Stefan Nagy

Assistant Professor
School of Computing
University of Utah

785-410-7260
snagy@cs.utah.edu
https://www.cs.utah.edu/ snagy/

Research Interests

Broadly, I am interested in security, software, and systems. Several areas that I work in include software testing, binary analysis, vulnerability triage, and bug repair. I am especially interested in making efficient and effective quality assurance possible for opaque and otherwise challenging software and systems.

Education

Ph.D., Computer Science	Virginia Tech	2016–2022
B.S., Computer Science	University of Illinois at Urbana-Champaign	2012–2016

Research Summary

Publications in top-tier venues:	**CCS'21**, **USENIX'21**, **Oakland'19**, **ICSE'18**
Other publications:	ACSAC'22, ISTAS'19, ICDF2C'15, SADFE'15

Publications

1. **One Fuzz Doesn't Fit All: Optimizing Directed Fuzzing via Target-tailored Program State Restriction.**
   Prashast Srivastava, Stefan Nagy, Matthew Hicks, Antonio Bianchi, Mathias Payer.
   Annual Computer Security Applications Conference (**ACSAC'22**). December 2022.

2. **Practical Feedback and Instrumentation Enhancements for Performant Security Testing of Closed-source Executables.** Ph.D. Thesis. Virginia Tech. May 2022.

3. **Same Coverage, Less Bloat: Accelerating Binary-only Fuzzing with Coverage-preserving Coverage-guided Tracing.**
   Stefan Nagy, Anh Nguyen-Tuong, Jason D. Hiser, Jack W. Davidson, Matthew Hicks.
   ACM Conference on Computer and Communications Security (**CCS'21**). November 2021.

4. **Breaking Through Binaries: Compiler-quality Instrumentation for Better Binary-only Fuzzing.**
   Stefan Nagy, Anh Nguyen-Tuong, Jason D. Hiser, Jack W. Davidson, Matthew Hicks.
   USENIX Security Symposium (**USENIX'21**). August 2021.

5. **A Case Study on a Sustainable Framework for Ethically Aware Predictive Modeling.**
   Thomas Lux, Stefan Nagy, Mohammed Almanaa, Sirui Yao, Reid Bixler.
   IEEE International Symposium on Technology and Society (**ISTAS'19**). November 2019.

6. **Full-speed Fuzzing: Reducing Fuzzing Overhead through Coverage-guided Tracing.**
   Stefan Nagy, Matthew Hicks.
   IEEE Symposium on Security and Privacy (**Oakland'19**). May 2019.

7. **Secure Coding Practices in Java: Challenges and Vulnerabilities.**
   Na Meng, Stefan Nagy, Danfeng Yao, Wenjie Zhuang, Gustavo A. Argoty.
   International Conference on Software Engineering (**ICSE'18**). May 2018.

8. **Digital Forensics Education: A Multidisciplinary Curriculum Model.**
   Imani Palmer, Elaine Wood, Stefan Nagy, Gabriela Garcia, Masooda Bashir, Roy H. Campbell.
   International Conference on Digital Forensics and Cyber Crime (**ICDF2C'15**). October 2015.

9. **Schedule-Based Side-Channel Attack in Fixed-Priority Real-time Systems.**
   Chien-Ying Chen, Amiremad Ghassami, Stefan Nagy, Man-Ki Yoon, Sibin Mohan, Negar Kiyavash, Rakesh B Bobba, Rodolfo Pellizzoni.
   Illinois Digital Environment for Access to Learning and Scholarship. October 2015.

10. **An Empirical Study on Current Models for Reasoning about Digital Evidence.** Stefan Nagy, Imani Palmer, Sathya C. Sundaramurthy, Xinming Ou, Roy H. Campbell. International Conference on Systematic Approaches to Digital Forensic Engineering (**SADFE'15**). September 2015.

Research Impacts

1. ZAFL (**USENIX'21**) added to AFL++ (the leading production-grade fuzzer): https://github.com/AFLplusplus/AFLplusplus/blob/dev/docs/fuzzing_binary-only_targets.md#zafl

2. UnTracer (**Oakland'19**) integrated in AFL++: https://github.com/AFLplusplus/AFLplusplus/tree/stable/utils/afl_untracer

3. UnTracer (**Oakland'19**) utilized in research by Google Project Zero: https://googleprojectzero.blogspot.com/2020/04/fuzzing-imageio.html

4. Java security work (**ICSE'18**) news media coverage:
   - The Linux Foundation: "Secure Coding in Java: Bad Online Advice and Confusing APIs"
   - The Register: "Java security plagued by crappy docs, complex APIs, bad advice"
   - The Morning Paper: "Secure coding practices in Java: challenges and vulnerabilities"
   - Slashdot: "Java Coders Are Getting Bad Security Advice From Stack Overflow"
   - Help Net Security: "Secure coding in Java: Bad online advice and confusing APIs"

Research Artifacts

1. Dr. Disassembler (**Trail of Bits**): A platform for transparent and mutable binary disassembly. https://github.com/lifting-bits/dds

2. HeXcite (**CCS'21**): High-Efficiency eXpanded Coverage for Improved Testing of Executables. https://github.com/FoRTE-Research/hexcite

