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.
Trusted Code/Data

All code and static data loaded for any trusted subject must correspond to known and trusted hashes by the remote party.

Measure code/data, subject and role (optional) if subject is trusted.

\[ m_d = (d \| s \| r) \]

\[ H(X_{i+1}) = H(X_i \| H(m_d)) \]

\[ M_{i+1} = M_i \| m_d \]

Remote party verifies that code/data, subject, and role (optional) are all of high integrity.
Information Flow

All information flows to a trusted subject must come from another trusted subject.

MAC policy => information flow, so PRIMA measures information flow by measuring MAC policy.

\[ H(X_{i+1}) = H(X_i \| H(p)) \]

\[ M_{i+1} = M_i \| m_p \]

Remote party uses hashes to verify measurement list, then uses MAC policy => information flow, then verifies all flows to trusted subjects are from trusted subjects.
Initial Verification

The initial verification procedure code must be of high integrity and the verification must be successful.

No new measurements are needed to capture the IVP!

IVP subject and IVP code covered by code/data measurement, IVP code then measures the result of the IVP test.
Filtering Interfaces

Any claim that a particular interface discards or upgrades all low integrity inputs must be verifiable.

Part of trusted subjects, so it’s code is already measured!
Filtering Subjects

The permission to receive low integrity inputs must only be available to filtering subjects, and these subjects must only run within the context of a filtering interface.

Extend $m_T$ to include if the subject has an associated filtering subject.

This allows the remote party to verify the filtering interfaces.
Review of Measurements

Code and static data
MAC Policy*
Trusted Subjects*
Code-Subject Mapping*

* means new measurement
Verification of CW-Lite Formally

This is what the remote party must do to trust you.
High Integrity Code Loaded in Trusted Subjects.

**Requirement:** Remote party must verify code/data digest is known and of high integrity. Must verify the role as well if it is specified.

**What PRIMA does:** Prima measures all code loaded into trusted subjects, and the code/subject mapping.
CW-Lite Information Flow Requirements

**Requirement:** For every trusted subject, all directly connected information flows must be from trusted subjects. For filtering and untrusted subjects there are no requirements.

**What PRIMA does:** PRIMA measures the MAC policy => information flow so we can verify all trusted subjects only have inputs from trusted subjects.
Initial Verification

**Requirement:** The IVP subject must pass the regular “High Integrity Code loaded in Trusted Subjects” requirements. It also must be trusted to do integrity verification, and the integrity verification must succeed.

**What PRIMA does:** The IVP is a trusted subject, so its code is measured. The IVP can then run with trusted results.
Filtering Interface Correctness and Use

**Requirement:** Any trusted subject with an associated filtering subject, must pass the “High Integrity Code Loaded into Trusted Subjects Requirement” and be trusted to only activate filtering subjects within filtering interfaces.

**What PRIMA does:** Filtering interface code is measured, and its existence is indicated in trusted subject list. The remote party must check that filtering subjects are only used at filtering interfaces, and that the filtering interfaces are trusted to discard or upgrade low integrity data.
PRIMA’s Big Advantages

1) Captures information flow and allows upgrading of low integrity inputs!

2) Doesn’t measure untrusted subjects.