Automated Trust Analysis for Layered Attestations

Submitted by ik on Tue, 04/20/2021 - 4:11pm. Contributors:

Ian KretzJohn D. RamsdellPaul D. Rowe

ABSTRACT

In distributed systems, trust decisions are often based on remote attestations in which evidence is gathered about the integrity of subcomponents. Layered attestations leverage hierarchical dependencies among the subcomponents to bolster the trustworthiness of evidence. Complex dependency relationships in production systems can lead to equally complex layered attestations. The power of human analysts to reason about the correctness of an attestation in the presence of an active adversary becomes greatly diminished amid such complexity. We present an automated toolchain for reasoning about the trustworthiness of attestations and provide a formal proof of its correctness. Copland is a domain-specific language for specifying complex layered attestations. A Copland phrase expresses an attestation as a composition of the local activities of subcomponents -- requesting evidence, performing measurements and cryptographic operations, bundling evidence and replying to requests. Phrases themselves may be composed: if phrase P gives evidence of A's runtime state assuming B's state is pristine, and P' gives evidence of B's runtime state, then composing P' with P gives evidence of A's runtime state. In the absence of an adversary, the trust properties of phrases P and P' compose additively regardless of the order in which they are executed. However, an active adversary can undermine the additive nature of this composition. How phrases are composed bears directly on the trustworthiness of the evidence they produce. We introduce a method for analyzing executions of attestations specified by Copland phrases in an adversarial setting. We develop a general theory of executions with adversarial corruption and repair events. Our approach is to enrich the Copland semantics according to this theory. Using the model finder Chase, we characterize all executions consistent with a set of initial assumptions. From this set of models, an analyst can discover all ways an active adversary can corrupt subcomponents without being detected by the attestation. These efforts afford trust policymakers the ability to compare attestations expressed as Copland phrases against trust policy in a way that encompasses both static and runtime concerns.

Ian Kretz is a Cyber Security Engineer at the MITRE Corporation. He was educated at Rice University and Northeastern University. His work has focused on cryptographic protocol analysis, verified implementation and layered attestation.

Ian Kretz | John D. Ramsdell | Paul D. Rowe
License: Creative Commons 2.5

Other available formats:

Automated Trust Analysis for Layered Attestations
Switch to normal viewerSwitch to experimental viewer

Presentation HCSS 2021