DR. STEFAN NAGY
Assistant Professor
Kahlert School of Computing, University of Utah

+1 (801) 581-8224
snagy@cs.utah.edu
cs.utah.edu/∼snagy

RESEARCH INTERESTS

I lead research and teach students in the areas of Software Engineering, Software Quality Assurance, and Computer Systems. Topics I work on include software testing, program analysis, 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.

RESEARCH SUMMARY

Publications in top-tier conferences (14):	**FSE** (x3), **ICSE** (x3), **CCS** (x2), **SEC** (x2) **ASE** (x1), **ATC** (x1), **ISSTA** (x1), **S&P** (x1)
Total awarded research funding (as PI/Co-PI):	**$5,610,000**
Individual share of awarded research funding:	**$1,616,000**
Reported software bugs & security vulnerabilities:	**227** (futures.cs.utah.edu/bugs)

APPOINTMENTS

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

EDUCATION

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

PUBLICATIONS

Names of my advised students are underlined.

1. **SnakeCharmer: Automatic Fuzzing Harness Generation for Pure and Hybrid Python Libraries.**
   Gabriel Sherman and Stefan Nagy.
   ACM International Conference on the Foundations of Software Engineering (**FSE'26**).
2. **PROGnosticator: Testing Source-to-Source Code Translators via Construct-oriented Fuzzing.**
   Yeaseen Arafat and Stefan Nagy.
   ACM International Conference on the Foundations of Software Engineering (**FSE'26**).
3. **Binvariants: Enhancing Fuzzing of Closed-source Binary Executables via Register-level Likely Invariants.**
   Zao Yang and Stefan Nagy.
   ACM International Conference on the Foundations of Software Engineering (**FSE'26**).
4. **TeTRIS: General-purpose Fuzzing for Translation Bugs in Source-to-Source Code Transpilers.**
   Yeaseen Arafat and Stefan Nagy.
   Annual Computer Security Applications Conference (**ACSAC'25**).
5. **GUIFuzz++: Unleashing Grey-box Fuzzing on Desktop Graphical User Interfacing Applications.**
   Dillon Otto, Tanner Rowlett, and Stefan Nagy.
   IEEE/ACM International Conference on Automated Software Engineering (**ASE'25**).
6. **Bin2Wrong: a Unified Fuzzing Framework for Uncovering Semantic Errors in Binary-to-C Decompilers.**
   Zao Yang and Stefan Nagy.
   USENIX Annual Technical Conference (**ATC'25**).
7. **WildSync: Automated Fuzzing Harness Synthesis via Wild API Usage Recovery.**
   Wei-Cheng Wu, Stefan Nagy, and Christophe Hauser.
   ACM International Symposium on Software Testing and Analysis (**ISSTA'25**).
8. **No Harness, No Problem: Oracle-guided Harnessing for Auto-generating C API Fuzzing**

Harnesses.
Gabriel Sherman and Stefan Nagy.
IEEE/ACM International Conference on Software Engineering (**ICSE'25**).

