Research Statement | Yunming Xiao, Fall 2023

The Internet today underpins a wide array of global services, including e-commerce, social media, and critical infrastructure. Despite their apparent seamlessness, these services are vulnerable to cybersecurity threats, data leaks, and frequent downtimes. My overarching research vision is anchored in fortifying Internet infrastructure and services to be inherently ***secure, private,*** and ***reliable***. Recognizing the dynamic and multi-layered nature of online systems, my approach cuts ***across various network layers***, forging a holistic path to robust cybersecurity.

One core tenet of my research strategy is the belief that understanding our present systems is key to fortifying our future. To that end, I have first undertaken ***comprehensive measurements*** of existing Internet services. These deep dives into the architecture and operations of online platforms shed light on both overt and subtle vulnerabilities – be they intentional design oversights or unforeseen by-products of their evolving nature. This diagnostic phase is crucial as it helps to isolate points of failure or exploitation.

Armed with these observations, the subsequent phase revolves around innovation and rectification. Rather than just paper-bound solutions, I am an advocate *for* ***translating theoretical designs into actual systems***. Overall, my system design philosophy is three-fold: firstly, I recognize that *the realm of cryptography*, with its rapidly advancing tools and techniques, offers a reservoir of solutions. Seamlessly integrating cutting-edge cryptographic solutions into existing systems is a challenge I eagerly embrace. Secondly, by *identifying and tweaking system components central to the discovered inefficiencies or flaws*, I can reconceptualize information flows and component interactions, addressing the existing issues while pre-empting potential vulnerabilities. Lastly, my research philosophy embodies *a commitment to bridging the divide between theoretical concepts and practical implementation*. This entails creating systems that properly incentivize all stakeholders and cater to their needs. This holistic approach bridges the theory and reality, fostering the successful adoption of my proposed systems.

During my PhD journey, I initiated my research by conducting multiple measurement studies within home networks. The insights gleaned from these studies served as the catalyst for proposing enhancements and extensions to existing designs, bolstering security and privacy measures. Besides these research projects, I fostered collaborations with industry leaders to develop systems aimed at enhancing the reliability of Internet services and data center networks. In the future, I plan to build upon these foundational efforts by providing comprehensive insights into vulnerabilities in security, privacy, and reliability within current Internet infrastructure and services and further improving upon them. In the long term, I am committed to leveraging systematic measurement techniques and proposing system design frameworks to contribute to the creation of a fully secure, private, and resilient Internet.

Current Research

My inquiry fundamentally stems from a ground-up approach, commencing with an in-depth examination from the most accessible vantage point within the Internet landscape – the perspective of a home network. This viewpoint has unveiled the intricacies yet predictability of Internet of Things (IoT) device traffic [1], exposed potential vulnerabilities within media platforms like Kodi [2, 3], and unraveled the complexities of decentralized VPNs [4]. The last work further highlighted the imperative of privacy flaws within the design of Domain Name System (DNS) and HTTP systems, leading towards my subsequent endeavors to revamp these systems [5, 6].

Beyond this micro perspective, I have also extended my gaze to the macrocosm of the cloud. Through collaborations with industry stalwarts such as Tencent, I have delved into fortifying the Internet's infrastructure. This has included efforts to enhance the reliability of the Border Gateway Protocol (BGP) [7], a cornerstone of Internet operation, and to minimize failures within data center networks [8], vital components to Internet today.

Measurement as the Foundation

Computer networks, in contrast to fields like computer vision, are less readily observable given their visually imperceptible nature and limited number of available vantage points. This inherent obscurity renders network measurement a difficult yet crucial task in enhancing our understanding of network systems. Indeed, despite the Internet's pivotal role in routines, it remains far from being fully comprehended by engineers and researchers today.

My research begins with Internet measurements, focusing on security and privacy issues. While this may appear to be an audacious undertaking, I recognize that the most vulnerable targets to security and privacy breaches are the billions of end-users constituting the Internet's endpoints. Consequently, my measurement efforts center on the home network, where most users embark on their Internet journeys.

Overall, my measurement covers diverse aspects of home networks, including IoT devices [1], the multimedia platform Kodi [2, 3], and the decentralized virtual private network (DVPN) [4]. Below I will focus on the last project. Specifically, DVPN is an upgraded version of traditional centralized VPNs, which are commonly used for user anonymity and privacy. However, they lack mechanisms to prevent proxies from monitoring user behavior, raising privacy concerns unless the users unconditionally trust the VPN providers.

