Title: Hiding in Plain Sight: Enabling Metadata Protection with Mixnets

Speaker: Dr. Piyush Kumar Sharma, Postdoctoral Research Fellow, University of Michigan

Venue: KD 101

Date: 20th Feb 2025

Time: 3:30 PM

Abstract:

Mix networks, or mixnets, are an advanced anonymous overlay network system that provides metadata protection in the form of communication anonymity towards global adversaries, who are capable of observing all communication links over the Internet. To achieve anonymity, messages are routed through multiple intermediary mixnodes, where each mixnode transforms and reorders messages by randomly shuffling and delaying them before forwarding along the route. However, strong privacy in mixnets comes at the cost of increased latency, limiting the applications that are usable when accessed through it. Recent large-scale mixnet deployments such as the Nym network are only able to support high-latency tolerance applications such as email and crypto wallets.

Thus, in this talk, I will discuss my recent work LARMix, where we propose a novel latency-aware routing scheme for mixnets that can significantly reduce latency without much impact on anonymity. I will discuss different challenges (balancing the network load and developing a new method of quantifying routing anonymity) in developing LARMix and how we address them. Our experimental evaluation under different scenarios and using realistic latency data demonstrates LARMix's usefulness in reducing latency, where one can achieve as high as 8x latency reduction. We perform a thorough security analysis under an adversary that controls a subset of mixnodes in the network, and establish that LARMix does not significantly increase any adversarial advantage. Overall, LARMix helps support a wide range of applications to be accessed via the mixnet, essentially contributing towards enhancing end-user privacy.

Brief Bio:

Dr. Piyush Kumar Sharma is a senior research fellow at the University of Michigan. Before joining University of Michigan, Piyush was a postdoctoral researcher at the COSIC research group at KU Leuven (Belgium) for two years. He completed his PhD in network security from IIIT-Delhi, India, in 2021 where he received a doctoral dissertation award for his PhD thesis. His research lies at the intersection of systems, networks,

security, and privacy, where he focuses on developing frameworks, conducting empirical investigations, and building systems to ensure metadata security and privacy. He is particularly passionate about researching VPNs, traffic fingerprinting, anonymous communication networks, and Internet balkanization. He regularly publishes his research in top security and privacy forums, such as NDSS, PETS, AsiaCCS, and IMC. He recently received a Rising Star award at the Free and Open Communication over Internet (FOCI) community associated with the Privacy Enhancing Technologies Symposium. He is an active part of the academic community, being a PC member of top venues like Usenix Security, CCS, WWW, Euro S&P, PETS, etc. `