# CDNG Brisbane, 24 & 25 March 2020

## Day 1

## 24 March 2020

| | |
|---|---|
| **8:30am – 5:00pm** | **Conference Registration** |
| 9:00am – 9:15am | **CDNG opening address:**<br>**Major General Marcus Thompson**<br>*Head of Information Warfare for the Australian Defence Force* |
| 9:15am – 10:15am | **Keynote 1:**<br>**Title: CyBoCk: Building on the Cyber Security Knowledge Base**<br>**Professor Andrew Martin**<br>**University of Oxford** |
| 10:15am – 10:45am | **Morning Tea/Coffee Break** |
| **Session 1: Networked Systems Security, Software Systems and Database Security** | |
| 10:45am – 11:00am | **Paper Presentation 1**<br>**PLAR: Towards a Pluggable Software Architecture for Securing IoT Devices**<br>*Uzma Maroof, Arash Shaghaghi and Sanjay Jha* |

| | |
|---|---|
| 11:00am – 11:15am | **Paper Presentation 2**<br>**Title: TeleHammer: A Stealthy Cross-Boundary Rowhammer Technique**<br>*Zhi Zhang, Yueqiang Cheng, Dongxi Liu, Surya Nepal and Zhi Wang* |
| 11:15pm – 11:30am | **Paper Presentation 3**<br>**Title: Trust Management in Decentralized IoT Access Control System**<br>*Guntur Dharma Putra, Volkan Dedeoglu, Salil Kanhere and Raja Jurdak* |
| 11:30pm – 11:45am | **Paper Presentation 4**<br>**Title: Towards Flow Sampling for Deep Content Analysis**<br>*Guillaume Jourjon, Achintha Wijesinghe, Kanchana Thilakarathna and Suranga Seneviratne* |
| **11:45am – 1:00pm** | **Lunch Break** |

| | |
|---|---|
| **1:00pm – 2:15pm** | **Industry Panel** |
| **2:15 – 2:45pm** | **Coffee Break** |
| **Session 2: Cyber AI and Autonomy** | |
| 2:45pm – 3:00pm | **Paper Presentation 1**<br>**Title: AIFuzz: Artificial Intelligence-Guided Fuzzing**<br>*Shigang Liu, Chao Chen, Jun Zhang, Yang Xiang, Paul Montague and Olivier De Vel* |

| | |
|---|---|
| 3:00pm – 3:15pm | **Paper Presentation 2**<br>**Title: Nopt versus Proda: Efficient Poisoning Attacks and Defenses for Regression Learning**<br>*Jialin Wen, Minhue Xue and Haifeng Qian* |
| 3:15pm – 3:30pm | **Paper Presentation 3**<br>**Title: Unsupervised learning for network micro-segmentation**<br>*Mahmood Yousefiazar, Mohamed Ali Kaafar and Andy Walker* |
| 3:30pm – 3:45pm | **Paper Presentation 4**<br>**Title: The Audio Auditor: Participant-Level Membership Inference in Internet of Things Voice Services**<br>*Yuantian Miao, Benjamin Zi Hao Zhao, Minhui Xue, Chao Chen, Lei Pan, Jun Zhang, Mohamed Ali Kaafar and Yang Xiang* |
| 3:45pm – 4:00pm | **Coffee Break** |
| **Session 3: Cyber AI and Autonomy, Software Systems and Database Security** | |
| 4:00pm – 4:15pm | **Paper Presentation 1**<br>**Title: On Inferring Training Data Attributes in Machine Learning Models**<br>*Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Raghav Bhaskar and Mohamed Ali Kaafar* |
| 4:15pm – 4:30pm | **Paper Presentation 2**<br>**Title: Towards the Development of Robust Reinforcement Learning Algorithms in Cybersecurity Applications**<br>*Paul Montague, Tamas Abraham, Yi Han, Michael Pope, Olivier de Vel, Benjamin Rubinstein, Sarah Erfani, Tansu Alpcan and Christopher Leckie* |

| | |
|---|---|
| 4:30pm – 4:45pm | **Paper Presentation 3**<br>**Title: Characterizing and Detecting Money Laundering Activities on the Bitcoin Network**<br>*Yining Hu, Suranga Seneviratne, Kanchana Thilakarathna, Kensuke Fukuda and Aruna Seneviratne* |
| 4:45pm – 5:00pm | **Paper Presentation 4**<br>**Title: Automating Mission to Cyber Dependency Mapping for Mission Assurance**<br>*Ben Luo, Sophie Underwood, Minh Tran, Amy Stringfellow, Alexander Chambers and Ian Johnston* |