DVPN enhances security and privacy by dispersing traffic across multiple parties, making it harder to centralize information. Several DVPN systems have gained popularity by capitalizing on the increasing idle traffic of Internet users, allowing them to monetize spare bandwidth. To investigate the DVPN ecosystem in depth, I conducted both active and passive measurements, joining as a user as well as a DVPN provider/node. The results show that DVPNs have footprints rivaling commercial centralized VPNs while offering comparable or superior performance. Further modeling suggests DVPNs foster an efficient bandwidth marketplace.

Despite these achievements, I still find DVPNs unable to guarantee complete security and privacy since it cannot prevent its nodes from monitoring traffic. This challenge is inherently difficult without full network control. Anecdotally, the passive measurements I conducted exploited this privacy flaw, revealing that a node provider could gain substantial insight into user intent because of being able to observe a significant portion of DNS traffic and some HTTP traffic from users as encryption was absent. This insight underscores two key considerations: (i) we cannot rely solely on proxies and (ii) we should work on enhancing the security and privacy of the Internet services themselves, which I will elaborate on in the following two sections.

Incorporating Advanced Cryptographic Tools

The DNS is the phonebook of the Internet which maps IP addresses like “151.101.195.5” to human-friendly names like “cnn.com”. At the birth of the Web, security and privacy were not contemplated, leaving DNS traffic as plaintext and subject to monitoring by intermediaries. This situation persisted for three decades until DoT/DoH introduced end-to-end encryption to address these concerns. Unfortunately, they are still not adopted by most DNS traffic, as revealed in my DVPN measurement. Besides unsatisfactory DoT/DoH adoption rate, user privacy demand has further been extended to recursive resolver (ReR) operators, who possess the users’ full DNS logs. To tackle this issue, Oblivious DoH (ODoH) disconnects user identities from DNS requests by introducing a proxy between the DNS client and ReR, where the proxy remains oblivious to encrypted DNS queries, and the ReR remains unaware of the client's IP address. User privacy is thus enforced as long as the proxy and ReR do not collude. However, non-collusion is hard to enforce and verify in reality, e.g., both proxy and ReR can be subjects of a subpoena, at which point privacy is again sacrificed. Finally, ODoH still allows the ReR to gather knowledge about the users as a whole, e.g., answering questions like “what is the most popular online newspaper, and its potential political affiliation, in a given region?”

I came to realize that ensuring complete user privacy requires ReRs to operate *in the blind*, i.e., resolving domain names without knowing their content. This counterintuitive concept aligns with advanced cryptographic techniques in Private Information Retrieval (PIR). Indeed, private DNS often serves as a motivating example in PIR research, yet no practical solution currently exists. It follows that my research is to bridge the gap between PIR and DNS. I did so by designing PDNS [5], a Privacy-Preserving DNS based on PIR designed to *augment* rather than replace DNS, akin to DoH and ODoH. At the first glance, the solution seems to be straightforward: we just need to enhance the ReR’s cache with PIR premises. However, two major challenges emerge as I dove deeper.

Firstly, PIR encompasses various solutions with distinct advantages and disadvantages, and not all fit well within the DNS context. For instance, some PIR solutions are unsuitable for DNS due to limitations in handling high request volumes and cache updates. After extensive investigation, I determined that single-server stateless PIR schemes, particularly Spiral, are the most suitable for DNS due to their low overhead, efficient query processing times, and compatibility with the lack of non-collusion requirements.

Secondly, PIR protocols assume that a database (or cache in DNS context) is either given or privately populated, which differs from current DNS where the ReR populates its cache based on user requests. Clearly, a *blind* ReR cannot perform such operation which should be tackled by the client instead. To address this, I proposed my own DNS extension that enables a client to communicate its ReR's IP address when cache misses occur, allowing authoritative name servers to populate the ReR cache securely.

Together with further optimizations and security designs, I led a few students to implement PDNS and showed that it achieves competitive performance and strong privacy-preserving guarantees as envisioned.

Rethinking the System Premises

I further extend my investigation into HTTP systems, which is evolving significantly, incorporating numerous extensions such as HTTPS. The adoption rate of HTTPS is over 90% reported by Google, much better than DoT/DoH. However, many websites still transmit messages in plaintext and allow third parties like DVPN node providers, as demonstrated in my previous measurement study, to intercept user requests. While this situation is expected to improve, I have identified a more pressing privacy concern within another HTTP extension – HTTP cookies.

HTTP cookies enable Web servers to deliver customized content to returning users. Most current HTTP cookies are *semantic-oblivious*, i.e., carrying no direct user information but only a user identifier serving as a key for user data stored in an associated profile database. Yet, this approach has two significant drawbacks.

