Building Trust in Peer-to-peer Trusted Execution Environment (TEE) Networks

Ceren Kocaogullar, University of Cambridge

Mobile and IoT devices, cloud computing, industrial control systems, and ambient computing support a wide range of security-, privacy-, or safety-critical tasks such as preventing collision in self-driving cars, processing private data in the cloud, and securely sharing sensor data among IoT devices. Therefore, it is essential to securely deploy and maintain these large, dynamic, self-organising networks. In addition, ensuring that each node in these networks is carrying out its computation tasks securely and privately is critical.

When it comes to privacy, traditional encryption techniques can protect data while it is *at rest* or *in transit*. However, in networks where sensitive data is used and shared with other nodes for multiparty computation tasks, it is crucial to ensure that the data is kept privately at all times, including while *in use*, i.e. while stored in RAM and during computation. For example, in a network of self-driving cars where nodes train on shared data to enhance their models, a malicious node could still extract sensitive driver information from others, despite encryption and secure data sharing.To address these challenges, hardware-based trusted execution environments (TEEs) can be used to process data while maintaining its confidentiality.

In addition to protecting data *in-use*, TEEs can also provide strong security properties and enable nodes to establish trust with one another through a technique called *remote attestation*. Remote attestation can verify that a remote node's hardware configuration is correct, and it is running the correct software. This is a significant improvement over authenticating nodes using a traditional digital certificate scheme such as TLS, which verifies the identity of the node, not the integrity of its hardware or software. However, the traditional approach of establishing trust among TEEs through remote attestation requires a quadratic number of attestations in terms of the number of TEEs, which becomes infeasible as the network size grows. Therefore, we need ways to efficiently establish and maintain large and dynamic distributed networks made of mutually-trusting nodes.

Ad hoc networks in the real world not only need to be scalable, but also have to cope with a diversity of nodes supporting different attestation protocols, and unreliable connectivity. For instance, in the case of a network of self-driving cars, establishing point-to-point trust among nodes is not straightforward, as the cars in the network may be manufactured by different companies and equipped with various TEEs requiring different attestation protocols. Moreover, some of these attestation protocols may require access to a remote server, but the cars in the network may not have reliable internet connectivity. Therefore, there is an urgent need for attestation protocols that can accommodate heterogeneous networks with unreliable connectivity to establish and maintain trust among TEE nodes efficiently.

In this talk, we present Careful Whisper, an attestation protocol for effectively forming and maintaining trusted ad hoc TEE networks. Careful Whisper is designed to accommodate networks with inconsistent connectivity and nodes equipped with various TEEs. It uses gossiping to disseminate trust information efficiently, based on the premise that trust can be transitive when established and sustained within a trusted computing base. Using gossiping allows for the efficient dissemination of trust information without the need for routing, network topology knowledge, or constraints on network topology changes. Unlike existing collective attestation protocols, Careful Whisper supports ad hoc networks by allowing nodes to decide which nodes they can trust, eliminating the need for a central authority for network deployment and maintenance.