Rowan Hart

(505)-321-2544 https://github.com/novafacing
rowanbhart@gmail.com

Experience

- **Intel Corporation - Security Research Engineer** **September 2022 - Present**
  - Developed and open-sourced TSFFS, a fuzzer for the SIMICS full system simulator for securing UEFI and Kernel
  - Enabled fuzzing of Windows kernel drivers using Kernel Fuzzer for Xen
  - Software architecture and cryptography review of upcoming technologies
  - Collaborated with teams across business units to enable fuzzing firmware and drivers on all platforms
  - Managed an intern project to develop a scalable AI-assisted fuzzing harness generation tool
  - Led the formation of a Rust CoP and championed adoption of memory safe languages for system software
- **Research Innovations Incorporated - Security Researcher II** **August 2020 - August 2022**
  - Vulnerability research of large software projects across server, embedded, and mobile environments using AFL++ and Jazzer alongside manual and symbolic techniques
  - Developed diverse Binary Ninja plugins to assist vulnerability research integrating symbolic execution with Z3
  - Experimental applications of AI including transformers and reinforcement learning in vulnerability research
  - Developed automated tools leveraging angr to perform analysis of firmware
- **Purdue University - Undergraduate & Graduate Research Assistant** **January 2020 - December 2022**
  - Developed automated binary patching tools to improve coverage of closed-box binary fuzzing using angr & LLVM
  - Developed automated exploit rehosting tools using the angr symbolic execution framework
- **Purdue University - Undergraduate & Graduate Teaching Assistant** **August 2019 - May 2021**
  - Wrote and maintained the standard linting tool for C programming courses using LLVM and clang-tidy
  - Taught and assisted students with C, systems programming, operating systems development, and gdb debugging
  - Developed project specifications and handouts, project and solution source code, and automated test cases
- **Northrop Grumman Xetron - Security Researcher Intern** **May 2018 - August 2020**
  - Reverse engineering of operating system internals and Windows applications, developed C/C++/Python projects
  - Developed an IDA Pro plugin for control flow analysis and path emulation for vulnerability research
  - Hosted a Capture The Flag competition, created infrastructure and reverse engineering challenges
  - Extended a binary comparison tool with additional functionality for metric acquisition in C++ and python
- **Purdue University b01lers Capture The Flag Team - Vice President** **August 2017 - December 2021**
  - Coordinated, hosted, and developed challenges for multiple public CTF competitions with over 600 scoring teams
  - Coordinated and created training curriculum in binary exploitation and reverse engineering with 1000+ attendees
  - Solved challenges RE, binary exploitation, web & cryptography, led team to 7th place national ranking

Education

Purdue University, West Lafayette IN

- Master of Science in Computer Science, GPA 3.66/4.0 **December 2022**
- Bachelor of Science in Computer Science, GPA 3.55/4.0 **December 2020**

Technical Skills

- Programming Languages: Rust, Python, C/C++, Java, Typescript, Shell
- Open Source: AFLplusplus/LibAFL, intel/tsffs, angr/angr, trailofbits/maat, rust-lang/rust, novafacing/qemu-rs
- Compilers: LLVM compiler for MiniC, LLVM instrumentation passes, Clang-Tidy Check development
- Reverse Engineering: Reversing large systems and plugin development with Binary Ninja, Ghidra, and IDA Pro
- Kernel Development: Linux, Windows and XINU kernel & kernel module/driver development
- DevOps: Linux, Windows, MacOS system administration, Docker, GitHub actions, GitLab pipelines

Awards, Publications, & Talks

- **Intel Security Leadership Award** for Fuzzing the Unfuzzable **June 2024**
- **Intel Corporation Division Recognition Award** for Project Mercury **May 2024**
- **BSides PDX (Talk)**: This Chip Does Not Exist: Pre-Silicon Fuzzing **October 2023**
- **Intel Corporation Division Recognition Award** for Securing Intel Developer Cloud **September 2023**
- **Intel Corporation Division Recognition Award** for CONFUSE: Shift-left fuzzing at Intel **June 2023**
- **ACM SIGCSE Technical Symposium (Paper & Talk)** **March 2023**
  Eastwood-Tidy: C Linting For Automated Code Style Assessment in Programming Courses
- **Masters Thesis (Paper)** **December 2022**
  Fuzzing Deeper Logic With Impeding Function Transformation
- **Eagle Scout Award** **2013**