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

I lead research and teach students in the areas of Cyber Security, Software, and Computer Systems. Topics that I work on 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 difficult-to-vet software and systems to make computing safer and more reliable for all.

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 (6):	**CCS(x2)**, **USENIX(x2)**, **Oakland(x1)**, **ICSE(x1)**
Other publications (6):	ACSAC(x1), ISTAS(x1), ICDF2C(x1), SADFE(x1)

PUBLICATIONS

1. **Profile-guided System Optimizations for Accelerated Greybox Fuzzing.** Yunhang Zhang, Chengbin Pang, **Stefan Nagy**, Xun Chen, Jun Xu. ACM Conference on Computer and Communications Security (**CCS'23**).
2. **No Linux, No Problem: Fast and Stateful Windows Binary Fuzzing via Target-embedded Snapshotting.** Leo Stone, Rishi Ranjan, **Stefan Nagy**, Matthew Hicks. USENIX Security Symposium (**USENIX'23**).
3. **The Fun in Fuzzing: The Debugging Technique Comes into Its Own. Stefan Nagy**, Peter Alvaro. Association for Computing Machinery (ACM) Queue Magazine.
4. **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**).
   – Best poster award.
5. **Practical Feedback and Instrumentation Enhancements for Performant Security Testing of Closed-source Executables.** Ph.D. Thesis. Virginia Tech.
6. **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**).
7. **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**).
8. **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**).
9. **Full-speed Fuzzing: Reducing Fuzzing Overhead through Coverage-guided Tracing. Stefan Nagy**, Matthew Hicks. IEEE Symposium on Security and Privacy (**Oakland'19**).
10. **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**).
11. **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**).
12. **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.
13. **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**).

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. SieveFuzz (**ACSAC'22**): Optimized directed fuzzing via Target-tailored State Restriction.
   https://github.com/HexHive/SieveFuzz
2. Dr. Disassembler (**Trail of Bits**): A platform for transparent and mutable binary disassembly.
   https://github.com/lifting-bits/dds
3. HeXcite (**CCS'21**): High-Efficiency eXpanded Coverage for Improved Testing of Executables.
   https://github.com/FoRTE-Research/hexcite
4. ZAFL (**USENIX'21**): A compiler-quality instrumentation platform for binary fuzzing.
   https://git.zephyr-software.com/opensrc/zafl
5. UnTracer (**Oakland'19**): Accelerated binary fuzzing via Coverage-guided Tracing.
   https://github.com/FoRTE-Research/untracer-afl
6. AFL-FID (**Oakland'19**): A suite of performance benchmarking tools for software fuzzing.
   https://github.com/FoRTE-Research/afl-fid
7. FoRTE-FuzzBench (**Oakland'19**): A corpus of open-source fuzzing evaluation benchmarks.
   https://github.com/FoRTE-Research/forte-fuzzbench

Awards

Best Poster Award	ACSAC'22	2022
Hume Center for National Security and Technology	Graduate Fellowship	2017–2022

Invited Talks & Articles

Security & Privacy at The U. Kahlert School of Computing Summer Bridge Program.	8/2023
Extending Fuzzing to New Targets and Open Challenges. Trail of Bits.	6/2023
Advancing the Fuzzing Frontier. The Ohio State University.	3/2023
The Fun in Fuzzing: The Debugging Technique Comes into Its Own. ACM Queue.	2/2023
Toward a Best-of-Both-Worlds Binary Disassembler. Trail of Bits Blog.	1/2022
Advancing and Accelerating Vetting of the Closed-source Software Ecosystem.	
– Security Research Seminar at Northwestern University.	5/2022
– BINSEC Webinar at Université Paris-Saclay.	12/2021
Fast Binary Fuzzing via Coverage-preserving Coverage-guided Tracing. ACM CCS.	11/2021
Compiler-quality Instrumentation for Better Binary Fuzzing.	
– USENIX Security Symposium.	8/2021
– MIT Lincoln Lab.	7/2021
Fast and Fine-grained Binary Fuzzing Coverage. HUME Center Colloquium.	4/2021
Fuzzing and the New Performance Frontier. Purdue University.	2/2021
The Open-source Fuzzing Ecosystem. Antithesis Operations LLC.	7/2020
Cross-platform, High-performance Fuzzing. HUME Center Colloquium.	4/2020
Reducing Fuzzing Overhead through Coverage-guided Tracing. IEEE S&P.	5/2019

Professional Experience

University of Utah	Assistant Professor	7/2022–now
Virginia Tech	Graduate Research / Teaching Assistant	8/2016–5/2022
MIT Lincoln Lab	Graduate Summer Intern	6/2021–8/2021
Trail of Bits	Graduate Winter Intern	12/2020–1/2021
Antithesis Operations	Graduate Summer Intern	6/2020–8/2020
Kansas State University	Undergrad Research Assistant	6/2015–8/2015
University of Illinois	Undergrad Research / Teaching Assistant	5/2014–12/2015

Teaching Experience

CS4440: Introduction to Computer Security	Sp23, Fa23
– Webpage: cs.utah.edu/∼snagy/courses/cs4440	
CS5963/6963: Applied Software Security Testing	Fa22
– Webpage: cs.utah.edu/∼snagy/courses/cs5963	

Advising & Mentorship

Current Graduate Students:

– Zao Yang (Ph.D.)	University of Utah	2023–now
– Yeaseen Arafat (Ph.D.)	University of Utah	2023–now
– Christopher Andrew Lee (M.S.)	University of Utah	2023–now
– Shubham Mazumder (M.S.)	University of Utah	2023–now

Current Undergraduate Students:

– David Clark (B.S. Thesis)	University of Utah	2023–now
– Gabe Sherman (B.S. Thesis)	University of Utah	2023–now

Thesis Committee Member:

– Ruotong Yu (Ph.D.)	University of Utah
– Vikram Narayanan (Ph.D.)	University of Utah

Service

Departmental Service:

– Faculty Advisor, ACM Student Chapter	2023–now
– Faculty Advisor, Student Cybersecurity Club	2023–now
– Member, Undergraduate Curriculum Committee	2022–now
– Member, Graduate Admissions Committee	2022–now

Program Committees:

– Co-Chair, NDSS Workshop on Binary Analysis Research	BAR’23
– Member, ACM Transactions on Software Engineering and Methodology	TOSEM’22
– Member, Intl. Symposium on Research in Attacks, Intrusions and Defenses	RAID’22
– Member, IEEE Symposium on Security and Privacy (Poster Session)	Oakland’22
– Member, 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

Other Service:

– Reviewer, Davidson Fellows Scholarship	2023
– Web Admin, ACM Workshop for Women in Cyber Security	2017

References

Matthew Hicks
Associate Professor
Virginia Tech
mdhicks2@vt.edu

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

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

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