Firstly, it poses a privacy risk by allowing Web providers to record any user information as much as they can for an indefinite duration, unless the users actively clean up – most users are not aware of it at all, or even worse, many websites do not provide appropriate cookie cleaning method despite the RFC document suggests doing so. Secondly, as infrastructure increasingly moves to the network edge, semantic-oblivious requests cannot be analyzed until they reach distant data centers, hindering edge systems' ability to process them efficiently.

To protect user privacy, I propose revising this system premise by introducing semantic cookies – encrypted data structures set by the server and stored on the user's end. Unlike conventional HTTP cookies, which effectively point to semantic user databases, semantic cookies directly embed user information without individually identifiable information. This facilitates analytical processing of user requests by collaborating with edge components, primarily edge servers and potentially ISP switches, without altering existing protocols. I further designed and implemented Snatch [6], the first edge network analytics prototype based on the assumption of semantic cookies. With the assistance of DVPNs for global-scale experiments, evaluations demonstrate that Snatch accelerates user analytics by up to 200x and by 10-30x in typical scenarios while preserving user privacy.

Improving Reliability

Reliability constitutes the third pillar of my research vision. Unlike the other two aspects, which primarily concern the user's perspective, reliability is centered around server-side considerations. Therefore, I expanded my research horizons in collaboration with Tencent to delve into the intricacies of data center gateways [7] and networks [8].

In particular, one observation at Tencent revealed the challenge of maintaining the Border Gateway Protocol (BGP), a critical inter-domain protocol. BGP vulnerabilities to various failure triggers, such as application glitches and router hardware malfunctions, threatening network stability and leading to packet losses. Non-stop routing (NSR) thus becomes essential for network operators to ensure inter-domain connectivity continuity. Tencent researchers and I jointly developed TENSOR [7], a BGP system with kernel-modification-free replication design and lightweight architecture. This innovation reduced reliance on OS kernel changes, enabling gateway virtualization, robust performance, and system reliability. TENSOR's deployment in Tencent's cloud gateway overseeing thousands of BGP peering connections significantly reduced development, deployment, and maintenance costs while maintaining SLAs.

Future Directions

The overall mission of my research is to understand and address deficiencies in Internet infrastructure and services, enhancing their ***security, privacy,*** and ***reliability***. I plan to first expand my measurement efforts to gain a more comprehensive understanding of the Internet landscape. Then, I will apply my expertise to systematically improve security, privacy, and reliability across various network layers by creating systems that rectify existing issues and proactively fortify these aspects. In the longer term, I will leverage my skills to establish a formal framework for evaluating and developing new systems with robust security, privacy, and reliability guarantees. This framework will guide the creation of solutions that meet evolving user demands, ensuring the integrity and resilience of Internet.

Towards a Framework for Secure and Privacy-Preserving Systems

In response to the growing demand for online privacy, there have been many privacy-preserving system proposals based on advanced cryptographic tools, including my own PDNS proposal [5]. This trend aligns with my core research philosophy where I envision cryptographic serving as foundational building blocks in the future Internet.

Systems with Distributed Trust. It is noteworthy that different from my PDNS proposal which relies on single-server cryptographic tools, another trend has emerged where a plethora of proposals increasingly rely on multi-

server cryptographic tools. Examples include ODoH, private statistics aggregators, multi-party relays, privacy-preserving advertisement auctions, and more. These tools necessitate the establishment of non-collusion agreements among two or more entities within the network, thereby constituting what is referred to as "distributed trust". Indeed, multi-server cryptographic tools offer lightweight computing requirements and a broad array of functions, outperforming single-server alternatives, making them an attractive option for various systems.

Thus, my next research phase involves a comprehensive measurement study of privacy-preserving systems built on distributed trust. This study aims to identify such systems, understand non-collusion agreements, explore parties involved, assess geographical constraints, and compare their performance to systems without such constraints. I will also scrutinize potential misapplications of these agreements, ensuring a holistic understanding of this concept.

Based on the insights gained, I will develop best practices for implementing non-collusion agreements and evaluate technical solutions for their precise execution while allowing users to verify their correct implementation. Ultimately, I aim to create a formalized framework that guides the development of practical, privacy-preserving systems rooted in the concept of distributed trust. This framework will ensure that digital privacy becomes an inherent feature of future Internet infrastructure and services.

Relieving Systems from the Trust Assumptions. Nonetheless, it is important to recognize that systems with non-collusion constraints still rely on trust assumptions, which can be challenging to meet in certain scenarios. For instance, global Internet services working with different partners across regions may face policy conflicts, rendering distributed trust impractical. Therefore, the quest for the most robust privacy-preserving systems should not depend on distributed trust, though it is worth noting that not all systems can entirely forgo this criterion, as single-server cryptographic tools often have computation limitations compared to their multi-server counterparts.

