

Jasper Rühl

24.07.1998

jasperruehl@protonmail.com
linkedin.com/in/jasperruehl
github.com/haxkor

EXPERIENCE

Associate Engineer Cyber Analytics & Defense

Nov 2024 - present

fernao magellan

part of Cyber Analytics & Defense Team Splunk, Elastic, Kubernetes, Terraform

- + maintain and develop platform operation service (Kubernetes, Github Workflows)
- + develop checks against Elastic environments
- + write searches (SPL) and custom search commands (Python)
- + administered customers' Elastic Cloud Deployments using Terraform

Working Student

May 2023 - Oct 2023

Guardsquare

prototyped dependency detection feature for iOS AppSweep Python, C++

- + statically linked libraries are successfully detected
- + each symbol of the iOS app is matched to its origin (native or external library)
- + repository of libraries is automatically built and necessary information is extracted

Working Student

Mar 2022 - April 2023

Controlware

DevOps for SOC team's *TheHive* Infrastructure, creating various tools Python

- + Incident importer for several XDR platforms (MS Defender, SentinelOne, Cortex XDR)
- + IntelCaching that periodically parses info Wikipage for the AutoSOC/MailTextGenerator
- + MailTextGenerator that uses easily editable text templates and fills them with incident info
- + AutoSOC that automatically resolves trivial MS Defender incidents
- + introduced function decorator to make our python programs significantly more fault resilient

Research Assistant

Jan 2021 - Dec 2021

Fraunhofer AISEC

aided in development of an LLVM based MemSafety tool C++, Python

developed PoC's for anti-ControlFlowIntegrity exploitation techniques (DOP, COOP, LOP)

Student Tutor

WS21-22 / WS22-23

Chair of IT Security

hosted weekly tutorials on the IT Security lecture

- + presented and taught students about the fundamentals of IT Security
- + classes ranged from 5-25 students

PROJECTS

Congestion Control for Application Flows on Shared QUIC connections Master Thesis

SS24

explore methods to enable lower latency for realtime communication Go

- + add a stream prioritization mechanism to quic-go
- + high priority data (real time video) can be transferred while sending a file
- + github.com/haxkor/quic-go

Risotto: A DBT for Weak Memory Models Guided Research

published at ACM ASPLOS 2023

improved emulation of x86 `cmpxchg` instruction on ARM architectures C

- + introduced a new CAS instruction for QEMUs TCG
- + appropriate ARM instruction is generated
- + dl.acm.org/doi/10.1145/3567955.3567962

Raspberry Pi VPN Endpoint Interdisciplinary Project

SS23

Gürtler & Roach Cybersecurity

developed program to setup Raspberry Pi microcomputers

- + Pi's are a tailscale exit node
- + Access Control List ensures no outgoing connections from the Pi
- + *Ansible* is used to automatically setup the Pi

Forkever Bachelor Thesis

SS20

GDB-like debugger for binary exploitation Python, C

- + create copies of program-state by injecting `fork` system calls
- + memory can be visualised and manipulated with a hexeditor
- + Forkever is used by the students of the binary exploitation lab course
- + github.com/haxkor/forkever

EDUCATION

MSc. Informatics <i>Technical University Munich</i> focus on security and computer architecture Grade: 2.2	2021 - 2024
BSc. Informatics <i>Technical University Munich</i> Minor: Mathematics Grade: 2.2	2016 - 2020
BSc. Computer Science - Exchange Semester <i>Malaysia Multimedia University, Cyberjaya</i>	2018 - 2019

SKILLS

<i>Programming Languages</i>	Python, Go, C, C++, Bash
<i>Technologies</i>	Splunk, Elastic, Docker, QEMU, Kubernetes, Ansible, Terraform, git, Linux,
<i>Languages</i>	German, English C2, Malay A1, Thai A1

PERSONAL

MINGA Mentor for two international students at TUM	2017 - 2020
English tutor Assisted in teaching pupils	2013 - 2015