JEVIN SWEVAL

1226 Old Mill Ln., Lafayette, IN 47905 (925) KOR-DUMP (567-3867) *(cell)*; jevin.sweval@gmail.com

SKILLS

◇ **Programming and Systems**

- Skilled in C/C++/Obj-C, assembly (x86, ARM, PPC), Python, Perl, VHDL/Migen/LiteX/Amaranth
- Extensive experience in reversing binaries (unprotected and protected/obfuscated) using IDA Pro, Ghidra, and Binary Ninja
- Experience developing exploits from PlayStation 3-5 hacking and ARM bootloader vulnerability research
- Experienced with LLVM passes (in particular, obfuscation passes) and backends and Linux/Android/iOS low-level toolchain internals
- Understanding of cryptography and DRM, including white-box cryptography
- Test Driven Development using Google Test, pytest, and VHDL/cocotb test benches
- Intimately familiar with XNU and Linux userspace/kernel internals, including limited driver development
- Deep knowledge of Linux/Android/iOS/macOS low-level toolchain internals and libc's (in particular, dynamic loaders)
- Adept at Git, Perforce, Subversion VCS, and associated review tools
- Expert at debugging root-cause issues using debuggers, delta debugging, test case reduction, simulators (QEMU, CoMET/METeor), JTAG, and Clang sanitizers

◇ **Electronics**

- Experience with PCB layout using Eagle and KiCad
- Low-level hardware experience, including exception vectors, SPI/I^2C peripherals, PWM, etc.
- SMD soldering skills and experience using lab test equipment (logic analyzers, oscilloscopes, AWGs)
- Hardware side-channel attack experience using DPA, DFA, and clock/voltage glitching

◇ **Processes and Communication**

- Significant team-oriented and cross-functional communication experience with both local and globally remote groups
- Six years experience with SCRUM workflow and JIRA

WORK EXPERIENCE

◇ **Apple Inc.** **Senior Security Engineer - Apple Pay** **Feburary 2019 – May 2022**

- Coordinated the Apple Pay response to checkra1n SecureROM vulnerability
- Developed PMU mitigations against checkra1n and introduced a further hardening change in the next generation SoC
- Coordinated the Apple Pay response to blackbird SEPOS vulnerability that produced three coordinated backport fix releases along with the fix in the next iOS
- Implemented NFC relay attack against CarKey and implemented verification hardware for the anti-relay mitigation implementation prompted by my finding
- Found a persistent unsigned code execution vulnerability in `REDACTED` and exploited it using SLOP
- Fuzzed `REDACTED.kext` with a custom userspace IOKit stub to find and fix several memory corruption issues
- Broke the `REDACTED.kext` white-box cipher that otherwise prevented an attacker from exploiting the above vulnerabilities using DFA techniques
- Discovered a vulnerability with VAS passes that allowed attackers to bypass signature validation
- Implemented a MobileDevice backup viewer/editor based on FUSE to exploit the above vulnerability
- Developed numerous tweaks/injected libraries to rapidly prototype mitigation ideas and other PoCs without requiring complete project rebuilds/roots

- Maintained an internal fork of Frida to support internal, next iOS/macOS changes that several security teams inside Apple utilized

◇ **Arxan Technologies** **Software Security Engineer** **July 2012 – March 2018**

- Developed numerous new binary obfuscation and anti-tamper protection techniques implemented in LLVM IR and binary rewriting tools
- Added PS3 support to LLVM's PPC backend and EnsureIT protection engine in only three months for a AAA game title
- Developed tools to automate testing on iOS devices by reversing Apple utilities' internal implementations
- Created guards that detect root/jailbreak, image tampering, library injection, Frida hooking, and crash hostile debuggers
- Ported the GuardIT x86 protection product to protect Windows/Linux ARM/AArch64 binaries

◇ **Purdue University** **Research Assistant** **October 2010 – July 2012**

- Tasked by the Missile Defense Agency to research future missile defense system architectures
- Lead engineer of the communication network models and co-lead of the actor-based simulation architecture

◇ **Purdue University** **Lead ECE 364 TA** **August 2010 – December 2010**

◇ **Qualcomm *(internship)*** **Software Verification Engineer** **May 2010 – August 2010**

- Lead architect of next-generation infrastructure simulator for the MediaFLO mobile TV system
- Crafted a simulator packaging and deployment scheme to ease deployment to overseas offices
- Formalized best practices, coding, and documentation standards for the simulator

◇ **Qualcomm *(internship)*** **Software Integration Engineer** **May 2009 – August 2009**

- Specified, designed, and implemented an interactive server backend into the existing test framework
- Wrote client API for the interactive server and cross-platform CLI and GUI clients using said API

◇ **Delphi Electronics *(internship)*** **Software Verification Engineer** **May 2007 – May 2010**

- Created and maintained several ASIC simulation models and their verification tests
- Researched and implemented automated code coverage analysis for our ASIC unit tests
- Designed and implemented a remote interface for a prototype car using Python + Qt on a Nokia N900

EDUCATION

◇ **Purdue University** **West Lafayette, IN**

- **Doctor of Philosophy in Computer Engineering** **August 2010 – July 2012** ***(incomplete, left for industry)***
  Researched proof-based network security with a focus on intrusion detection
  Member of the Dependable Computing Systems Laboratory
- **Bachelor of Science in Computer Engineering** **August 2006 – May 2010**
  Minor in Communications
  Cumulative GPA 3.7

AWARDS

◇ AMD Design Award — AES on ASIC with PCIe interface **June 2009**

◇ Dean's List and Semester Honors **August 2006 – May 2010**

◇ SocialDevCamp Chicago hackathon winner **2010 and 2011**

PUBLICATIONS

◇ AMD LM32-based System Management Unit Exploitation and Bootrom Dumping — Discovered and exploited an unpatchable flaw in pre-Zen AMD CPUs/APUs/GPUs that grants attackers total control of DRAM, IO, and x86 execution

◇ Modelo-Howard, G., **Sweval, J.**, Bagchi, S.: Secure Configuration of Intrusion Detection Sensors for Changing Enterprise Systems. In: *Proc. of the 7th ICST Conference on Security and Privacy for Communication Networks (SecureComm'11)*. London, United Kingdom, September 2011.