Research Statement

Diwen Xue, PhD Candidate, University of Michigan

The security of Internet communication has always hinged on two questions: What can adversaries on the Internet really do, and how can we sustain meaningful security as those capabilities change? My research tackles these questions empirically—conducting Internet measurements at scale, using those observations to refine and update threat models, and building countermeasures based on what the evidence shows. Over the past decade, significant shifts in the threat landscape have positioned network infrastructure itself as a potential adversary. Rapid advances and commoditization of networking technologies such as Deep Packet Inspection (DPI), combined with loosened regulations like the repeal of net neutrality, have granted the network with unprecedented capability and freedom to inspect, modify, throttle, or even hijacks the traffic it transports at fine granularity and line rate. What were once neutral "dumb pipes" have evolved into capable and sometimes adversarial network intermediaries—ranging from malicious middleboxes and rogue ISPs to compromised routers and untrusted transit networks—all creating new threats that increasingly erode user privacy, autonomy, and overall trust in connectivity.

This shifting threat landscape motivates my research vision: to build the next generation of secure and private network ecosystems that safeguard users' communication on this increasingly adversarial Internet. Realizing this vision broadly involves two complementary efforts: modeling how network intermediaries behave today and how they might evolve in the future, and developing principled countermeasures that are sound in theory and deployable at scale. To this end, I develop frameworks, perform large-scale empirical measurements, and build privacy-focused systems that empower both users and researchers. These efforts typically sit at the intersection of **Security & Privacy and Systems & Networks**, structured around four main research Thrusts:

1. Characterizing Emerging Threats from Network Intermediaries (IMC'21, IMC'22, Preprint'A)
- Measuring traffic interferences (e.g., interception, throttling) at global scale.
- Developing scalable systems to characterize network intermediaries responsible for such interference.

2. Principled Approach to Network Traffic Obfuscation (USENIX'22, USENIX'24A, NDSS'25, FOCI'25)
- Evaluating state-of-the-art obfuscation techniques against emerging traffic fingerprinting attacks.
- Developing novel formalisms to reason about the distinguishability of network protocols.

3. Scalable, Privacy-preserving Traffic Analysis Infrastructure (USENIX'22, Preprint'B)
- Building analytical frameworks that empower researchers to extract security insights from ISP-scale user traffic with strict privacy requirements.

4. Empirical Evaluation of Privacy-Enhancing Technology (NDSS'22, PETS'24, USENIX'24B, PETS'25)
- Assessing the security, usability, and challenges of privacy-enhancing tools in adversarial contexts.

A guiding principle in my research is to choose pragmatic problems—problems that are not only academically appreciated but also directly serve the security and privacy needs of real people. Pursuing such problems grants me the privilege to collaborate both within academia and beyond it, working alongside everyday users, developers of privacy-enhancing tools, and engineers from across the tech industry such as Merit Network and Cloudflare. Such collaborations, while taking efforts to build and maintain, are crucial for translating academic insights into meaningful impacts beyond the research community. The value of this approach has been recognized through multiple honors, including the First Prize of the Internet Defense Prize (the most prestigious award in network security), the Distinguished Paper Award at USENIX Security, First Place at the CSAW Applied Research Competition, and the Towner Prize for Distinguished Academic Achievement. My line of research has received extensive media attention, with features in Ars Technica, Reuters, and a front-page story in the New York Times.

