AVISPA

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Review Report N°: 1

Covering period 01.01.2003 - 31.12.2003

1st Year Review

Report Preparation Date: 03.02.2004

Classification:

Contract Start Date: 01.01.2003 Duration: 30 months

Project Co-ordinator: Allesandro Armando

Information Society Technologies

Date of the Review: 27.01.2004

Place of the Review: Brussels

Consortium Present:

David Basin, ETH Zurich
Jorge R. Cuellar, Siemens AG, Munich
Laurent Vigneron, INRIA -Nancy
Sebastian Modersheim, ETH Zurich
Michael Rusinowitch, INRIA-Lorraine

Reviewers:

Howard Barringer (UK, rapporteur)
Manuel J. Fernández Iglesias (ES)
Konrad Wrona (PL)

European commission: Leonardo de Flores

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

1.2. Summary description of the project

The project aims to develop technology and tools for the formalisation and analysis of industrial strength security protocols and security-related aspects of general communications protocols, based on the results of a previous FET-funded assessment project (AVISS). The intended contributions span from the theoretical foundations of protocol verification to the tools needed to test and verify security in communication protocols.

Keywords: formal methods, verification, security, cryptography.

1.3. Follow up from previous review

This is the first review of this project.

2. GENERAL ASPECTS

2.1. Overall appraisal of the status of the project

Significant progress has been made during the first year towards the goals and objectives of AVISPA. All planned deliverables for the reporting period have been produced and all the success criteria, as specified in the Technical Annex, have been achieved. In particular:

- The development and enhancement of HLPSL and its TLA-based semantics, a security protocol specification language whose basic design was initiated during a previous project (AVISS);

- The development of IF, a lower level representation formalism to represent security-related aspects of communication protocols. IF provides a common representation framework for all the verification and analysis tools in the AVISPA toolset;
- The establishment of the AVISPA library and initial population with a wide selection of security protocols and associated properties (the problem set) mostly being drafted by the IETF;
- Assessment of the current AVISPA verification tools against the current problem set of the library.

Notwithstanding these successes, it appears the AVISPA specification languages and tools have been developed in a rather isolated way. Clearly there are other approaches to the formal verification of security-related aspects of protocols and it would be appropriate for some justification to be given on why particular choices have been made and that, in particular, it is not appropriate to reuse developed technology and tools from other areas of formal modelling and verification. The reviewers are not being critical of the successes, but they believe it is important to justify the particular direction being followed.

For the future, it is recommended that between work packages 6, 7 and 8, the consortium clarifies for future potential external users and practitioners the capabilities and limits of the AVISPA toolset. At present, it is not clear what specific aspects of security are considered beyond the scope of the project. Note that security is more and more a key aspect in protocol design, and what a user of AVISPA can expect from it should be crystal clear from the beginning.

2.2. Relevance of the work carried out and planned to the current state-of-the-art in the field

The members of the consortium seem to be working at the leading edge. Significant advances have been reported in international conferences and journals.

However, as pointed out above, it is not clear how the advances and/or approaches of other leading research groups impact upon the AVISPA approach; some future clarification would be helpful.

2.3. Status and overall assessment of Deliverables

List of deliverables DUE to be submitted for this review and which ones if any that have not been received or were not ready.

D1.1	Periodic Progress Report No 1	Accepted
D2.1	The High-Level Protocol Specification Language	Accepted

D2.3	The Intermediate Format	Accepted
D3.3	Session Instances	Accepted
D4.2	Partial-Order Reduction	Accepted
D4.3	Heuristics	Accepted
D4.4	The AVISPA Tool v.1	Accepted
D5.1	Abstractions	Accepted
D6.1	List of Selected Problems	Accepted
D7.1	Experimental Setup	Accepted
D7.2	Assessment of the AVISPA Tool	Accepted
D8.2	Project Presentation	Accepted
D8.3	Dissemination and Use Plan	Accepted

The team has produced a comprehensive set of deliverables, as specified in the work plan, addressing relevant achievements made during the year and linking to the partners' published papers. The quality of work and professionalism is very high; scientifically the work appears to be very good and at the leading edge in this particular field. The team has a good project website where the deliverables and related material can be found. However, the reviewers noted that some of the outputs attributed to the first year's work clearly developed from much earlier work (e.g. there was an article submitted for journal publication at least 2 years earlier, and also two PhD theses. It is clearly unnecessary for the team to over-claim on their outputs and we hope, for the future, they are able to keep a clearer separation between direct output of the project and other related deliverables.

