp. 1433-1450. 2023.
4. Pau-Chen Cheng, Wojciech Ozga, Enriquillo Valdez, Salman Ahmed, Zhongshu Gu, Hani Jamjoom, Hubertus Franke, and James Bottomley. "Intel TDX Demystified: A Top-Down Approach." arXiv preprint arXiv:2303.15540 (2023).
5. Michael V. Le, Salman Ahmed, Dan Williams, and Hani Jamjoom. 2023. Securing Container-based Clouds with Syscall-aware Scheduling. In Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security (ASIA CCS '23), USA, 812–826. https://doi.org/10.1145/3579856.3582835.
6. Salman Ahmed, A M Ishtiaque Mahbub, Mohammad A. Hoque, Jackeline Rios-Torres, Andreas A. Malikopoulos and, Asad Khattak. Cooperative Freeway Merging using Connected Vehicle Technology with Cellular Networks: Challenges and Approaches (under preparation)
7. Ya Xiao, Salman Ahmed, Xinyang Ge, Bimal Viswanath, Na Meng, and Danfeng (Daphne) Yao. Comprehensive Comparisons of Embedding Approaches for API Completion Tasks. Submitted to 44th International Conference on Software Engineering (ICSE 2022).
8. Salman Ahmed, Ya Xiao, Gang Tan, Kevin Snow, Fabian Monrose, and Danfeng (Daphne) Yao. Methodologies for Quantifying (Re-)randomization Security and Timing under JIT-ROP. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS'20), October 2020, Pages 1803–1820, https://doi.org/10.1145/3372297.
9. Long Cheng, Hans Liljestrand, Salman Ahmed, Thomas Nyman, Trent Jaeger, N. Asokan, and Danfeng (Daphne) Yao. “Exploitation Techniques and Defenses for Data-Oriented Attacks.” IEEE Secure Development Conference (SecDev). McLean, VA. Sept. 2019.
10. Salman Ahmed, Mohammad A Hoque, Jackeline Rios-Torres, Asad Khattak. A Cooperative Freeway Merge Assistance System using Connected Vehicles. Proceedings of the Transportation Research Board 97th Annual Meeting, Washington DC, United States, 2018.
11. Salman Ahmed and Mohammad A. Hoque. “Partitioning of Urban Transportation Networks Utilizing Real-world Traffic Parameters for Distributed Simulation in SUMO.” In Proceedings of IEEE Vehicular Network Conference (VNC), Columbus, OH, USA, 2016.
12. Salman Ahmed, Mohammad A. Hoque, and Phil Pfeiffer. “Comparative Study of Connected Vehicle Simulator.” In Proceedings of IEEE Southeast Conference (SoutheastCon), pp. 1-7, Norfolk, VA, 2016.

Journal Articles and Magazines

1. Ya Xiao, Wenjia Song, Salman Ahmed, Xinyang Ge, Bimal Viswanath, Na Meng, and Danfeng Yao. Measurement of Embedding Choices on Cryptographic API Completion Tasks. ACM Transactions on Software Engineering and Methodology (2023).

2. Salman Ahmed, Ya Xiao, Taejoong (Tijay) Chung, Carol Fung, Moti Yung, and Danfeng (Daphne) Yao, "Privacy Guarantees of Bluetooth Low Energy Contact Tracing: A Case Study on COVIDWISE," in Computer, vol. 55, no. 2, pp. 54-62, Feb. 2022, doi: 10.1109/MC.2021.3125611.

3. Long Cheng, Salman Ahmed, Hans Liljestrand, Thomas Nyman, Haipeng Cai, Trent Jaeger, N. Asokan, and Danfeng (Daphne) Yao. “Exploitation Techniques for Data-Oriented Attacks with Existing and Potential Defense Approaches.” ACM Transactions on Privacy and Security (TOPS) 24, no. 4 (2021): 1-36.
4. Mohammad A. Hoque, Xiaoyan Hong, and Salman Ahmed. “Parallel Closed-loop Connected Vehicle Simulator for Large-scale Management of Transportation Networks: Challenges, Issues, and Solution Approaches.” In IEEE Intelligent Transportation Systems Magazine 11, no. 4 (2018): 62-77.
5. Mohammad A. Hoque, Jackeline Rios-Torres, Ramin Arvin, Asad Khattak & Salman Ahmed (2020). “The extent of reliability for vehicle-to-vehicle communication in safety critical applications: an experimental study.” In Journal of Intelligent Transportation Systems, 24:3, 264-278, DOI: 10.1080/15472450.2020.1721289
6. Salman Ahmed, Jennifer Houser, Mohammad A. Hoque, Rezaul Raju, Phil Pfeiffer. “Reducing Inter-process Communication Overhead in Parallel Sparse Matrix-Matrix Multiplication.” In International Journal of Grid and High-Performance Computing, Vol. 9, No. 3, 2017.

