

AUTHENTICATION FOR THE FUTURE INTERNET OF THINGS

Melbourne, Australia / November 28-30, 2018

PROGRAMME

WEDNESDAY NOVEMBER 28. 2018

8:30-9:15. Registration

AUD65 payment for the Thursday evening Workshop Dinner.

PLEASE NOTE: Advance registration was requested for dinner and the evening workshop.

As there are no credit or debit card facilities available, all payments are due in cash; tickets and receipts will be provided upon payment.

+++++

UNLESS OTHERWISE STATED, ALL PLENARY SESSIONS ARE IN ROOM TBA

Workstream rooms will be allocated on a daily basis.

9:15 – 10:30. Session Chair, Prof. Lynn Batten, Deakin University, Australia

9:15-9:30. Introduction and announcements. Lynn Batten, Deakin University

9:30-10:30. Mr. Matt Tett, Managing Director of Enex TestLab, 274 Victoria Street

Brunswick Victoria, and Chair WS5 – Cyber Security & Network Resilience IoT Alliance Australia.

Title: Why authentication is critical to security in an IoT world.

10:30-11:00. Break outside the plenary room

11:00 – 12:30. Work streams in allocated rooms.

12:30-1:30. LUNCH in the basement food fair

1:30 – 3:30. Session Chair Dr. Harry Bartlett, QUT.

1:30- 2:30. KEYNOTE HUGH WILLIAMS, Emeritus Professor, Department of Mathematics and

Statistics, University of Calgary, Alberta, Canada.

Title: The Role of Number Theory in Authentication: An Overview.

2:30 – 3:30. Professor Margreta Kuijper, Department of Electrical and Electronic Engineering,

Melbourne University.

Title: Resilient linear systems under attack.

3:30 – 4:30. Work streams in allocated rooms.

4:30- 5:45. RECEPTION in the central foyer. HOST: Deakin's Centre for Security, Resilience and Innovation (CSRI).

6:00 – 10:00. Dr. Ray Hunt, University of Canterbury, New Zealand.

Demonstration at Building 8, Level 9, Room 48 (8.9.48), 360 Swanston Street

Melbourne, entitled “Practical Experience with IoT INSecurity - A Hands-on IoT Workshop”:
Those who are participating in the evening demonstration meet with Dr Ray Hunt at 5:30 at the Reception to go to RMIT. Please remember to take along your tickets.

DINNER: Please make your own arrangements; suggestions can be found on the workshop website.

THURSDAY NOVEMBER 29. 2018

UNLESS OTHERWISE STATED, ALL PLENARY SESSIONS ARE IN ROOM TBA

8:45 -10:45. Session Chair Professor Lejla Batina, Radboud University, The Netherlands.

8:45 – 9:45. Dr. Damith Ranasinghe, Director, AutoID Lab, School of Computer Science, University of Adelaide, South Australia.

Title: Can Physical Unclonable Functions be used to realize lightweight dynamic authentication for IoT devices?

9:45 – 10:45. Dr. Jürg von Kaenel, Senior Manager, IBM Research – Australia Lab, Melbourne.

Title: I really don't want to manage my IoT devices.

10:45 – 11:15. Break in the lobby area

11:15 – 12:30. Work streams in allocated rooms

12:30 – 1:30. LUNCH in the basement food fair

1:30 – 3:30. Session Chair Professor Seng Loke, Deakin University.

1:30 – 2:30. Lejla Batina, Professor, Institute of Computer and Information Sciences, Radboud University, Nijmegen, The Netherlands.

Title: Side-channel attacks on IoT devices.

2:30 – 3:30. PANEL moderator **Professor Ghassan Beydoun**, University of Technology, Sydney.

Title: Security Compliance and Regulations in IoT Age

Panel Members:

Prof. Bart Preneel,

Dr. Jürg von Kaenel,

Mr. Julian Faye,

Ms Helaine Leggat.

3:30 – 4:00. Break outside the plenary room

4:00 – 5:30. Work streams in allocated rooms

6:30. Meet at Batmans Hill hotel, 623 Collins St at Spencer St, to walk to dinner together.

19:00-22:00. Workshop Dinner (for those who have signed up and paid). Saint & Rogue, 582 Little Collins Street. *(All food is halal and includes appetisers, choice of main, choice of dessert. Drinks must be paid for yourself as you order. Tap water will be provided be on the tables.)*

Please bring your ticket as it will be proof of payment.

FRIDAY NOVEMBER 30. 2018

UNLESS OTHERWISE STATED, ALL PLENARY SESSIONS ARE IN ROOM TBA

8:45 – 10:45. Session Chair Ms. Helaine Leggat, MAICD, CISSP, CISM, CIPP/US, CIPP/IT, Principal Lawyer at Sladen Legal.

