Brian **Johannesmeyer**

PhD Candidate · Systems Security Engineer & Researcher · VUSec

bjohannesmeyer@gmail.com | bjohannesmeyer.github.io | bjohannesmeyer | bjohannesmeyer |
@bjohannesmeyer | Brian-Johannesmeyer

Summary

Systems security researcher with VUSec, specializing in building advanced tools for kernel vulnerability discovery and exploit generation. Contributed performance improvements and security patches to the Linux kernel, including mitigations for speculative type confusion and memory corruption bugs. Published in top-tier conferences (e.g. *USENIX Sec.*, *IEEE S&P*) with multiple best-paper award recognitions.

Passionate about bridging academic research and industry practice—particularly in automated program analysis, OS internals, and high-impact security tooling. Proficient in C/C++, Python, LLVM, Linux internals, and x86/arm64 assembly, with a strong track record in open-source collaboration. Enjoy teaching, sharing knowledge, and continuously exploring new ways to break (and then fix) complex software systems.

Work Experience

Vrije Universiteit Amsterdam (VUSec)

Amsterdam, The Netherlands

Graduate Researcher — *Apr. 2019 – Present*

- Designed and implemented a DMA race-condition scanner for the Linux kernel, uncovering hundreds of device-to-kernel vulnerabilities [1].
- Created a data-only attack generator that produced hundreds of mitigation-bypassing exploits for major server applications [3], [4].
- Built a speculative execution gadget scanner for the Linux kernel, revealing hundreds of previously undiscovered gadgets [5].
- Co-developed research demonstrating that recent mitigations against memory deduplication still remain vulnerable to side-channel attacks [6].
- Served as Teaching Assistant, developing assignments related to e.g., exploiting network protocols and web vulnerabilities.

Qualcomm

San Diego, California

Product Security Engineering Intern — *Jun. 2018 – Sep. 2018*

- Examined side-channel vulnerabilities in digital signal processors and proposed mitigation strategies.

UC San Diego

San Diego, California

Graduate Researcher — *Sep. 2015 - Jun. 2018*

- Reverse-engineered avionics communications management units to uncover security flaws [7].
- Co-designed a domain-specific language and compiler for writing constant-time code [8], [9].
- Exposed compiler-introduced security issues (e.g., from dead-store elimination) and developed fixes [10].
- Served as Teaching Assistant, developing assignments related to e.g., control-flow hijacking and side-channel attacks.

University of Arizona

Tucson, Arizona

Undergraduate Researcher — *May 2012 - May 2015*

- Created proof-of-concept malware employing advanced anti-analysis defenses (e.g., obfuscation and anti-tampering) [11], [12], [13].
- Served as Teaching Assistant, developing an SDR-based lab assignment for filter design and real-time frequency analysis.

Honors & Awards

Research Awards

2024	**Best Paper Award Runner-up**, CSAW Applied Research Competition *(for [3])*	*Valence, France*
2024	**Best Paper Award Runner-up**, Dutch Cyber Security Research *(for [5])*	*The Hague, The Netherlands*
2022	**Innovation Fellowship Runner-up**, Qualcomm	*Amsterdam, The Netherlands*
2015	**Best Paper Award Runner-up**, CSAW Applied Research Competition *(for [11])*	*New York, New York*
2015	**Outstanding Undergraduate Research Award**, University of Arizona	*Tucson, Arizona*

Community

2013–2015	**Member and Officer**, Eta Kappa Nu	*Tucson, Arizona*
2013–2015	**Member**, Tau Beta Pi	*Tucson, Arizona*
2013–2015	**Member**, Phi Beta Kappa	*Tucson, Arizona*
2011	**High Honors Tuition Scholarship**, Arizona Board of Regents	*Tucson, Arizona*
2009	**Eagle Scout with Bronze Palm**, Boy Scouts of America	*Tucson, Arizona*

Education

Vrije Universiteit Amsterdam
Amsterdam, The Netherlands

PhD in Computer Science — *2019 – Present*

- Supervisor: Herbert Bos.
- Topic: Developed novel dynamic data-flow analyses to automatically identify and exploit complex vulnerabilities [2].

