Benjamin Liu

U.S. Citizen
Lexington, Massachusetts
☎ 339-240-2265 ✉ benliu0001@gmail.com github.com/benliu0001

Education

University of Toronto **September 2021 - December 2025**
Honors Bachelor of Science, Computer Science *Toronto, Canada*

Relevant Coursework

- **Computer Vision**
- **Deep Learning**
- **Algorithms**
- **Software Engineering**
- **Databases**
- **Operating Systems**
- **Data Structures**
- **Multivariable Calculus**
- **Probability and Statistics**

Projects

Deep Learning Side Channel Attack | *Python, PyTorch, Numpy, Scipy* **January 2024 – Present**

- Developed LSTM, Resnet, and Transformer models to perform a deep-learning side channel attack on an STM32 microcontroller running TinyAES.
- Assumed profiling attack paradigm to collect training data using a microcontroller and oscilloscope to capture power traces of plaintext-ciphertext pairs.
- Researched various methods to extract features from power traces and optimize the models to improve the attack's success rate.
- Recruited, organized, and led a team of 6 other students to work on the project, and managed the project's timeline.
- Presented weekly to introduce essential concepts in hardware security to team members.

MIT Embedded Security CTF | *C, Python* **February 2020 – August 2020**

- In a team of 4, designed and implemented a secure firmware update system for an IoT device using C and Python.
- Based on MITRE eCTF competition, assumed man in the middle paradigm to attack other teams by exploiting vulnerabilities in their firmware update systems using python scripts, earning 3rd place in the competition.
- Utilized an HMAC to authenticate users, AES, RSA, and SHA to encrypt firmware, and a Stream Cipher for key generation.
- Received intensive instruction from leading researchers on embedded software, computer architecture, memory management, assembly, cryptography, security, interface analysis, and bit manipulation.

Mental Health Sentiment Analysis | *Python, PyTorch, Hugging Face, Pandas, AWS* **January 2024 – April 2024**

- Trained a BERT model to analyze the sentiment of users' responses to mental health assessment questions.
- Used Pandas to clean and preprocess Hugging Face datasets to fine tune the BERT model to achieve 60% accuracy.
- Worked with startup to develop a mental health assessment platform, taking into account use cases and user experience.
- Deployed Postman API to AWS and then Railway to allow for other teams to access the model.

Eedi Assessment Analysis | *Python, PyTorch, NumPy, SciKit Learn* **August 2023**

- Developed a suite of Machine Learning models to analyze and predict the relationship between provided student answers and future performance in an online learning assessment system.
- Compared validation accuracies for Logistic Regression, PCA Matrix completion, and Autoencoder models to decide on a best approach, reaching 75% accuracy.
- Leveraged augmentations such as regularization penalties to raise the models' accuracies and better generalize predictions.

Conspiracy Analysis in Social Media | *Python, Flair, Pyplot* **December 2021**

- Utilized Reddit API in Python to collect data from various subreddits to analyze the spread of conspiracy theories surrounding COVID-19.
- Used Flair for frequency analysis to categorize posts and comments into different conspiracy theories and graphed the spread of each theory over time using pyplot.

Technical Skills

Languages: Python, Java, C/C++, SQL, Assembly Languages
Developer Tools: Shell Scripting in Linux, Git, Agile Methodologies, Google Cloud CLI, Docker, AWS
Technologies/Frameworks: SQL, Numpy, OpenCV, PyTorch, Pandas, Pyplot, Scipy