MRG

IST–2001-33149

Mobile Resources Guarantees

Review Report N°: 3

Covering period 1.1.2004 - 30.4.2005

FINAL REVIEW

Report Preparation Date: 11.4.2004

Classification:

Contract Start Date: 1.1.2002 Duration: 40 months

Project Co-ordinator: Donald Sannella, University of Edinburgh

Information Society Technologies

Date of the Review: 5.4.2004, 16:00-19:00.

Place of the Review: Univ. of Edinburgh, Appleton Tower, Crichton Street, AT 2.02.

Consortium Present: see attendance list.

Reviewers:

Prof. Christopher Hankin (UK)

Prof. Paola Inverardi (IT)

Prof. Miroslaw Malek (DE)

European Commission:
Wide Hogenhout

Table of Contents

1. INTRODUCTION

1.1. Purpose of the review

According to Annex III of the contract (Special Conditions for the IST Programme - FET) the technical verification should objectively establish:

- The degree of fulfillment of the *project* work plan;
- The degree of achievement of the *project* objectives as described in Annex I;
- The degree of fulfillment of the deliverables as described in Annex I;
- Any elements which may give rise to reasonable doubts as to the reality of the resources that the *contractors* purport to have employed;
- Any elements which may give rise to reasonable doubts as to the use of reasonable endeavours by the *contractors* to achieve the results aimed at by the *project;*
- Any elements which may give rise to reasonable doubts as to the likelihood of the achievement of the results aimed at by the *projec*t, or which can reasonably be expected to result in a considerable diminution of the use potential of such results

and may recommend:

Any course of action that may be required in order to achieve the project objectives and/or remedy non-performance .

1.2. Summary description of the project

The overall aim of MRG project is to develop proof-carrying code for resource-related properties where proofs are generated from typing derivations in a resource-aware type system. It is one of the 13 projects that is a part of the **Global Computing** initiative.

This review covers the final project period (including the four months extension) 1.1.2004-30.4.2005.

1.3. Follow up from previous review

The previous review was positive. After some initial difficulties with project's start-up, already at the time of the second review the project caught up with all deliverables and started producing leading edge research in the area of Proof Carrying Code with guarantees of resource usage. There were no specific recommendations in the 2nd review except for staying on track and encouraging a dissemination of this work among embedded systems and related industrial communities. It seems that with new links to industrial partners such as SAP and Siemens in the follow-up project MOBIUS this ambitious goal can be achieved.

The consortium has stayed on track with quality research and therefore followed the recommendation.

2. GENERAL ASPECTS

2.1. Overall appraisal of the status of the project

For critical applications, resource awareness is a crucial asset. This project developed an infrastructure needed to equip mobile code with independently verifiable certificates describing resource behaviour.

The project has successfully reached its key objectives. In particular, the following achievements are noted:

- Development of proof carrying code techniques for resource-related properties, mainly concerning heap-usage.

- A working proof carrying code system for programs written in a high-level language such as Java which are compiled to byte-code language (Grail). Heap-usage bounds are automatically inferred and incorporated in certificates carrying unforgeable proofs ensuring that the bounds are respected.

- Development of a framework for formal certificates of resource consumption, consisting of a program logic for an appropriate virtual machine.

- Development of an end-to-end methodology and case study for a heap problem.

- Development of methods for machine generation of certificates for appropriate high-level code (Camelot and Java), e.g., in the form of invariants using type systems.

We thus acknowledge the successful completion of the project.

2.2. Status and overall assessment of Deliverables

All deliverables have been received on time, although some of them in a draft form but we feel confident that by the end of April the team will not only deliver all expected deliverables in their final form but will also surpass some goals.

