Wajih Ul Hassan

Phone: +1 217-904-5884 Email: hassan@virginia.edu Website: http://cs.virginia.edu/~hur7wv/

Research Interests

System Security, Data Provenance, Intrusion Detection, Digital Forensics.

PROFESSIONAL APPOINTMENTS

The University of Virginia (UVA) Assistant Professor Department of Computer Science and School of Data Science	Fall 2022 – Present
Lahore University of Management Sciences (LUMS), Pakistan Visiting Assistant Professor Department of Computer Science	Fall 2021 - Spring 2022
Stellar Cyber, USA Research Scientist, Machine Learning Security Team	2021 - 2022
Corelight, USA Research Intern	2020 - 2021
Symantec Labs, USA Research Intern	Summer 2019
NEC Labs, USA Research Intern, System Security Division	2018 - 2019
Intel Labs, USA Research Intern, Programming Systems Group	Summer 2016
Education	
Ph.D., Computer Science University of Illinois at Urbana-Champaign (UIUC) Advisor: Dr. Adam Bates Thesis: Investigating System Intrusions with Data Provenance Analytics	2015 - 2021
Bachelor of Science, Computer Science Lahore University of Management Sciences (LUMS)	2011 - 2015
Awards & Honors	
Weaver Faculty Fellowship, UVA.Mavis Future Faculty Fellowship, UIUC.	2022-2025 2020
 Heidelberg Laureate Forum Young Researcher. 	2019

• Symantec Graduate Fellowship, 1 of 3 students selected worldwide.	2019
RSA Security Scholarship, RSA Conference 2018.	2018
 Feng Chen Memorial Award, CS Dept. UIUC. 	2017
 Distinguished Paper Award, ACM SIGSOFT. 	2016
 Sohaib and Sara Abbasi Fellowship, CS Dept. UIUC. 	2015 - 2020
Global Undergraduate Exchange Program, U.S. Department of States.	2014
 Pakistan National ICT scholarship, CS Dept. LUMS. 	2011 - 2015

CONFERENCE PUBLICATIONS

[C1] Muhammad Adil Inam, Yinfang Chen, Akul Goyal, Jason Liu, Jaron Mink, Noor Michael, Sneha Gaur, Adam Bates, and Wajih UI Hassan. SoK: History is a Vast Early Warning System: Auditing the Provenance of System Intrusions.
IEEE Symposium on Security and Privacy (SSP) 2022

IEEE Symposium on Security and Privacy (S&P) 2023

- [C2] Muhammad Adil Inam, Akul Goyal, Jason Liu, Jaron Mink, Noor Michael, Sneha Gaur, Adam Bates, and Wajih UI Hassan. FAuST: Striking a Bargain between Forensic Auditing's Security and Throughput. Annual Computer Security Applications Conference (ACSAC) 2022
- [C3] Muhammad Adil Inam*, Wajih Ul Hassan*, Ali Ahad, Adam Bates, Rashid Tahir, Tianyin Xu, Fareed Zaffar. Forensic Analysis of Configuration-based Attacks. Network and Distributed System Security Symposium (NDSS) 2022 (* = co-primary authors)
- [C4] Carter Yagemann, Mohammad Noureddine, Wajih Ul Hassan, Simon Chung, Adam Bates, and Wenke Lee. Validating the Integrity of Audit Logs Against Execution Repartitioning Attacks. ACM Conference on Computer and Communications Security (CCS) 2021
- [C5] Wajih Ul Hassan, Ding Li, Kangkook Jee, Xiao Yu, Kexuan Zou, Dawei Wang, Zhengzhang Chen, Zhichun Li, Junghwan Rhee, Jiaping Gui, Adam Bates. This is Why We Can't Cache Nice Things: Lightning-Fast Threat Hunting using Suspicion-Based Hierarchical Storage. Annual Computer Security Applications Conference (ACSAC) 2020
- [C6] Noor Michael, Jaron Mink, Jason Liu, Sneha Gaur, Wajih Ul Hassan, Adam Bates. On the Forensic Validity of Approximated Audit Logs.
 Annual Computer Security Applications Conference (ACSAC) 2020
- [C7] Wajih Ul Hassan, Adam Bates, Daniel Marino. Tactical Provenance Analysis for Endpoint Detection and Response Systems.
 IEEE Symposium on Security and Privacy (S&P) 2020.
- [C8] Wajih UI Hassan, Mohammad Ali Noureddine, Pubali Datta, Adam Bates. OmegaLog: High-Fidelity Attack Investigation via Transparent Multi-layer Log Analysis. ISOC Network and Distributed System Security Symposium (NDSS) 2020
- [C9] Riccardo Paccagnella, Pubali Datta, Wajih Ul Hassan, Adam Bates, Christopher Fletcher, Andrew Miller, Dave Tian. Custos: Practical Tamper-Evident Auditing of Operating Systems Using Trusted Execution. ISOC Network and Distributed System Security Symposium (NDSS) 2020

