Kenneth Brezinski

Data Scientist

brezinkk@myumanitoba.ca
kbrezinski.github.io

Research and Industry Experience

09/22-12/22 **Visiting Researcher,** *National Institute for Informatics*, Tokyo, Japan

- Develop a graph autoencoder to detect network anomalies from backbone network traffic connecting Japanese Academic institutions to North America
- Automate firewall rule generation using node embeddings, GNNExplainer and explainable AI and scale the application to billions of network packets daily

05/22-08/22 **Data Scientist Intern,** *Microsoft*, Redmond, WA

- Worked with the Windows Defender for Endpoint Team on developing detectors to alert customers in the early stages of an exfiltration or ransomware attack
- Leveraged PySpark and cross-product telemetry to improve the signal-noise-ratio of the detector to 80% and to scale to billions of live customer events
- Coordinate with Security Engineers and Threat Researchers on identifying the most important precursors to malicious network connections

05/21-08/21 **Applied Research Scientist II Intern**, Amazon *Web Services*, New York, NY

- Worked with the Amazon GuardDuty threat detection research team on developing novel semi-supervised techniques to apply weak labelling to Linux binaries
- Established a working group of Security Engineers and SWE to coordinate and consult on the ongoing project.

10/19-10/22 **Research Intern Lead,** *Canadian Tire Corp.,* Winnipeg, MB

First authored six publications in close collaboration with an industry collaboration with Canadian Tire executives with a focus on Malware detection of enterprise security threats. Paper Highlights include:

- Working on an application of Graph-Attention Networks for the classification of malicious Windows OS and kernel API calls usage patterns using Pytorch (B7)
- Collect the process execution behavior of over 200 Malware and 500 Benignware in a custom sandbox environment (B3) to simulate a real host environment
- Use informational Complexity-based measure for improved training and generalization performance in Multi-layer Perceptrons (B6)
- Developed custom tokenizer and transformer model for detecting malicious stack traces based on Windows OS and kernel API calls; developed vocabulary using Huggingface and Pytorch based on Registry, File System and Thread activity to achieve 94+ F1 score (B4)
- Incorporated Kolmogorov Fractal Dimension in a Convolutional Neural Network architecture for the categorical classification of 9300+ malicious binaries into 25 Malware families with 96%+ macro accuracy using Tensorflow (C1)

Technical Skills

Languages	Python, Java, Matlab, LaTeX
Frameworks	Pytorch, Tensorflow, PySpark, Git, JAX, Flax, AWS (EMR)
MLops	Streamlit, Plotly, MLFlow, Kinesis
Malware Analysis	Static analysis tools such as PE View, Bintext, Dependency Walker, PEiD, OllyDBG, IDAPro; Dynamic tools such as Procmon, BurpSuite, Wireshark, API monitor; Splunk

Education

since 08/18 **Doctor of Philosophy,** *University of Manitoba*, Winnipeg, MB.
Electrical and Computer Engineering

01/16-09/18 **Master of Science,** *University of Manitoba*, Winnipeg, MB.
Civil Engineering

08/10-08/15 **Bachelor of Science,** *University of Winnipeg*, Winnipeg, MB.
Chemistry

Fellowships and Awards

2022 **Emily and Lynette Hain Graduate Engineering Scholarship**
2021-2022 **University of Manitoba Graduate Fellowship**
2021-2022 **Edward R. Toporeck Graduate Fellowship in Engineering**
2021 **Mitacs Globalink - JSPS**
2020 **A. Keith Dixon Graduate Scholarship in Engineering**
2021-2022 **Philip and Marjorie Eckman Scholarship in Engineering**
2019-2022 **Mitacs Accelerate – Ph. D**
2019 **NSERC – CGS M**
2016 **Mitacs Accelerate – M.Sc.**

Journal and Book Publications

B7 **Graph-Oriented Modelling of Process Event Activity**
Brezinski, K., Ferens, K., 2023. Transactions on Computational Science & Computational Intelligence. Springer Nature (book); under consideration

J2 **Metamorphic Malware and Obfuscation - A Survey of Techniques, Variants and Generation Kits,** Brezinski, K., Ferens, K., 2022. Security and Communications (journal); submitted, under review

B6 **Incorporating Topological Complexity into a Multilayer Perception,** Brezinski, K., Ferens, K., 2022. Transactions on Computational Science & Computational Intelligence. Springer Nature (book); accepted, in press

B5 **Classifying SARS-CoV-2 and Common Co-infections from Genome Assemblies,** Mohaimen Rahman**,** Brezinski, K., Ferens, K., 2022. Transactions on Computational Science & Computational Intelligence. Springer Nature (book); accepted, in press

B4 **Transformers – Malware in Disguise,** Brezinski, K., Ferens, K., 2021. Advances in Security, Networks, and Internet of Things, In book: Transactions on Computational Science & Computational Intelligence Chapter. Springer Nature (book)

B3 **Sandy Toolbox: A Framework for Dynamic Malware Analysis and Model Development,** Brezinski, K, Ferens, K., 2021. Security & Management (SAM'21). Advances in Security, Networks, and Internet of Things. Springer Nature (book)

B2 **An Adaptive Tribal Topology for Particle Swarm Optimization,** Brezinski, K, Ferens, K., 2020. Advances in Artificial Intelligence and Applied Cognitive Computing. Springer Nature (book)

J1 **Population Based Equilibrium in Hybrid SA/PSO for Combinatorial Optimization,** Brezinski, K, Ferens, K., 2020. International Journal of Software Science and Computational Intelligence (journal)

B1 **Cognitive Hybrid PSO/SA Combinatorial Optimization,** Brezinski, K, Ferens, K., 2020. Advances in Security, Networks, and Internet of Things. Springer Nature (book)

For a full list of my refereed works, please visit by personal ResearchGate or my personal website.

Conference Publications

C2 **Complexity-Based Lambda Layer for Time Series Prediction,** Brezinski, K., Ferens, K., 2021. IEEE Congress on Evolutionary Computation (oral)

C1 **Complexity-Based Convolutional Neural Network for Malware Classification,** Brezinski, K, Ferens, K., 2020. International Conference on Computational Science and Computational Intelligence (oral)

Students Supervised

Undergrad **Michael Guevarra,** University of Manitoba, 2019

Committees, Positions and Volunteering

since 05/20 **Reviewer**, International Journal of Software Science and Computational Engineering

09/18 – 05/21 **Student Peer Mentor**, University of Manitoba Students' Union

01/19 – 01/21 **Language Partner Volunteer**, English Language Center

09/19 – 09/20 **Faculty of Science Mentor**, Faculty of Science

04/19-12/19 **Language Exchange Program Volunteer**, International Center

06/19 – 01/21 **President and Founder,** University of Manitoba Engineering Masters (UMEM)

since 06/20 **Personal Disaster Response Volunteer,** Canadian Red Cross

11/16-11/17 **Vice-President,** University of Manitoba Water and Environmental Foundation (UMWEF)