Preface

This volume collects the revised proceedings of the 22nd International Security Protocols Workshop, held at Sidney Sussex College, Cambridge, England, from March 19 to 21, 2014.

The theme of this workshop was "Collaborating with the Enemy." There is an ambiguity about collaboration, as the dictionary definition[1] reveals:

col-lab-o-rate:
1. To work together, especially in a joint intellectual effort.
2. To cooperate treasonably, as with an enemy occupation force in one's country.

It has always been tricky to understand who is the enemy of Alice, under what circumstances that animosity might change, or what happens when Bob declares his stance (either toward Alice or her enemy). But we have certainly seen all our paranoid dreams of the last 20 years come true. And so the question becomes – what shall we wish for next?

"Attackers" now control so much of our infrastructure that we cannot achieve any serious distributed service without their cooperation. Interestingly, this remains true even if we interchange our view about whom we regard as the service provider, and whom as the protocol hacker subverting the (supposed) legitimate service. Spies have no privacy now either. Is this a zero-sum game, resulting in a straightforward shoving match, or are there security innovations that both parties have a positive incentive to support?

As with previous workshops in this series, each paper was revised by the authors to incorporate ideas that emerged during the workshop. These revised papers are followed by a revised transcript of the presentation and ensuing discussion.

Our thanks to Lori Klimaszewska for the initial transcription of the recorded workshop discussions, and to all but two of the authors for their kind and timely collaboration with revising these transcripts and their position paper. Particular thanks to Simon Foley and Virgil Gligor for joining us on the Program Committee. Last but not least, we thank GCHQ for providing us, perhaps appropriately, with financial support.

We hope that reading these proceedings will encourage you to join in the debate yourselves, and perhaps even to send us a position paper for the next workshop.

September 2014

Bruce Christianson
James Malcolm
Vashek Matyáš
Petr Švenda
Frank Stajano
Jonathan Anderson

[1] http://www.thefreedictionary.com/collaborate, accessed September 2, 2014

http://www.springer.com/978-3-319-12399-8

Security Protocols XXII
22nd International Workshop, Cambridge, UK, March 19-21, 2014, Revised Selected Papers
Christianson, B.; Malcolm, J.; Matyas, V.V.; #venda, P.; Stajano, F.; Anderson, J. (Eds.)
2014, XI, 373 p. 40 illus., Softcover
ISBN: 978-3-319-12399-8