

Senior HW Exploitation Engineer

Department 13 (D13) is looking for a Senior HW Exploitation Engineer to help our team to understand the firmware code implemented on various proprietary hardware systems and exploit their vulnerabilities. The candidate must have a keen understanding of commonly used microcontrollers and baseband radios and their implementations. They should be able to expose vulnerabilities and devise attack from multiple angles in order to do things like recover debugging interfaces, dump firmware, and inject custom payloads.

The position is located at the Columbia, MD site.

Duties and Responsibilities:

- Identifying and exploiting hardware debug interfaces
- Dumping firmware on read-protected devices
- Disassembling firmware dumps to assist the team in understanding HW behavior
- Identify protocol vulnerabilities through software
- Development of software to exploit uncovered vulnerabilities

Desired Qualifications:

- Experience in embedded system design and programming
- Understanding of common hardware interfaces (PCIe, I2C, UART, SPI, JTAG) and how to identify/interact with them
- Reverse engineering firmware and software
- Software Skills:
 - High Level in IDA/Radare3, GDB, Binary Ninja, cross compilation
 - Good knowledge of Linux OS
 - Android proficiency
 - Functional knowledge of Python or C/C++
- Lab skills: soldering/desoldering, experience with logic analyzers/oscilloscopes
- Understanding of cryptography
- Security Clearance: Not Required

Education:

- Preferred: BS in Electrical Engineering, Computer Science, Information Systems, or related field (exceptions will be made for individuals with equivalent work experience)

Additional Job Requirements:

- Must be authorized to work in the United States

Benefits:

- Join a dynamic startup
- Flexible work hours and telecommuting options
- Generous vacation policy
- Health insurance
- 401(k) matching
- Competitive salary commensurate with experience and performance