2.4. Project management and co-operation

The core of this partnership has been working together in previous projects and hence startup costs were considerably lessened. The general organisation and management of the overall project appears to be highly professional. Cooperation and collaboration amongst the partners also appears to be very successful.

2.5. Relation to other projects

The periodic progress report for year 1, D1.1, provides an update to the State-of-the-Art contained in the Technical Annex and action has been taken to ensure that there is some form of interaction between the related European projects as well as some US-based work. There are other related activities, e.g. the iTRUST network, within the general area of security and trust and it may be appropriate for the AVISPA consortium to expand their range of contacts.

2.6. Plans for dissemination of results

Dissemination of the project's work has been good. The interaction with the standardisation groups/bodies is strong and the AVISPA team may well have the potential to influence on-going work – but the difficulties of achieving this are only too readily understood.

2.7. Impact assessment of project results

It is perhaps too early to try to provide an assessment on the potential effectiveness of the AVISPA toolset, however, what has been achieved so far shows much promise.

3. TASKS AND ACTIVITIES

3.1. Performance of technical tasks

The work undertaken within the technical tasks is in line with the expectations and there are no major concerns. The Progress Report describes thoroughly the main achievements for the period evaluated (i.e. first year) and no significant doubts arise with respect to the reality of the resources employed. No significant delays have been identified either.

3.2. Scientific evaluation and performance

The progress made on the characterization of security-related aspects of communication protocols is remarkable. However, most of the results apply to fully functional aspects that can be modelled in a lazy intruder scenario, like the procedural aspects of key management or key-based authentication. Additionally, there are other aspects of security that should be considered, either to be supported by AVISPA or to make a clear statement on the contrary. As noted above, in the field of security it is important to clearly identify the aspects that can be handled by the AVISPA toolset. Examples of this are denial of service attacks, inter-layer security issues, or security in ad-hoc networks where the channel model considered in AVISPA might not be sufficient.

Similarly the progress on the application of "model-checking" technology is also excellent. However, the domain is highly specialised, and it appears that the verification and analysis tools gain purchase, or leverage, precisely through being tailored for the specific application area. A drawback with such an approach, however, can occur when a greater range of application is required. It is unclear what impact widening the current scope of the toolset will have upon its effectiveness. It might be appropriate for the team to give some consideration to this alongside the comments in the above paragraph. On the other hand, the reviewers note the progress that has been achieved in the falsification of security protocols.

4. APPLICATION - EXPLOITATION PERSPECTIVES

The application perspectives of AVISPA are good. Due to the proliferation of electronic services like e-commerce, security is one of the most important issues in new communication protocols.

5. SUMMARY CONCLUSIONS / RECOMMENDATIONS

Overall, the AVISPA project appears to have been excellently managed and is well on track with its initial plan. Much of this success relates to the team having worked together previously on the assessment project AVISS. We recommend no major changes in direction but do recommend that the team gives some consideration to the following points.

1. Work towards the development of a clearly identifiable AVISPA software distribution, for there are clearly users around the world who would appreciate access, even at this stage of development. At present, the AVISPA tool seems to be a collection of tools available from different places and glued together through the representation formalism, IF. Practitioners from industry will benefit from an integrated solution. For example, a user should be able to define a protocol in HLPSL and verify its properties without being aware of IF and the related intermediate steps.
2. Clarify the standing of AVISPA with respect to other approaches in formal verification of security. Analyze the pros and cons of the AVISPA approach. Specifically, contrast the pros and cons of tailored model checking (AVISPA) with respect to general model checking.
3. Try to characterize the different aspects of security that might be handled by a (any) formal verification tool, and clearly identify which of them can be analyzed using AVISPA. Give reasons not to consider the aspects left out.
4. Strengthen the efforts on dissemination of the AVISPA project, results and the toolset capabilities to industrial / professional engineers, especially those new to the field of security – the latter being a group which is most likely to gain through the use of the analysis tools.

6. OTHER POINTS OF SPECIAL INTEREST

None yet.