Refereed Conference Posters, Tutorials, and Demos

1. Jinghao Jia, Michael V. Le, Salman Ahmed, Dan Williams, and Hani Jamjoom. "Practical and Flexible Kernel CFI Enforcement using eBPF." In Proceedings of the 1st Workshop on eBPF and Kernel Extensions, pp. 84-85. 2023.
2. Salman Ahmed, Ya Xiao, Taejoong (Tijay) Chung, Carol Fung, Moti Yung, and Danfeng (Daphne) Yao. 2022. POSTER: Privacy Guarantees of BLE Contact Tracing for COVID-19 and Beyond: A Case Study on COVIDWISE. In Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security (ASIA CCS ’22), May 30-June 3, 2022, Nagasaki, Japan. ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3488932.3527279.
3. Ya Xiao, Salman Ahmed, Xinyang Ge, Bimal Viswanath, Na Meng, Danfeng (Daphne) Yao. Poster: Comprehensive Comparisons of Embedding Approaches for Cryptographic API Completion. In 44th International Conference on Software Engineering (ICSE 2022), Pittsburgh, USA.
4. Salman Ahmed, Hans Liljestrand, N. Asokan, Danfeng (Daphne) Yao. Poster: Automatic Identification and Protection of Memory-resident Sensitive Data to Defend Against Data-Oriented Attacks. In 43rd IEEE Symposium on Security and Privacy, MAY 23-26, 2022, SAN FRANCISCO, CA, USA.
5. Salman Ahmed, Long Cheng, Hans Liljestrand, N. Asokan, Danfeng (Daphne) Yao. Tutorial: Investigating Advanced Exploits for System Security Assurance. In IEEE Secure Development Conference (SecDev'21), October 18 - 20, 2021.
6. Salman Ahmed, Ya Xiao, Gang Tan, Kevin Snow, Fabian Monrose, & Danfeng (Daphne) Yao. “Poster: Methodologies for Quantifying (Re-) Randomization Security and Timing under JIT-ROP. In Network and Distributed Systems Security (NDSS) Symposium 2020, San Diego, CA, USA.
7. Salman Ahmed, Ya Xiao, Gang Tan, Kevin Snow, Fabian Monrose, & Danfeng (Daphne) Yao. “POSTER: Quantifying the Impact of Fine-grained Code Randomization on Attack Surface Reduction.” IEEE Secure Development Conference (SecDev). McLean, VA. Sept. 2019.
8. Salman Ahmed, Danfeng (Daphne) Yao, and Haipeng Cai. “POSTER: Extracting Anti-specifications from Vulnerabilities for Program Hardening.” In IEEE Secure Development Conf. (SecDev). Cambridge, MA. Sept. 2018.
9. Salman Ahmed, Mohammad A. Hoque, Jackeline Rios-Torres, and Asad Khattak. “Demo: Freeway Merge Assistance System using DSRC.” In Proceedings of the 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services, pp. 83-84, Snowbird, Utah, USA, October 2017.

10. Salman Ahmed and Mohammad A. Hoque. “Demo: Real-time Vehicle Movement Tracking on Android Devices Through Bluetooth Communication with DSRC Devices.” In Proceedings of IEEE Vehicular Network Conference (VNC), Columbus, OH, USA, 2016.

Presentation

1. Quantitative Metrics and Measurement Methodologies for System Security Assurance, Computer Science Graduate Seminar, November 19, 2021.
2. Tutorial: Investigating Advanced Exploits for System Security Assurance, IEEE Secure Development Conference (SecDev) October 18 - 20, 2021
3. Methodologies for Quantifying (Re-)randomization Security and Timing under JIT-ROP. ACM CCS’20. November 2020, Talk is available at https://youtu.be/VjI4wChFQ5M.
4. Importance of Information Leakage to Bypass ASLR. DARPA Cyber Assured Systems Engineering (CASE) program. Final report meeting. August 31, 2018.
5. Partitioning of Urban Transportation Networks Utilizing Real-World Traffic Parameters for Distributed Simulation in SUMO, IEEE Vehicular Networking Conference (VNC) December 8–10, 2016.
6. Demo: Real-time Vehicle Movement Tracking on Android Devices Through Bluetooth Communication with DSRC Devices, IEEE Vehicular Networking Conference (VNC) December 8–10, 2016.
7. Reducing inter-process communication overhead in parallel sparse matrix-matrix multiplication, ACM Mid-Southeast Chapter Conference November 11, 2016.
8. Comparative study of connected vehicle simulators, IEEE SoutheastCon 2016 March 30–April 3, 2016

Selected Academic Projects

1. Automatic Commit Generator: A commit message generator from source code differences between two versions of a software. The source code differences are described using natural language and then the natural language description is translated into commit messages using a pre-trained neural machine translation model.
2. Compiler: A compiler capable of generating intermediate code (assembly x86) from a Pascal program.
3. Blinds’ Eye: A navigation tool for blind people using an Ultrasonic sensor, MicroSD card, and Micro-controller. The interfacing language was C.
4. 4-bit CPU: A 4-bit MIPS architecture-based Computer capable of executing 28 instructions using at most 8 clock cycles. The system could execute basic instructions like add, multiply, push, pop, jump, call, halt, move, and, or, etc.

References

Available upon request.