Kenneth Brezinski

Curriculum Vitae

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

05/22-08/22 **Data Scientist Intern,** *Microsoft*, Redmond, WA
- Worked with 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 labels 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
- Working on an application of Graph-Attention Networks for the classification of malicious Windows OS and kernel API calls usage patterns using Pytorch
- 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)

- Improved the time series prediction for recurrent neural networks using variance fractal dimension as a preprocessing lambda layer in Pytorch (C2)

since 09/18 **Graduate Researcher,** *University of Manitoba,* Winnipeg, MB

- Authored a python package which extracts information related to Registry, File System, Network and Process activity, and tracks the spawn process behavior and propagation of malware for collection (B3) using Networkx and Pandas
- Implemented a parameter-free particle swarm optimization utilizing tribal members (B2); coupled simulated annealing and particle swarm optimization for combinatorial optimization (B1, J5) using Matlab

Teaching Experience

since 08/16 **Teacher's Assistant**, *University of Manitoba*, Winnipeg, MB

- Worked as a Teacher's Assistant for over 21 appointments for 9 unique courses the Departments of Civil, Electrical and Computer, Mechanical, P2E2 and Chemistry
- Created course materials, guest lectured, and supervised students in the laboratory

08/17-04/18 **Engineering Graduate Student Tutor,** *Academic Learning Center***,** *University of Manitoba,* Winnipeg, MB

- Proofread manuscripts, thesis dissertations, award applications and course deliverables for graduate students in the department of Biosystems, Civil, Electrical and Computer Engineering

Technical Skills

Languages	Python, Java, Matlab, LaTeX
Frameworks	Pytorch, Tensorflow, PySpark, Git, JAX, Flax, AWS (EMR)
Visualization	Streamlit, Plotly, Flask, Django, MLFlow
Reverse Engineer	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

J7 **Metamorphic Malware and Obfuscation - A Survey of Techniques, Variants and Generation Kits,** Brezinski, K., Ferens, K., 2022. Cybersecurity (journal); submitted, under consideration

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, In book: Transactions on Computational Science & Computational Intelligence Chapter. 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)

J6 **Ozonation of natural organic matter and aquatic humic substances: the effects of ozone on the structural characteristics and subsequent trihalomethane formation potential,** Sadrnourmohamadi, M., Brezinski, K, Gorczyca, B., 2020. Water Quality Research Journal of Canada (journal)

J5 **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 (book)

J4 **Multi-spectral characterization of natural organic matter (NOM) from Manitoba surface waters using high performance size exclusion chromatography (HPSEC),** Brezinski, K., Gorczyca, B., 2018. Chemosphere (journal)

J3 **An overview of the uses of high-performance size exclusion chromatography (HPSEC) in the characterization of natural organic matter (NOM) in potable water, and ion-exchange applications,** Brezinski, K., Gorczyca, B., 2018. Chemosphere (journal)

J2 **Ion-Exchange for Trihalomethane control in potable water treatment – A municipal water treatment case study in Rainy River, Ontario, Canada,** Brezinski, K, Sadrnourmohamadi, M., Gorczyca, B., 2018. Water Quality Research Journal of Canada (journal)

J1 **Effect of total organic carbon and aquatic humic substances on the occurrence of lead at the tap.** Winning, L.D., Gorczyca, B., Brezinski, K., 2017. Water Quality Research Journal of Canada (journal)

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 04/17 **Reviewer**, Journal of Desalination and Water Treatment

since 11/17	**Reviewer,** Journal of Water Science and Technology
since 05/20	**Reviewer**, International Journal of Software Science and Computational Engineering
09/18 – 05/21	**Student Peer Mentor**, University of Manitoba Students' Union
since 01/19	**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
since 06/19	**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)