Trustworthy Computing for a Secure Smart Nation

Grant Call Launch 2020

Prof. Abhik Roychoudhury
Professor, National University of Singapore
Lead PI and Academic Director, Singapore Cyber-security Consortium
Director, National Satellite of Excellence in Trustworthy Software Systems

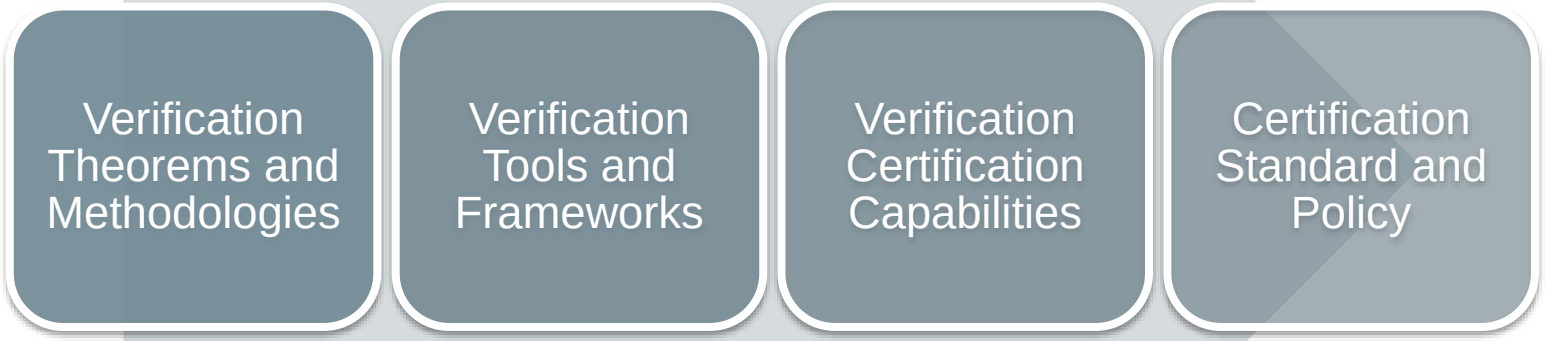
Mission

The goal of the Center of excellence on Trustworthy Systems at Singapore is as much on establishing core capabilities in **software system certification**, as it is on building concrete use cases of deployed certified software systems.

From the regulatory perspective, the center seeks to establish guidelines for software in safety and security critical smart systems thereby contributing to the vision of **Secure Smart Nation**.

https://www.comp.nus.edu.sg/~nsoe-tss/

Securify (Past work at NTU)



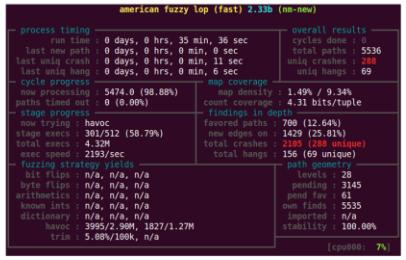
- Semantics Formalization and Analysis
- (HW and SW) Model Checking
- (Refinement based) Theorem Proving
- Compositional Verification
- Runtime Monitoring
- Equivalence Checking

- Reusable and Scalable Verification and Tools
- Secure Code Generation
- Verified and Enhanced Security Micro-kernel
- Comprehensive Side Channel Analysis and Verification

TSUNAMi (past work at NUS)

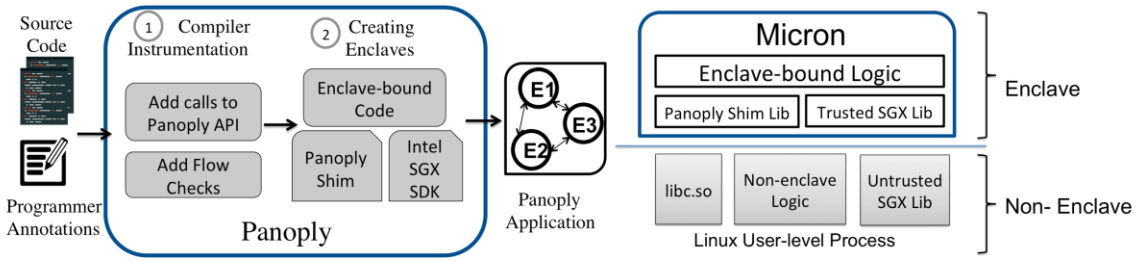
- *Trustworthy Systems from UN-trusted component AMalgamations*
  - The TSUNAMi center focuses on software and system security for commercial off-the-shelf (COTS) software components via ingenious combinations of analysis, testing, verification, hardening, isolation and system design.

