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 levitation towards the betterment of societal well-being.

Previous Research: During the winter of my 3rd year of undergraduate studies at the University of Michigan (UMich), I was offered the opportunity to work under the supervision of doctoral student **Patrick Kon** and **Prof. Ang Chen**. We co-led a project titled ***'Unveiling the Nexus: Harnessing IoT Ecosystems for Evading Internet Censorship,'*** presented at the 2024 UROP Spring Symposium at UMich [1]. In this fruitful collaboration, we primarily focused on devising a research proposal utilizing the heterogeneous architectures of IoT, which has witnessed exponential growth over the past eight years [2; 3] and introduced complex security concerns with great potential for future studies [3–7]. I was responsible for designing and implementing the topology of the IoT system's distributed framework, which could utilize the redundant amount of computability as edge computers and IPv6 spaces to fragment and obfuscate packet-level network traffic. With this design, we aimed to introduce IoT devices into the scene of internet censorship circumvention research.

Distinguished from 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 the all-inclusive review of pieces of literature ranging from ML classifiers—e.g., **AdaBoost and Support Vector Machines (SVMs)**— deployed to detect high-throughput obfuscated traffic [3; 5; 6; 8; 9] to known techniques utilized by nation-states to fingerprint possible VPN tunnels [10; 11]. With our proposed low-computational-power **Unreadability Algorithm**—which processes and fragments traffic into ASCII-unreadable packets at the bit level—and route the fragmented packets through a network of IoT devices via a **Distributed Hash Table (DHT)**, all of these surveillance techniques would be theoretically rendered obsolete.

Besides the model of circumvention, we also discovered **kernel-level vulnerabilities** for physical and over-the-air hacking: the lack of usage of eFuse to protect from firmware downgrade attacks [12]; vulnerabilities related to UART port hot-wiring [13]; REST API-based control hijacking [14; 15]. These findings unveiled IoT devices' alarming yet prolonging state, where malicious firmware and unauthorized software can be injected with very few defenses.

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

Decentralized Censorship Circumvention: I plan to base my futrue Censorship Circumvention research on the rationale stated in an article by **Prof. Amir Houmansadr** et al. [16] as the ground

truth, in which the authors contemplated that seeking obfuscation methods beyond mimicry but a higher layer of covert communication, i.e., network binary data into a sound wave, is direly essential. 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)**, rendering real-time packet-pair or traffic correlation surveillance techniques obsolete without significant performance cost.

Privacy-preserving Methods Against ML Models: I look forward to expanding upon the work by **Shawn Shan** and **Prof. Ben Zhao** et al. [17], for which 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. I would also like to explore **ML masking or watermarking techniques** further as defensive mechanisms for the privacy of individuals subjected to ML training data collections.

IoT Security and Novel Applications: I want to explore IoT security of governmental, infrastructural, and commercial venues. For instance, despite extensive research efforts in Smart City initiatives, severe embedded-level protocol vulnerabilities still haunt governmental and civilian users [18; 19]. 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 [20].

References

[1] P. Kon, Y. Shi, and W. Ashley, "Unveiling the nexus: Harnessing IoT ecosystems for evading internet censorship," in *University of Michigan UROP Symposium 2024*, University of Michigan, 2024.

[2] S. Kumar and et al., "Internet of things is a revolutionary approach for future technology enhancement: A review," *Journal of Big Data*, vol. 6, no. 1, 2019.

[3] S. Herwig and et al., "Measurement and analysis of hajime, a peer-to-peer IoT botnet," in *Proceedings of the 2019 Network and Distributed System Security Symposium*, 2019.

[4] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast internet-wide scanning and its security applications," in *Proceedings of the 22nd USENIX Security Symposium (USENIX Security 13)*, pp. 605–620, 2013.

[5] W. Jo, S. Kim, C. Lee, and T. Shon, "Packet preprocessing in CNN-based network intrusion detection system," *Electronics*, vol. 9, no. 7, 2020.

[6] R. R. Chowdhury and P. E. Abas, "A survey on device fingerprinting approach for resource-constrained IoT devices: Comparative study and research challenges," *Internet of Things*, vol. 20, 2022.

[7] J. Hong, A. Levy, L. Riliskis, and P. Levis, "Don't talk unless i say so! securing the internet of things with default-off networking," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018.

[8] 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.

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

[10] 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.

[11] J. Beznazwy and A. Houmansadr, "How china detects and blocks shadowsocks," in *Proceedings of the ACM Internet Measurement Conference*, Association for Computing Machinery, 2020.

[12] A. Knapp, E. Wamuo, M. A. Rahat, S. Torres-Arias, G. Bloom, and Y. Zhuang, "Should smart homes be afraid of evil maids? identifying vulnerabilities in IoT device firmware," in *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)*, (Las Vegas, NV, USA), pp. 467–473, 2024.

[13] I. Clinton, "A survey of various methods for analyzing the amazon echo," 2016.

[14] A. Mendoza and G. Gu, "Mobile application web API reconnaissance: Web-to-mobile inconsistencies & vulnerabilities," in *2018 IEEE Symposium on Security and Privacy*, (San Francisco, CA, USA), pp. 756–769, 2018.

[15] M. Ibrahim, Z. Kasiran, and M. A. M. Ariffin, "API vulnerabilities in cloud computing platform: Attack and detection," *International Journal of Engineering Trends and Technology*, vol. 1, pp. 8–14, Oct 2020.

[16] 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.

[17] 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.

[18] J. Ahamed and A. V. Rajan, "Internet of things (IoT): Application systems and security vulnerabilities," in *2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, (Ras Al Khaimah, United Arab Emirates), pp. 1–5, 2016.

[19] 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.

[20] 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.