PRESS RELEASE

NRF awards seven projects under the inaugural National Cybersecurity R&D Grant Call

Singapore, 15 October 2014 (Wednesday) – The National Research Foundation (NRF), Prime Minister's Office, Singapore, announced today the award of seven research projects totalling S$42 million in funding under the National Cybersecurity R&D inaugural grant call[1] for proposals. The NRF worked closely with the National Security Coordination Secretariat (NSCS), Ministry of Home Affairs (MHA), Ministry of Defence (MINDEF), Infocomm Development Authority (IDA), and Economic Development Board (EDB) in the evaluation and selection of these research projects.

The inaugural grant call, made earlier on 7 March 2014, seeks to develop research expertise and capabilities in cybersecurity for Singapore. The grant call proposals were guided by the research themes in the areas of cybersecurity, namely: scalable trustworthy systems; resilient systems; effective situation awareness and attack attribution; combating insider threats; threats detection, analysis and defence; and cyberspace governance and policy research. Please refer to Annex A for details on the research themes.

The grant call closed on 2 May 2014 with more than 20 proposals received from the local Institutes of Higher Learning and Research Institutes. All submitted proposals were evaluated by a panel of experts in the cybersecurity domain as well as representatives from government affiliated agencies.

The projects awarded cover research topics in mobile security, cyber physical systems security, hardware and software security, digital forensics, and securing data in the cloud. These projects seek to strengthen Singapore's R&D capabilities in cybersecurity, protect our critical infrastructure, and improve the resiliency of cyber infrastructure. Please refer to Annex B for the list of awarded projects.

Mr George Loh, Director, Physical Sciences and Engineering, NRF, said: "We have adopted an inter-agency approach in developing R&D capabilities to respond to cyber threats and cyber intrusions. For this call, we are pleased to see good ideas coming from local universities and research institutes."

Mr William Lau, Deputy Chief Executive Officer (Research), DSO National Laboratories, who chaired the evaluation panel said: "I am encouraged to see universities, research institutes, government agencies and private sector companies working together to develop R&D expertise and capabilities in cybersecurity for Singapore. The projects that the panel has recommended for the inaugural grant call

[1] At the meeting of the Research, Innovation and Enterprise Council on 25 October 2013, the Council announced the establishment of the National Cybersecurity R&D Programme, which harnesses R&D to improve the trustworthiness of cyber infrastructures to address a growing national challenge.

have the potential to significantly strengthen Singapore's cybersecurity. We are, however, only at the beginning. A lot more work lies ahead of us to give the researchers the time and space to innovate and then to get the projects translated to actual deployment."

Enclosures:
ANNEX A – National Cybersecurity R&D Research Themes
ANNEX B – Awarded Projects under National Cybersecurity R&D Grant Call

----- END -----

Issued by: National Research Foundation, Prime Minister's Office, Singapore

Date: 15 October 2014

For media queries or interviews, please contact:

Ms Cheryl LOH
Head, Corporate Communications
National Research Foundation, Prime Minister's Office, Singapore
DID: 6694 2928
Handphone: 9880 5507
Email: Cheryl_Loh@nrf.gov.sg

ANNEX A

National Cybersecurity R&D Research Themes

1. R&D proposals are guided but not limited by the following themes:

a. Theme (1): Scalable Trustworthy Systems. Research into technologies to make computing systems' hardware, firmware and software function dependably to reduce the risk of them becoming a source of Insider Attacks.

b. Theme (2): Building Resilient Systems. Research into technologies for improving resiliency, system robustness, adaptability, and capacity for rapid response and recovery for information, cyber-physical and other supporting infrastructures (e.g. power, water, communication) and those which depend on them in the face of persistent, stealthy, and sophisticated attacks focused on cyber resources.

c. Theme (3): Effective Situation Awareness and Attack Attribution. Research into technologies to enhance cyber situation awareness with meaningful cyber information that enables all national agencies to provide continuity and ensure security for agencies and national infrastructure and key government operations. Related to attribution is cyber-forensics, which ensures that digital media can be examined in a sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about the information, an especially important discipline related to Cybercrime.

d. Theme (4): Efficient & Effective Digital Forensics. Research into technologies to automate digital evidence acquisition and forensics tasks to overcome the cyber asymmetry created due to the lowering of the expertise threshold for potential hackers, increasing systems' complexity, rapid security situational changes, and scarcity qualified security practitioners.

e. Theme (5): Combatting Insider Threats. Research into technologies to combat insider threats will enable us to create, analyse, evaluate, and deploy mechanisms and strategies that can provide detection, prevention and identification of insiders and their activities.

f. Theme (6): Threats detection, Analysis and Defence. Research into technologies to combat malware and botnets will enable us to create, analyse, evaluate, and deploy mechanisms and strategies that can provide detection, prevention, immunisation, source identification and recovery.

g. Theme (7): Cyberspace Governance and Policy Research. Research on how or whether control or regulation can be applied to a communication medium that is decentralised and global; balancing trade, innovation, freedom of expression and cyber security into a comprehensive policy. This track also includes usable security in system design and quantitative research on factors that could shape or induce forms of human behaviour in Cyberspace.

