# 21st Information Security Conference

## ISC 2018

Guildford, September 9-12, 2018

## Conference Program

<table>
<thead>
<tr>
<th>Day</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 0</td>
<td>Sunday, 09.09.2018</td>
<td>18:00 – 20:00</td>
<td>Registration and Welcome Reception in Surrey Business School Foyer</td>
</tr>
<tr>
<td>Day 1</td>
<td>Monday, 10.09.2018</td>
<td>09:00 – 09:30</td>
<td>Registration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>09:30 – 09:40</td>
<td>Opening remarks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>09:40 – 11:20</td>
<td><strong>Session I: Software Security</strong> (Chair: Thanassis Giannetsos)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Secure Code Execution: A Generic PUF-driven System Architecture</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>Stephan Kleber, Florian Unterstein, Matthias Hiller, Frank Slomka, Matthias Matousek, Frank Kargl and Christoph Bösch</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ Lumus: Dynamically Uncovering Evasive Android Applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>Vitor Afonso, Andre Gregio, Paulo Geus, Anatoli Kalysch, Tilo Müller and Daniela Oliveira</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ ICUFuzzer: Fuzzing ICU Library for Exploitable Bugs in Multiple Software</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>Kun Yang, Yuan Deng, Chao Zhang, Jianwei Zhuge and Haixin Duan</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ How Safe is Safety Number? A User Study on SIGNAL's Fingerprint and Safety Number Methods for Public Key Verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>Kemal Bicakci, Enes Altuncu, Muhammet Sakir Sahkulubeys, Hakan Ezgi Kiziloz and Yusuf Uzunay</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>11:20 – 11:50</td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11:50 – 12:00</td>
<td><strong>Invited talk</strong> (Chair: Mark Manulis)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ouroboros - designing and deploying a global distributed ledger based on proof of stake</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><em>Aggelos Kiayias (University of Edinburgh, UK)</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12:50 – 14:00</td>
<td>Lunch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14:00 – 15:40</td>
<td><strong>Session II: Symmetric Ciphers and Cryptanalysis</strong> (Chair: Kaitai Liang)</td>
</tr>
</tbody>
</table>
- Speeding up MILP Aided Differential Characteristic Search with Matsui’s Strategy
  *Yingjie Zhang, Siwei Sun, Jiahao Cai and Lei Hu*

- Automatic Search for Related-key Differential Trails in SIMON-like Block Ciphers Based on MILP
  *Xuzi Wang, Baofeng Wu, Lin Hou and Dongdai Lin*

- Linear Cryptanalysis of Reduced-Round Speck with a Heuristic Approach: Automatic Search for Linear Trails
  *Daniel Bodden*

- Conditional Cube Searching and Applications on Trivium-Variant Ciphers
  *Xiaojuan Zhang, Meicheng Liu and Dongdai Lin*

15:40 – 16:10 Coffee break

16:10 – 17:00 *Session III: Data Privacy and Anonymization* (Chair: Jan Camenisch)

- Practical Attacks on Searchable Encrypted Relational Databases
  *Mohamed Ahmed Abdelraheem, Tobias Andersson, Christian Gehrmann and Cornelius Glackin*

- A Simple Algorithm for Estimating Distribution Parameters from n-Dimensional Randomized Binary Responses
  *Staal Vinterbo*

**Day 2  Tuesday, 11.09.2018**

09:30 – 09:40 Registration

09:40 – 11:20 *Session IV: Outsourcing and Assisted Computing* (Chair: Eiji Okamoto)

- Enforcing Access Control for Cryptographic Cloud Service Invocation based on Virtual Machine Introspection
  *Fangjie Jiang, Quanwei Cai, Le Guan and Jingqiang Lin*

- Multi-Authority Fast Data Cloud-Outsourcing for Mobile Devices
  *Yanting Zhang, Zongyang Zhang, Jianwei Liu and Yang Hu*

- Hide The Modulus: A Secure Non-Interactive Fully Verifiable Delegation Scheme for Modular Exponentiations via CRT
  *Osmanbey Uzunkol, Jothi Rangasamy and Lakshmi Kuppusamy*

- Offline Assisted Group Key Exchange
  *Colin Boyd, Gareth T. Davies, Kristian Gjøsteen and Yao Jiang*

11:20 – 11:50 Coffee break

11:50 – 12:50 *Invited talk* (Chair: Liqun Chen)

- Modular Cryptographic Protocol Design
  *Jan Camenisch (IBM Research Zurich, Switzerland)*
12:50 – 14:00  Lunch

14:00 – 15:40  Session V: Advanced Encryption (Chair: Keita Emura)

- Function-Dependent Commitments for Verifiable Multi-Party Computation
  Lucas Schabhüser, Denis Butin, Denise Demirel and Johannes Buchmann

- On Constructing Pairing-free Identity-Based Encryptions
  Xin Wang, Bei Liang, Shimin Li and Rui Xue

- Multi-Key Homomorphic Proxy Re-Encryption
  Satoshi Yasuda, Yoshihiro Koseki, Ryo Hiromasa and Yutaka Kawai

- Verifiable Decryption for Fully Homomorphic Encryption
  Fucai Luo and Kunpeng Wang

15:40 – 16:10  Coffee break

16:10 – 17:00  Session VI: Privacy-Preserving Applications (Chair: Steve Schneider)

- Platform-independent Secure Blockchain-Based Voting System
  Bin Yu, Joseph Liu, Amin Sakzad, Surya Nepal, Paul Rimba, Ron Steinfeld and Man Ho Au

- Privacy in Crowdsourcing: A Systematic Review
  Abdulwhab Alkharashi and Karen Renaud

19:00  Conference Dinner in Guildford Harbour Hotel

Day 3  Wednesday, 12.09.2018

09:30 – 09:40  Registration

09:40 – 10:55  Session VII: Advanced Signatures (Chair: Gareth Davies)

- Anonymous yet Traceable Strong Designated Verifier Signature
  Veronika Kuchta, Rajeev Anand Sahu, Vishal Saraswat, Gaurav Sharma, Neetu Sharma and Olivier Markowitch

- Strongly Unforgeable Signature Resilient to Polynomially Hard-to-Invert Leakage under Standard Assumptions
  Masahito Ishizaka and Kanta Matsuura

- A Revocable Group Signature Scheme with Scalability from Simple Assumptions and Its Implementation
  Keita Emura and Takuya Hayashi

10:55 – 11:25  Coffee break

11:25 – 12:40  Session VIII: Network Security (Chair: Ioana Boureanu)

- Fast Flux Service Network Detection via Data Mining on Passive DNS Traffic
  Pierangelo Lombardo, Salvatore Saeli, Federica Bisio, Davide Bernardi and
Danilo Massa

- Beyond Cookie Monster Amnesia: Real World Persistent Online Tracking
  Nasser Mohammed Al-Fannah, Wanpeng Li and Chris J Mitchell

- Cyber-risks in the Internet of Things: Towards a Method for Continuous Assessment
  Carolina Adaros Boye, Paul Kearney and Mark Josephs

12:40 – 14:00 Lunch & End