Deli .No.	Deliverable Name	WP No.	Est. Pers	Deli. Type	Planned Delivery	Receipt Date
D6g	Total correctness	**WP6**	18.7	prototype	4/05	3/05
D7a	Extension of type system by allowing user annotations (optional task)	**WP7**	4	report	6/04	1/05
D7c	Extension of basic type system to object-oriented language	**WP7**	6	prototype, report	9/04	[4/05]
D7d	Methods to infer type annotations automatically	**WP7**	10	report, maybe prototype	5/04	1/05
D7e	Extension of basic type system to mutable state and concurrency	**WP7**	2	report	9/04	3/05
D8a	Relationship between proof-based certificates and present-day security management	**WP8**	6	report	10/04	2/05
D8b	Certificate-based resource manager	**WP8**	6.5	prototype	4/05	3/05
D8d	Methods for estimating costs of native methods	**WP8**	2	report	8/04	1/05
D8e	Expressing and relating resource policies	**WP8**	4	report	4/05	[4/05]
D9b /c	Advanced techniques of certification	**WP9**	2.5	report	12/04	3/05
D11 e	Workshop and end of Year 3	**WP11**	0	workshop proceedings	4/05	4/05
D11 i	Final assessment of progress	**WP11**	0	report	4/05	[4/05]
D11 k	Technological implementation plan	**WP11**	0	report	4/05	[4/05]

All remaining Workpackages (6, 7, 8, 9, 11) are thereby completed.

All deliverables are of high quality and are accepted. No deliverables are missing except for the final version of the final report.

The group should actively pursue the dissemination of their results, especially having the software industry as the target.

WP6: Generation of certificates

Objectives: Define format of certificates and implement a certificate generator.

This package is concerned with generating mobile guarantees of resource boundedness. The guarantee, or certificate, is shipped together with the code, as

irrefutable evidence for the consumer that the code obeys the desired resource constraints. The deliverable is *accepted*.

WP7: Advances in high-level type systems
Objectives: Improve expressiveness, user-friendliness, and accuracy of the type systems developed in WP4 and WP5. The goal of this workpackage is to improve expressiveness, user-friendliness, accuracy of the type systems developed under 4 and 5. A fully automated system generating byte-code has been developed.
The deliverable is *accepted*.

WP8: Integration with existing security model
Objectives: Implement resource manager and relate proof-checking infrastructure to present-day security management.
The preceding workpackages have detailed a proof-checking infrastructure which advances the state of the art in security management capabilities. This workpackage extends understanding of this infrastructure by relating it to present-day security policies. This work provides incorporation of security policies. Automatic verification has been developed. A web-based demonstration platform that incorporates the entire MRG proof-carrying code infrastructure was completed. Key components are a certifying compiler for Camelot on the producer side, a high-level proof checker on the consumer side, and a light-weight encoding of certificates to enable automatic and independent verification. The deliverable is *accepted*.

WP9: Reducing size of certificates; negotiation vs. proof
Objectives: Explore alternatives to 100%-guaranteed certificates when these are infeasible. This workpackage is more tentative and visionary than the other ones. Proof checkers such as Isabelle need a laptop's processing power and certificate size is proportional to the code size (about 80% of the code size was required in the presented case study). The first implementation of PCP was shown. The deliverable is *accepted*.

WP11: Project management, dissemination and evaluation
Objectives: Project management, dissemination and evaluation.
The project requires close collaboration between the two sites and provides many opportunities for dissemination. Integration with other projects within global computing on mobility is encouraged. It seems that the main phase of dissemination will occur in a follow-up project in GC2 (MOBIUS) because the working code has just been completed. The deliverable is *accepted*.

2.3. Project management and co-operation

The project was well managed, in part, due to its small size. Therefore, a cooperation between the University of Edinburgh and and LMU Munich was quite intense and produced an executable PCP system.

All in all, the project made a coherent impression with close collaboration among the individual project partners.