# CDNG 2020 Day 2 (Next Page)

# CDNG Brisbane, 24 & 25 March 2020

## Day 2

## 25 March 2020

| | |
|---|---|
| 8:30am – 5:00pm | **Conference Registration** |
| 9:00am – 10:00am | **Keynote 2:**<br>**Title: Global communication guarantees in the presence of adversaries**<br>**Professor Adrian Perrig**<br>**ETH Zurich** |
| 10:00am – 10:30am | **Morning Tea/Coffee Break** |
| | **Session 4: Networked Systems Security, Software Systems and Database Security** |
| 10:30am – 10:45am | **Paper Presentation 1**<br>**Title: Measuring and Analysing the Chain of Implicit Trust: A Study of Third-party Resources Loading**<br>*Muhammad Ikram, Rahat Masood, Gareth Tyson, Mohamed Ali Kaafar and Noha Loizon* |
| 10:45am – 11:00am | **Paper Presentation 2** |

| | |
|---|---|
| | **Title: A Framework of Military Wireless Body Area Networks Converged with Low Power Wide Area Networks**<br>*James Jin Kang, Wencheng Yang and Michael Johnstone* |
| 11:00am – 11:15am | **Paper Presentation 3**<br>**Title: Spatial Privacy Leakage in 3D Mixed Reality Data**<br>*Jaybie de Guzman, Kanchana Thilakarathna and Aruna Seneviratne* |
| 11:15am – 11:30am | **Paper Presentation 4**<br>**Title: Predicting random numbers with neural networks**<br>*Jihyeon Ryu and Hyoungshick Kim* |
| 11:30am -- 11:45am | **Morning Tea Break** |
| **Session 5: Formal Methods; Secure Software Engineering** | |
| 11:45am – 12:00pm | **Paper Presentation 1**<br>**Title: Corpus Distillation for Effective Fuzzing: A Comprehensive Evaluation**<br>*Adrian Herrera, Hendra Gunadi, Liam Hayes, Shane Magrath, Maggi Sebastian, Felix Friedlander, Michael Norrish and Antony Hosking* |
| 12:00pm – 12:15pm | **Paper Presentation 2**<br>**Title: Extended Abstract: Towards Practical Verified Information Flow Security for Concurrent Programs**<br>*Toby Murray* |
| 12:15pm – 12:30pm | **Paper Presentation 3**<br>**Title: What is a Secure Programming Language?**<br>*Cristina Cifuentes and Gavin Bierman* |

| | |
|---|---|
| 12:30pm – 12:45pm | **Paper Presentation 4**<br>**Title: Verified Verifiers for Verified Elections**<br>*Thomas Haines, Rajeev Gore and Mukesh Tiwari* |
| 12:45pm – 2:45pm | **Lunch Break and Poster Session**<br>**(19 Poster Presentations)** |
| **Session 6: Formal Methods; Secure Software Engineering And Cryptography** | |
| 2:45pm – 3:45pm | **Keynote 3:**<br>**Title: Machine Learning for Realistic Cyber Deception**<br>**Dr. David Liebowitz**<br>**PenTen** |
| 3:45pm – 4:00pm | **Paper Presentation 1**<br>**Title: An abstract semantics of speculative execution for reasoning about security vulnerabilities**<br>*Robert Colvin and Kirsten Winter* |
| 4:00pm – 4:15pm | **Paper Presentation 2**<br>**Title: datAFLow-guided Fuzzing**<br>*Adrian Herrera, Mathias Payer and Antony Hosking* |
| 4:15pm – 4:30pm | **Paper Presentation 3**<br>**Title: Passive Packet Sniffing Tools for Enabling Wireless Situational Awareness**<br>*Kwon Choi, Harini Kolamunna, Kanchana Thilakarathna, Suranga Seneviratne, Ralph Holz, Mahbub Hassan and Albert Zomaya* |
| 4:30pm – 4:45pm | **Paper Presentation 4** |

| | |
|---|---|
| | **Title: Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability**<br>*Yannan Li, Guomin Yang, Willy Susilo, Yong Yu, Man Ho Au and Dongxi Liu* |
| 4:45pm – 5:00pm | **Closing Remarks** |