PRIMA

Paper By: Trent Jaeger, Reiner Sailer, and Umesh Shankar

Presented By: Wyatt Lloyd, Robert Melervy

Overview

- How PRIMA meets the 6 requirements
  - Trusted Subjects
  - Trusted Code/Data
  - Information Flow
  - Initial Verification
  - Filtering Interfaces
  - Filtering Subjects
- Verification of CW-Lite Formally
  - High Integrity Code Loaded in Trusted Subjects
  - CW-Lite Information Flow Requirements
  - Initial Verification
  - Filtering Interface Correctness

Trusted Subjects

The set of trusted subjects in the MAC policy must be trusted by the remote party.

Add trusted subjects to measurement list, and their hashes to the hash chain.

$H(X_{i+1}) = H(X_i \parallel H(T))$

$M_{i+1} = M_i \parallel m_T$

Remote party verifies that it trusts all subject on measurement list, and that hashes checks.