Domen Puncer Kugler

Software Engineer

Personal Statement

I like to know how things work.

I believe that makes me a good software developer in general, and also it comes really useful when discovering software vulnerabilities. I have over two decades of experience developing and assessing the security of embedded systems, anywhere from small microcontroller based products to server firmware. While I have strong background developing and reviewing C code and Linux kernel, I don't shy away from other programming languages and have recently grown quite fond of Rust.

I am capable and used to independent work, but prefer working with skilled coworkers.

WORK EXPERIENCE

Principal Security Consultant — 2022-Present

NCC Group, UK Remote

A core member of Hardware & Embedded Systems team.

Working on a variety of security assessments, anything from source code assessments, specification reviews, black-box device assessments to exploit development.

Most recent memorable work was a source code review of Caliptra hardware root of trust, which is also publicly available.

Senior Software Engineer — 2012-2022

Samsung Electronics, UK

Ethical Hacker (since 2013): Security assessment of Linux Kernel, system software, Android framework and mobile applications on latest flagship mobile devices.

This included source code analysis, reverse engineering, network traffic interception and analysis. I used a variety of existing tools for Linux and Android analysis and testing. Wrote my own tools, for example a one-liner CLI tool to construct buffer and call any ioctl, or a Java package explorer that used reflection to enumerate and call all methods. Main result were reports of analysed vulnerabilities with proof-of-concept exploits. During my time there, I have discovered on average nearly thousand vulnerabilities.

BSP Engineer (until 2013): Member of a team working on board bringup, Linux Kernel and Android. Improving and creating debugging tools to get RAM dumps, extract data from them and upload firmware binaries to mobile devices.

Other achievements: Top level on global in-company software competition (like ACM contests, or TopCoder). Consistent above-average performance reviews.

Software Engineer — 2008-2012

Visionect, Slovenia

Lead Firmware Developer: Software support on microcontroller platforms, from reset handlers to simple user interfaces. Cooperated with hardware team to discover and eliminate bugs in prototype hardware.

Main company project at that time was V-tablet, an e-paper based, water-resistant product to be used in hospitality. I was the main developer of the firmware running on the tablet: capturing user input, sending data to and from PC through wireless modules, displaying pictures on e-paper display, implementing simple configuration GUI and making sure device was power efficient with weeks of autonomy.

I was also the firmware developer for microcontrollers of various sensorics and industrial smart lighting projects. Most work was done on STM32 platform (arm-cortex-m3).

Part-Time Software Engineer **2006-2008**
Ultra and Telargo, Slovenia

BSP Engineer: Linux Kernel support Lite5200scmb (PowerPC) and DbAu1200 (MIPS) embedded platforms.

Development of complete support for sleep modes, and merging of it into mainline Linux and Das U-Boot. This made mpc52xx the second PowerPC platform to have suspend-to-RAM support in official Linux.

Other development and Linux upstreaming.

EDUCATION

OSCP - Offensive Security Certified Professional **2021**
Offensive Security

ISCED 5A (BSc/MSc equivalent) in Computer Science **2001-2008**
Faculty of Electronics and Computer and Information Sciences (FERI), University of Maribor, Slovenia

PUBLICATIONS

Rustproofing Linux **2023**
Author of blog post series

https://research.nccgroup.com/?p=18577

Caliptra Security Assessment **2023**
Consultant on the assessment

NCC_Group_Microsoft_MSFT283_Report_2023-10-04_v1.1.pdf

SKILLS

Software Development and Security

Languages	C, Rust, C++, Bash, Python, Java, PHP, Assembly on multiple architectures
Network	Wireshark, mitmproxy, Burp, nmap, dirbuster
Debugging	gdb, strace, ltrace, Frida, ASAN, KASAN, basic hardware debugging
Reverse Engineering	objdump, gdb, IDA, Ghidra, radare2
Operating Systems	Linux system, kernel and drivers, Android
Open Source	Was Linux kernel committer and maintainer of Kernel Janitors project
Electronics	Microcontrollers, communications busses, wireless