9. **A Little Goes a Long Way: Tuning Configuration Selection for Continuous Kernel Fuzzing.**
   Sanan Hasanov, Stefan Nagy, and Paul Gazzillo.
   IEEE/ACM International Conference on Software Engineering (**ICSE'25**).
10. **Profile-guided System Optimizations for Accelerated Greybox Fuzzing.**
    Yunhang Zhang, Chengbin Pang, Stefan Nagy, Xun Chen, and Jun Xu.
    ACM Conference on Computer and Communications Security (**CCS'23**).
11. **No Linux, No Problem: Fast and Stateful Windows Binary Fuzzing via Target-embedded Snapshotting.**
    Leo Stone, Rishi Ranjan, Stefan Nagy, and Matthew Hicks.
    USENIX Security Symposium (**USENIX'23**).
12. **The Fun in Fuzzing: The Debugging Technique Comes into Its Own.**
    Stefan Nagy and Peter Alvaro.
    Association for Computing Machinery Queue Magazine (**ACM Queue'23**).
13. **One Fuzz Doesn't Fit All: Optimizing Directed Fuzzing via Target-tailored Program State Restriction.**
    Prashast Srivastava, Stefan Nagy, Matthew Hicks, Antonio Bianchi, and Mathias Payer.
    Annual Computer Security Applications Conference (**ACSAC'22**).
    – Best poster award.
14. **Practical Feedback and Instrumentation Enhancements for Performant Security Testing of Closed-source Executables.** Ph.D. Thesis. Virginia Tech.
15. **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, and Matthew Hicks.
    ACM Conference on Computer and Communications Security (**CCS'21**).
16. **Breaking Through Binaries: Compiler-quality Instrumentation for Better Binary-only Fuzzing.**
    Stefan Nagy, Anh Nguyen-Tuong, Jason D. Hiser, Jack W. Davidson, and Matthew Hicks.
    USENIX Security Symposium (**USENIX'21**).
17. **A Case Study on a Sustainable Framework for Ethically Aware Predictive Modeling.**
    Thomas Lux, Stefan Nagy, Mohammed Almanaa, Sirui Yao, and Reid Bixler.
    IEEE International Symposium on Technology and Society (**ISTAS'19**).
18. **Full-speed Fuzzing: Reducing Fuzzing Overhead through Coverage-guided Tracing.**
    Stefan Nagy and Matthew Hicks.
    IEEE Symposium on Security and Privacy (**S&P'19**).
19. **Secure Coding Practices in Java: Challenges and Vulnerabilities.**
    Na Meng, Stefan Nagy, Danfeng Yao, Wenjie Zhuang, and Gustavo A. Argoty.
    IEEE/ACM International Conference on Software Engineering (**ICSE'18**).
20. **Digital Forensics Education: A Multidisciplinary Curriculum Model.**
    Imani Palmer, Elaine Wood, Stefan Nagy, Gabriela Garcia, Masooda Bashir, and Roy H. Campbell.
    International Conference on Digital Forensics and Cyber Crime (**ICDF2C'15**).
21. **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, and Rodolfo Pellizzoni.
    Illinois Digital Environment for Access to Learning and Scholarship.
22. **An Empirical Study on Current Models for Reasoning about Digital Evidence.**
    Stefan Nagy, Imani Palmer, Sathya C. Sundaramurthy, Xinming Ou, and Roy H. Campbell.
    International Conference on Systematic Approaches to Digital Forensic Engineering (**SADFE'15**).

Research Funding

1. **Enhancing VMF: Source-agnostic Techniques for Code Coverage, Crash Triage, and Harnessing.**
   – Sponsor: Defense Advanced Research Projects Agency.
   – Duration: 01/01/2025–12/31/2027.
   – Personnel: Jack Davidson (PI), Stefan Nagy (Co-PI), Matthew Hicks (Co-PI).
   – My share: $1,102,500. Utah share: $1,102,500. Total: $4,410,000.
2. **CICI: TCR: Practical, Systematic Fuzz Testing for Securing Scientific Software.**
   – Sponsor: National Science Foundation.
   – Duration: 10/01/2024–09/30/2027.
   – Personnel: Stefan Nagy (PI), Jack Davidson (Co-PI).
   – My share: $513,500. Utah share: $513,500. Total: $1,200,000.

Research Impacts

1. Our transpiler fuzzing framework TeTRIS (**ACSAC'25**) reviewed by the Go2Hx dev community: https://community.haxe.org/t/go2hx-work-in-progress/2821/24#p-14532-research-paper-review-1
2. Our GUI fuzzing framework GUIFuzz++ (**ASE'25**) integrated in AFL++: https://github.com/AFLplusplus/AFLplusplus/pull/2566
3. Our decompiler fuzzing research (**ATC'25**) featured in a blog by Binary Ninja creator Vector35: https://binary.ninja/2024/06/19/restructuring-the-decompiler.html#footnotes–credits
4. 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
5. UnTracer (**Oakland'19**) integrated in AFL++: https://github.com/AFLplusplus/AFLplusplus/tree/stable/utils/afl_untracer
6. UnTracer (**Oakland'19**) utilized in research by Google Project Zero: https://googleprojectzero.blogspot.com/2020/04/fuzzing-imageio.html
7. 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"

Awards

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

Invited Talks & Articles

Extending Fuzzing's Reach via Oracle-guided Harness Generation.
– TrustedCI NSF Cybersecurity Center of Excellence. 9/2025

Cybersecurity and Video Games.
– Utah Division of Games at the University of Utah. 2/2024

Extending Fuzzing to New Targets and Open Challenges.
– Boise State University. 10/2023
– Trail of Bits. 6/2023
– The Ohio State University. 3/2023

Security & Privacy at The U: Faculty, Research, and Student Clubs.
– Mountain West Undergrad Computing Research Showcase in Computing. 11/2023
– Kahlert School of Computing Summer Bridge Program. 8/2023

The Fun in Fuzzing: The Debugging Technique Comes into Its Own.
– ACM Queue Magazine. 2/2023

