Exploring the Trusted Platform Module to Establish Mutual Trust in High Performance Computing

Devon Bautista and Rebecca Whitten

LA-UR-21-27746

Abstract

When using computers to process sensitive data, one needs to be able to trust that the senders and receivers of that data are authentic. One way to provide that trust is with cryptographic proof that a sender and receiver are who they claim to be. Mutual Transport Layer Security (mTLS) is a protocol that builds off of TLS to provide mutual cryptographic proof-of-identity between a sender and receiver. One major difficulty in cryptographic systems, in general, is secure key storage. This is a particular challenge in HPC, where nodes are typically stateless, meaning they don’t have any persistent storage. The Trusted Platform Module, or TPM, is a secure, independent cryptoprocessor that provides many cryptographic functions, including secure key storage, in its own separate, non-volatile storage. This can be a good solution even for nodes with persistent storage too. Keys and certificates used for mutual authentication, like in mTLS, can be stored in this tamper-resistant piece of hardware without the need for secondary storage.

This project explores how the TPM can be used to securely store keys and perform cryptographic operations to establish mutual trust between nodes using mTLS. We explore how to interact with the TPM via various software stacks and evaluate useful applications of the TPM, including how to implement mTLS using the TPM to store secrets and enforce mutual authentication.