Directed and Efficient Greybox Fuzzing [CCS 2016, 2017 & TSE 2019]



- **AFLGo: Directed Greybox Fuzzing (CCS 2017)**
  - 1st directed greybox fuzzing. 17 CVEs. Integrated into OSS-Fuzz.
  - Outperforms state-of-the-art in patch testing and crash reproduction
- **AFLFast: Coverage-based Greybox Fuzzing as Markov Chain (TSE 2018)**
  - 10x faster than the state of the art. Integrated into AFL fuzzer.
  - Outperforms KLEE on vulnerability detection

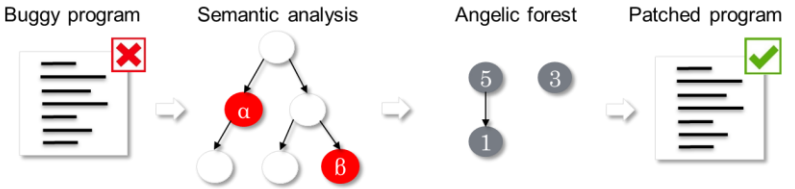
Panoply – Low-TCB Linux Applications with SGX Enclaves [NDSS 2017]



- Supports POSIX APIs with 2x smaller TCB
- Microns: Library-enclaves created by Panoply

Automated Program Repair

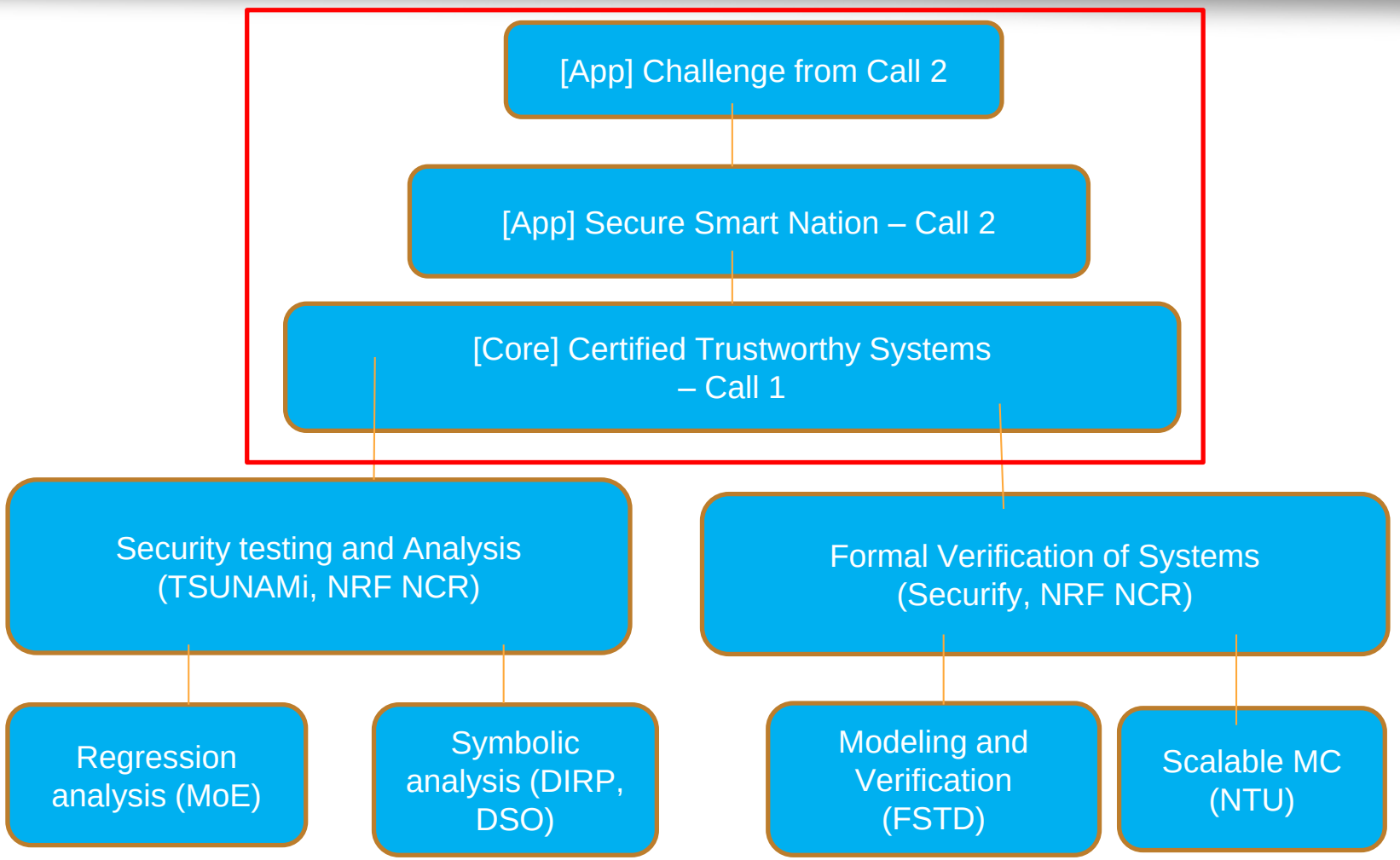
- Angelix is the first automated program repair tool based on symbolic methods that scales to large real world programs (PHP, Python, etc.)
- The main technical novelty of Angelix is the concise semantic signature:



- Angelix managed to generate a patch for the famous Heartbleed vulnerability
  http://angelix.io/

ACM SIGSOFT Outstanding Dissertation Award in 2019 for “Semantic Program Repair.”

Chronological Evolution of Capabilities

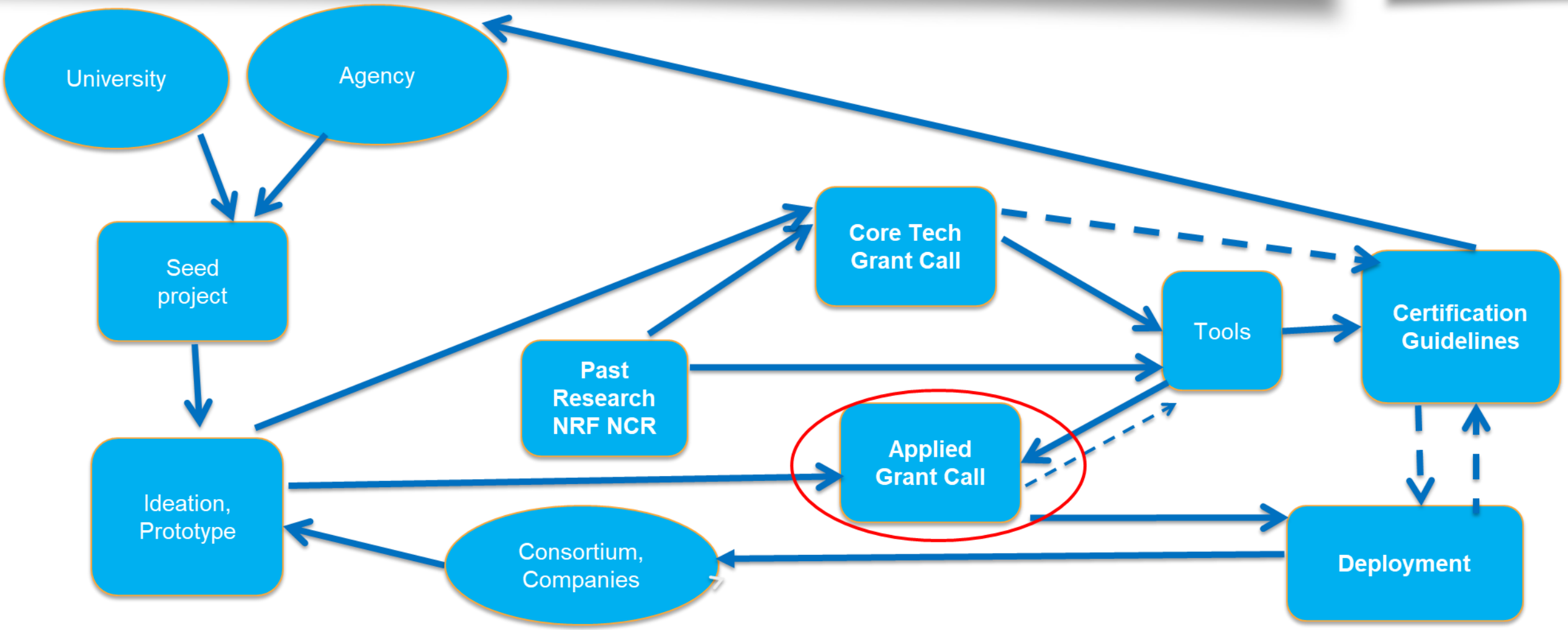


Point Projects MINDEF, MoE… [2009-12, 2011-14, 2013-15]

Targeted Capability NCR 1 TSUNAMi(2015 – 19) Securify(2015 - 20)

Satellite Center of Excellence (2019-23)

Program Workflow



Structure of Research

Core NSoE-TSS Research Team

Grant Call 1

Trustworthy Software Systems Core Technologies Grant

TSS-CTG2019

7 projects funded
Focus on core technologies for trustworthy software systems

Grant Call 2a

Trustworthy Computing for a Secure Smart Nation Grant

TCSSN2020

4 projects to be funded
Focus on translation for a secure smart nation

Grant Call 2b

Secure Smart Nation Challenge

SSNC2021

1 project to receive (up to) $1M of additional funding.
Mini-grand challenge open only to winners of grant call 2

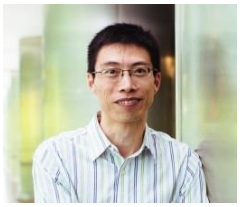
TBA

Grant Call 2019 Awardees (Grant Call 1)

Associate Professor Gao Debin
Enhanced function signature recovery for control-flow integrity enforcement on compiler optimized executables

Associate Professor Sun Jun
SpecTest: Specification-based Compiler Fuzzing

Professor David S. Rosenblum
Evaluating the Trustworthiness of Deep Learning Systems



Associate Professor Ding Xuhua
A Novel Hybrid Kernel Symbolic Execution Framework for Malware Analysis

Associate Professor Bo An
Improving Trustworthiness of Real-world AI systems through Adversarial Attack and Effective Defense

Associate Professor Chin Wei-Ngan
Trustworthy Distributed Software with Safety and Liveness Guarantees