3. ZAFL (**USENIX'21**): A compiler-quality instrumentation platform for binary fuzzing. https://git.zephyr-software.com/opensrc/zafl

4. UnTracer (**Oakland'19**): Accelerated binary fuzzing via Coverage-guided Tracing. https://github.com/FoRTE-Research/untracer-afl

5. AFL-FID (**Oakland'19**): A suite of performance benchmarking tools for software fuzzing. https://github.com/FoRTE-Research/afl-fid

6. FoRTE-FuzzBench (**Oakland'19**): A corpus of open-source fuzzing evaluation benchmarks. https://github.com/FoRTE-Research/forte-fuzzbench

Invited Talks

Toward a Best-of-Both-Worlds Binary Disassembler. Trail of Bits Blog. 2022
https://blog.trailofbits.com/2022/01/05/toward-a-best-of-both-worlds-binary-disassembler
Advancing and Accelerating Vetting of the Closed-source Software Ecosystem.
Northwestern University. 2022
BINSEC Webinar at Université Paris-Saclay. 2021
Fast Binary Fuzzing via Coverage-preserving Coverage-guided Tracing. ACM CCS. 2021
Compiler-quality Instrumentation for Better Binary Fuzzing. USENIX Security. 2021
Compiler-quality Instrumentation for Better Binary Fuzzing. MIT Lincoln Lab. 2021
Fast and Fine-grained Binary Fuzzing Coverage. HUME Center Colloquium. 2021
Fuzzing and the New Performance Frontier. Purdue University. 2021
The Open-source Fuzzing Ecosystem. Antithesis Operations LLC. 2020
Cross-platform, High-performance Fuzzing. HUME Center Colloquium. 2020
Reducing Fuzzing Overhead through Coverage-guided Tracing. IEEE S&P. 2019

Awards

Hume Center for National Security and Technology — Graduate Fellowship — 2017–2022
ACM CCS Workshop for Women in Cyber Security — Travel Grant — 2017

Professional Experience

University of Utah	Assistant Professor	July 2022–now
Virginia Tech	Graduate Research / Teaching Assistant *Advised by Matthew Hicks*	August 2016–May 2022
MIT Lincoln Lab	Graduate Summer Intern *Mentored by Tim Leek*	Summer 2021
Trail of Bits	Graduate Winter Intern *Mentored by Peter Goodman*	Winter 2020
Antithesis Operations	Graduate Summer Intern *Mentored by Harrison Brown*	Summer 2020
Kansas State University	Undergrad Research Assistant *Mentored by Xinming Ou*	Summer 2015
University of Illinois	Undergrad Research / Teaching Assistant *Mentored by Roy H. Campbell*	May 2014–December 2015

Teaching Experience

Virginia Tech	CS2104: Introduction to Problem Solving	GTA	Fa16
Virginia Tech	CS3604: Professionalism in Computing	GTA	Sp20
Virginia Tech	CS4264: Principles of Computer Security	GTA	Fa16/18/19, Sp17
Virginia Tech	CS5024: Ethics and Professionalism	GTA	Fa20
Virginia Tech	CS5560: Information Security	GTA	Sp18
UIUC	CS498-AL1: Digital Forensics I	UTA	Fa15

Mentorship

Leo C. Stone (M.S. student)	Virginia Tech
Rishi Ranjan (visiting scholar)	Virginia Tech, IIT Roorkee
Arash Ale Ebrahim (independent researcher)	EURECOM

Service

Reviewer:

International Symposium on Research in Attacks, Intrusions and Defenses	RAID'22
IEEE Symposium on Security and Privacy (Poster Session)	Oakland'22
IEEE Transactions on Dependable and Secure Computing	TDSC'20

External Reviewer:

USENIX Security Symposium	USENIX'21,'22
ACM Transactions on Software Engineering and Methodology	TOSEM'21
IEEE Symposium on Security and Privacy	Oakland'19,'21
ACM Conference on Data and Applications Security and Privacy	CODASPY'18
Annual Computer Security Applications Conference	ACSAC'17
International Conference on Dependable Systems and Networks	DSN'17
ACM Asia Conference on Computer and Communications Security	ASIACCS'17
ACM Conference on Security and Privacy in Wireless and Mobile Networks	WiSec'17
International Conference on Distributed Computing Systems	ICDCS'17
ACM Workshop on Forming an Ecosystem Around Software Transformation	FEAST'17
ACM Workshop on Applying the Scientific Method to Cyber Defense Research	SafeConfig'17
ACM Workshop on Managing Insider Security Threats	MIST'16

Web Admin:

ACM Workshop for Women in Cyber Security	CyberW'17

References

Matthew Hicks (Ph.D. advisor)
Assistant Professor
Virginia Tech
mdhicks2@vt.edu

Jack W. Davidson
Professor
University of Virginia
jwd@virginia.edu

Mathias Payer
Associate Professor
École Polytechnique Fédérale de Lausanne
mathias.payer@nebelwelt.net

Gang Wang
Assistant Professor
University of Illinois at Urbana-Champaign
gangw@illinois.edu