Wajih Ul Hassan

Thomas M. Siebel Center for Computer Science
201 North Goodwin Avenue
Urbana, IL 61801-2302

Phone: +1 2179045884
Email: whassan3@illinois.edu
Website: https://whassan3.web.engr.illinois.edu

Research Interests

System Security, Intrusion Detection, Forensic Analysis, Data Provenance.

Education

University of Illinois at Urbana-Champaign (UIUC)
Ph.D., Computer Science 2015 – Present
Advisor: Dr. Adam Bates (Expected July 2021)

Lahore University of Management Sciences (LUMS)
B.S., Computer Science 2011 – 2015

Awards & Honors

- **Mavis Future Faculty Fellowship, UIUC** 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, UIUC 2017
- **ACM SIGSOFT Distinguished Paper Award** 2016
- **Sohaib and Sara Abbasi Fellowship, UIUC** 2015 – 2020
- Global Undergraduate Exchange Program, U.S. Department of State 2014
- Pakistan National ICT Scholarship 2011 – 2015
- National Outreach Programme Scholarship, LUMS 2011 – 2015

Conference Publications

[C13] 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 [pdf]

[C12] 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 [pdf]

[C11] 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 [pdf]

[C10] Wajih Ul 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 [pdf]

[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 [pdf]

[C8] 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 [pdf]

[C7] Wajih Ul 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 [pdf]

[C6] 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 [pdf] (* = co-primary authors)

[C5] Wajih Ul Hassan, Mark Lemay, Nuraini Aguse, Adam Bates, Thomas Moyer. *Towards Scalable Cluster Auditing through Grammatical Inference over Provenance Graphs*.
ISOC Network and Distributed System Security Symposium (NDSS) 2018 [pdf]

[C4] 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 [pdf]

[C3] 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 [pdf]

[C2] 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 [pdf]

[C1] 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 [pdf]
✯ **ACM SIGSOFT Distinguished Paper Award**

Journal Publications

[J2] 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 [C1]. [html]

[J1] Adam Bates, Wajih Ul Hassan. *Can Data Provenance Put an End to the Data Breach?*
IEEE Security & Privacy Magazine. July 2019 [pdf]

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 [pdf]

Posters

[P3] Riccardo Paccagnella, Pubali Datta, Wajih Ul Hassan, Adam Bates, Christopher Fletcher, Andrew Miller. *Securing Operating System Audit Logs*.
ISOC Network and Distributed System Security Symposium (NDSS) 2019

[P2] Wajih Ul Hassan, Mark Lemay, Adam Bates, Thomas Moyer. *Deduplicating Container Provenance with Graph Grammars*.
International Workshop on Theory and Practice of Provenance (TaPP) 2017

[P1] Qi Wang, Wajih Ul Hassan, Adam Bates, Carl Gunter. *Provenance Tracing in the Internet of Things*.
International Workshop on Theory and Practice of Provenance (TaPP) 2017

Submitted Conference Papers

[I1] Wajih Ul Hassan Muhammad Adil Inam, Ali Ahad, Adam Bates, Rashid Tahir, Tianyin Xu, Fareed zaffar. *Dossier: Fine-Grained Forensic Analysis of Configuration-based Cyber Attacks*.

Patents

- Ding Li, Kangkook Jee, Zhengzhang Chen, Zhichun Li, Wajih Ul Hassan. *Automated threat alert triage via data provenance.*
U.S. Patent Application 16/507,353. 2020 (pending)

- Adam Bates, Wajih Ul Hassan, Mohammad Noureddine. *Transparent Interpretation and Integration of Layered Software Architecture Event Streams*
U.S. Provisional Patent Application (Filed on November 25, 2019)

Impact

- Alert triage and audit log reduction techniques proposed in the RapSheet system [C11] were integrated into the Symantec enterprise security product.
- NoDoze system [C7] has been deployed at NEC Labs America to facilitate threat hunting.
- My proposed techniques [C6] to enhance location privacy have been integrated into the production systems of Strava, Garmin Connect, and MapMyTracks fitness tracking applications.
- My study [C1] on bug-finding effectiveness of formal specification found 195 bugs in 218 open source projects. Developers of those projects have already confirmed 74 bugs.

