Singapore Cybersecurity Consortium

Anchored at NUS | Computing

Cybersecurity Camp II (Deep Learning Security Workshop)
14 - 15 December 2017

School of Computing, National University of Singapore (NUS)
Seminar Room 1, COM1 #02-06
Computing 1, 13 Computing Drive, Singapore 117417

PROGRAMME

DAY 1

14 DECEMBER 2017 - RESEARCH FORUM

08:30 - 09:00	Registration
09:00 - 09:20	Introduction
09:20 - 10:40	**RESEARCH FORUM - SESSION 1** ① **USER ACTION AS AN AUTHENTICATION MECHANISM TO IMPROVE SMARTPHONE SECURITY** Arul Prakash Samathuvamani ② **PRIVACY LEAKAGE IN LONG SHORT TERM MEMORY** Lun Wang ③ **ATTACKING THE IMAGE CAPTIONING MODEL - TAKE SHOW AND TELL MODEL AS AN EXAMPLE** Jiaqi Tong ④ **COMPARATIVE EVALUATION OF SYNTHETIC DATA GENERATION METHODS** Ashish Dandekar, Remmy A. M. Zen and Stephane Bressan
10:40 - 11:00	Tea break & Poster Exhibition
11:00 - 12:20	**RESEARCH FORUM - SESSION 2** ⑤ **Side-Channel Analysis and Machine Learning: A Practical Perspective** Sylvain Guilley and Matthieu Lec'Hvien ⑥ **On the Search for Invertible Generative Adversarial Networks** Jiyi Zhang, Hung Dang, Hwee Kuan Lee and Ee-Chien Chang. ⑦ **On the Application of Deep Learning Techniques to Website Fingerprinting Attacks and Defenses** Marc Juarez and Vera Rimmer ⑧ **Recovering Types from Binaries** Teodora Baluta, Shiqi Shen and Alexandros Dimos
12:20 - 13:20	Lunch & Poster Exhibition

Subject to changes

13:20 - 15:00	**RESEARCH FORUM – SESSION 3** ⑨ **End-to-End Privacy Preserving Hadoop** Rudrapatna Shyamasundar. SecHadoop ⑩ **Learning Relations between Variables Using Deep Learning** Shiqi Shen and Soundarya Ramesh ⑪ **A Try at Task-based Dialogue Building** Sishan Long ⑫ **Early Detection of Crossfire Attacks using Deep Learning** Saurabh Misra, Mengxuan Tan, Mostafa Rezazad and Ngai-Man Cheung ⑬ **Do We Need Original Data for Training? Toward Designing Privacy-Preserving Machine Learning** Qingrong Chen, Minhui Xue, Chong Xiang, Bo Li, Haizhong Zheng and Haojin Zhu
15:00 - 15:20	Tea break & Poster Exhibition
15:20 - 16:40	**RESEARCH FORUM – SESSION 4** ⑭ **Neural Architecture Search: Insights and Long-term Horizons** Mingjie Sun ⑮ **Noise Data Augmentation for Speaker Recognition Using Conditional Generative Adversarial Networks** Peiyao Sheng ⑯ **On Lyapunov Exponents and Adversarial Perturbations** Vinay Prabhu and John Whaley ⑰ **Transferability of Adversarial Attacks in Model-Agnostic Meta-Learning** Riley Edmunds, Noah Golmant, Vinay Ramasesh, Phillip Kuznetsov, Piyush Patil and Raul Puri
16:40 - 18:00	Networking Tea Reception & Poster Exhibition

Subject to changes

Singapore Cybersecurity Consortium

Anchored at NUS | Computing

Cybersecurity Camp II (Deep Learning Security Workshop)
14 - 15 December 2017

School of Computing, National University of Singapore (NUS)
Seminar Room 1, COM1 #02-06
Computing 1, 13 Computing Drive, Singapore 117417

PROGRAMME — DAY 2

15 DECEMBER 2017 - WORKSHOP

08:30 - 09:00	Registration
09:00 - 09:30	Introduction
09:30 - 10:20	**Structure2vec: Deep Learning for Security Analytics over Graphs** Associate Professor Le Song, Georgia Institute of Technology; Principle Engineer, Ant Financial
10:20 - 10:40	Tea break & Poster Exhibition

SESSION I : DEEP LEARNING FOR SECURITY

10:40 - 11:20	**An Implementation of Web Application Firewall Based on a Deep Neural Network Detection Engine** Mr. Liang Shi, Staff Expert and Manager of Security Data Science team, Alibaba Cloud Security Mr. Min Ye, Senior Security Expert, Alibaba Cloud Security Mr. Tianlong Liu, Senior Algorithm Engineer, Alibaba Cloud Security
11:20 - 12:00	**Deep Learning for User Authentication** Dr. John Whaley, Founder and CEO, UnifyID
12:00 - 13:30	Lunch & Poster Exhibition

SESSION II : SECURITY FOR DEEP LEARNING

13:30 - 14:10	**Data Privacy in Machine Learning** Dr. Reza Shokri, Assistant Professor, National University of Singapore
14:10 - 14:50	**Adversarial Deep Learning: Attacks and Defenses** Dr. Ian Fischer – Researcher, Google Research
14:50 - 15:30	**Demo on Biometrics Security** Mr. Gao Shupeng, Baidu
15:30 - 15:40	Break
15:40 - 16:40	Research Forum Award Ceremony and Short Presentations
16:40 - 18:00	Networking Tea Reception & Poster Exhibition

Subject to changes