1 Measurement and Characterization of Network Intermediaries

Although the layered network stack provides an "end-to-end" abstraction of Internet communication, in reality, every bit of traffic traverses a chain of network intermediaries—access points, edge routers, transit ISPs, Internet exchange points, and middleboxes and firewalls along the network path—each with its own policies and incentives. Advances in networking technology over the last decades granted these intermediaries the computing power to not only forward traffic but also to actively interfere with it. My early research efforts focused on modeling the threats from network intermediaries by measuring the effects of such interferences on users' traffic and identifying the intermediary devices responsible. In 2021, I investigated the practice of bandwidth throttling on Russia's Internet [1]. Throttling is an elusive form of interference, difficult to measure and even harder to attribute. For this, I developed novel measurement techniques to differentiate imposed throttling from benign network congestion or natural jitter, providing the first documented evidence of large-scale, targeted throttling by network intermediaries. A significant finding of the study was the uniform throttling behavior across thousands of privately-owned ISPs, indicating a cluster of middleboxes performing coordinated interferences. For this, I led a two-year measurement effort to locate and characterize these throttling middleboxes, which were largely unknown to the world before our work. I designed and carried out remote measurements to characterize their architecture, capabilities, and deployment scope [2]. In particular, I devised a novel fingerprinting method based on side channels from IP fragmentation, successfully identifying over 6,000 such middleboxes across 650 Russian networks and alerting the public to the significant privacy and security implications from such deployments.

Previous work on measuring network intermediaries, including our own efforts in [1,2], have mainly tackled the problem on a case-by-case, ad-hoc basis. Such approach highlights a significant gap in our current capability to measure the Internet: existing measurement tools like Nmap or ZMap were designed to probe end-hosts, leaving network intermediaries like firewalls largely invisible to these standard scanning methods. To bridge this gap, I developed *dMAP* [12], a novel, generalizable measurement framework specifically designed for performing active reconnaissance on network intermediaries at the Internet scale. *dMAP* works by fuzzing network protocols (TCP/IP) to generate ambiguous probing traffic—traffic with multiple possible interpretations whose handling often varies across implementations—and then using how network intermediaries resolve such ambiguities as their behavioral fingerprints to identify and characterize them. Measuring the global Internet with *dMAP* advanced our community's knowledge, transparency, and accountability regarding the deployment of these traffic-interfering intermediaries.

Future work I aim to expand this Thrust both in scope and toward continuous, longitudinal measurements of network interference. Most current measurement efforts focus on interference within the traditional TCP/HTTP(S) stack. Yet, emerging protocols (QUIC/ECH/PQC), transports (satellite networks, 5G), and addressing schemes all present new security challenges to deal with and demand new ways to empirically understand the shifting attack surface. But even for common interference like IP blocking, we still struggle with basic questions that industry cares the most like "How can we reliably detect when our server IP is blocked from a particular network?" Answering these requires continuous, longitudinal measurements paired with robust alerting systems.

An overarching goal of this Thrust is to *truly understand what happens to user traffic as it moves across networks*. The Internet's vast size, multitude of stakeholders, and routing complexity make such measurements challenging even in the absence of intentional interference. What we need is a more expressive form of Traceroute, one capable not only of enumerating the hops traffic passes through, but also characterizing each intermediary by device type, vendor, and behaviors (e.g., what kind of router is running on which hop). Future work will advance this empirical science of measuring intermediaries—interfering or otherwise—by generalizing methodologies underlying *dMAP* and applying them to map out the Internet infrastructure at scale.

2 Principled Approach to Network Traffic Obfuscation

Targeted network interferences rely fundamentally on distinguishing specific classes of traffic from others on the network. While encryptions protect the cryptographic secrecy of packet payloads, they were never intended to obscure all characteristics of the traffic—such as packet timing, sizes, or other metadata. The ability to deduce information from metadata, in order to distinguish one encrypted flow from another, is known as *traffic analysis*. Efforts to counter such analysis are called *traffic obfuscation*. In this Thrust, my research 1) identifies precisely what features enable analysis to distinguish classes of traffic; 2) evaluates existing obfuscation schemes in realistic scenarios; and 3) moves toward designing principled and theoretically grounded obfuscation techniques.

