shr@cs.utexas.edu
Assistant Professor
University of Texas at Austin
https://shravanrn.com

Shravan Ravi Narayan

Education

2022–2023 **PostDoc**, *University of California, San Diego*
2016–2022 **Ph.D.**, *University of California, San Diego*
2009–2013 **B.Eng**, *McGill University*, Montreal

Publications

1. S. Narayan, T. Garfinkel, M. Taram, J. Rudek, D. Moghimi, E. Johnson, C. Fallin, A. Vahldiek-Oberwagner, M. LeMay, R. Sahita, D. Tullsen, D. Stefan. Going Beyond the Limits of SFI: Flexible and Secure Hardware-Assisted In-Process Isolation with HFI. Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2023.
2. E. Johnson, E. Laufer, Z. Zhao, S. Narayan, S. Savage, D. Stefan, F. Brown. WaVe: a verifiably secure WebAssembly sandboxing runtime. IEEE Symposium on Security and Privacy (S&P), 2023.
3. H. Yavarzadeh, M. Taram, S. Narayan, D. Stefan, D. Tullsen. Half&Half: Demystifying Intel's Directional Branch Predictors for Fast, Secure Partitioned Execution. IEEE Symposium on Security and Privacy (S&P), 2023.
4. S. Narayan, T. Garfinkel, E. Johnson, D. Thien, J. Rudek, M. LeMay, A. Vahldiek-Oberwagner, D. Tullsen, D. Stefan. Segue & ColorGuard: Optimizing SFI Performance and Scalability on Modern x86. Programming Languages and Analysis for Security (PLAS), 2022.
5. M. Kolosick, S. Narayan, C. Watt, M. LeMay, D. Garg, R. Jhala, and D. Stefan. Isolation without taxation: Near zero cost transitions for SFI. Principles of Programming Languages (POPL), 2022.
6. S. Narayan, C. Disselkoen, and D. Stefan. Tutorial: Using RLBox to sandbox unsafe C code. IEEE Secure Development Conference (SecDev), 2021.
7. S. Narayan, C. Disselkoen, D. Moghimi, S. Cauligi, E. Johnson, Z. Gang, A. Vahldiek-Oberwagner, R. Sahita, H. Shacham, D. Tullsen, D. Stefan. Swivel: Hardening WebAssembly against Spectre. USENIX Security Symposium, 2021.
8. E. Johnson, Y. Alhessi, D. Thien, S. Narayan, F. Brown, S. Lerner, T. McMullen, S. Savage, and D. Stefan. Доверя́й, но проверя́й: SFI safety for native-compiled Wasm. Network and Distributed System Security Symposium (NDSS), 2021.
9. T. Garfinkel, S. Narayan, C. Disselkoen, H. Shacham, and D. Stefan. The road to less trusted code: Lowering the barrier to in-process sandboxing. Article in USENIX ;login; journal, Winter 2020.
10. S. Narayan, C. Disselkoen, T. Garfinkel, N. Froyd, E. Rahm, S. Lerner, H. Shacham, and D. Stefan. Retrofitting fine grain isolation in the Firefox renderer. USENIX Security Symposium, 2020.
11. J. Talpin, J. Marty, S. Narayan, D. Stefan, and R. Gupta. Towards verified programming of embedded devices. Invited paper at Design, Automation and Test in Europe Conference, 2019.
12. M. Smith, C. Disselkoen, S. Narayan, F. Brown, and D. Stefan. Browser history re:visited. USENIX Workshop on Offensive Technologies (WOOT), 2018.
13. F. Brown, S. Narayan, Riad S. Wahby, Dawson Engler, R. Jhala, and D. Stefan. Finding and preventing bugs in JavaScript bindings. IEEE Symposium on Security and Privacy (S&P), 2017.

Others

14. Don't Get Owned by Your Dependencies: How Firefox Uses In-process Sandboxing To Protect Itself From Exploitable Libraries. Strange Loop Conference, 2022.
15. Don't Get Owned by Your Dependencies: How Firefox Uses In-process Sandboxing To Protect Itself From Exploitable Libraries. Black Hat USA Conference, 2022.

16. S. Narayan and D. Stefan. Making software sandboxing practical using language-based techniques. Article in SIGPLAN PL Perspectives blog, Jul'21.
17. RLBox: Retrofitting fine grain isolation in the Firefox renderer. IEEE Symposium on Security and Privacy (S&P), 2021. Invited poster.
18. S. Narayan, T. Garfinkel, S. Lerner, H. Shacham, and D. Stefan. Gobi: WebAssembly as a practical path to library sandboxing. In arXiv preprint arXiv:1912.02285, Jan'19, updated Nov'19.

Awards

2023 NSF CCF # 2327338. Collaborative Research: SaTC: CORE: Medium. *Refine the Gap: Establishing Safety for Modern Foreign Function Interfaces.* $1,200,000 (total), $300,000 (UT Austin).

