Scott Griffy

✉ *scottgriffy@gmail.com*
scottgriffy.com
Updated: Jun 14, 2023

Publications and workshops

EPRINT 2023 **PACIFIC: Privacy-preserving automated contact tracing scheme featuring integrity against cloning**, *Scott Griffy, Anna Lysyanskaya*, Cryptology ePrint Archive.

DIMACS 2020 **Abradable Key Wrapping**, *Scott Griffy, Charles V. Wright, Mayank Varia*, DIMACS Workshop on Co-Development of Computer Science and Law, Poster session and lightning talk.

IEEE DSN 2019 **The Strength of Weak Randomization: Easily Deployable, Efficiently Searchable Encryption with Minimal Leakage**, *David Pouliot, Scott Griffy, and Charles V. Wright*, 49th IEEE/IFIP International Conference on Dependable Systems and Networks.

Master's Thesis 2019 **Crumpled and Abraded Encryption: Implementation and Provably Secure Construction**, *Scott Griffy*, Portland State University Master's Thesis, Advisor: Charles V. Wright.

Education

2021 to current **PhD, Computer Science**, *Brown University*, Providence, RI, *3.75 GPA*.
- Advisor: Anna Lysyanskaya
- Taking classes on cryptography, probability, and algebra.
- Researching anonymous credentials and structure-preserving signatures.
- Running a cryptography reading group.

2017 to 2019 **Master of Science, Computer Science**, *Portland State University*, Portland, OR, *3.95 GPA*.
- Advisor: Charles V. Wright
- Took classes in computer security and cryptography.
- Researched searchable encryption, co-authoring a paper at DSN 2019.
- Defended my thesis relating to exceptional access in June, 2019.
- Wrote an educational Windows 10 32-bit rootkit that included a keylogger.
- Helped create the Portland State University video game development club.
- Configured and performed database benchmarks such as TPC-C and SPARTA, a framework from MIT Lincoln Laboratory.
- Wrote a script to crawl Github and put security related information in a PostgreSQL database.

2010 to 2016 **Bachelor of Science, Computer Science**, *Oregon State University*, Corvallis, OR, *3.0 GPA*.
- Computer Systems Option, ABET Accredited
- Awarded best capstone project. This project used single board computers for computer vision.

Work experience

September 2021 to present **Research/Teaching Assistant**, *Brown University*, Providence, RI.
- TA for cryptography.
- Researching cryptography and anonymous credentials.

July 2019 to July 2021 **Security Engineer/Researcher**, *Intel Corporation*, Hillsboro, OR.
- Worked with memory encryption, virtualization-based security, nested virtualization, and other OS technologies.
- Debugging operating systems and hardware.
- Filed a patent.
- Wrote exploits for Intel products.
- Researching timing attacks through hardware power signal analysis.

September 2018 to June 2019 **Research/Teaching Assistant**, *Portland State University*, Portland, OR.
- Designed new cryptographic protocols for privacy and exceptional access
- Worked on symbolic execution in ethereum contracts
- TA for computer security

June 2018 to September 2018 **Graduate Technical Intern**, *Intel Corporation*, Hillsboro, OR.
- Developed a proof of concept, securing a virtual machine with new technologies
- Worked with memory encryption and TPMs
- Worked with Windows virtualization technologies

March 2018 to June 2018 **Quality Assurance Intern**, *Iovation*, Portland, OR.
- Pen tested web applications including code auditing in Java
- Ran and analyzed scans with Qualys, Burp Suite

July 2017 to March 2018 **Quality Assurance Analyst**, *PlusQA*, Portland, OR.
- Regression and exploratory software testing on Mac, iOS, Android, and Windows
- Debugging devices with Xcode and adb
- Scripting to support some automation

July 2016 to December 2016 **Software Contractor**, *Empirical Inc*, Portland, OR.
- Added voice recognition to an existing python project
- Developed a test suite for a React/Redux web application

Skills

Programming Languages:
Java, C/C++, HTML/CSS, JavaScript, PHP, SQL, Python, OpenGL, CUDA, Haskell

Utilities/Tools:
bash, git, ssh, Apache HTTP, ftp/scp, vim, Debian/Ubuntu, CentOS/Fedora, LaTeX, gdb, Metasploit, PowerShell, Visual Studio, Eclipse, WinDBG, Android SDK/NDK, PostgreSQL, Libvirt, qemu

References and full form resume available upon request