Joel Reymont

+41 78 242 30 00 joelr1@gmail.com Kyiv, Ukraine

Summary

Rust developer and embedded hacker, specializing in firmware development and reverse-engineering. Over 20 years of software development and technical project management experience.

Autodidact and a life-long learner. No problem is too small and no amount of prior information is too little. Will acquire any knowledge necessary to to tackle a problem and successfully solve it!

Experience

OCT 2024-PRESENT

Wrote a compiler from Ghidra Sleigh to Hex-Rays IDA Pro to generate C++ processor module code. Rewrote the compiler in OCaml and Rust to target the Binary Ninja interactive decompiler.

FEB 2022-OCT 2024

Developed a Yocto Linux (embedded Linux distribution) build to deploy a drone anonymization solution. Ported this solution from Windows to Linux. Learned the Forth language and used it for drone hacking. Wrote a binary protocol DSL in Lisp.

Built an onboard computer for DJI Enterprise drones to autonomously navigate out of the zone of active electronic countermeasures. Added capabilities to support an external ELRS (drone control) receiver, as well as the ability to connect an external GPS receiver.

Reverse-engineered the DJI Mavic 3E flight controller, and the DJI Payload SDK (PSDK), to enable onboard computer to control the drone under all kinds of conditions.

Reverse-engineered the DJI Mavic 3 user-space firmware and learned the internal DJI architecture, message bus and message format. Mastered Hex-Rays IDA Pro and Binary Ninja interactive disassemblers, ARM assembler and reconstruction of software models from machine code. Learned to identify structure layout, field mapping, FreeRTOS data structures and functions, etc.

Reverse-engineered the DJI RTK module to have the onboard computer spoof GPS coordinates when no GPS signal is present, and ensure control authority by the onboard computer.

DEC 2023-FEB 2024

Learned the internal architecture of Microsoft AirSim, as well as Unreal Engine 5, for kamikaze drone terminal acquisition and guidance in C++. Learned the Julia language and the ReinforcementLearning.jl toolkit. Made fixes to the latter.

JUL 2022-DEC 2023

Bought the Sensys R4 magnetometer, Radsys Zond Aero 1000 geo-radar, DJI Matrice 300 and 30 drones for mapping mine fields. Made several field trips to liberated areas of Ukraine to scan and map mine fields. Received a letter of commendation from the Kharkiv region government.

Went through a 2-month onsite State Emergency Service of Ukraine mine clearing course and acquired a Ukrainian deminer certification and license.

STEGOS AG — DEC 2017-JUL 2020

Founded Stegos AG in Zug, Switzerland. Raised 15 million USD for the Stegos blockchain and put together a team of developers, marketers and writers. Delivered the blockchain after 2 years of development. Learned blockchain marketing. Made all the possible mistakes. Learned to run a company, as well as the dangers of micromanagement. Pivoted. Killed the project after finding no uptake from users and running out of money.

AETERNITY — JUN 2017-DEC 2017

Joined Aeternity as their third Erlang developer. Stepped up to CTO. Put together and ran a remote development team. Projected for users a great image matching the development process. Raised 2 million USD in 2 days for a crypto project of my own (Stegos AG).

Projects

OPENPOKER

This is a scalable and fault-tolerant poker server written in Erlang. I started writing it back in 2004 and improved it over the years. Sold it to Electronic Arts (EA) to power EA World Series of Poker (WSOP). Contracted for EA to integrate and extend OpenPoker, as well as teach Erlang to the team.

COREAUDIO (HAL) DRIVER

The driver was to present a rack of Bruel&Kjaer LAN-XI data acquisition devices as a multi-channel sound card on Mac OSX.

Started with C++11, Boost and cpp-netlib, then switched to plain Objective-C since it was easier to debug and did not affect performance. Added recording and streaming capabilities to the driver, a System Preferences pane for configuration, as well as a test application.

LABVIEW DRIVER

A LabView interface for the Agilent 82357B USB/GPIB High-Speed Interface. Reverse-engineered a major chunk of LabView for Mac using the IDA Pro disassembler. Wrote a Mac USB device driver and the NI VISA Passport driver interface to sit on top of it. Spent close to a month on the iPhone production line in Shenzhen to troubleshoot various issues.

AD SERVER IN GO

Bidding for ads at various online ad exchanges for a private customer.

SCALABLE XMPP MESSAGING SERVER IN GO

Part of the Thomson Reuters Eikon product. Designed and implemented most of the server over the course of 9 months.

ISSUU

Lots of Erlang enhancements for the Issuu backend over the years.

OCaml implementation of the Issuu ad network.

MOZILLA

Worked on speeding up Firefox startup on the Mac. Wrote plenty of DTrace scripts over the course of my contract to identify bottlenecks and implement performance enhancements. Discovered that C++ static initialization significantly affects startup performance.

OTHER

Mac C++ device driver for a now defunct iTwin USB thumb stick.

Apache CouchDB Mac optimizations. Implemented a Erlang NIF backend for writing data to disk. Tested performance using DTrace.

Core Erlang enhancements. Ported the High-performance Erlang Compiler (HiPE) to the Mac. Extended the Erlang built-in database (Mnesia) to allow arbitrary storage strategies.

Live-blogging server in Erlang. Designed and implemented a high-performance scalable broadcast server. Scaled the server to hundreds of thousands of users on Amazon EC2 while keeping latency to a bare minimum.

Compiler from a SQL-like language to Erlang. Wrote the compiler in OCaml to generate Erlang code that targeted my Amazon DynamoDB wrapper for Erlang. The objective was to automatically enforce referential integrity while documenting the database schema and eliminating boilerplate code.

Port of a commercial Forth from Linux to Mac OSX.

Mac driver for a 24-core Forth CPU on a USB thumb stick by now defunct Intellasys.

WORTH NOTING

I successfully sold trading software for 1.5 years, remotely and strictly on commission. I can good at explaining issues and dealing with customers.