ANNOUNCEMENT OF WORKSHOP ON:

AUTHENTICATION FOR THE FUTURE INTERNET OF THINGS

November 28 – 30, 2018, Melbourne, Australia

Location: Deakin Downtown, Level 12 Tower 2 at 727 Collins Street, Melbourne, 3000

Website: http://www.authiot2018.conferences.academy

Organizers: Professor Lynn Margaret Batten, Deakin University Centre for Cyber Security Research and Innovation, and Dr Leonie Simpson, School of Electrical Engineering and Computer Science, Science and Engineering Faculty, Queensland University of Technology.

NOTE: This is a tentative list only; a final list of speakers and presentations will be provided closer to the event.

KEYNOTE SPEAKERS:

1. Professor Emeritus Hugh Williams was a Professor in the Department of Mathematics and Statistics at the University of Calgary, Alberta, Canada where he held the prestigious Innovation iCORE Chair in Algorithmic Number Theory and Cryptography. Hugh graduated from the University of Waterloo with Bachelor and Master's degrees in Mathematics and a PhD in Computer Science on the topic '*A Generalization of the Lucas Functions'*. *He was awarded a* Killam Research Fellowship by the Canada Council for the period 1983-85, 'designed to provide support to scholars of exceptional ability who are engaged in research projects of broad significance and widespread interests'. In 1998, Wiley-Interscience in conjunction with the Canadian Mathematical Society published his book *'Edouard Lucas and Primality Testing'*. During his career, he has published many papers on applications of number theory to cryptography. On departing the University of Calgary, he worked for several years at the Canadian Communications Security Establishment, the Government of Canada's national cryptologic agency.

2. Bart Preneel received the Doctorate in Applied Sciences from the Katholieke Universiteit Leuven (KULeuven), Belgium, where he is currently a Professor and Director of the **Co**mputer **S**ecurity and **I**ndustrial **C**ryptography group (COSIC) which has recently officially opened its Embedded Systems Security Lab, the culmination of a five-year project sponsored by a 400k EUR grant from the Hercules Foundation for fundamental and strategic research.
Bart is a world-renowned cryptography expert, and aside from his other responsibilities, is on the board of management of EEMA, the leading independent non-profit, European think tank focusing on identification, authentication, privacy, risk management, cyber security, the Internet of Things and mobile applications.
Bart is also a well-known saxophone player and jazz conductor. You can see Bart conducting his band in The Netherlands here: https://www.youtube.com/watch?v=13Ndz0qKiuM and in Rio de Janeiro on this page: http://thewordmagazine.com/the-hundreds/bart-preneel/

3. Dr. Veena Pureswaran is a Research Engineer who has spent more than 12 years in the Electronics industry and has held leadership positions in product development, strategy and management. She is currently the Global Electronics Industry Leader at the IBM Institute for Business Value, responsible for developing thought leadership for the industry. She is a co-author of "Pureswaran, V. and Brody P. (2014) Device Democracy: Saving the Future of the Internet of Things, IBM. 25 pages. Available at: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03620USEN

INVITED PRESENTATIONS:

Auto-ID Labs, The University of Adelaide, represented by its Director, Damith Ranasinghe. The Lab investigates Security for IoT as well as Wearable Computing and Embedded Systems, and applications of these to health and smart cities.

IoTAlliance Australia represented by Matt Tett, Managing Director and also the Cyber Security and Network Resilience Workstream Chair. Matt is also Managing Director of Enex TestLabs in Melbourne. Matt will provide workshop attendees with an overview on the IoTAA Security Strategy and the IoTAA direction for the future of IoT Security in Australia.

Prof. Seng Loke, Deakin University, Melbourne. 'Crowd-powered mobile computing and smart things.'

Prof. Lejla Batina, Radboud University, Nijmegen, The Netherlands. 'Side-channel attacks on IoT devices.'

Space is limited to 50 people, so please register (for free) early. Watch this space.
Accommodation at various levels of pricing and close to the venue will be listed on our website nearer the event.

Travel Support: See the separate form with notification of possibilities for financial support in various categories. Doctoral students with some formal knowledge of cryptography are encouraged to participate and may also apply for some travel support.

In addition to attending plenary sessions with speakers or demonstrations, each participant will belong to a work-stream, listed below. The purpose of the work-streams is to identify problems on which the corresponding team will continue to work beyond the workshop, resulting in journal publications over the years following. Doctoral research students and others with little knowledge of cryptography will be asked to participate in the 'Introduction to Cryptography' stream where the focus is on developing skills in this area.

Work-streams

1. Mathematical problems related to cryptographic authentication in low-resource environments
2. Cryptographic algorithms for authenticated encryption with associated data
3. Secure implementation of authenticated encryption algorithms with associated data
4. Legal and regulatory aspects of authentication in the IoT
5. Introduction to Cryptography (for attendees with little formal knowledge of the subject; PhD students should check this box, but read the additional requirements on the website.)

NOTES:
(i) In advance of the workshop, all major speakers will be asked to propose 2 or 3 possible research projects.
(ii) All work-streams will be led by facilitators and given detailed instructions. Facilitators and panellists will be chosen well in advance of the workshop.
(iii) By the end of the workshop, we will have identified three to five major research projects and leading players who will carry them into the future with targets of obtaining publications and funding to meet their objectives. Every workshop participant is required to join one of these teams.