Dover, NH
https://seanpesce.github.io

Sean Pesce

Public copy; phone number redacted
pesce.sean@gmail.com

Employment

Principal Staff Penetration Tester — **Motorola Solutions, Inc.** — **2021 – Present**

Threat Management Group | Products & Services Red Team

- Device pentesting – Analysis and exploitation of device behavior via flash extraction, network communications, USB/ serial, Bluetooth, NFC, web interfaces, AWS IoT Core, etc.
- Application pentesting – Security assessments of desktop, mobile (Android), cloud, and web-based SaaS solutions
- Mentoring & leadership – Acted as an information security SME, coaching less-experienced pentesters and providing subject matter expertise to management
- Process improvement & automation – Automated internal processes for requesting and scheduling penetration tests using Python and Google Workspace (Forms, Sheets, Apps Script, etc.)
- Tool development – Developed custom tooling in several languages to assist in analysis of product security
- Cross-domain collaboration – Collaborated with development teams for threat modeling, secure design, and code review. Collaborated with SOC teams to assist with detection, monitoring, and incident response
- Intellectual property protection – Demonstrated cracking of licensed software. Presented solutions for hardening of IP protection mechanisms

Security Researcher — **Software Engineering Institute, Carnegie Mellon University** — **2018 – 2021**

Platform Insight Team

- Federal security clearance – Top Secret / Sensitive Compartmented Information (TS/SCI)
- Reverse engineering – Android APKs, device firmware, native Linux binaries, proprietary network protocols, web services, file formats, etc.
- Android app analysis – Using tools such as JEB Decompiler for static analysis and Frida for runtime instrumentation, evaluated aspects of mobile apps including IPC mechanisms, network communications, data collection, and root/emulator detection techniques
- Vulnerability research and proof-of-concept (PoC) exploit development
- Network traffic analysis – all OSI layers
- Technical reporting – monthly slides, white papers, and presentations for DoD customers

Education & Professional Certifications

Offensive Security Certified Professional (OSCP) — **2021**

- Certification ID: OS-101-34893

Stony Brook University — **2013 – 2018**

- B.S. in Computer Science

Other Technical Experience

Personal Projects & Information Security Research

- **Android App Research** (2023). Regular analysis of Android apps resulting in the discovery of critical vulnerability chains including insufficient URL validation, vulnerable WebView implementations, insecure exported IPC components, arbitrary remote code execution (RCE), and more. All findings were responsibly disclosed through the relevant bug bounty programs.
  (Click for video demonstrations: Home Depot, Hago Chat & Games, Tango Live Stream)
- **SELinux Research** (2023). Discovered a vulnerability chain facilitating remote code execution (RCE) and elevation to kernel privileges during an assessment of an undisclosed IoT device. This included the development of a custom Linux kernel module and loader to demonstrate a novel approach to attacking flawed SELinux policies. (Click here for full blog write-up)
- **CVE-2022-45028** (2022). Pre-authenticated stored WAN-to-LAN cross-site scripting (XSS) vulnerability in the configuration web UI of the Arris NVG443B Gateway (firmware version 9.3.0h3d36). The finding was disclosed to MITRE and received a CVSS severity rating of 6.1 (Medium). (Click here for NIST disclosure)
- **Many more**. See my GitHub profile, personal website, and research blog for other projects.

Languages, Technologies, and Technical Skills

- Java, Python, Bash, C, C++, LaTeX, SQL, HTML, JavaScript / TypeScript, PHP, x86 assembly
- Android SDK, Ghidra, IDA Pro, JEB Decompiler, Frida, Burp Suite, WireShark, GDB, Buildroot
- Reverse engineering, network traffic analysis, web security, code review, technical writing, oral communication