Research Statement

I aspire to pursue Computer Security as an enduring academic subject. In particular, I am interested in studying **Anti-censorship Internet Measurement**, **Secure Designs for Infrastructure Systems**—such as **Supervisory Control and Data Acquisition** (SCADA), **Cloudless Computing**, and **Internet of Things** (IoT)—and **Privacy-Preserving Adversarial Methods** to defend against privacy violation attacks from commercial Machine Learning (ML) models. These topics captivate me for they directly adhere not only to my technical interest in building reliable systems, but also address the challenges of information freedom and data privacy that have been central to my commitment to employ computing as a means towards the betterment of societal well-being.

Research Experiences: In January of 2024, I was offered the opportunity to work under the supervision of doctoral student **Patrick Kon** and **Prof. Ang Chen** during my third year of undergraduate studies at the University of Michigan (UMich). Currently, we are co-leading a project titled ***"Unveiling the Nexus: Harnessing IoT Ecosystems for Evading Internet Censorship"***, presented at the 2024 UROP Spring Symposium at UMich. In this fruitful collaboration, I primarily focused on devising a research proposal utilizing the heterogeneous architectures of IoT to design and implement a distributed system topology, aiming to fully utilize the abundant amount of computational power as edge computers and IPv6 spaces to fragment and obfuscate packet-level network traffic.

In contrast to traditional circumvention techniques such as the centralized Virtual Private Network (VPN) and the decentralized Tor Project based on distributed systems formed by volunteers' personal computers, our usage of an IoT-based distributed network could complicate the **Deep Packet Inspection** (DPI), **Device Fingerprinting** (DFP), and other traffic-correlation analyses sanctioned by nation-states. We hypothesized possible attack models based on a comprehensive review of prior works ranging from ML classifiers deployed to detect high-throughput obfuscated traffic [1; 2] to known techniques utilized by nation-states to fingerprint possible VPN tunnels [3]. With our proposed low-computational-power ***Unreadability Algorithm***—which processes and fragments traffic into ASCII-unreadable packets at the bit level—and routing the fragmented packets through a network of IoT devices via a **Distributed Hash Table (DHT)**, existing surveillance techniques are theoretically rendered obsolete.

With promising signs of success even with only naive byte-padding schemes on the packets without fragmentation, we plan to publish *Nexus* at the annual **Privacy Enhancing Technologies Symposium (PETS) this coming year** after completing our final tests, introducing it as the first of its kind in the scene of censorship circumvention research.

Future Research Agenda: First and foremost, **my core agenda is to ensure that future technology serves the betterment of human rights**. However, to be specific:

Decentralized Censorship Circumvention: I plan to base my future Censorship Circumvention research direction on the argument stated in the paper, *"The Parrot Is Dead"*, by **Prof. Amir Houmansadr** et al. as a key premise. In the paper, the authors demonstrated that obfuscation by mimicry—hiding a prohibited stream of traffic as if it's a regular service such as Skype—is a fundamentally flawed approach [4]. As a doctoral researcher, I aim to address this concern by developing novel circumvention models based on distributed systems. One example would be to further my design of utilizing the sheer number of IoT devices in the wild for network routing purposes with **fragmented packets sent in parallel (parallelism)**, paralyzing real-time packet-pair or traffic correlation surveillance techniques without significant performance cost.

Privacy-preserving Methods Against ML Models: I look forward to expanding upon the project, *"Glaze"*, by **Shawn Shan** and **Prof. Ben Zhao** et al., where they utilized a data augmentation technique that applies imperceptible perturbations to artists' images and protects them from diffusion-based text-to-image models from mimicking their unique artistic styles [5]. Projects like this prompt me to further explore **ML masking or watermarking techniques** as defensive mechanisms for individuals subjected to unsolicited ML training data collections.

IoT Security and Novel Applications: I want to investigate the security of IoT in government, infrastructural, and commercial spaces. For example, despite extensive research efforts in Smart City initiatives, serious embedded-level protocol vulnerabilities still plague government and civilian users [6]. Another overlooked cybersecurity area in this domain is the vulnerability of military-related IoT devices, namely the **Internet of Battlefield Things** (IoBT) and **Internet of Medical Things** (IoMT), which are subjected to heavy interference during cyberwarfare and on battlefields [7].

References

[1] R. Perdisci, T. Papastergiou, O. Alrawi, and M. Antonakakis, "IoTFinder: Efficient large-scale identification of IoT devices via passive DNS traffic analysis," in *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, (Genoa, Italy), 2020.

[2] R. Li and et al., "DeviceRadar: Online IoT device fingerprinting in ISPs using programmable switches," *IEEE/ACM Transactions on Networking*, 2024.

[3] D. Xue, R. Ramesh, A. Jain, M. Kallitsis, J. A. Halderman, J. R. Crandall, and R. Ensafi, "OpenVPN is open to VPN fingerprinting," in *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)*, USENIX Association, 2022.

[4] A. Houmansadr, C. Brubaker, and V. Shmatikov, "The parrot is dead: Observing unobservable network communications," in *2013 IEEE Symposium on Security and Privacy*, pp. 65–79, 2013.

[5] S. Shan and et al., "Glaze: Protecting artists from style mimicry by text-to-image models," in *Proceedings of the 32nd USENIX Security Symposium*, 2023.

[6] B. Babu, T. Ijyas, P. Muneer, and J. Varghese, "Security issues in SCADA-based industrial control systems," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, (Abha, Saudi Arabia), pp. 47–51, 2017.

[7] O. Westerlund and R. Asif, "Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things," in *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*, (Muscat, Oman), pp. 1–10, 2019.