- [C10] Qi Wang, Wajih Ul Hassan, Ding Li, Kangkook Jee, Xiao Yu, Kexuan Zou, Junghwan Rhee, Zhengzhang Chen, Wei Cheng, Carl A. Gunter, Haifeng Chen. You Are What You Do: Hunting Stealthy Malware via Data Provenance Analysis.
 ISOC Network and Distributed System Security Symposium (NDSS) 2020
- [C11] Wajih UI Hassan, Shengjian Guo, Ding Li, Zhengzhang Chen, Kangkook Jee, Zhichun Li, Adam Bates. NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage. ISOC Network and Distributed System Security Symposium (NDSS) 2019
- [C12] Wajih Ul Hassan*, Saad Hussain*, Adam Bates. Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide?. USENIX Security Symposium (SEC) 2018 (* = co-primary authors)
- [C13] Wajih Ul Hassan, Mark Lemay, Adam Bates, Thomas Moyer. Towards Scalable Cluster Auditing through Grammatical Inference over Provenance Graphs. ISOC Network and Distributed System Security Symposium (NDSS) 2018
- [C14] Qi Wang, Wajih Ul Hassan, Adam Bates, Carl Gunter. *Fear and Logging in the Internet of Things*. ISOC Network and Distributed System Security Symposium (NDSS) 2018
- [C15] Calin Iorgulescu, Florin Dinu, Aunn Raza, Wajih Ul Hassan, Willy Zwaenepoel. Don't cry over spilled records: Memory elasticity of data-parallel applications and its application to cluster scheduling. USENIX Annual Technical Conference (ATC) 2017
- [C16] Adam bates, Wajih Ul Hassan, Kevin Butler, Alin Dobra, Brad Reaves, Patrick Cable, Thomas Moyer and Nabil Schear. Transparent Web Service Auditing via Network Provenance Functions. World Wide Web Conference (WWW) 2017
- [C17] Owolabi Legunsen, Wajih Ul Hassan, Xinyue Xu, Grigore Roşu and Darko Marinov. How Good are the Specs? A Study of the Bug-Finding Effectiveness of Multi-Object API Specifications.
 IEEE/ACM Automated Software Engineering (ASE) 2016
 ★ ACM SIGSOFT Distinguished Paper Award

JOURNAL PUBLICATIONS

- [J1] Owolabi Legunsen, Nader Al Awar, Xinyue Xu, **Wajih Ul Hassan**, Grigore Roşu, and Darko Marinov. How Effective are Existing Java API Specifications for Finding Bugs during Runtime Verification? Automated Software Engineering Journal **(ASEJ)**, 2019. Extension of ASE 2016 paper.
- [J2] Adam Bates, Wajih Ul Hassan. Can Data Provenance Put an End to the Data Breach?. IEEE Security & Privacy Magazine. July 2019.

WORKSHOP PUBLICATIONS

[W1] Mark Lemay, **Wajih Ul Hassan**, Thomas Moyer, Nabil Schear, Warren Smith. Automated Provenance Analytics: A Regular Grammar Based Approach with Applications in Security. International Workshop on Theory and Practice of Provenance (TaPP) 2017

- [P1] Riccardo Paccagnella, Pubali Datta, **Wajih Ul Hassan**, Adam Bates, Christopher Fletcher, Andrew Miller. *Securing Operating System Audit Logs*, **NDSS** 2019
- [P2] Wajih Ul Hassan, Mark Lemay, Adam Bates, Thomas Moyer. *Deduplicating container provenance with graph grammars*. TaPP 2017
- [P3] Qi Wang, Wajih Ul Hassan, Adam Bates, Carl Gunter. Provenance tracing in the internet of things. TaPP 2017

