November 2016 | Issue 01

Concourse

A Singapore Cybersecurity Consortium Newsletter

In this issue:

KICK-OFF EVENT: TECHNOLOGY TALK

The inaugural Technology Talk was held on 2 November 2016 at the Singapore Cybersecurity Consortium, located at School of Computing, National University of Singapore (NUS). The venue was livened up with showcases of security products and services from Consortium members, whose representatives attended the event and engaged in the talks and discussions.

Welcome Address: "Partnerships in Cyber-Security"

Prof. Abhik Roychoudhury
Academic Director and Lead Principal Investigator
Singapore Cybersecurity Consortium

In the welcome address, Prof. Roychoudhury shared the objectives for setting up the Singapore Cybersecurity Consortium and the intention to create an innovation eco-system in cybersecurity involving the industry, academia, and government agencies. Depending on the maturity of the organization, the form of engagement can start from training, stepping up to discussion and advice, to finally reach research collaborations. He introduced activities to support this vision, including Consortium activities, potential translation projects, and the security education programs established at NUS as an example.

Opening Talk: "Cybercrime Trends: Need for LEA Strategy Recalibration"

Dr Madan Mohan Oberoi
Director, Cybercrime,
INTERPOL Global Complex for Innovation (IGCI), Singapore

Dr Oberoi opened the talk with a staggering statistics that showed the challenge in bringing cybercrime cases all the way to prosecution. He presented the findings on global trends in cybercrime that included new forms of crimes such as ransomware and Crime-as-a-Service, which necessitated the change in the role and strategies of Law Enforcement Agencies (LEA). Dr Oberoi shared several examples of INTERPOL's collaboration with various companies and research organizations to tap on their expertise in cybersecurity, resulting in successful investigation of cybercrime cases.

Visit *https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation* for more information on IGCI.

Talk: "Moving Forward with Cybersecurity: Key Findings from GSISS 2017 on Singapore"

Mr Vincent Loy
Partner, Financial Crime & Cyber & Data Analytics Leader,
PwC Singapore

The Global State of Information Security Survey (GSISS) 2017 is a worldwide study by PwC, CIO and CSO, conducted online from 4 April 2016 to 3 June 2016. In this talk, Mr Loy presented the key findings from the survey, showing the responses from Singapore in comparison with the global state. Among the highlights is the increase of incidents in Singapore in spite of decreasing global incidents, with phishing attacks topping the list. Information security budget is also growing for Singapore companies while global spending remains flat, which could be due to the local investment in security being at a lower maturity level compared to the global. A number of trends identified in the study are investment in security talents, biometrics, managed security services, open-source software, and Internet of Things (IoT).

Visit *http://www.pwc.com/gsiss2017* to further explore the data.

NCR PROGRAMME PROJECT PRESENTATIONS

The National Cybersecurity R&D (NCR) Programme, coordinated by the National Research Foundation (NRF) and related government agencies, was established in 2013 to develop R&D expertise and capabilities in cybersecurity for Singapore. The program spans six themes:

1. Scalable Trustworthy Systems
2. Resilient Systems
3. Effective Situation Awareness and Attack Attribution
4. Combatting Insider Threats
5. Threats Detection, Analysis and Defence
6. Efficient and Effective Digital Forensics

More information on the NCR Programme is available at *http://www.nrf.gov.sg/about-nrf/programmes/national-cybersecurity-r-d-programme*

Seven projects were awarded under the inaugural NCR grant call in October 2014, and six of them were presented at the event.

"Secure Mobile Centre: Technologies and Solutions for Securing Mobile Computing"

Prof. Robert Deng
Professor
School of Information Systems
Singapore Management University (SMU)
Website: *http://smc.smu.edu.sg/*

The project aims to create novel technologies for end-to-end mobile computing security that are tested in real world settings. These span three aspects: platform, application, and internet service.

For platform security, mobile platforms are fortified with a user-centric trust anchor, a tiny software sitting between the hardware and the OS that can resist attacks from applications and OS, and which is trusted by user for various security purposes. Application security involves analyzing, detecting, and containing mobile malware – with outcomes including real-world traces and analysis results, customized Android ROM with malware containment system and malware detection engine. Internet service security involves access control for server data as well as authentication on mobile. One of the solution developed is FaceLive, a face authentication scheme with liveness detection to resist spoofing using photos and videos.

