CT Advanced Computing Center (CACC) Security Seminar Series 2024

Speaker: Ben Weintraub - Northeastern University
Date: November 13, 2024
Time: 11:15 12:30pm
Location: ITE 336
Meeting Link : https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m4d36ddf4d36edd727aa04331cdb7d7f6

Meeting number (access code): 2633 368 4613

Meeting password: MqmJMizs533

Payout Races and Congested Channels: A Formal Analysis of Security in the Lightning Network

The Lightning Network, a payment channel network with a market cap of over 192M USD, is designed to resolve Bitcoin's scalability issues through fast off-chain transactions. There are multiple Lightning Network client implementations, all of which conform to the same textual specifications known as BOLTs. Several vulnerabilities have been manually discovered, but to-date there have been few works systematically analyzing the security of the Lightning Network. In this presentation, I will discuss our foundational approach to analyzing the security of the Lightning Network with the help of formal methods. Based on the BOLTs' specifications, we built a detailed formal model of the Lightning network's single-hop payment protocol and verify it using the Spin model checker. Our model captures both concurrency and error semantics of the payment protocol. I will then discuss several security properties which capture the correct intermediate operation of the protocol, ensuring that the outcome is always certain to both channel peers, and using them, I will show how we re-discovered a known attack previously reported in the literature along with a novel attack, we refer to as a Payout Race. A Payout Race consists of a particular sequence of events that can lead to an ambiguity in the protocol in which innocent users can unwittingly lose funds. I will conclude by demonstrating how we confirmed the practicality of this attack by reproducing it in a local testbed environment, and discussing the implications of this novel attack vector.