Adhering to my research philosophy, I will meticulously identify the core premises at the heart of these inefficiencies or flaws. Once these issues are pinpointed, the strategic selection of cryptographic tools and the alteration of these foundational premises become paramount. Furthermore, I am committed to making a tangible impact in the real world. Thus, any viable solution must take practical considerations into account, ensuring that all parties involved in the system are properly incentivized. Neglecting this aspect could render even the most robustly designed system ineffectual in the real world. These principles have been consistently applied in my previous projects and will continue to be the guiding force behind my future endeavors. One example of this commitment is SafeKodi [3], an add-on that leverages Kodi users to explore the Kodi ecosystem and provides valuable insights on potentially malicious add-ons to users as return. This project gained significant media coverage and amassed a user base of over 30,000. This is a testament to my unwavering dedication to projects that have real-world significance, and I am committed to pursuing similar avenues in the future.

Lastly, while I have prior experience studying security and privacy issues in various network systems [1-6], I have actively fostered collaborations with researchers specializing in Security/Privacy/Cryptography in the past, and I find such collaborations to be instrumental for crafting optimal solutions. In the future, I am enthusiastic to collaborate with more researchers in these pertinent fields as I work relentlessly toward achieving my ultimate research goal.

Enhancing Reliability with Programmability

Enhancing the reliability of Internet services and infrastructure is the third pivotal pillar within my research agenda. While my previous work primarily focused on enhancing existing systems [7, 8], I also explored programmable devices such as programmable switches [6] and SmartNICs [9]. This exploration has enlightened me to the significant potential of programmable network devices, offering greater flexibility and functionality to enhance system reliability. One compelling example of this potential is evident in my work on achieving rapid network failover through deterministic flow re-pathing. Programmable switches make implementing such a mechanism straightforward, whereas traditional switches face substantial challenges [8]. Recognizing this, I am committed to further exploring this direction, harnessing programmable devices within the network to bolster system reliability, as well as exploring how to ensure the services reliability during migrating to such programmable devices.

I am also eager to continue and expand my collaborations with industrial entities, including data center operators and critical Internet service providers. These partnerships provide me with a unique perspective, exposing me to the complexities of network infrastructure beyond the view of ordinary Internet users. These collaborations not only enrich my research by addressing real-world challenges but also create opportunities to translate research findings into practical applications that benefit a broader user base.

# References **(* Equal Contribution)**

[1] **Yunming Xiao**, Matteo Varvello. *FIAT: Frictionless Authentication of IoT Traffic*. In CoNEXT 2022.

[2] Marc Anthony Warrior, **Yunming Xiao**, Matteo Varvello, Aleksandar Kuzmanovic. *De-Kodi: Understanding the Kodi Ecosystem*. In WWW 2019.

[3] **Yunming Xiao**, Matteo Varvello, Marc Anthony Warrior, Aleksandar Kuzmanovic. *Decoding the Kodi Ecosystem*. In TWEB 2023.

[4] **Yunming Xiao**, Matteo Varvello, Aleksandar Kuzmanovic. *Moneitizing Spare Bandwidth: The Case of Distributed VPNs*. In SIGMETRICS 2022.

[5] **Yunming Xiao**, Chenkai Weng, Ruijie Yu, Peizhi Liu, Matteo Varvello, Aleksandar Kuzmanovic. *PDNS: A Fully Privacy-Preserving DNS.* In Submission.

[6] **Yunming Xiao**, Yibo Zhao, Sen Lin, Aleksandar Kuzmanovic. *Snatch: Online Streaming Analytics at the Network Edge*. To appear in EuroSys 2024.

[7] Congcong Miao*, **Yunming Xiao***, Marco Canini, Ruiqiang Dai, Shengli Zheng, Jilong Wang, Jiwu Bu, Aleksandar Kuzmanovic, Yachen Wang. *TENSOR: Lightweight BGP Non-Stop Routing*. In SIGCOMM 2023.

[8] Yadong Liu*, **Yunming Xiao***, Congcong Miao, Xiang Li, Zekun He, Huihui Liu, Weizhen Dang, Aleksandar Kuzmanovic, Jilong Wang. *Fast And Practical Network Failover By Deterministic Re-Pathing.* In Submission.

[9] **Yunming Xiao**, Diman Zad Tootaghat, Aditya Dhakal, Lianjie Cao, Puneet Sharma, Aleksandar Kuzmanovic. *Conspirator: SmartNIC-Aided Control Plane for Distributed ML Workloads.* In Submission.