One class of traffic that often faces discrimination and interference is from tunneling protocols, such as VPN/Proxy, which encapsulate user data within encrypted tunnels. Such encapsulation reduces the visibility and control that ISPs and enterprise firewalls have over user traffic, motivating such intermediaries to block or throttle tunneling protocols to discourage their use. In response, a growing class of *obfuscated* tunneling protocols has gained traction, each deploying various ad-hoc obfuscation methods to avoid detection. As part of my dissertation, I have led a line of research [3-6] examining in-the-wild obfuscation schemes from the perspective of an adversarial network intermediary. In [3], for example, I developed a two-phase analysis framework that combines passive filtering with active probing, along with novel fingerprints targeting VPN traffic. Applying the framework to major obfuscated VPN services revealed that more than 80%—despite marketing claims of being "invisible" or "undetectable"—could be detected with alarming precision. In addition to highlighting weaknesses in existing obfuscation schemes, these findings raise serious concerns for users relying on tunnels for privacy and security.

A major contribution of my work in this domain was the discovery of a class of traffic fingerprints inherent to all proxying and tunneling traffic, *agnostic* to the specific obfuscation protocol used. This finding challenged a prevailing strategy in the obfuscation community—that of continuously creating new (imperfect) obfuscation protocols to outpace advances in traffic analysis. My work showcasing shared vulnerabilities [4] proved such a strategy may be less effective than previously assumed, prompting extensive discussion and rethinking of design principles among obfuscation developers. In more recent studies, we examined traffic features that are often overlooked in obfuscation schemes like inter-arrival times [5] and congestion control behaviors [6], demonstrating their discriminative power for traffic analysis and further revealing gaps in existing obfuscation protocols.

A guiding principle in my traffic obfuscation research is *practicality*. Meaningful research in this field should not just identify vulnerabilities but demonstrate practical exploits under realistic operational constraints faced by network intermediaries. Therefore, for this line of work, I always collaborated with actual ISPs to deploy and evaluate attacks on real user traffic at Internet gateways, simulating the threat models posed by real-world network intermediaries informed by previous measurements (e.g., those in Thrust 1). Such approach yields more convincing evidence of the feasibility of the attacks and provides a stronger call to action for developing principled obfuscation protocols.

Future work The current state-of-the-art for evaluating obfuscation protocols (including my own work [3-6]) is to define a specific attack and measure how detectable each protocol is under that attack. This approach, however, has two major limitations. First, resistance to a particular attack does not guarantee overall indistinguishability. Moreover, it confines the field of traffic analysis and obfuscation to an ongoing "arms race", where the success of obfuscation is judged based on its immunity against the latest detection techniques, rather than by any inherent obfuscation quality. My future research aims to develop novel formalisms to evaluate obfuscation without making assumptions about the attacker's specific detection technique or statistical model. Currently, I'm leading a collaborative effort between U-M/ASU to leverage information theory to reason about traffic distinguishability in order to build obfuscations that genuinely have a lasting advantage even as traffic analysis continues to evolve.

The long-term vision for this line of research is to answer fundamental scientific questions about what it takes to truly be indistinguishable from the Internet *background*—all concurrent traffic flows observed by a network intermediary. Consider an obfuscation protocol that randomizes every traffic characteristic (e.g., packet sizes, timing, etc). Such obfuscation may defeat certain traffic analysis attacks like website fingerprinting, but it cannot hide the act of obfuscation itself, since purely random behavior stands out from typical network traffic. But what defines "normal" on the scale of today's Internet? My ongoing work explores how to construct mathematical representations capturing the stochastic characteristics of traffic flows over time, and learns a background traffic profile empirically from the massive amount of traffic observed at Internet gateways.

3 Scalable, Privacy-preserving Traffic Analysis Infrastructure

Despite decades of progress in applied cryptography and the growing adoption of HTTPS, a substantial volume of Internet traffic today still lacks proper transport-layer encryption, threatening the privacy of end-users and the integrity of the networks they inhabit. Security researchers need to characterize such unencrypted traffic to answer questions like, "What types of applications continue to transmit data without proper encryption?" However, such investigations face an ethical dilemma: to understand and mitigate these threats, researchers often have to examine *the very information they seek to protect*, such as sensitive user data exposed in plaintext. Such tension raises ethical concerns and stalls research efforts to understand the threats posed by unencrypted traffic.

