MOBIUS: Mobility, Ubiquity, Security
Enabling proof-carrying code for Java on mobile devices

Gilles Barthe
INRIA, France

http://mobius.inria.fr
Mobius fact sheet

- Integrated project within Global Computing II
- Started Sept 2005, running until Aug 2009
- > 12M budget, > 6M funding, > 1000 man*monthes
- 16 partners, 100 participants, inc. 20 PhD students

![Map of Europe showing project partners]

- INRIA
- RU Nijmegen
- U. Edinburgh
- Tallinn U.
- UC. Dublin
- UP. Madrid
- SAP Research
- Trusted Logic
- LMU München
- ETH Zürich
- Chalmers U.
- Imperial College
- U. Warsaw
- TU Darmstadt
- France Telecom
- TLS

- Scientific Advisors M. Abadi, A. Felty and R. Leino
- End User Panel Microsoft, NASA, Siemens...
Defining the scientific objective

Some time before deadline for proposals
Support a security infrastructure based on Proof Carrying Code for global computers
Defining the scientific objective

Some time before deadline for proposals

Support a security infrastructure based on Proof Carrying Code for global computers

- Proof Carrying Code (PCC) is a radically new approach to security in which mobile code comes equipped with a logical certificate
Some time before deadline for proposals

Support a security infrastructure based on Proof Carrying Code for global computers

- Proof Carrying Code (PCC) is a radically new approach to security in which mobile code comes equipped with a logical certificate
Defining the scientific objective

6 months before deadline for proposals
Support a security infrastructure based on Proof Carrying Code for JVM-enabled devices

- Widely deployed and strong industrial interest
- Active research community and tool support
- Concrete and well understood security problems
Defining the scientific objective

4 months before deadline for proposals

Support a security infrastructure based on Proof Carrying Code that allows precise, efficient, and flexible enforcement of policies for JVM-enabled devices

- Use type systems and program logics
- for information flow and resource control policies, and for functional verification
- exploring new formats of certificates and novel certificate generation mechanisms
Defining the scientific objective

Some time after start of the project

Develop basic technologies to support a security infrastructure based on Proof Carrying Code that allows precise, efficient, and flexible enforcement of policies for JVM-enabled devices

In reaction to first review,

- the focus of the project was sharpened, and priority was given to developing basic technologies;
- tool development and experimentation, in particular on-device checking, was made a secondary objective.
Writing a detailed work plan is a very big investment, but also a good opportunity for exchanges between partners. Later, a well defined workplan is a great asset.

- Consortium
- Organization
- Workplan: focus and simplicity
From a scientific objective to a work plan

- **Consortium**
  - Human effort in an IP is large (> 1000 man*months)
  - Build your dream team!
  - When setting up the consortium, provide clear rules

- **Organization**

- **Workplan:** focus and simplicity
From a scientific objective to a work plan

- Consortium
- Organization
  - Share responsibilities
  - Hold regular conference calls
  - Arrange one physical meeting
  - Use collaborative tools

Workplan: focus and simplicity
From a scientific objective to a work plan

- Consortium
- Organization
- Workplan: focus and simplicity
  - leave side topics that deserve a EU project on their own
  - aim for a selected set of objectives, avoid dispersion and duplication
  - avoid tasks with too many partners, and partners with too many tasks
  - keep the structure of the project simple, and the number of deliverables reasonable
Hold a scientific kick-off meeting:
- Present overall approach and describe scientific challenges
- Refine work plan:
  - focus on MIDP
  - foundational certificates based in Coq
- Precise responsibilities

Arrange many small meetings:
- many tasks had their own kick-off meeting (proved valuable to initiate new collaborations!)
- for critical tasks, designated working groups held several small meetings (e.g. for the definition of the Mobius logics)

Use collaborative tools (forge, svn, wiki)
Starting the project
Management issues

- Set-up appropriate managerial structure and clear rules
- Be attentive towards partners situation and needs
  - hiring of personnel
  - change of partners
  - partners with inadequate status
- Keep management lightweight

A project office with one person dedicated to the project is an excellent means to ensure efficient and lightweight management!
Running the project

- Flexibility
  - Workplan: foundational certificates, on-device checking
  - Partner involvement: movements between tasks, changes of task leaders

- Promote internal communication and collaboration

- Encourage partners involvement in external communication
  - schools
  - tutorials
  - workshops
Focus of FET and critical mass of IP provide excellent opportunity to tackle challenging foundational problems.

After 2 years activity, Mobius has a strong identity and visibility, and is widely recognized as a main actor in security of programming languages.

- 150+ contributions in major journals and conferences, invited lectures in major venues, organization of workshops and schools, etc.

From the inside, the Mobius experience is much appreciated by younger and senior researchers of the consortium!