Temple University
College of Engineering

Fall Seminar Series
Department of Electrical and Computer Engineering
Wednesday, October 27, 2021
Noon – 1:00 PM EST
Zoom Video Conference: https://temple.zoom.us/j/99319863502

Partitioning Blockchains Efficiently: Attacks and Defenses

David Mohaisen, University of Central Florida

Abstract: The Bitcoin blockchain safety relies on strong network synchrony and a stable network configuration, and violating the blockchain safety properties, e.g., by a majority attack or information eclipsing, requires strong adversaries such as a mining pool with 51% hash rate or an ISP controlling millions of IP addresses. Since these requirements are prohibitively costly, notable attacks on the Bitcoin network have not been observed in the wild. Recently, we empirically demonstrate that the real-world Bitcoin network does not conform to its ideal specifications of synchrony and stable network configuration. As a result, we reduce the requirement for violating the blockchain safety by presenting two practical attacks called HashSplit and SyncAttack. In HashSplit, we first formulate an ideal functionality that exposes the correct communication model among the mining nodes that preserves the blockchain safety properties. Our model specifies that strong network synchrony can only be guaranteed as long as the mining nodes form a completely connected topology and receive blocks at the same time. The observed deviation can be exploited by a well-connected adversary to partition the network and continuously fork the chain in order to violate the blockchain safety and chain quality with only 26% hash rate. In SyncAttack, we argue that the existing security models have largely overlooked the permissionless property of the Bitcoin network, characterized by the network churn. By exploiting the network churn, an adversary can control all connections made by the newly arriving nodes by simply occupying all the incoming connection slots of the existing nodes. Our measurements and analysis reveal (1) a notable network churn, and (2) weaknesses in Bitcoin Core that can be exploited to partition the network by controlling less than 120 IP addresses. By segregating the newly arriving nodes from the existing ones, a SyncAttack adversary successfully double-spends without any mining power. We also propose attack countermeasures for both attacks by modifying the Bitcoin software client.

BIOGRAPHY: David Mohaisen earned his M.Sc. and Ph.D. degrees from the University of Minnesota in 2011 and 2012, respectively. He is currently an Associate Professor at the University of Central Florida. Earlier, he held several posts, in academia and industry: as an Assistant Professor at the University at Buffalo, (Senior) Research Scientist at Verisign Labs, and a Member of the Engineering Staff at the Electronics and Telecommunication Research Institute (ETRI). His research interests fall in the broad areas of networked systems and their security, adversarial machine learning, IoT security, AI security, and blockchain security. Among other services, he is currently an Associate Editor of IEEE Transactions on Mobile Computing and IEEE Transactions on Parallel and Distributed Systems. He is a senior member of ACM (2018) and IEEE (2015), a Distinguished Speaker of the ACM (2021-2023) and Distinguished Visitor of the IEEE Computer Society (2021-2023).