ANNEX B

Awarded Projects under National Cybersecurity R&D Grant Call

S/N	Title	Principal Investigator (PI) & Co-PIs
1.	Secure Mobile Centre - Technologies and solutions for securing mobile computing	PI: Prof Robert Deng Professor of Information Systems, School of Information Systems, Singapore Management University (SMU) Email: robertdeng@smu.edu.sg DID: 6828 0920 Co-PI: SMU
2.	Trustworthy systems from un-trusted components	PI: Prof Roychoudhury Abhik Professor, School of Computing, National University of Singapore (NUS) Email: abhik@comp.nus.edu.sg DID: 6516 8939 Co-PI: NUS
3.	Securing data in the cloud using information dispersal algorithm to disperse data in large number of dynamically configured storage nodes	PI: Mr Mar Kheng Kok Senior Lecturer, School of Information Technology, Nanyang Polytechnic Email: mar_kheng_kok@nyp.edu.sg DID: 6550 1647 Co-PI: Nanyang Polytechnic
4.	Securify: A compositional approach of building security verified system	PI: Prof Srikanthan Thambipillai Professor, School of Computer Engineering, Nanyang Technological University (NTU) Email: astsrikan@ntu.edu.sg DID: 6790 5788 Co-PI: NTU, NUS and SUTD
5.	A cyber-physical approach to securing urban transportation systems	PI: Dr Zhou Jianying Department Head, Infocomm Security, A*STAR Institute of Infocomm Research DID: 6408 2075 Email: jyzhou@i2r.a-star.edu.sg Co-PI: A*STAR, Advanced Digital Sciences Center (Singapore), SUTD, University of Illinois at Urbana Champaign (US)

6.	Cyber Forensics and Intelligence	PI: Dr Vrizlynn Thing Department Head, Cyber Security & Intelligence, A*STAR Institute of Infocomm Research Email: vriz@i2r.a-star.edu.sg DID: 6408 2041 Co-PI: A*STAR
7.	Project SUTD-ASPIRE: Design of Secure Cyber Physical Systems	PI: Prof Mathur Aditya Professor and Head of Information Systems Technology and Design, Singapore University of Technology and Design (SUTD) Email: Aditya_mathur@sutd.edu.sg DID: 9139 4552 Co-PI: SUTD

1. Secure Mobile Centre - Technologies and solutions for securing mobile computing

The Secure Mobile Centre by the Singapore Management University (SMU) aims to develop technologies and solutions that strengthen the security of mobile computing systems, applications and services. The new centre will carry out R&D projects that target three key aspects of mobile computing – mobility, connectivity, and extensibility. Research focuses on areas of analysis, detection and containment of malicious software, and the creation of novel authentication systems, and secure mobile Internet services.

SMU will partner with companies such as ST Electronics (Info-Security) Pte Ltd, Gemalto Pte Ltd, StarHub and McAfee Singapore to participate in the R&D projects. It will be collaborating with the Infocomm Development Authority (IDA), the Defence Science and Technology Agency (DSTA) and the Monetary Authority of Singapore (MAS) on the technical and practical requirements of the project. By building a research excellence in mobile computing security, this centre supports the vision of making Singapore a secure and sustainable Smart Nation.

2. Trustworthy systems from un-trusted components

The team from National University of Singapore (NUS) will focus on developing scalable methods for building trustworthy software systems. The goal is to build software which provides a high degree of assurance, even when the software is integrated out of un-trusted commercial off-the shelf (COTS) software components. The project plans to build secure and trustworthy systems from COTS components by analysing the components, and by containing the manner in which these components can compute, interact and manipulate sensitive data. The technologies developed in the project can be deployed under various usage scenarios – for building trustworthy systems, for analysis of malware, or for security assessment of specific COTS components.

The research team from NUS will collaborate with various universities from the USA such as UC Berkeley, Georgia Tech, University of Princeton, University of Maryland and the University of Oxford from the UK. In addition, they will also work with companies such as ST Electronics (Info-Security) Pte Ltd, NEC Labs and Symantec Asia Pacific Pte Ltd, and government agency such as DSTA.

