Security Standardisation Research 2014: Programme

Royal Holloway, 16th/17th December 2014

Tuesday 16th December 2014

8:30-9:00 Registration

9:00-9:15 Welcome and opening remarks

9:15-10:15 **Keynote 1** **Charles Brookson**, *How to Make Standards* (chair: Chris Mitchell)

10:15-10:45 **Coffee**

10:45-12:15 **Session 1** **Cryptographic Evaluation** (chair: Michael Ward)

Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azzurra Marson, Arno Mittelbach and Kenneth G. Paterson. *Unpicking PLAID – A Cryptographic Analysis of an ISO-standards-track Authentication Protocol*

Cas Cremers and Marko Horvat. *Improving the ISO/IEC 11770 Standard for Key Management Techniques*

Christopher Brown and Michael Jenkins. *Analyzing Proposals for Improving Authentication on the TLS/SSL-protected Web*

12:15-13:30 **Lunch**

13:30-15:00 **Session 2** **Standards Development** (chair: Kenny Paterson)

Phillip Griffin. *Standardization Transparency - An Out of Body Experience*

Jinwoo Lee and Pil Joong Lee. *Size-Efficient Digital Signatures with Appendix by Truncating Unnecessarily Long Hashcode*

Duncan Garrett and Michael Ward. *Blinded Diffie-Hellman: Preventing Eavesdroppers from Tracking Payments*

15:00-15:30 **Tea**

15:00-16:00 **Session 3** **Analysis with Formal Methods** (chair: Phillip Griffin)

Paul Rowe, Moses Liskov and Joshua Guttman. *Security Goals and Evolving Standards*

Antonio Gonzalez, Sonia Santiago, Santiago Escobar, Catherine Meadows and Jose Meseguer. *Analysis of the IBM CCA Security API Protocols in Maude-NPA*

Efstathios Stathakidis, Steve Schneider and James Heather. *Robustness Modelling and Verification of a Mix Net Protocol*

19:00-late **Conference dinner (Crosslands Suite)**

Wednesday 17th December 2014

9:15-10:15 **Keynote 2** **Marijke de Soete**. *Bridging Security Standardisation Research with Industry and Government* (chair: Liqun Chen)

10:15-10:45 **Coffee**

10:45-12:15 **Session 4** **Potential Future Areas of Standardisation** (chair: Catherine Meadows)

Alan Abdulla, Sabah Jassim and Harin Sellahewa. *Stego Quality Enhancement by Message Size Reduction and Fibonacci Bit-plane Mapping*

Mark Manulis, Douglas Stebila and Nick Denham. *Secure Modular Password Authentication for the Web using Channel Bindings*

Nils Fleischhacker, Mark Manulis and Amir Azodi. *A Modular Framework for Multi-Factor Authentication and Key Exchange*

12:15-13:30 **Lunch**

13:30-14:30 **Panel** **Formal Verification and Analysis of Protocols in Standards Development and Evolution** (panel chair: Joshua D Guttman; panel members: Karthikeyan Bhargavan, Cas Cremers, Chris Mitchell and Kenneth Paterson)

14:30-15:00 **Tea**

15:00-16:15 **Session 5** **Improving Existing Standards** (chair: Pil Joong Lee)

Feng Hao and Siamak Shahandashti. *The SPEKE Protocol Revisited*

Britta Hale and Colin Boyd. *Computationally Analyzing the ISO 9798-2.4 Authentication Protocol*

Closing remarks