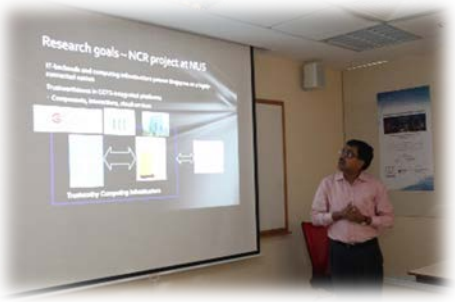
"Project SUTD-ASPIRE: Design of Secure Cyber Physical Systems"

Dr Nils Ole Tippenhauer
Assistant Professor
Information Systems Technology and Design Pillar
Singapore University of Technology and Design (SUTD)
Website: *http://itrust.sutd.edu.sg/research/projects/sutd-aspire/*

The project is a fundamental scientific research aiming to improve the security of Cyber-Physical System (CPS) of key services such as water and power. It undertakes six tasks to develop attack detection using physical-layer security techniques, dynamic control solutions, dedicated devices to provide layered defense, comprehensive and realistic attacker models, an economic framework for cost-efficient defences, and the solution deployment on physical testbeds.

Dr Nils showed the testbeds established by SUTD iTrust for Secure Water Treatment, Water Distribution, and Electric Power Intelligent Control. The project outcomes so far include EPANET-CPA Toolbox for simulating cyber attacks on water distribution systems, an attack detection algorithm that can help mitigate attacks on CPS such as Denial of Service (DoS), and proposed attacker profiles – from basic user to nation state – useful in CPS behavior analysis and security property validation., a face authentication scheme with liveness detection to resist spoofing using photos and videos.

"Trustworthy Systems from Untrusted Components"



Prof. Abhik Roychoudhury
Professor, School of Computing
National University of Singapore (NUS)
Website: *http://www.comp.nus.edu.sg/~tsunami/*

The project addresses the issue of trusting components, interactions, and cloud services in Commercial Off-the-Shelf (COTS)-integrated platforms used in Singapore's key infrastructures. Its goal is to build a trustworthy system through analysis to discover vulnerabilities, hardening of components against attacks, system-level verification involving component communication, and protection of shared data in untrusted clouds via key management as well as secure encrypted computation. While the analysis is useful to evaluate software before procurement, the hardening can fortify software that is already procured.

Prof Roychoudhury showed two videos demonstrating the tools resulting from the project – automated vulnerability detection via blackbox and whitebox fuzzing, and the Angelix automated program repair tool that successfully fixed Heartbleed. The solutions from the project had been integrated into Codejitsu, a finalist in the DARPA CyberGrand Challenge.

"Securify: A Compositional Approach of Building Security Verified System"

Dr Liu Yang
Nanyang Assistant Professor
School of Computer Science and Engineering
Nanyang Technological University (NTU)
Website: *http://securify.sce.ntu.edu.sg/*

Dr Liu shared that security verification of complex systems needed to be scalable, adaptable, and mindful of untrusted component. The Securify project aims to realize security-verified systems compositionally by performing security verification at each level of the execution stack.

Statically, this involves hardware verification, secure micro-kernel verification, security-enhanced library verification, and automatic program verification at the application level. At runtime, the verification consists of FPGA-based dynamic security analysis and runtime security verification.

Correspondingly, the project has produced ISA and VHDL verification (hardware), standard and specification verification (micro-kernel), memory safety verification (library), vulnerability verification and detection (application), malware and exploits detection (dynamic security analysis) and Android malware detection (runtime security verification).

"A Cyber-physical Approach to Securing Urban Transportation Systems"

Dr Zhou Jianying
Department Head
Infocomm Security
Institute for Infocomm Research (I2R), A*STAR
Website: *http://secuts.net*

Dr Zhou highlighted the importance of securing urban transportation system in a city with dense population like Singapore.

The project builds high-fidelity models of the cyber-physical constraints and human factors to capture potential attack propagation. Model-driven security measures are developed, which encompass legacy system protection, persistent access control, secure communications, and adaptive attack mitigation. The case study used for modelling and testing measures is the SMRT Integrated Supervisory Control System (ISCS).

One of the project outcomes is a two-factor authentication scheme for IoT devices that require a secret key / password and the device historical data, which is scalable for different devices. Other technologies include advanced SCADA firewall, virtually isolated network, network device access control, low-cost location integrity protection, and SecureRails – an open simulation platform for analysis of cyber-physical attacks on railways.

"Cyber Forensics and Intelligence"

Dr Dinil Mon Divakaran
Research Scientist
Cyber Security & Intelligence
Institute for Infocomm Research (I^2R), A*STAR
Website: *http://csi.i2r.a-star.edu.sg/*

Dr Divakaran shared that the project aimed to develop advanced forensic techniques in four areas: evidence acquisition, identification and authenticity verification, cybercrime trend analysis, and attribution and analysis.

