Mobius : Mobility, Ubiquity, Security

http:// mobius.inria.fr

Contract n° IST 015905

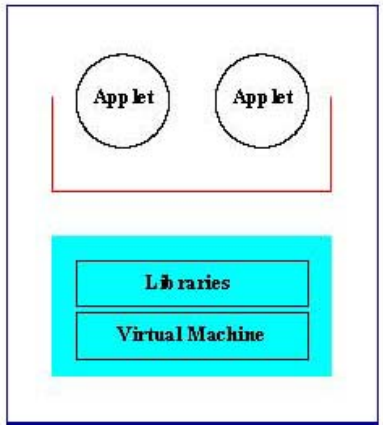
Objectives

Establish a security architecture appropriate for global computers:

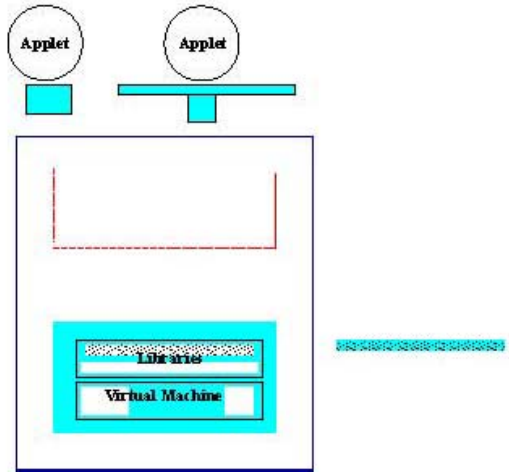
- Adopt a computational model that captures faithfully fundamental aspects of global computers,
- Identify the trust and security requirements of such a model,
- Develop on top of the computational model a security framework that enforces these requirements,
- Provide the enabling technologies necessary for implementing the framework,
- Validate the architecture.

Very large networks of JVM-enabled devices:

- *Flexibility and uniformity:* aimed at providing a global and uniform access to services,
- *Security and heterogeneity:* subject to resource and security constraints



Ideal Scenario



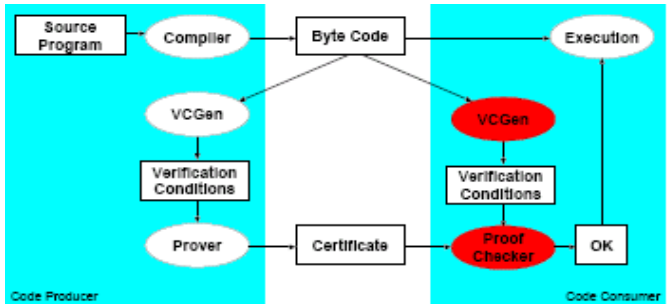
Scenario considered

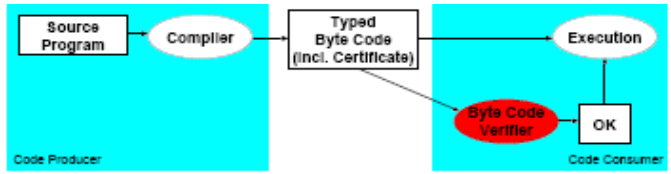
Security Issues

- Devices must be protected individually by means of static and resource aware enforcement mechanisms,
- No sharp distinction between static Trusted Computing Base and mobile applications,
- No central trust authority: trust infrastructures must allow verifiable evidence (cryptography is not enough),
- Need for expressive security policies and functional specifications:
  - Information flow and resource control policies,
  - Framework-level policies and application-level policies.

Security framework

To deliver a framework with appropriate characteristics we shall adopt ideas from *Proof Carrying Code* (PCC) and require that downloaded components come equipped with certificates, i.e. condensed and formalized mathematical proofs which are self-evident, unforgeable and straightforward to check.





Issues

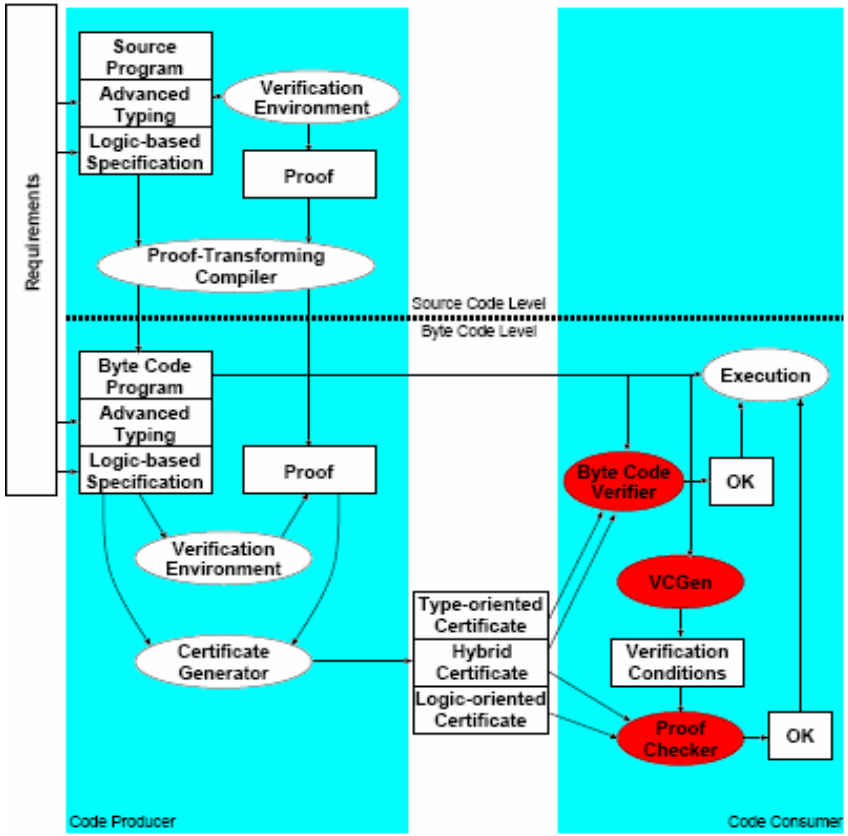
Enabling technologies: should provide enough precision and automation to guarantee applicability and scalability. *We shall develop techniques that draw from and tightly combine both automatic and interactive technologies.*

- Type systems:
  - Efficient, automatic, but specialized and imprecise
  - Used for information flow, resource usage, aliasing
- Program logics: general, precise, but interactive
  - Characterization of non-functional properties
  - Characterization of high-level security policies
  - Component correctness

PCC: infrastructure and scenarii should reflect nature of global computers.

Overall picture

Modern verification environments based on program logics typically operate on source programs. The Mobius project proposes to combine these environments with type systems, which provide an automated means to enforce many basic policies, and use the resulting framework to cover a wide range of security policies for global computers.



A three-layered framework

In order to target different application domains, we can select different layers in the framework

- Enhanced bytecode verification for efficient and automatic verification of generic security properties
- Logical verification of basic security rules:
  - Annotation assistants
  - Proof inference
- Logical verification of complex security and functionality properties:
  - Component validation
  - Proof construction
  - Proof checking

Consortium

- FP6 Integrated Project, beginning in Sept 2005 for 48 months.
- 12 academic and 4 industrial partners, *Coordinator INRIA Sophia-Antipolis, (France).*

- End User panel
  - **About a dozen members from different application domains (telephone, automotive, *etc…)***
  - **Shall be growing gradually as project results unravel**