This privacy dilemma inspired the development of our traffic analysis framework, *CryptoSluice* [13]. *CryptoSluice* is explicitly designed with the understanding that unencrypted traffic can (and likely will) contain sensitive information like PII that must never be viewed by humans or stored in persistent memory. At the same time, our framework still aims to grant researchers with meaningful visibility into packet payloads—in an anonymized and aggregated form—to understand the nature of the violating traffic. To achieve this, *CryptoSluice* shifts away from traditional, flow-based analysis model to a content-centric approach, where fixed-size payload segments serve as the primary unit for accumulating traffic insights. Using a multi-stage sifting pipeline inspired by malware detection, our framework incrementally filters gateway-volume traffic (> 50 Gbps) in real time and automatically isolates patterns that are most relevant to security yet *do not trace back to any specific user*. Our framework was deployed at a major ISP for one month, where it highlighted instances of privacy leaks, such as PII and user location transmitted in plaintext, and attributed these leaks to the specific applications responsible.

Future work *CryptoSluice* marks the beginning of a multi-year, cross-institutional collaboration to build traffic analysis infrastructure at Internet gateways for extracting security insights through measurements on aggregated real-user traffic. Most of the past vulnerabilities were surfaced through an application-centric approach—selecting specific applications for examination based on factors like download count. This approach, however, inherently introduces selection bias, potentially overlooking the vast "long tail" of insecure applications. More, as mobile applications increasingly move toward a "walled-garden" model, endpoint-based measurements—whether from browsers or servers—provide only partial views into the traffic on the Internet. In contrast, leveraging Internet gateways as vantage points provides a uniquely comprehensive perspective on traffic that no other vantage point can match. Harnessing such data, however, presents privacy and scalability challenges. Addressing both simultaneously is particularly difficult, as strict privacy requirements preclude storing raw traffic for later analysis, necessitating real-time frameworks capable of operating at line rates. I aim to continue to develop scalable, privacy-preserving, and general-purpose infrastructure to ethically extract security insights from user traffic, allowing us to reason about questions like, "Which applications still transmit data without transport-layer encryption?", "What referral paths funnel users toward scam/misinformation sites?", "How much visibility do powerful network intermediaries (large ISPs, state-level observers) have into user traffic?", etc.

4 Empirical Investigation of Privacy-Enhancing Technology

Growing public awareness of privacy and security threats has spurred explosive growth in the usage of privacy-enhancing technologies (PETs). For example, recent anecdotes of traffic interference and measurement studies like those from Thrust 1 have been cited by commercial VPN providers to justify broader VPN adoption, helping the VPN industry grow into a $45 billion market. Yet despite this surge of interest, relatively little research has examined whether PETs truly fulfill their intended functions—including whether they themselves suffer from security and privacy flaws. Even fewer studies have explored qualitative factors—technical, usability, and operational issues—that affect the adoption and effectiveness of PETs.

My team and I have conducted several investigations into various facets of the VPN ecosystem. We looked into lower-level primitives of VPN protocols and how they could undermine the very security VPNs are meant to provide. We found novel exploits targeting the connection-tracking frameworks of VPN protocols, enabling an attacker to intercept or redirect traffic supposedly secured by VPN [7]. We also developed *VPNalyzer* [8], a user-facing system designed for systematic, semi-automated evaluations of VPN products. With *VPNalyzer*, we conducted a large-scale study covering 80 commercial VPN services, finding that over one-third of them leaked traffic outside their intended tunnels. Some findings led to the assignment of CVEs, and we issued over 30 disclosures to VPN providers and protocol developers regarding the identified deficiencies. To amplify the impact of these works, we collaborated with Consumer Reports, a leading consumer advocacy organization, to produce data-driven recommendations on VPN usage for millions of their readers.