Evidence acquisition, with focus on mobile devices, involve methods for volatile and non-volatile memory acquisition, data extraction, correlation and semantic extraction, and file carving to help recover deleted data. Advances in identification include image tampering detection with region localization, video tampering detection, and video steganalysis algorithms, which are useful in investigating document fraud or surveillance video manipulation. The cybercrime trend analysis collects and categorizes data from user-generated reports to discover trends, leading to early crime detection. Outcomes in attribution and analysis are a network anomaly detection for enterprises to identify hosts-turned-bots, and an IP traceback solution with high success rate under partial coordination among ISPs.

SPECIAL INTEREST GROUPS FORMATION

At the event, the Consortium proposed formation of Special Interest Groups (SIGs) to better focus the exchange of knowledge and forming of collaborations on specific topics in cybersecurity. Each SIG will be led by an expert researcher in the SIG topic, and consist of Consortium members as well as researchers with interest in the topic. A Consortium member may join more than one SIGs.

The Consortium will facilitate the SIGs in the form of managing the membership, scheduling and hosting SIG meetings at the Consortium venues, as well as monitoring and following up on SIG activities. At least one meeting for each SIG can take place in-between major Consortium events. The Consortium proposed five SIG topics, which are aligned with NCR themes to increase the potential of formed projects or collaborations to go further under the NCR Programme. These topics are:

1. Threat Intelligence and Incident Response
2. Data Protection and Privacy
3. Mobile Security
4. System and Software Security
5. Cyber Physical System (CPS) and IoT Security

Members were invited to sign up for the SIGs, and also to propose new SIG topics, as the SIGs could be dynamic. The Consortium aims to form the initial set of SIGs in November 2016, and start SIG activities from December 2016.

INTRODUCTION TO NCL

Dr Guo Charng Rang
Programme Director
National Cybersecurity R&D Laboratory (NCL)
Website: *https://ncl.sg/*

Dr Guo introduced NCL, a shared national infrastructure that provided realistic testing environment for cybersecurity research. The NCL helps to simplify research and experimentation effort by eliminating the need for equipment purchase and testbed set-up. It sets up ready-to-use environments and tools such as DeterLab and OpenStack, and hosts a number of real-world data sets. The team also welcomes input on environments, tools, and data that NCL users would need.

The NCL charges a rate of S$ 0.24 per node per hour, with a promotional 50% discount until May 2017.

UPCOMING EVENTS

December 2016 onwards
Special Interest Group (SIG) Meetings

19 – 20 February 2017
Cybersecurity Camp
(in conjunction with SG-CRC 2017, 21 – 22 February 2017)

May 2017
Technology Talk + Wild and Crazy Ideas (WACI) Day

June 2017 (indicative)
Seed Grant Call Launch

August 2017
Technology Talk

The next major Consortium event, Cybersecurity Camp, will be held at School of Computing, NUS. Camp lessons will be delivered on the first day (19 February 2017), to be followed by a 24-hour hackathon with judging done at the end of the second day (20 February 2017).

Two topics are offered:

1. *Deep Learning and Cybersecurity*, chaired by Prof. Dawn Song (UC Berkeley)
2. *Fuzz Testing for Finding Vulnerabilities*, chaired by Assoc. Prof. Liang Zhenkai and Prof. Abhik Roychoudhury (NUS)

The Camp is held in conjunction of the Singapore Cybersecurity R&D Conference (SG-CRC) 2017, to be hosted at University Town, NUS. The conference features invited talks by international researchers, a panel on cybersecurity education, and NCL launch.

Visit *http://www.comp.nus.edu.sg/~tsunami/sg-crc17/* for more information.

ABOUT

Singapore Cybersecurity Consortium

Anchored at NUS National University of Singapore | Computing

The Singapore Cybersecurity Consortium (SGCSC) is established on 1 September 2016 for engagement between industry, academia and government agencies to encourage use-inspired research, translation, manpower training and technology awareness in the area of cybersecurity. It is funded by the National Research Foundation (NRF) and anchored at the National University of Singapore (NUS). The members of the Consortium are companies and government agencies with interest and expertise in cybersecurity. Institutions of Higher Learnings (IHLs) and Research Institutions (RIs) active in the field are represented in the Consortium.

The logo of the Consortium consists of three interlinked squares, representing the interconnection among the industry, the academia, and the government agencies in the Consortium.

Contact Us

http://sgcsc.sg ▪ cyber@comp.nus.edu.sg

CONSORTIUM MEMBERS (at time of publication)

Acronis

ATTILA CYBERTECH

BANFFCYBER TECHNOLOGIES

CLOAK

Custodio

DSO NATIONAL LABORATORIES

Excel Marco

j-Sprint Trust without Boundaries

蜜熊 KINKAYO

Nova Systems Experience Knowledge Independence

PARASOFT

PayPal

pwc

SecureAge

Singtel

Soliton

ST Electronics Info-Security A member of ST Engineering

Standard Chartered

StarHub

VANTAGEPOINT