UC San Diego
San Diego, California

MS in Computer Science — *2015 – 2018*

University of Arizona
Tucson, Arizona

BS in Electrical and Computer Engineering; BS in Computer Science (Magna Cum Laude, with Honors) — *2011 – 2015*

Open-Source Contributions

(In progress) **Linux kernel, LLVM project**: KernelDataFlowSanitizer (KDFSAN), a generalized dynamic data flow analysis for the kernel

(Submitted) **Linux kernel**: Mitigate a memory corruption vulnerability in the DMA pool allocator

(Submitted) **Linux kernel**: Fix hundreds of inconsistent DMA accesses in VMware's VMXNET3 driver

May 2024 **Linux kernel**: Add a fix for unaligned I/O accesses and a regression test to KernelMemorySanitizer (KMSAN)

Apr. 2024 **Linux kernel**: Improve the performance of the address-to-line script by 15x

Feb. 2022 **Linux kernel**: Mitigate speculative type confusion bugs in the list implementation

Oct. 2016 **OpenVPN, Kerberos, others (see [10])**: Mitigate cases of the compiler optimizing out sensitive memory clear operations

Publications

[1] Dynamic Detection of Vulnerable DMA Race Conditions
B. Johannesmeyer, R. Isemann, C. Giuffrida, and H. Bos. *(Under review)*.

[2] Information Flow-Based Vulnerability Modeling
B. Johannesmeyer. *PhD Thesis, Vrije Universiteit Amsterdam*, 2025.

[3] Practical Data-Only Attack Generation
B. Johannesmeyer, A. Slowinska, H. Bos, and C. Giuffrida. *USENIX Security*, 2024.

[4] Data-Only Attacks Are Easier than You Think
B. Johannesmeyer, H. Bos, C. Giuffrida, and A. Slowinska. *USENIX ;login:*, 2024.

[5] Kasper: Scanning for Generalized Transient Execution Gadgets in the Linux Kernel
B. Johannesmeyer, J. Koschel, K. Razavi, H. Bos, and C. Giuffrida. *NDSS*, 2022.

[6] On the Effectiveness of Same-Domain Memory Deduplication
A. Costi, B. Johannesmeyer, E. Bosman, C. Giuffrida, and H. Bos. *ACM EuroSec*, 2022.

[7] Triton: A Software-Reconfigurable Federated Avionics Testbed
S. Crow, B. Farinholt, B. Johannesmeyer, K. Koscher, S. Checkoway, S. Savage, A. Schulman, A. C. Snoeren, and K. Levchenko. *USENIX CSET*, 2019.

[8] FaCT: A DSL for Timing-Sensitive Computation
S. Cauligi, G. Soeller, B. Johannesmeyer, F. Brown, R. S. Wahby, J. Renner, B. Grégoire, G. Barthe, R. Jhala, and D. Stefan. *ACM PLDI*, 2019.

[9] FaCT: A Flexible Constant-Time Programming Language
S. Cauligi, G. Soeller, F. Brown, B. Johannesmeyer, Y. Huang, R. Jhala, and D. Stefan. *IEEE SecDev*, 2017.

[10] Dead Store Elimination (Still) Considered Harmful
Z. Yang, B. Johannesmeyer, A. T. Olesen, S. Lerner, and K. Levchenko. *USENIX Security*, 2017.

[11] A Generic Approach to Automatic Deobfuscation of Executable Code
B. Yadegari, B. Johannesmeyer, B. Whitely, and S. Debray. *IEEE S&P*, 2015.

[12] Identifying Understanding Self-Checksumming Defenses in Software
J. Qiu, B. Yadegari, B. Johannesmeyer, S. Debray, and X. Su. *ACM CODASPY*, 2015.

[13] A Framework for Understanding Dynamic Anti-Analysis Defenses
J. Qiu, B. Yadegari, B. Johannesmeyer, S. Debray, and X. Su. *ACM PPREW*, 2014.