AI, Artificial Intelligence, ML, Machine Learning, Pipelines, Docker, ML Ops

Krisztián **Szabó**

Master Student in Computer Science - Cyber security at UTwente

Enschede, open to relocate

(+31) 6 16853598 | developer.krisz+cv@gmail.com | v4k0nd | k-szabo-dev | V4K0ND

Technologies

Programming Languages	Python, Shell scripting, SQL, Golang, Java, Rust
Libraries/Frameworks	Torch, Numpy, Pandas, Hugging Face, Jupyter, Django, (Postgre|My)SQL
OS's	Windows, MacOS, Ubuntu ; and open to learning any *nix
Tools	Git, Docker, LaTeX, Android SDK
Languages	English (Cambridge C2), Hungarian (Mother tongue), Romanian

Education

University of Twente — *Enschede, Netherlands*

Msc. Computer Science - Cybersecurity Specialization — *2023 sept - Present*

- **Skills Gained**: Cybersecurity strategy development, MITRE ATT&CK, Ghidra, Advanced data analysis, Machine Learning in security, Privacy Enhancement, Risk Management, Natural Language Processing.
- **Projects**: Privacy preserving machine learning, IoT device traffic analysis, DNS Security Analysis, TLS Scanner and Analyzer

University of Twente — *Enschede, Netherlands*

Bsc. Technical Computer Science — *2017 jun - 2023 Apr*

- **Thesis title**: Morphing robust face recognition: Compared the resiliency of state-of-the-art face recognition methods to adversarial attacks.
- **Skills Gained**: Software systems design, algorithm optimization, functional programming, abstract algebra applications, shell scripting.
- **Projects**: AI algorithm to detect and filter out humans in wildlife camera

Experiences

Arise - Website, Linkedin — *Leiden, Netherlands / Remote*

ML Ops Engineer - Docker / Python / Django / Backend / Jira — *Nov 2022 - Present*

- Researched and implemented **ML Ops frameworks** (Weights and Biases, Mlflow, BentoML, ...) and built out **pipelines** for *versioning* and *serving* AI algorithms
- Restructured and implemented various **HuggingFace models** to be used at ARISE (GPU accelerated)
- Achieved an **89% accuracy in detecting humans** with an algorithm fine tuned for wildlife cameras, currently used to delete images of humans from wildlife camera datasets due to GDPR, which I have also converted to run on Snellius (Dutch Supercomputer)
- Configured and deployed an existing open source AI challenge app to automatically create leaderboard on specified metrics to integrate with the above mentioned frameworks
- Contributed to the development of AI algorithms which detect and identify species based on their genetic code for ARISE's platform

Local flower company

Website developer - HTML / CSS / JS / Python (Flask) / MySQL — *May 2019 - Present*

- Migrated website hosting from local company to hosterion for improved performance and reliability.
- Rewrote website using responsive design guidelines, generating a codebase with a static website generator.
- Developed frontend with HTML, CSS, and vanilla JavaScript, while backend utilized Python (Flask) for language switching and database fetching.

BestJobs — *Targu Mures, Romania*

Machine Learning Intern — *Jul 2019 - Aug 2019*

- Learned about and implemented Linear Regression Models
- Learning was largely based on Andrew Ng's coursera course named "Deep learning"

Projects

Self learning security

Security project *Since 2022*

- Deployed canarytokens on hosted server at **Hetzner** using https://github.com/thinkst/canarytokens, deployed a canarytoken instance to research itscapabilities.
- Installed and explored **Elasticsearch** to gain hands-on experience with its capabilities and filtering techniques
- Began using hardware keys across every online service

Home network upgrade

Home project *2020 - 2021*

- Completely upgraded my home networking stack to enable easier management/deployment for future home projects
- Purchased and deployed at home enterprise level networking equipment (Ubiquiti Edgemax and UniFi)
- Self hosting on Raspberry Pi's various software (HomeAssistant, Unifi Network Controller, PiHole)
- Configured VLAN for IoT devices

Self hostable and expandable IoT sensor home monitoring

University Group Project

- Developed a software which enables end users to self host and monitor sensor using MQTT
- Hardware used: Raspberry Pi, Arduinos with various sensors

Extracurricular Activities

Security / Privacy / OSINT

Interest

- Highly interested in and deeply passionate about security, privacy and OSINT
- Participated in and follow as many workshops / webcasts / conference as I can, my favourites being Blackhills Infosec, and PancakesCon

Twente Hacking Squad

Interest

- Part of the university hacking team, where Phd students present and walk through hacking methods in: Forensics, Reverse engineering, Pwning, Web hacking
- Some of the used software or techniques: **Ghidra**, **OWASP ZAP**, **SQLi**, **OWASP Top Ten**, **chainsaw** (windows forensics)
- Participated in multiple capture the flag (HacktheboxCTF, DownunderCTF, Cancakescon CTF, LA CTF) ctftime link