Security Analyst/Reverse Engineer (R969567)

Location: Haifa/ Jerusalem, Israel.

Business Entity
SPVSS has developed unique expertise in securing embedded systems mostly in the entertainment arena, where we have a 33% market share of conditional access for pay TV. Two years ago, SPVSS brought its security expertise to the aid of a major player in the automotive industry, which has also begun to face the kind of threats we have dealt with successfully for many years, and we are now extending our activities to Internet of Things (IoT), which faces similar security challenges. Cisco’s extensive security experience enables us to provide customers with state-of-the-art solutions that strike the right balance between security and price.

Role & Responsibilities
• Identify flaws and vulnerabilities in complex secure systems
• Reverse engineer systems, find software and hardware vulnerabilities
• Implement complex multi-stage exploits on multiple platforms and architectures
• Provide feedback to development teams
• Working with software, hardware, embedded systems, cryptography, networking, web apps...

Qualifications:
• Curiosity, Passion and Initiative
• Ability to learn and integrate new information very quickly, autodidact
• At least 3 years of experience in reverse engineering
• At least 3 years development in low-level language (C/C++/ObjC/ASM)
• Familiarity with Linux, embedded systems and hardware
• Ability to understand large code bases written by others
• Out-of-the box, abstract thinking. Creative problem solving

Nice to haves:
• Experience reverse engineering binary applications (ARM, x86, PPC, MIPS,...)
• Experience using IDA, gdb, idapython, ollydbg
• Experience with operating system and compiler internals
• Experience with vulnerability assessment and exploit development
• Experience with malware and rootkit analysis
• Experience developing on Windows, Linux, OS X, iOS, Android,...
• Knowledge of networking protocols
• Experience in network and/or web application penetration testing
• Experience with metasploit, burp, nmap
• Experience with large open-source projects
• Experience developing in Python
• Knowledge of electronics, digital system design and debugging (JTAG, logic-analyzer,...)
• Experience with embedded development
• B.Sc./M.Sc. in Computer Science, Electrical Engineering or Mathematics an advantage
• Knowledge of cryptographic principles
• Experience developing for security

In order to apply please go to: http://jobs.cisco.com/job/Haifa-Security-AnalystReverse-Engineer/215712800/