Future work In the coming years, I plan to build on lessons learned from our previous VPN investigations to explore other types of PETs, such as ad blockers, secure messengers, and anonymization networks, focusing on the security and privacy implications for their users. More broadly, I aim to deepen our understanding of *why users adopt PETs* and *what makes them effective in practice*. In an interdisciplinary study I recently led [9], we explored the technical, operational, and usability challenges prevalent within the PET ecosystems, highlighting issues such as usability hurdles, misconceptions, funding constraints, dark patterns and misbehaving players. From these insights, we proposed actionable recommendations for the PET community and developed solutions [10,11] to address specific technical problems—some of which are currently being integrated by Tor and other major PET providers. Looking ahead, I hope to broaden these efforts, expanding both the scope and depth of the investigations into PETs to catalyze meaningful improvements in user security and privacy.

Reference

[1] **Diwen Xue**, R. Ramesh, ValdikSS, L. Evdokimov, A. Viktorov, A. Jain, E. Wustrow, S. Basso, and R. Ensafi. Throttling Twitter: An Emerging Censorship Technique in Russia. In: ACM Internet Measurement Conference 2021 (IMC 2021)

[2] **Diwen Xue**, B.Mixon-Baca, ValdikSS, A. Ablove, B. Kujath, J. Crandall, and R. Ensaf. TSPU: Russia's Decentralized Censorship System. In: ACM Internet Measurement Conference 2022 (IMC 2022)

[3] **Diwen Xue**, R. Ramesh, A. Jain, M. Kallitsis, J. Halderman, J. Crandall, and R. Ensafi. OpenVPN is Open to VPN Fingerprinting. In: 31st USENIX Security Symposium (USENIX 2022)

[4] **Diwen Xue**, M. Kallitsis, A. Houmansadr, and R. Ensafi. Fingerprinting Obfuscated Proxy Traffic with Encapsulated TLS Handshakes. In: 33rd USENIX Security Symposium (USENIX 2024)

[5] **Diwen Xue**, R. Stanley, P. Kumar, and R. Ensafi. The Discriminative Power of Cross-layer RTTs in Fingerprinting Proxy Traffic. In: Network and Distributed System Security Symposium (NDSS 2025)

[6] W. Wang, **Diwen Xue**, P. Kumar, A. Mishra, Anonymous, and R. Ensafi. Is Custom Congestion Control a Bad Idea for Circumvention Tools? In: Free and Open Communications on the Internet (FOCI 2025)

[7] B. Mixon-Baca, J. Knockel, **Diwen Xue**, T. Ayyagari, D. Kapur, R. Ensafi, and J. Crandall. Attacking Connection Tracking Frameworks as used by Virtual Private Networks. In: 24th Privacy Enhancing Technologies Symposium (PETS 2024)

[8] R. Ramesh, L. Evdokimov, **Diwen Xue**, and R. Ensafi. VPNalyzer: Systematic Investigation of the VPN Ecosystem. In: Network and Distributed System Security Symposium (NDSS 2022)

[9] **Diwen Xue**, A. Ablove, R. Ramesh, G. Kwak-Danciu and R. Ensafi. Bridging Barriers: A Survey of Challenges and Priorities in the Censorship Circumvention Landscape. In: 33rd USENIX Security Symposium (USENIX 2024).

[10] **Diwen Xue** and R. Ensafi. The Use of Push Notification in Censorship Circumvention. In: Free and Open Communications on the Internet (FOCI 2023)

[11] P. Kumar, **Diwen Xue**, A. Ortwein, C. Bocovich, Harry, and R. Ensafi. Blocking Resistant Communication for Censorship Circumvention using Push Notification. In: 25th Privacy Enhancing Technologies Symposium (PETS 2025)

[12] **Diwen Xue**, A. Huremagic, W. Wang, R. Sundara Raman, R. Ensafi. Fingerprinting Deep Packet Inspection Devices by their Ambiguities. Under submission.
(Preprint'A: https://diwenx.com/assets/files/dmap.pdf)

[13] B. Mixon-Baca, **Diwen Xue**, R. Ensafi, J. Crandall. CryptoSluice: Privacy-Preserving Traffic Analysis of Weak Transport Layer Encryption at Internet Gateways. Under submission.
(Preprint'B: https://diwenx.com/assets/files/cryptosluice.pdf)