The 8th International Conference on Applications and Technologies in Information Security (ATIS 2017)

Program-at-a-Glance

All talks are in MBS2.15

Thursday, 6 July, 2017	
8:15 – 17:00	On-site Registration outside MBS2.15
8:30 – 9:10	Opening/Maori and general welcome Ceremony (Wait outside MBS2.15)
9:15 – 10:15	Keynote 1 Professor Tsutomu Matsumoto (Chair: Lynn Batten)
10:15 – 10:45	Coffee/Tea Break in MBS2.04
10:45 – 12:15	Session 1 (3 papers) (Chair: Jean-Guillaume Dumas)
12:15 – 13:15	Lunch in MBS2.04
13:15 – 14:45	Session 2 (3 papers) (Chair: Clark Thomborson)
14:45 – 15:15	Coffee/Tea Break in MBS2.04
15:15 – 16:45	Session 3 (3 papers) (Chair: Sharon Lee)
16:45 – 18:30	**Reception in** MBS2.04 Sign up to go to dinner with a group.

Friday, 7 July, 2017	
8:45 – 16:45	On-site Registration
9:00 – 10:00	Keynote 2 Professor Clark Thomborson (Chair: Lynn Batten)
10:00 – 10:30	Coffee/Tea Break in MBS2.04
10:30 – 12:00	Session 4 (3 papers) (Chair: Xuyun Zhang)
12:00 – 13:00	Lunch in MBS2.04
13:00 – 14:30	Session 5 (3 papers) (Chair: Dong Seong Kim)
14:30 – 15:00	Coffee/Tea Break in MBS2.04
15:00 – 16:30	Session 6 (3 papers) (Chair: Dong Seong Kim)
16:30 – 16:45	**Closing Remarks** (By Lynn Batten)

Thursday, 6 July, 2017**

Pōwhiri, a Māori welcome ceremony, provides a special opportunity for visitors to experience Māori traditions. As a start to the conference, ATIS is privileged to be welcomed by people of the local Māori communities. The welcome takes about 45 minutes from when people arrive, and includes refreshments as follows:

8.30am ATIS attendees are asked to wait outside room MBS2.15 where they can also pick up their registration bags at the registration desk.Rita explains the pōwhiri procedure.
Karanga – Rita calls us in and directs us to our seats. Everyone sits.

8.35am Haahi Walker offers a prayer. Everyone stands for the himene (hymn) that follows, then sits down again.
Haahi welcomes everyone in Māori, and when he's finished, the hosts (led by Rita) sing in support.
Haahi explains what he has said, and offers the visitors an opportunity to respond in their own way.

8.45am Clark Thomborson responds briefly, thanking the welcoming party on behalf of ATIS.

8.50am Haahi responds briefly and demonstrates how to do the hongi, its meaning and purpose of bringing people together on their arrival into this region in partnership with Massey University. He invites the front line of visitors to come and greet the hosts, by hongi and/or shaking hands.

9.00am Haahi brings the formalities to a conclusion with a short prayer inviting everyone to have a cup of something and a biscuit.

9:10am The welcoming party leaves while conference attendees remain seated and the conference is opened by Lynn Batten.

** See https://www.youtube.com/watch?v=nxQ66-7sRP4. Lyrics: "Te aroha / Te whakapono / Te rangimarie /Tātou, tātou e". English translation: "Love / Faith / Peace / For us all".