3. Securing data in the cloud using information dispersal algorithm to disperse data in large number of dynamically configured storage nodes

This research project is in the field of data storage security. The research team from the Nanyang Polytechnic will look into methods and techniques of securing data on untrusted storage platforms, in particular, public cloud storage and user-contributed storage. The project will look into novel methods of managing a large number of data stores in the storage cluster, which can continue to function during massive failures. In addition, through this project, the research team will derive techniques to efficiently check for proof of retrievability and integrity of data in the cloud.

The research team from the Nanyang Polytechnic will work closely with its industry collaborators such as Infinito Games Pte Ltd and iM Custom USA to further define the specific-use cases and security requirements.

4. Securify: A compositional approach of building security verified system

This research project by the Nanyang Technological University (NTU) will embark on cybersecurity research to verify both software and hardware systems using mathematical-based techniques (formal methods). The aim is to mathematically prove that systems consisting of software and hardware behave in the manner intended to ensure that there are no vulnerabilities and security weaknesses. This project seeks to develop novel methods to build secure and verifiable systems from ground-up and the eventual goal is to develop a computing system (consisting of hardware, micro-kernel and libraries), named Securify, which is formally proved to be correct and secure. The project will also develop a systematic approach which allows system designers to build applications on top of Securify, using third-party untrusted components without compromising the security of the overall system.

The research team will collaborate with both local and overseas universities such as NUS, SUTD, ETH Zurich (Switzerland), Oxford University (UK), Royal Holloway, University of London (UK), Hong Kong University of Science and Technology; and companies such as ST Electronics (Info-Security) Pte Ltd, WINCOR Nixdorf Pte Ltd, and Deloitte & Touche Enterprise Risk Services Pte Ltd.

5. A cyber-physical approach to securing urban transportation systems

The research project from Agency for Science, Technology and Research (A*STAR) Institute for Infocomm Research (I²R) will focus on safeguarding urban transportation systems against potential cyber-attacks by taking a cyber-physical approach to designing security technologies.

The research team will build models and security mechanisms to capture and defend against the propagation of attacks through both cyber and physical systems. These models and security mechanisms would be validated by leveraging the systems and practices from industrial collaborators (namely SMRT, ST Electronics Ltd and Northrop Grumman). The research team will collaborate with Advanced Digital Sciences Center (Singapore), Singapore University of Technology and Design (SUTD) and University of Illinois at Urbana Champaign (US) and Land Transport Authority (LTA).

This research project will provide fundamental research in cyber-physical system security, and seeks to safeguard the urban transportation infrastructure in Singapore and beyond.

6. Cyber Forensics and Intelligence

Network prevalence and data asset digitalisation enable higher productivity, enhanced communications and greater convenience. However, the borderless cyber space brings challenges to cyber forensics, such as in identifying the perpetrators.

Technological advancement in techniques to undermine forensics investigations directly or indirectly, such as big data, forgery, insiders' and perpetrators' sophistication, further exacerbates the problem. The research team from A*STAR I2R aims to advance the field of cyber forensics by focusing on research ranging from areas of evidence acquisition and identification, attribution and response; to actionable threat intelligence.

The research team will collaborate with overseas universities such as Imperial College London, University of Oxford, University of Cambridge, and University of Hong Kong. They will also work with companies such as Certis Cisco, Development Bank of Singapore (DBS), ST Electronics (Info-Security), Palo Alto Networks, Transmex Systems International, and Custodio Pte Ltd in the research project. The team will also seek inputs from Singapore Police Force (SPF), Ministry of Home Affairs (MHA) and Infocomm Development Authority of Singapore (IDA).

The outcome of the research will enhance the national security through the developed advanced cyber forensic technologies in this project.

7. Project SUTD-ASPIRE: Design of Secure Cyber Physical Systems

The research project from the Singapore University of Technology and Design (SUTD) focuses on the security of Cyber Physical Systems (CPS). The research objective aims to improve the security of Singapore's Cyber-Physical Systems through the application of experimentally validated research by using CPS test-bed such as Smart Power Grid. The research project will also develop the techniques, software and hardware tools to enable the detection, mitigation and recovery from cyber-attacks on CPS.

Academic partners include NTU, Massachusetts Institute of Technology (MIT), Advanced Digital Sciences Center (ADSC, Singapore), and University of Illinois at Urbana-Champaign (UIUC). The industry partners include NEC Laboratories Pte Ltd, Cisco Systems Pte Ltd, National Instruments Singapore, StarHub Ltd, and Singapore Power PowerGrid Ltd (SPPG) and government agencies such as Public Utilities Board (PUB).