Formal Protocol Verification Applied
07421 Executive Summary

L. Chen S. Kremer M. D. Ryan

March 18, 2008

1 Introduction

Security protocols are a core part of distributed computing systems, and are part of our everyday life since they are used in web servers, email, mobile phones, bank transactions, etc. However, security protocols are notoriously difficult to get right. There are many cases of protocols which are proposed and considered secure for many years, but later found to have security flaws. Formal methods offer a promising way for automated security analysis of protocols. While there have been considerable advances in this area, most techniques have only been applied to academic case studies and security properties such as secrecy and authentication. The seminar brought together researchers deploying security protocols in new application areas, cryptographers, and researchers from formal methods who analyse security protocols. The interaction between researchers from these different communities aims to open new research topics, e.g., identify new security properties that need verification and refine abstractions of the abstract models of crytpographic primitives.

2 The seminar

Because of the multi-disciplinary nature of the workshop, not all of the participants knew each other in advance. We devoted the first morning to five-minute introductions of ourselves and our areas of research, given by each participant (including those who did not later give a full talk). Additionally, we scheduled some tutorial talks on the first day in order to enable all of the participants to understand the relevant foundations. We had four tutorials from internationally renouned speakers, as follows:

- Kenny Paterson: Introduction to Provable Security
- Hubert Comon-Lundh: Introduction to Formal Methods Approach to Protocol Verification
- Catuscia Palamidessi: Overview of Formal Approaches to Information-hiding
- Ahmad-Reza Sadeghi: Tutorial on Security Protocols on Trusted Platforms

In addition, we had 24 technical talks, each of which brought together two or more of the themes of the workshop. The following table attempts to give a flavour for how the talks cut across and brought togther the themes of the workshop. Naturally, most of the talks involved several themes so the categorisation represented by the table should not be taken too seriously.

Dagstuhl Seminar Proceedings 07421
Formal Protocol Verification Applied
http://drops.dagstuhl.de/opus/volltexte/2008/1418

	Analysis aspect		
Protocol aspect	Design	Provable	Formal meth.
Application			
Key exchange		Armknecht Tsay	Etalle
Identity management			Bhargavan
Denial of service	Chadha		
Trusted computing		Chen	Maffei Rudolph
Payment			Klay
Password-based prot	Kremer		
Contract signing		Küsters	
Coupons		Löhr	
Voting			Ryan
Web services			Vigneron
Theory		Blanchet	Chatzikokolakis Comon-Lundh Corin Cremers Fournet Gordon Mödersheim Ritter Smyth

3 Microsoft sponsorship

The seminar was sponsored by Microsoft Research Cambridge. A special dinner was held on Thursday evening to note this contribution.

4 Conclusion

The seminar has led to much extensive discussion among the participants during and after the event. Quite a few of the papers presented have now been published.