AVISS — Automated Verification of Infinite State Systems

(IST-2000-26410)

Report of the Kick-Off Meeting

Freiburg, Germany, May 10–11, 2001

1 Overview

The following researchers participated in the kick-off meeting of the AVISS project, which took place in Freiburg, Germany, May 10–11, 2001:

ALUFR: Sebastian Mödersheim, Luca Viganò (chair of the meeting for the absent David Basin).

UNIGE: Alessandro Armando, Luca Compagna.

INRIA: Yannick Chevalier, Michaël Rusinowitch, Laurent Vigneron.

The first day of the meeting was devoted to talks presenting the work of each contractor to the others and to an open session devoted to the comparison of the different approaches, while the second day was spent in planning and scheduling the future activities. The following sections illustrate this in more detail and summarize the results of the meeting. Further information can be found on the website of the project

`http://www.informatik.uni-freiburg.de/~softech/research/projects/aviss/`

which includes the sub-pages of the kick–off meeting.

2 Scientific Program

The meeting was held according to the following program:

Thursday, May 10		
9:30 - 13:00	**Session 1: Presentations** **Chair:** Luca Viganò	
	9:30 - 10:30	**Sebastian Mödersheim** and **Luca Viganò** Lazy Infinite-State Analysis of Security Protocols
	11:00 - 12:00	**Alessandro Armando** and **Luca Compagna** SAT-based Model-checking for Protocol Verification
	12:00 - 13:00	**Yannick Chevalier**, **Laurent Vigneron** and **Michaël Rusinowitch** Theorem-proving with Constraints for Protocol Verification
14:30 - 18:00	**Session 2: Presentation, Discussion and Brainstorming** **Chair:** Michaël Rusinowitch	
	14:30 - 15:00	**Rafael Accorsi** (ALUFR – guest talk) Towards an awareness-based semantics for security protocols
	16:00 - 18:00	Discussion and Brainstorming

Friday, May 11		
9:30 - 13:00	**Session 3: Discussion, Workplan** **Chair:** Alessandro Armando	
14:30 - 17:00	**Session 4: Conclusion** **Chair:** Luca Viganò	
	First draft of Deliverable D1.1, timetable	

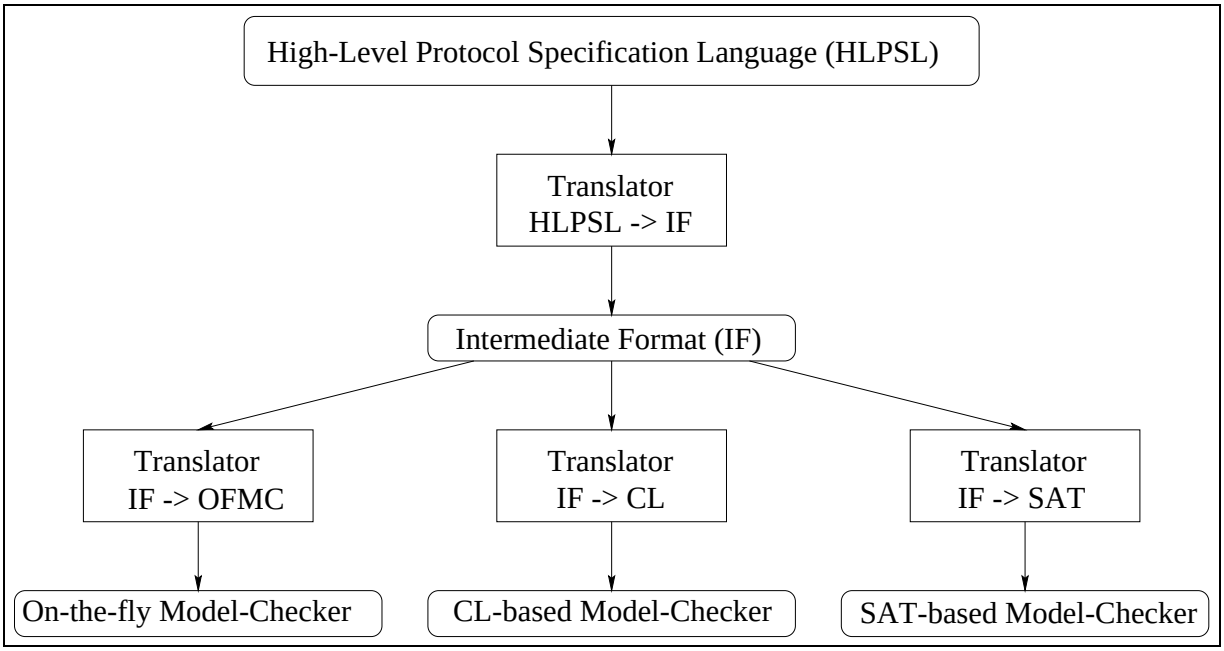

Figure 1: HLPSL and IF as a common basis for the three approaches

The presentations helped to give all sites a more detailed understanding of each other's recent work and served as a basis for the further discussions. Rafael Accorsi (ALUFR) gave a guest talk on his work focusing on new accounts for the definition of the concept of 'attack', which is crucial in our work.

In the discussion and brainstorming sessions we began working on the syntax and semantics of a common language for describing protocols (see also Section 3). To this end, we discussed critical aspects of the way such a language models the protocols: attacker model, time model, description of protocol goals (thereby defining which protocol runs would give rise to an attack), and session instances (which agents are assumed and in which role they participate in the protocol).

The last session of the meeting was devoted to the writing of the first draft of this meeting report, to planning and scheduling future activities and to administrative issues, including:

- The appointment of the Project Coordination Committee consisting of Prof. Dr. David Basin (the Project Coordinator and leader of the coordinating site ALUFR), Dr. Alessandro Armando (the leader of UNIGE) and Dr. Michaël Rusinowitch (the leader of INRIA).
- The definition of a timetable for the second workpackage (WP2 – Translation from High-Level to Intermediate Format), appointing INRIA as the lead participant, confirming the workplan of the proposal.
- The programming of the next meeting for September 2001.

3 Results — Protocol Description Languages

As described in our proposal and shown in Figure 1, in WP2 we will define a protocol description language and an Intermediate Format as a common basis for our three approaches.

The consortium agreed to use Casrul and the Casrul intermediate format, developed by INRIA, as a basis for the high level protocol specification language (HLPSL) and the intermediate format (IF). The following weeks will be spent on analyzing these languages to see which further modifications are necessary to serve the needs of the three approaches and to develop the final version of our HLPSL and IF (Deliverables D2.1, D2.2, D2.3).

4 Workpackages and Deliverables

The kick-off meeting marks the start of two workpackages. WP1 (Management and Assessment), for which ALUFR is the lead contractor, and WP2 (Translation from High-Level to Intermediate Format), for which INRIA is the lead contractor, controlling the definition of the HLPSL and IF and the development of a prototype translator.

The first deliverable of WP1 is this Report (D1.1).

Email (via the project mailing list `aviss@informatik.uni-freiburg.de`), telephone and, in particular, the project website and the shared on-line repository of the project code and documentation (managed by ALUFR using the version-management tool CVS) will foster the communication between the different sites until the next meeting.

The project website contains a summary of the project, contact information, and pointers to internal pages with restricted access (which will contain preliminary notes and ideas of the project members and is therefore not intended for the public), and will thus provide a communication and synchronization basis. During the course of the project, the website will be extended with the latest informations and results to finally form the deliverable D4.1 (final project website).