2.4. Relation to other projects

Cooperation with the current GC projects has been identified in various forms:

- DEGAS: the mobile phone multiplayer game has been used as a case study for MRG's Camelot
- AGILE: investigation of the use of MRG framework to UML. Direct cooperation with Terlecki in Warsaw and Wirsing in Munich
- MYTHS: direct transfer, Klin, ex-MRG has joined MYTHS
- PROFUNDIS: Amadio, ex-MRG continued the MRG-related research at Marseille

Also, direct involvement and links are established with the Global Computing Initiative's follow-up projects:

- EmBounded is an FET-Open STREP project on resource bounds in embedded systems that started in early 2005, building on the results of the MRG project and specifically work on Grail and the Grail byte-code logic. Partners include LMU Munich and AbsInt.
- MOBIUS is a FET-GC2 Integrated Project proposal that will build on the results of MRG.

3. TASKS AND ACTIVITIES

3.1. Performance of technical tasks

Work essentially progressed as planned and showed excellent and good results in all WPs. The results in all these workpackages are presented in the deliverables. Assessment of the final year results is provided in Section 2.2.

3.2. Scientific evaluation and performance

The project has pursued in a comprehensive manner proof carrying code techniques for resource-related properties in mobile software systems. It has developed fully automatic certificate generation techniques and web-based demonstration platform that incorporates the entire MRG proof-carrying code infrastructure.

Major project results were the development of PCC infrastructure, certificate generation, heap space inference, termination logic, determining inadequacy of probabilistically checkable proofs with respect to efficiency and a demonstration platform supporting Java. The project is at the forefront of research and represents the-state-of –the-art in proof carrying code techniques for resource-related properties in mobile environments.

The project's publication record is of a high quality and with over 20 refereed publications should make a scientific impact within and beyond the limits of the security and mobility communities.

4. APPLICATION - EXPLOITATION – DISSEMINATION PERSPECTIVES

4.1. Plans for dissemination of results

The project pursues the usual academic dissemination plans, in particular by publications, presentations at public events, organization of workshops and by the operation of a public project website at http://groups.inf.ed.ac.uk/mrg/. A flyer summarising the key contributions of the project should be soon available.

Several attempts have been made to develop relationships with some of the companies that have shown interest in MRG by setting up collaborative follow-on projects. So far, the following attempts to secure funding have been successful or seem likely to succeed:

- EmBounded is an FET-Open STREP project on resource bounds in embedded systems that started in early 2005, building on the results of the MRG project and specifically work on Grail and the Grail bytecode logic. Partners include LMU M unchen and AbsInt.
- MOBIUS is a FET-GC2 Integrated Project proposal that will build on the results of MRG. Partners include Edinburgh and LMU Munich and industrial partners such as Trusted Logic, France Telecom and SAP. An industrial User Panel includes about a dozen companies from a range of relevant sectors of industry.
- The Edinburgh group have a proposal for a collaborative project with Helixion (a local SME in the mobile phone sector) on digital rights management and secure multimedia.

4.2. Impact assessment of project results

The project may have long-term impact on the industrial practice of certificate and resource management in mobile systems. The project results should be considered as foundational and preliminary, such that immediate wide-spread industrial application cannot be expected. The promising venue to achieve industrial impact seems to be a follow-up project MOBIUS where industrial partners expressed interest in proof carrying code technology. Long term, the actual use of developed frameworks, methodologies and techniques in the form of concrete case studies that are formulated by industrial partners and concern variety of resources might result in a successful technology transfer.

Since the work is continued in the frame of the new GC2 programme in the forthcoming MOBIUS integrated project there are excellent prospects to make an impact on research and industry.

5. RECOMMENDATIONS

The tradeoff between high precision of proof systems and high efficiency should be further pursued. In order to improve the prospects of wide-spread use of the project results, we recommend preparation of a brochure which clearly presents the main project results and tradeoffs to potential users. This brochure should clearly describe:

- the proof carrying code infrastructure and its use,
- the case study and potential applications to resource-related properties,
- specification of potential benefits of resource-aware computing as well as time and space overhead.

6. OTHER POINTS OF SPECIAL INTEREST

None.