Employment

Corelight, USA	Summer 2020	Research Intern	Mentors: Jamie Brim & Vern Paxson
Symantec Labs, USA	Summer 2019	Research Intern	Mentor: Daniel Marino
NEC Labs, USA	Summer 2018	Research Intern	Mentor: Ding Li
Intel Labs, USA	Summer 2016	Research Intern	Mentor: Ehsan Totoni
LUMS, Pakistan	2014 – 2015	Research Asst.	Advisor: Fareed Zaffar
EPFL, Switzerland	Summer 2014	Research Intern	Mentors: Florin Dinu & Willy Zwaenepoel

Undergrad Student Research Advising

Adil Inam (LUMS)	Co-supervised senior year thesis. Co-authored [I2]. Post-grad: PhD at UIUC	2019 – 2020
Ali Ahad (LUMS)	Co-supervised senior year thesis. Co-authored [I2]. Post-grad: PhD at Uni. of Virginia	2019 – 2020
Noor Michael	Co-authored [C12]. Post-grad: SWE at Citadel	2019 – 2020
Kexuan Zou	Co-authored [C8] and [C13]. Post-grad: SWE at Cargill	2019 – 2020
Dawei Wang	Co-authored [C13]. Post-grad: MS at UIUC	2019 – 2020
Rahij Imran Gillani (LUMS)	Co-supervised senior year thesis, Post-grad: Uni. of Waterloo	2018 – 2019
Zeeshan Sadiq Khan (LUMS)	Co-supervised senior year thesis	2018 – 2019
Syeda Bizzah Batool (LUMS)	Co-supervised senior year thesis	2018 – 2019
Muhammad Imran	Supervised semester-long research project through the PURE[1] program.	2018 – 2019
Meghana Muthekepalli	Supervised semester-long research project through the PURE program	2018 – 2019
Nuraini Aguse	Co-authored [C5]. Post-grad: MS at UIUC	2017 – 2018
Jack DeDobbelaere	Supervised semester-long research project through the PURE program. Post-grad: SWE at C3.ai	2017 – 2018
Jerry Chen	Supervised semester-long research project through the PURE program. Post-grad: SWE at Intel	2017 – 2018

Teaching

- **Guest Lecturer:**
  - CS423: Operating Systems Design — Spring 2018
    Presented a 60-minute lecture on kernel-level data provenance.
  - CS422: Introduction to Computer Security — Fall 2019
    Presented a 75-minute lecture on how to use Linux audit subsystem for forensic analysis.

[1] Promoting Undergraduate Research in Engineering at UIUC

- **Teaching Assistant:**
  - Introduction to Programming for Engineers and Scientists (UIUC) Fall 2016
  - Network-Centric Computing (LUMS) Spring 2015
  - Operating Systems (LUMS) Fall 2014

Service to Professional Community

- **Program Committee:**
  - USENIX Security 2021
  - Workshop on Privacy in the Electronic Society 2020
  - IEEE Symposium on Security & Privacy (Shadow PC) 2020
  - Workshop on Privacy in the Electronic Society 2018

- **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
  - IEEE Conference on Software Testing, Validation and Verification 2016

- **Journal Reviewer:**
  - Journal of Computer Security 2020
  - IEEE Transactions on Dependable and Secure Computing 2019

Open Source Software Contributions

Zeek Agent Zeek Agent is an endpoint monitoring tool that continuously collects enterprise-wide host audit logs and then seamlessly correlates those audit logs with Zeek network logs. I contribute to the development of Zeek Agent project. Zeek Agent is available at https://github.com/zeek/zeek-agent

HPAT High Performance Analytics Toolkit (HPAT) is a Julia-based framework for big data analytics on clusters that is both easy to use and extremely fast; it is orders of magnitude faster than alternatives like Apache Spark. I integrated structured data processing (Data Frames) into HPAT. HPAT is available at https://github.com/IntelLabs/HPAT.jl

Travel Grants

- Heidelberg Laureate Forum, Germany 2019
- IEEE Symposium on Security and Privacy, USA 2017
- ISOC Network and Distributed System Security Symposium, USA 2017

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

- *Zeek Agent: Correlating Host and Network Logs for Better Forensics*,
  ZeekWeek Conference (virtual), October 13-15, 2020.
- *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.