What is PRIMA?

- Policy-Reduced Integrity Measurement Architecture
- Integrity measurement approach based on information flow integrity
- Extension of the Linux Integrity Measurement Architecture (IMA)
- Measures code run on a system and which information flows are present among processes
Integrity Measurements

- **High Integrity**: Known, trusted software
  - Passes verification
- **Low Integrity**: Unknown, un-trusted software
  - Fails verification
- **Hardware-Based Measurement**: computing a cryptographic hash (of code or data)
  - extending a hardware-protected hash chain with it
    - Trusted Platform Module (TPM)
- **Application level measurement and verification**:  
  - IMA: measures code loaded and static data files or configurations.
  - Remote system can verify the measured system has no low-integrity components
Load-time Integrity

- Measure the loaded code and static data to approximate runtime integrity (load-time measurements)
  - Not accurate for runtime (Network data use)
  - Inefficient
    - All measured entities must be known and trusted
    - Entities that do not impact target application must still have high integrity
  - Fails when low integrity code is loaded
  - Ignores the impact of low integrity network data
(1) Measurement
(2) Attestation
(3) Verification

Attesting System
Verifying System
Information Flow Integrity

- Biba Integrity model
  - Code executed and data read by a process must be at its integrity level or higher

- LOMAC
  - Integrity of a process = Minimum (integrity of inputs)

- Fails if any “low-to-high” integrity flow is present
  - Example: UNIX high-integrity processes (sshd services) receiving low-integrity inputs
Clark-Wilson Lite Integrity

- **Original Clark Wilson model has two problems:**
  - Complete assurance of high integrity applications is impractical
  - Only a few application interfaces are expected to handle low integrity data

- **CW-Lite**
  - Only interfaces accepting low integrity data must have filters
  - Complete, formal assurance of the program is not required
Summary:

- Load-time measurement fails when any low integrity code is loaded, but ignores the impact of low integrity network data.
- Biba integrity considers information flows, but fails if any low-to-high integrity flow is present.
- CW-Lite allows some low-to-high flows via filtering interfaces only.
PRIMA’s Integrity Model

- Extend load-time integrity measurements to information flow IM’s.
- Extend Biba (info. Flow) to support CW-Lite
Six Requirements

1. **Trusted Subjects**: The set of trusted subjects in the MAC policy must be trusted by the remote party.

2. **Trusted Code/Data**: All code and static data loaded for any trusted subject must correspond to known and trusted hashes by the remote party.

3. **Information Flows**: All information flows to a trusted subject must come from another trusted subject.

4. **Initial Verification**: The initial verification procedure code must be of high integrity and verification must be successful.

5. **Filtering Interfaces**: Any claim that a particular interface discards or upgrades all low integrity inputs must be verifiable.

6. **Filtering Subjects**: The permissions to receive low integrity inputs must only be available to filtering subjects, and these subjects must only run within the context of filtering interfaces.