8:45 – 9:45. KEYNOTE BART PRENEEL, Professor and Director of the **Computer Security and Industrial Cryptography** group (COSIC), KULeuven, Leuven, Belgium.

Title: Technology and Regulatory Challenges for the IoT.

9:45 – 10:45. Professor Seng Loke, School of Information Technology, Deakin University.

Title: Cooperative IoT: a Trust Challenge.

10:45 – 11:15. Break outside the plenary room

11:15 -12:30. Work streams in allocated rooms

12:30 – 1:30. LUNCH in the basement food fair

1:30 – 2:45. PANEL: Moderated by **Dr. Leonie Simpson**, Queensland University of Technology.

Title: University/industry internships – pros and cons

Panel Members:

Dr. Veelasha Moonsamy, Utrecht University, The Netherlands,

Ms. Golnoosh Tajadod, co-founder of FlexRule,

Dr Peter Steinle, Science & Innovation Group, Bureau of Meteorology,

Ms. Rachel Geddes, Senior Business Developer, ARP]ntern.

This panel is supported by ARP]NTERN (<https://aprintern.org.au/>).

2:45 – 3:15. Break outside the plenary room

3:15 – 4:45. Work streams in allocated rooms

4:45 – 5:30. Wrap-up presentations by each work stream leader in the plenary room. Moderated by Prof. Lynn Batten.

WORK-STREAM LEADERS AND MEMBERS

1. Mathematical problems related to cryptographic authentication in low-resource environments. *Diane Donovan and Lynn Batten stream co-leaders*

Diane Donovan, UQ
Lynn Batten, Deakin
Hugh Williams, University of Calgary, Canada
Srinivasa Rao Subramanya Rao, Edith Cowan University
Margreta Kuijper, Melbourne University
Joanne Hall, RMIT
Jessica Liebig, CSIRO
Lokendra Magar, Open Learning Society
Craig Costello, Microsoft Research
Zhangang Tang, Melbourne University

2. Cryptographic algorithms for authenticated encryption with associated data. *Leonie Simpson stream leader.*

Leonie Simpson, QUT
Farhad Farokhi, Data61 and Melbourne University
Serdar Boztas, RMIT
Julian Fay, Senetas
Sitalakshmi Ventakraman, Melbourne Polytechnic
Trent Marbach, Nankai University (postdoc)
Jhak Bahadur Pun, Ministry of Health & Population, Gov't of Nepal
Harry Bartlett, QUT
Anagi Gamachchi, Deakin and RMIT (postdoc)
Naila Mukhtar, Macquarie University
Alice Johnstone, RMIT

3. Secure implementation of authenticated encryption algorithms with associated data. *Damith Ranasinghe stream leader.*

Damith Ranasinghe, University of Adelaide
Veelasha Moonsamy, Utrecht, The Netherlands
Nauman Khan, RMIT
Lejla Batina, Radboud University, The Netherlands
Ray Hunt, Christchurch, NZ
Seng Loke, Deakin University
Praveen Gauravaram, Tata Consultancy Services Limited
Su Yang, University of Adelaide
Rajeev Muralidhar, Telstra
Phil Hawkes, Qualcomm
Bao Doan, University of Adelaide

4. Legal and regulatory aspects of authentication in the IoT.

Ghassan Beydoun stream leader.

Ghassan Beydoun, UTS

Bart Preneel, University of Leuven, Belgium

Jurg von Kanel, IBM Research, Melbourne

David Goad, University of Sydney

Matt Tett, IoTAlliance, Australia

Helaine Leggat, Principal Lawyer, Sladen Legal

Laura Tomidei, UTS

Asif Gill, UTS

Igor Tesic, Telstra

Memoona Anwar, UTS

RESULTING PUBLICATIONS:

Our publication sponsors have agreed to special journal issues for which several of our participants have agreed to work. Please keep this in mind when developing research papers connected to the theme of this workshop.

Special issue: "IoT Authentication in Cryptography"— a special issue of *Cryptography* (ISSN 2410-387X). <https://www.mdpi.com/journal/cryptography> Guest editors: Leonie Simpson (lr.simpson@qut.edu.au) and Harry Bartlett (h.bartlett@qut.edu.au).

Special Issue: "IoT Authentication and Trusted Sensing" - a special issue of *Sensors* (ISSN 1424-8220). https://www.mdpi.com/journal/sensors/special_issues/AuthFIoT2018

Guest editors Seng Loke (seng.loke@deakin.edu.au), Salil Kanhere

(salil.kanhere@unsw.edu.au), Robin Doss (robin.doss@deakin.edu.au), and Leonie Simpson (lr.simpson@qut.edu.au).