

Unbounded Verification, Falsification, and Characterization of Security Protocols by Pattern Refinement

Shaima AL AWADI, Hassan ALNOON, Sultan ALTAMIMI,
Omar BANI HASHIM and Antoine ROJAT

November 20, 2009

The paper by Cas J.F. Cremers presents the conclusions of tests conducted to produce a new verification algorithm for security protocols that allows for unbounded falsification and characterization. The algorithm makes use of the recent trend towards patterns and utilizes pattern refinement techniques to conclude a finite set of realizable patterns that represent the same set of traces as the original pattern. The paper also mentions that an instance of the new algorithm is assembled in the Scyther tool; so our presentation will put great emphasis on the description of the Scyther tool.

Our presentation will describe the techniques illustrated in the Cremers' paper; The following is a summary of the main topics discussed in each section.

- **Introduction**

As an introduction, the goals and objectives of this paper will be presented. Then a brief overview of the available tools that perform analysis on security protocols is given. Then definitions of key concepts such as unbounded verification, falsification and Characterization will be explained.

- **Security Protocol Model Overview**

In this section we're highlighting some of the main aspects in the structure of the protocol models that are compatible with existing protocol formalisms. Some of the aspects that are covered is the type of terms, events and traces used to represent the messages that are exchanged during the protocol session.

- **Pattern Notions**

In this section, we will introduce the notion of patterns in order to reason about infinite sets of traces of a protocol. An explanation on how a directed acyclic graph (DAC) can be considered a pattern is given. Realizable patterns are a type of patterns that will be explained and will also lead us to the refinement which is detailed next.

- **Pattern Refinement**

In this section we talk about the procedure used to refine a patterns representing a set of traces a into a finite set of realizable patterns of the same traces.

- **Algorithm and Proof**

In this section we highlight aspects of the new algorithm that was developed by the article writer, that analyzes security protocols. The algorithm uses the pattern refinement technique discussed in previous section and gives a proof on the correctness of the algorithms using the pattern refinement.

- **Verifying Security Properties**

In this section we show how the algorithm defined in the previous section is used for verification, falsification and characterization.

- **Performance and Comparison**

In this section, the performance of the algorithm designed using a number of various security protocols is analyzed. Then a comparison between the Scyther tool and a number of other tools is made.

- **Conclusion**

Finally, in the conclusion a summary of the overall work done and a proposal for a future work is discussed.

Bibliography :

- Cas Cremers Unbounded Verification, Falsification, and Characterization of Security Protocols by Pattern Refinement In CCS '08 : Proceedings of the 15th ACM conference on Computer and communications security, Alexandria, Virginia, USA.
- The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols In Computer Aided Verification Proceedings of the 20th International Conference on Computer Aided Verification (CAV 2008), Princeton, USA, 2008.
- Scyther - Semantics and Verification of Security Protocols Thesis, University Press Eindhoven, 2006. ISBN 90-386-0804-7. - ISBN 978-90-386-0804-4