Bekhzod Anvarov

Cybersecurity Analyst
Network Intrusion Detection, Network Traffic Analysis, Anomaly Detection

Turin, Italy
virtsudo@proton.me | virtsudo.me | linkedin.com/in/virtsudo | github.com/virtsudo

SUMMARY

Computer Engineering graduate (MSc, Cybersecurity track) from Politecnico di Torino, focused on network intrusion detection. For my thesis I built an intrusion detection pipeline and tested it on real backbone traffic from 2011, 2016 and 2021. Open to junior roles and internships in cybersecurity, on-site or remote.

EDUCATION

Master of Science in Computer Engineering (Cybersecurity track)
Politecnico di Torino, 2026

Bachelor's Degree in Computer Engineering
Politecnico di Torino, 2022

RESEARCH EXPERIENCE

JEPA Representation Learning for Intrusion Detection on Real-World Drifting Network Traffic
Master's thesis, Politecnico di Torino, 2026
Supervisors: Prof. Guido Marchetto, Prof. Alessio Sacco, Cristiano Serra, MSc
Does a representation learned from unlabeled network traffic keep an intrusion classifier more accurate than raw flow features on traffic recorded years later?

- **Built** an intrusion detection pipeline in Python with flow preprocessing, a self-supervised JEPA model in PyTorch and four classifiers (logistic regression, decision tree, random forest, XGBoost), using real Internet backbone traffic from 2011, 2016 and 2021 (MAWIFlow benchmark with CICFlowMeter flow features and MAWILab labels).
- **Tested** each year's classifiers on every year. The representation made anomalous traffic easier to separate with a linear model but did not reduce the drop across years, and the labels changed meaning after 2011.
- **Audited** the benchmark. Showed that its scaling lost most of the resolution in the flow features and replaced it, and found that its published metrics contradict its published samples for two of the three years.

Stack: Python, PyTorch (CUDA), scikit-learn, XGBoost, Polars, NumPy, Matplotlib

PROJECTS

Deep Learning for Cybersecurity Labs
Stack: Python, PyTorch, Jupyter, Hugging Face
Built an FFNN for network intrusion detection and FFNN, RNN and GNN models for malware classification.
Fine-tuned BERT to analyze SSH logs and tag them with MITRE ATT&CK tactics.
GitHub: github.com/virtsudo/dl-cybersecurity-labs

SKILLS

Security tools (coursework): Wireshark, Nmap, Burp Suite
Programming & tools: Python, C/C++, SQL (MySQL, SQLite), Linux shell, Git/GitLab
Machine learning: PyTorch, scikit-learn, XGBoost, Hugging Face

RELEVANT COURSEWORK

- **Security Verification and Testing:** vulnerability assessment, penetration testing, static code analysis.
- **Information Systems Security:** attacks and risk analysis, PKI, IPsec, TLS, SSH, firewalls and IDS, VPNs.
- **Cybersecurity:** federated authentication (SAML, OIDC), Trusted Execution Environments, forensic analysis.
- **Data Protection, Privacy and Anonymity:** identity and access management, anonymization, re-identification.
- **AI and Cybersecurity:** deep learning, anomaly detection, traffic classification.
- **Cryptography:** AES, RSA, SHA-3, digital signatures, ECDH, cryptographic programming in C and Python.
- **Computer Network Technologies and Services:** IPv4/IPv6 network design, Internet routing, VPNs, MPLS.

LANGUAGES

Uzbek (Native), Russian (C1), English (B2), Italian (B1)