

Preface

In 2017, for its 25th edition, the International Security Protocols Workshop returned to Cambridge, UK, but moved from charming Sidney Sussex to the majestic grounds of Trinity College, where it will remain for the foreseeable future as one of us is now a Fellow there.

Our theme this year was “multi-objective security”. Security protocols often have more than one objective. For example, entity authentication holds only during the protocol run, but data implicitly authenticated by the session persists long afterwards. When are such temporal disparities essential and when are they inadvertent? Protocols may also have multiple objectives because they have multiple stakeholders with potentially-competing interests. Alice’s access may be Bob’s risk: how do we design protocols to satisfy both? How do we detect protocols serving one master better than the other? Do we even know where the protocol came from and what its authors’ objectives are? How do they interact with the policies of resource owners? What about data provenance?

As usual, the workshop theme at SPW is not prescriptive. It is not intended to restrict the topic of the paper, but to help provide a particular perspective and focus to the discussions. Our intention is to stimulate discussion likely to lead to conceptual advances, or to promising new lines of investigation, rather than to consider finished work. If you are considering participating in a future SPW, and we hope you do, please consider the year’s theme as a springboard rather than a fence.

An initial draft of each position paper was circulated informally at the workshop. The post-proceedings volume you hold in your hands contains revised versions that were edited and updated by the authors to reflect the discussions and contributions triggered by the lively discussions accompanying the workshop presentations. Following SPW tradition, for each paper we also present a curated transcript of the ensuing discussion. Wherever possible we have excised the initial monologue in which the presenter said the same things that can be found in more polished form in the post-proceedings paper.

The SPW admits participants by invitation only. To be considered for invitation, please send us a short, indicative submission by the announced deadline. The call for papers for the next available workshop, while not yet out at the time of writing, is widely distributed: with a modest amount of luck you will be able to find it on the web using your favourite search engine.

August 2017

Frank Stajano
Jonathan Anderson
Bruce Christianson
Vashek Matyáš

Security Protocols XXV

25th International Workshop, Cambridge, UK, March
20–22, 2017, Revised Selected Papers

Stajano, F.; Anderson, J.; Christianson, B.; Matyáš, V.
(Eds.)

2017, XI, 307 p. 19 illus., Softcover

ISBN: 978-3-319-71074-7