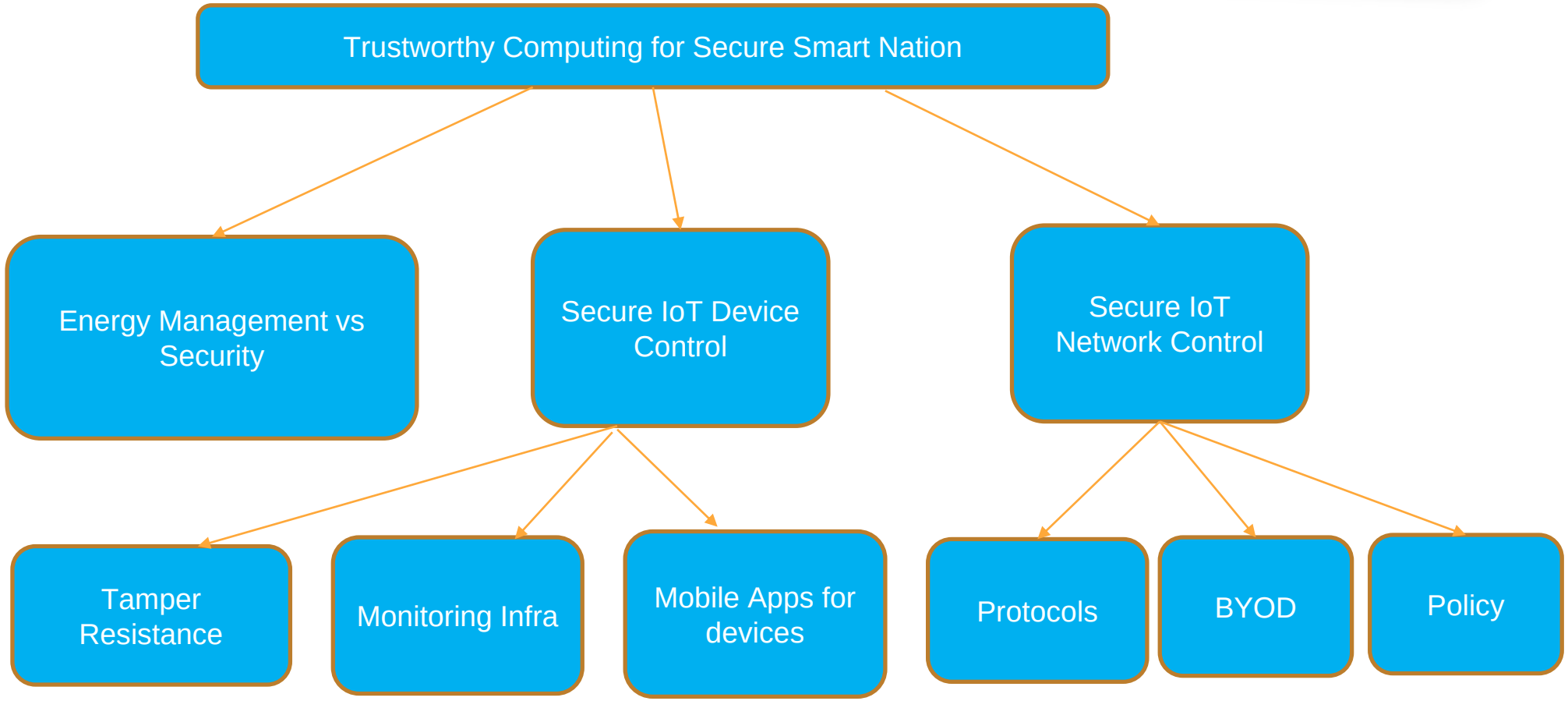
Associate Professor Ilya Sergey
CertiChain: A Framework for Mechanically Verifying Blockchain Consensus Protocols

Grant Call 2020 (Grant Call 2a)

*This grant call encourages diverse and innovative proposals for the development and deployment of tools and services to certify the security and resilience of embedded software systems, or the development and deployment of trustworthy software systems to enable certification for the advancement of a secure **Smart Nation**.*

- Grant 2019: focus on core research
- Grant 2020: focus on core research ***and*** translation
- Grant 2021: focus on translation (more details soon)

Sample Topics to be covered – Quick Look



Grant Call 2020 Sample Topics

- *Trustworthy Software for the Internet of Things and Smart Devices*
  - The rise of the IoT and a Smart Nation go hand-in-hand
  - Rapid growth means security and privacy may be neglected
  - Diversity of manufacturers makes IoT security challenging

Theme	Potential Topics
Trustworthy Software for IoT and smart devices for schools, homes and businesses	• Security and energy management • IoT device security • "Bring your own device" (BYOD) issues • Tamper-resistant devices • Wearable devices or smartphones • Secure mobile apps to control devices • Binary rewriting with minimal impact • Post-crash analysis techniques