Advancing and Accelerating Vetting of the Closed-source Software Ecosystem.
– Security Research Seminar at Northwestern University. 5/2022

Teaching

CS4440: Introduction to Computer Security Sp23, Fa23/24/25
– Webpage: cs.utah.edu/∼snagy/courses/cs4440

CS5963/6963: Applied Software Security Testing Fa22, Sp24/25
– Webpage: cs.utah.edu/∼snagy/courses/cs5963

Advising & Mentorship

Current Graduate Students Advised:

– Tanner Rowlett (Ph.D.)	University of Utah	2026–now
– Carson He (M.S. Thesis)	University of Utah	2025–now
– Gabriel Sherman (Ph.D.)	University of Utah	2024–now
– Yeaseen Arafat (Ph.D.)	University of Utah	2023–now
– Zao Yang (Ph.D.)	University of Utah	2023–now

Current Undergraduate Students Advised:

– Corinna Healey (B.S. Thesis)	University of Utah	2025–now
– Clark Parry (B.S. Thesis)	University of Utah	2025–now
– Ethan Collier (Undergrad RA)	University of Utah	2025–now

Past Students Advised:

– Tanner Rowlett (B.S. Thesis)	University of Utah	2025
– Dallin Hoyt (Undergrad RA)	University of Utah	2025
– Hudson Schmidt (Undergrad RA)	California Polytechnic	2025
– Austin Garcia (Undergrad RA)	University of Utah	2025
– Raj Reddy (Undergrad RA)	University of Utah	2024–2025
– Dillon Otto (B.S. Thesis)	University of Utah	2024–2025
– Joshua Dean (B.S. Thesis)	University of Utah	2024–2025
– David Clark (B.S. Thesis)	University of Utah	
– Gabriel Sherman (UROP Program, B.S. Thesis)	University of Utah	
– Andrew Lee (Undergrad / Grad RA, UROP Program)	University of Utah	
– Yash Ghanathe (Undergrad RA, UROP Program)	University of Utah	
– Alberto Del Rosario (Undergrad Independent Study)	University of Utah	
– Zeshan Ahmed Nobin (Undergrad External Student)	SUST Bangladesh	

Thesis Committee Member:

– Yunhang Zhang (Ph.D.)	University of Utah
– Yu Pan (Ph.D.)	University of Utah
– Wei-Cheng Wu (Ph.D.)	Dartmouth University
– Mahima Vijay Pawar (M.S.)	University of Utah
– Ruotong Yu (Ph.D.)	University of Utah
– Vikram Narayanan (Ph.D.)	University of Utah

SERVICE

Departmental Service:

– Co-Organizer, Graduate Recruiting Weekend	2026
– Co-Organizer, Graduate Program Open House	2025
– Member, Faculty Research Committee	2025–now
– Faculty Advisor, Utah Student Cybersecurity Club	2023–now
– Member, Undergraduate Curriculum Committee	2022–now
– Co-Faculty Advisor, Utah ACM Student Chapter	2023–2024
– Co-Organizer, Faculty Writing Group	2024
– Member, Graduate Admissions Committee	2022–2023

Conference and Journal Service:

– PC Member, NDSS Workshop on Binary Analysis Research	BAR'25,'26
– PC Member, ACM Conference on Computer and Communications Security	CCS'24,'25,'26
– PC Member, Network and Distributed System Security Symposium	NDSS'26
– PC Member, International Fuzzing Workshop	FUZZING'24,'26
– Poster Session Host, Annual Computer Security Applications Conference	ACSAC'25
– PC Member, EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles	SmartSP'25
– Session Chair, USENIX Annual Technical Conference	ATC'25
– Poster Jury, International Conference on Software Engineering	ICSE'25
– Reviewer, ACM Transactions on Software Engineering and Methodology	TOSEM'22,'25
– Reviewer, IEEE Transactions on Dependable and Secure Computing	TDSC'20,'24
– Reviewer, IEEE Transactions on Software Engineering	TSE'24,'25
– Co-Chair, NDSS Workshop on Binary Analysis Research	BAR'23,'24
– PC Member, Intl. Symposium on Research in Attacks, Intrusions and Defenses	RAID'22
– Poster Jury, IEEE Symposium on Security and Privacy	Oakland'22

Other Service:

– Panelist, National Science Foundation (OAC)	2025
– Reviewer, Davidson Fellows Scholarship	2023–now
– Web Admin, ACM Workshop for Women in Cyber Security	2017