2023 Most engaging speaker, UT Austin Research Topics Seminar (Course CS398T).

2023 Distinguished paper award at ASPLOS 2023. *Going beyond the Limits of SFI: Flexible and Secure Hardware-Assisted In-Process Isolation with HFI.*

2023 Distinguished paper award IEEE Symposium on Security and Privacy (S&P), 2023. *WaVe: a verifiably secure WebAssembly sandboxing runtime.*

2023 Noteworthy Reviewer Award at USENIX Security Symposium 2023.

2022 Mozilla research award. *RLBox v2: Extending RLBox for more performant, ubiquitous sandboxing.*

2022 Winner, IEEE Cybersecurity Awards for Practice 2022. *Retrofitting fine grain isolation in the Firefox renderer.*

2022 Honorable mention, NSA Best Scientific Cybersecurity Paper. *Retrofitting fine grain isolation in the Firefox renderer.*

2022 Recognized contributor to the Bytecode Alliance's formal verification efforts.

2021 Google V8 research award. *Practical, portable, and verified library sandboxing using Wasm.*

2021 Fastly's "*The edge computer project*" award. Verifiable and spectre-safe sandboxing at the edge.

2021 Finalist, Applied Research Competition, CSAW 2021. *Доверяй, но проверяй: SFI safety for native-compiled Wasm.*

2020 Winner, Doctoral Award for Excellence in Research, Computer Science and Eng., UC San Diego.

2020 Winner, Applied Research Competition, CSAW 2020. *Retrofitting fine grain isolation in the Firefox renderer.*

2020 Distinguished paper award at the USENIX Security Symposium 2020. *Retrofitting fine grain isolation in the Firefox renderer.*

Activities/service

Jan'24–Apr'24 Graduate admissions committee at UT Austin 2024.

Jun'23–Jun'24 Program committee of the USENIX Security Symposium 2024.

Aug'23 Program committee of the Kernel Isolation, Safety, and Verification 2023.

Jun'22–Jun'23 Program committee of the USENIX Security Symposium 2023.

Nov'22 Program committee of the Programming Languages and Analysis for Security (PLAS), 2022.

Nov'22 Mentor in GradAMP graduate application mentorship program at UC San Diego.

Oct'22 Invited participant in Consumer Reports' Memory safety convening.

Sep'22 Invited external reviewer on IEEE Symposium on Security and Privacy (S&P) 2023.

Aug'22 Program committee of the Applied Research Competition, CSAW 2022.

Jun'22 Program committee of the IEEE Secure Development Conference 2022.

Sep'21–May'22 Mentor in Early Research Scholars Program (ERSP) undergraduate research program at UC San Diego CSE department.

2019–2021 Student reviewer of papers in IEEE Symposium on Security and Privacy (S&P) 2019, ACM Symposium on Operating Systems Principles 2019, USENIX Security Symposium 2020 and 2021.

Talks

Oct'23 At Wasm Research Day 2023. Optimizing SFI Performance, Scalability, and Spectre Resistance on Modern CPUs.

Sept'23 At WasmCon 2023. Don't Get Owned by Dependencies: How Firefox Uses Wasm to Protect Itself from Exploitable Libraries.

Aug'23 At RISC-V Security meeting and RISC-V Runtime Integrity SIG. Going beyond the Limits of SFI: Flexible and Secure Hardware-Assisted In-Process Isolation with HFI.

May'23 At KTH Royal Institute of Technology's Software Research Meetup. Retrofitting fast and secure sandboxing in real systems.

Apr'23 At Intel Corp. Going Beyond the Limits of SFI: Flexible and Secure Hardware-Assisted In-Process Isolation with HFI.

Mar'23 At ASPLOS 2023. Going Beyond the Limits of SFI: Flexible and Secure Hardware-Assisted In-Process Isolation with HFI.

Mar'23 At Dagstuhl Seminar: Foundations of WebAssembly. Going Beyond the Limits of SFI: Flexible and Secure Hardware-Assisted In-Process Isolation with HFI.

Dec'22 At the Programming Languages and Analysis for Security (PLAS), 2022. Segue & ColorGuard: Optimizing SFI Performance and Scalability on Modern x86.

Nov'22 At UBC's graduate security class. Swivel: Hardening WebAssembly against Spectre.

Nov'22 At CMU's security class. Retrofitting fast and secure sandboxing in real systems.

Sept'22 At the Strange Loop Conference 2022. Don't Get Owned by Your Dependencies: How Firefox Uses In-process Sandboxing To Protect Itself From Exploitable Libraries.

Aug'22 At the Black Hat USA Conference 2022. Don't Get Owned by Your Dependencies: How Firefox Uses In-process Sandboxing To Protect Itself From Exploitable Libraries.

June'22 At UCSD's graduate security class. Retrofitting fast and secure sandboxing in real systems.

Oct'21 At the IEEE Secure Development Conference 2021. Using RLBox to sandbox unsafe C code.

Aug'21 At the USENIX Security Symposium 2021. Swivel: Hardening WebAssembly against Spectre.

Jul'21 At Intel Corp. Swivel: Hardening WebAssembly against Spectre.

Oct'20 At MIT's CSAIL security seminar. Retrofitting fine grain isolation in the Firefox renderer.

Oct'20 At the Center for Networked Systems' Research Review. RLBox: secure sandboxing for buggy application components.

Aug'20 At the USENIX Security Symposium 2020. Retrofitting fine grain isolation in the Firefox renderer.

Jul'20 At Brave Software, Inc. Retrofitting fine grain isolation in the Firefox renderer.

Classes

Fall 2023 Securing real-world systems at UT Austin (CS395T)

Software

rlbox A general purpose library sandboxing framework that supports sandboxing plugins.

rlbox-wasm2c An rlbox plugin that supports using libraries sandboxed with wasm2c.

veriwasm Sandbox validator for Cranelift WebAssembly compiler.

swivel Spectre-resistant WebAssembly compiler.