Grant Call 2020 Sample Topics

- *Trustworthy Software for Smart Networks and Sensors*
  - Smart networks are vulnerable to eavesdropping, disruption and hijacking
  - Power+environmental constraints makes smart network security cumbersome

Theme	Potential Topics
Trustworthy Software for Sensor Networks, interconnected smart devices, and next generation connectivity	• Smart sensor networks • Secure protocols for networked devices • Intelligent control systems for devices • Next generation connectivity

Grant Call 2020 Sample Topics

- *Trustworthy Software for Smart Cyber Physical Systems*

Theme	Potential Topics
Trustworthy Software for smart cyber physical systems, drones and autonomous vehicles.	• Drones and autonomous vehicles • Physical infrastructure augmentation • Cyber-Physical system security

- *General Topics in Trustworthy Software and a Secure Smart Nation*
  - The grant call is meant to be general, other topics are encouraged

Theme	Potential Topics
Trustworthy Software for the advancement of a secure smart nation	• Infrastructure for the digital economy • Governance and policy issues • Big data • Fintech

Timeline

Submission Opens	**7th January 2020**
Submission Closes	**6th May 2020, 11:59pm** Singapore time Short-listed grant applicants will be asked to make a presentation during the evaluation period.
Notification	**By 7th August 2020** Successful applicants are to submit final proposals within 14 days of notification.
Grant Award	**1st September 2020**
Project Starts	**1st October 2020** Successful applicants are to set a date to start the project within this period. Award acceptance and research collaboration agreements must be signed before the project start date.

Eligibility

- The grant call is open to all researchers from a publicly-funded Singaporean
  - *Institute of Higher Learning* (IHL) or
  - *Research Institute* (RI)
- The Principal Investigator (PI) must be **full-time** researcher (or part-time with at least 75% appointment).
- Other requirements:
  - It is favourable (but not required) for a Co-PI to be a member of relevant industry/agency.
  - Collaborators are not restricted to any category, but are not eligible to receive any funding.
  - All project work must be done in Singapore, unless expressly approved by the NSoE-TSS.
  - Proposals already funded by other funding agencies are not eligible.

Translation

- A pathway to **translation** of the proposed research is ***essential***. Research must be oriented towards some real-world impact:
  - Deployment in industry or practice e.g. by having an industry or agency collaborator
  - Highlight plans to curate usable artifacts by wider community e.g. malware database in specific settings, open-source tools within the secure smart nation theme.

- What is ***not*** translation:
  - Using grant funds to develop a single app or productization
    (Evidence of research novelty and/or scientific merit is very much required)

Intellectual Property

- Flexible *Intellectual Property* (IP) arrangements will be supported
  - **Option A**: IHL/RI has **100%** IP ownership
  - **Option B**: IP ownership is shared **50/50** with a Singaporean company & permissively licensed, with appropriate justification)
  - **Option C**: Some other arrangement (with justification)

- For all arrangements, **justification** should be provided
  - E.g., the company may contribute funding for greater share of IP rights
  - Justifications will be taken into consideration during evaluation

Submission

- Grant applicants shall submit the full proposals by the specified deadline through the online submission site, check out

https://www.comp.nus.edu.sg/~nsoe-tss/grantCall2launch.htm
https://www.comp.nus.edu.sg/~nsoe-tss/grantCall2.htm

- Three documents are required as attachments:
  - Full Proposal in PDF format
  - Budget, Objectives, Deliverables, KPIs, Gantt Chart in MS Excel document
  - Slide deck of 5 slides explaining significance of work proposed in PDF format

Budget and Project Duration

- The budget of the projects to be submitted should be between 400,000 and 600,000 SGD. A typical project quantum is **500,000 SGD** for a period of **2 years or 2.5 years**.
- This grant call will provide the funding support of approved qualifying direct costs and **10%** of indirect costs of a project.

More details

- Please wait for grant call document to be sent to all universities. Grant call document will also be put up from
  https://www.comp.nus.edu.sg/~nsoe-tss/grant.htm

- Shortlisted applicants will be presenting to the evaluation committee on **20th July 2020 (tentative).**

- **Awarded projects will start by 1st October 2020.**