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 <small>Splunk, Elastic, Kubernets, Terraform</small>
+ 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 <small>Python, C++</small>
+ 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 <small>Python</small>
+ 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 <small>C++, Python</small>
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 <small>Masther Thesis</small>   SS24

explore methods to enable lower latency for realtime communication <small>Go</small>
+ 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 <small>Guided Research</small>   published at ACM ASPLOS 2023

improved emulation of x86 `cmpxchg` instruction on ARM architectures <small>C</small>
+ 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 <small>Interdisciplinary Project</small>   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 <small>Bachelor Thesis</small>   SS20

GDB-like debugger for binary exploitation <small>Python, C</small>
+ 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 2021 - 2024
Technical University Munich
  focus on security and computer architecture
  Grade: 2.2

BSc. Informatics 2016 - 2020
Technical University Munich
  Minor: Mathematics
  Grade: 2.2

Exchange Semester 2018 - 2019
Malaysia Multimedia University, Cyberjaya

Abitur 2016
CJD Königswinter
  Grade: 1.5

SKILLS

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

PERSONAL

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