Davis Zvejnieks

zvej.net
github.com/phantom-voltage

- Client-facing, principal security consultant with strong written and verbal skills and experience leading large teams
- Well-rounded security experience, with focus on embedded hardware, operating systems, and containerization

Professional Experience

2017-Current **Principal Consultant**, Deja vu Security/Accenture,
Technical security consultant, lead engagements, threat modeled, and responded to RFPs for Fortune 500 companies.

- Managed large teams (7+)
- Career counselor and mentor
- Developed embedded hardware training
- Git and documentation maintaner

Security Expertise

Embedded	Firmware analysis, boot loader security, chain of trust bypass, protocol and signal analysis, native C review, design and component review
Boot	Intel Secure Boot implementation, Coreboot & U-Boot configuration, PCH utilization, e-fuse configuration, memory management, side-channel attacks (DMA, implants)
Containerization	OCI, Kubernetes, runc, & Docker with focus on tenant isolation for large cloud platforms, isolation of containers from host, IPC review
Fuzzing	Writing harnesses for fuzzing Linux kernel drivers, SIP clients, and other native applications using syzkaller and AFL
Other	GNU/Linux & OS X security configuration, trusted execution environment (TEE), secure enclaves, web & API review, cryptographic implementations, Android apps
Languages	C, C++, Python, Rust, Java, Bash, JavaScript

Engagement Highlights

Secure Boot Implementation — Threat modeled implementation of Intel Secure Boot with Coreboot bootloader. Meticulous architectural, process, and documentation review. Reviewed embedded hardware key utilization with firmware utilization, hardware protected RO sections combined with Coreboot's cryptographic verification.

Physical Security Device — Reviewed commonly used enterprise device for physical security. Discovered multiple unprotected threat vectors, including supply chain attacks, U-Boot bypasses, GNU/Linux misconfigurations, vulnerable web applications

2FA Token — Discovered buffer vulnerabilities used for OTP, reuse of buffer data, USB protocol misutilization, Denial of Service, counter token reuse and side-channel attacks

Personal Projects

2019 **SNES ROM Hacking**, 🖱 `https://github.com/phantom-voltage/milandra_translation`.

Reverse engineering Super Nintendo game. Identified table for Japanese characters and text extraction for translation. Learned 65816 assembly and various ROM and cartridge memory layouts.

2014-2017 **ROGUE NEXUS**, Creator and maintainer of multi-game roguelike server.

ROGUE NEXUS is a server for playing roguelike games over SSH or in the browser with over 700 unique users. Highlights in work include:

- 9 supported games, each of which have support for IRCbot notifications
- Services instantiated with Docker
- Databases maintained in sqlite3
- Multitude of scripts written in Python & Bash
- Implemented many patches in C & C++
- IRCbot written in Python

Education

2010 - 2016 **BS in Mathematics**, *University of Washington*, Seattle,
Number Theory, Cryptography, Combinatorics, Probability, Mathematical Modeling.
GPA – 3.7

2010 - 2016 **BA in Scandinavian Studies**, *University of Washington*, Seattle,
Latvian area studies, History of Baltic States, Scandinavian Cinema.
GPA – 3.7

2007–2010 **Computer Science**, *University of Central Florida*, Orlando,
C, OOP, Assembly, Virtual Machines, Computer Vision, Discrete Mathematics.
GPA – 4.0