

Building Secure Networked Systems with Code Attestation (Invited Talk)

Adrian Perrig

CyLab / Carnegie Mellon University
Pittsburgh, USA
perrig@cmu.edu

Attestation is a promising approach for building secure systems. The recent development of a Trusted Platform Module (TPM) by the Trusted Computing Group (TCG) that is starting to be deployed in common laptop and desktop platforms is fueling research in attestation mechanisms. In this talk, we will present approaches on how to build secure systems with advanced TPM architectures. In particular, we have designed an approach for fine-grained attestation that enables the design of efficient secure distributed systems, and other network protocols. We demonstrate this approach by designing a secure routing protocol.