Patents

- Transparent interpretation and integration of layered software architecture event streams Adam Bates Yuile, Wajih Ul Hassan, Mohammad Noureddine. US Patent Application Number 17247038 https://patents.google.com/patent/US20210157583A1/en
- Automated threat alert triage via data provenance. Ding Li, Kangkook Jee, Zhengzhang Chen, Zhichun Li, Wajih Ul Hassan. US Patent Application Number 16507353 https://patents.google.com/patent/US11194906B2/en

TEACHING EXPERIENCE

- Assistant Professor, University of Virginia
 - CS 4630: Defense Against the Dark Arts
- Visiting Assistant Professor, Lahore University of Management Sciences
 - CS 473: Network Security, Spring 2022
 - CS 370: Operating Systems, Fall 2021

• Guest Lecturer:

- CS 423: Operating Systems Design, Presented a 60-minute lecture on Kernel-level Data Provenance (Spring 2018)
- CS 422: Introduction to Computer Security, Presented a 60-minute lecture on how to use Linux audit system for forensic analysis (Fall 2019)

• Teaching Assistant:

Spring 2021
Fall 2016
Spring 2015
Fall 2014

PROFESSIONAL SERVICE

- Program Committee:
 - IEEE Symposium on Security & Privacy
 - USENIX Security

2020 (Shadow PC), 2023 2021, 2022

 Workshop on Privacy in the Electronic Society 	2018, 2020
• Journal Reviewer:	
 IEEE Transactions on Dependable and Secure Computing 	2019, 2021
 IEEE Transactions on Information Forensics & Security 	2021
• External Reviewer:	
• USENIX Security	2018
 USENIX Annual Technical Conference 	2018
 ISOC Network and Distributed System Security Symposium 	2018
 ACM Conference on Computer and Communications Security 	2017
$\circ~$ IEEE Conference on Software Testing, Validation and Verification	2016

IMPACT

- NoDoze threat alert triage system, which was proposed in NDSS 2019 paper, has been deployed at NEC Labs America.
- Location privacy techniques proposed in Usenix Security 2018 paper have been integrated into Strava, Garmin Connect, and MapMyTracks fitness tracking apps.

Media Coverage

- Jodi Heckel. "Fitness trackers not the safest route." The News-Gazette. 28 August 2018. http://www. news-gazette.com/blogs/starting-line/2018-08/fitness-trackers-not-the-safest-route.html
- Heather Schlitz. "Researchers, police caution sharing exercise routes online." The Daily Illili. 27 August 2018. https://dailyillini.com/news/2018/08/27/researchers-police-caution-sharing-exercise-routes-online/
- Joseph Astrouski. "U of I researchers find, fix fitness app security flaws." WAND-TV. 20 August 2018. http://www.wandtv.com/story/38923296/u-of-i-researchers-find-fix-fitness-app-security-flaws

INVITED TALKS

- Detecting and Investigating System Intrusions with Provenance Analytics, Stellar Cyber Inc., 2021.
- Detecting and Investigating System Intrusions with Provenance Analytics, Lahore University of Management Sciences, 2021.
- Tactical Provenance Analysis for Endpoint Detection and Response Systems, IEEE Symposium on Security and Privacy, May 18-20, 2020.
- OmegaLog: High-Fidelity Attack Investigation via Transparent Multi-layer Log Analysis, Network and Distributed System Security Symposium, San Diego, CA, February 23-26, 2020.
- NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage, Network and Distributed System Security Symposium, San Diego, CA, February 24-27, 2019.
- NoDoze: Combatting Threat Alert Fatigue with Automated Provenance Triage , NEC Labs, Princeton, NJ, USA, August 22, 2018.

- Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide?, USENIX Security Symposium, Baltimore, MD, USA, August 15-17, 2018.
- Towards Scalable Cluster Auditing through Grammatical Inference over Provenance Graphs, Network and Distributed System Security Symposium, San Diego, CA, February 18-21, 2018.

References

Made available upon request.