Thursday, 6 July, 2017	
8:15 – 17:00	On-site Registration
8:30 – 9:10	Opening/welcome Ceremony (Outside MBS2.15)
9:15 – 10:15	**Keynote 1 (**MBS2.15**)** Chair: Professor Lynn Batten Professor Tsutomu Matsumoto, Yokohama National University, Japan. **Identity of Things: Nano Artifact Metrics Using Silicon Random Nanostructures**
10:15 – 10:45	Coffee/Tea Break in MBS2.04
10:45 – 12:15	**Session 1: Crypto Algorithms and Applications I** Chair: Jean-Guillaume Dumas • Michal Kedziora, Yang-Wai Chow and Willy Susilo. Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems • Praveen Gauravaram, Shoichi Hirose and Douglas Stebila. Security Analysis of a Design Variant of Randomized Hashing • Mohammad-Hossein Yalame, Mohammad-Hossein Farzam and Siavash Bayat-Sarmadi. Secure Two- Party Computation Using an Efficient Garbled Circuit by Reducing Data Transfer
12:15 – 13:15	Lunch in MBS2.04
13:15 – 14:45	**Session 2: Privacy Preserving Techniques** Chair: Clark Thomborson • Kaleb Leemaqz, Sharon Lee and Geoffrey Mclachlan. Private Distributed Three-Party Learning of Gaussian Mixture Models • Sibghat Bazai, Julian Jang-Jaccard and Xuyun Zhang. A Privacy Preserving Platform for MapReduce • Le Trieu Phong, Yoshinori Aono, Takuya Hayashi, Lihua Wang and Shiho Moriai. Privacy-Preserving Deep Learning: Revisited and Enhanced
14:45 – 15:15	Coffee/Tea Break in MBS2.04
15:15 – 16:45	**Session 3: Attacks** Chair: Sharon Lee • Bo Sun, Xiapu Luo, Mitsuaki Akiyama, Takuya Watanabe and Tatsuya Mori. Characterizing Promotional Attacks in Mobile App Store • Takeru Koie, Takanori Isobe, Yosuke Todo and Masakatu Morii. Low-Data Complexity Attacks on Camellia • Tetiana Yarygina. RESTful Is Not Secure
16:45 – 18:30	Reception in MBS2.04 Several restaurant options will be available for dinner; sign up to go in a group.

Note: underlined names indicate the speaker.

Friday, 7 July, 2017	
8:45 – 17:00	On-site Registration
9:00 – 10:00	**Keynote 2 (MBS2.15)** Chair: Professor Lynn Batten. Professor Clark Thomborson, Computer Science Department, University of Auckland **Five Decades of Software Obfuscation: A Retrospective**
10:00 – 10:30	Coffee/Tea Break in MBS2.04
10:30 – 12:00	**Session 4: Crypto Algorithms and Applications II** Chair: Xuyun Zhang • Sharmila Deva Selvi, Arinjita Paul and Chandrasekaran Pandu Rangan. An Efficient Non-transferable Proxy Re-Encryption Scheme • Wenjie Qin and Kewei Lv. Rounding Technique's Application in Schnorr Signature Algorithm: Known Partially Most Significant Bits of Nonce • Sourya Kakarla, Srinath Mandava, Dhiman Saha and Dipanwita Roy Chowdhury. On the Practical Implementation of Impossible Differential Cryptanalysis on Reduced-Round AES
12:00 – 13:00	Lunch in MBS2.04
13:00 – 14:30	**Session 5: Malware and Malicious Events Detection** Chair: Dong Seong Kim • Ruibin Zhang, Chi Yang, Shaoning Pang and Abdolhossein Sarrafzadeh. UnitecDEAMP: Flow Feature Profiling for Malicious Events Identification in Darknet Space • Naqqash Aman, Yasir Saleem, Fahim Abbasi and Farrukh Shahzad. A Hybrid Approach For Malware Family Classification • Muhamed Fauzi Bin Abbas and Thambipillai Srikanthan. Low-complexity Signature-based Malware Detection for IoT Devices
14:30 – 15:00	Coffee/Tea Break in MBS2.04
15:00 – 16:30	**Session 6: System and Network Security** Chair: Dong Seong Kim • Xiang Tian, Yu Wang, Yujia Zhu, Yong Sun and Qingyun Liu. De-anonymous and Anonymous Technologies for Network Traffic Release • Sang Guun Yoo and Jhonattan J. Barriga A. Privacy-aware Authentication for Wi-Fi based Indoor Positioning Systems • Christian Otterstad. On the effectiveness of non-readable executable memory against BROP
16:30 – 16:45	**Closing Remarks**