DOI: 10.1145/3378552

# Singapore's Cybersecurity Ecosystem

By Karen Teh, Vivy Suhendra, Soon Chia Lim, and Abhik Roychoudhury

A successful digital economy requires cybersecurity to be a vital enabler, protecting the interests of individuals and businesses and enabling the resilience of businesses and services. Since 2013, Singapore's medium- to long-term directions for cybersecurity is to develop R&D expertise and capabilities to improve the trustworthiness of cyber infrastructures and systems with an emphasis on security, reliability, resilience, and usability among government agencies, academia, and industry. Various initiatives to support research, innovation, and enterprise have been implemented under the Whole-of-Government National Cybersecurity R&D (NCR) Programme.[8] The program supports a synergistic range of initiatives to advance technological state-of-the-art in thematic National Satellites of Excellence in universities, grants for local research projects, international research collaborations, and joint technology developments with industry. Innovation is fostered through cross-sector R&D discussions and partnerships and fast-tracked by national testbeds for safe and repeatable cybersecurity experiments.

**Research impact**. Research entities in Singapore have adopted a multi-disciplinary, mission-oriented approach in solving cybersecurity problems with notable outcomes. There are several such examples of research impact in cyber-security being achieved by Singapore's institutions including in software security, systems security, and Internet of Things (IoT) security.

A noticeable impact has been achieved in the field of vulnerability detection in programs, namely fuzz testing. AFLFast[2] is an extension of the widely used AFL[16] developed at Google, a greybox fuzzer, which uses lightweight program instrumentation to gain coverage information for guiding program path exploration. AFLFast achieved tenfold speed-up over AFL using strategies to gravitate path exploration toward low-frequency paths, which enabled it to expose several previously unreported CVEs that could not be exposed by AFL in 24 hours. It contributed to the runner-up team Codejitsu at DARPA Cyber Grand Challenge (2016) and has been integrated into mainstream AFL.

Scantist[9] is a university spin-off with technologies for scalable vulnerability scanning and analysis at binary as well as source code levels, providing vulnerability management tools with low effort and expertise requirements. It combines static analysis in the form of signature-based matching

and metrics to detect vulnerable functions, with dynamic analysis in the form of smart fuzzing to discover memory corruption vulnerabilities. The tools produce highly targeted remediation advice to allow quick and accurate fixes.

Anquan[1] is another spin-off providing distributed ledger and trusted computing platforms for financial markets. It was appointed as a technology partner, alongside Deloitte and Nasdaq, in a 2018 project by the Monetary Authority of Singapore (MAS) and Singapore Exchange (SGX) to develop delivery versus payment (DvP) capabilities for reduced-risk settlement of tokenized assets across different blockchain platforms.[6] Anquan's DvP solution design in this project is based on its permissioned blockchain with capabilities developed by the research group in Singapore,[5,10] including scalability through a network sharding technique, security protection against malicious nodes, a smart contract language amenable to formal verification, and privacy with hardware-rooted trusted execution environment.

Research in cyber-physical system security has also generated sophisticated algorithms, software, and devices to detect physical, sensor, network, and information attacks.[15] Among the practical outcomes is VVATER,[11] a mixed-reality visualization of process states and attacks in Operational Technologies such as water treatment and distribution plant, to help operators investigate and respond to attacks timely and comprehensively without advanced cybersecurity skills. A key novelty of VVateR is its ability for visualizing the interconnection of various infrastructures in historical plant operation and path of attacks in complex scenarios, as well as the resulting process anomalies and whether or not the anomaly is detected.

**Support for Research, Innovation, Enterprise**

Ecosystem support plays an important role in ensuring research endeavors are responsive to and impactful on cybersecurity needs of the industry and society. Building on the research successes, Singapore has set up three National Satellites of Excellence: on Trustworthy Software Systems at the National University of Singapore, on Mobile Systems Security at the Singapore Management University, and on Secure Critical Infra-structure at the Singapore University of Technology and Design. These satellites provide strategic thrusts in a focus area and help to develop the research and innovation ecosystem in Singapore, working closely with various national initiatives such as the Singapore Cybersecurity Consortium.

The Singapore Cybersecurity Consortium[12] is an organized construct to grow communities, foster partnerships across academia, industry, and agencies, and seed technology explorations around research to multiply and amplify its impact. Operating environment challenges and related

research outcomes are discussed in its thematic Special Interest Groups, leading to better appreciation of research capabilities, problems for research, and joint innovation development.

The National Cybersecurity R&D Laboratory[7] and iTrust Laboratories[14] are shared infrastructures facilitating Enterprise-IT and OT security research experimentation, technology evaluation, and training. Research teams from academia and industry seeking to commercialize cybersecurity technologies are mentored on customer discovery and product positioning in the Lean LaunchPad Singapore: Cybersecurity Track,[4] which integrates both business and technological perspectives. Complementing the effort in this space is Innovation Cybersecurity Ecosystem at Block 71 (ICE71),[3] which provides entrepreneurship, accelerator, upscaling programmes for start-ups, contributing to ecosystem growth in ASEAN.

**Positioning Singapore as a Regional Cybersecurity Hub**

Leveraging this comprehensive R&D foundation and its reputation as a trusted financial hub, Singapore is well-positioned to be a cybersecurity hub for the region. It attained the status of a Common Criteria Certificate Authorising Nation in January 2019. With this status, developers based in Singapore can enjoy lower costs and shorter time in attaining an internationally-recognised certification mark. This facilitates the exportability of cybersecurity products produced in Singapore. The Singapore International Cyber Week[13] is the region's most established annual cybersecurity event, providing an ideal platform to discuss, strategize, and form partnerships across the nations.

All such efforts help to nurture the cybersecurity innovation ecosystem in Singapore and the region, which remains locally rooted and globally connected. This regional-global interplay is indeed a marked characteristic of all cybersecurity initiatives in the region featured in this issue. The cybersecurity capacity maturity assessments of countries in the Pacific region (for more information, see the Rudolph et al. article in this section) is part of a global initiative on cybersecurity capacity building and is an application of the research on the Cybersecurity Capacity Maturity Model for Nations developed in U.K.'s University of Oxford. The assessment project is accompanied with research on the evolving cybersecurity context of the region, with findings feeding back to the research on the model itself with possible benefits to other regions. Asiacrypt, the regional flagship IACR conference for advances in security and cryptography research, gathers researchers in Asia and Oceania for closer collaboration while staying aligned to the international body of IACR and making borderless research contributions. (For more information on Asiacrypt, see the Phan et al. article in this section). These initiatives and ours nurture the cybersecurity ecosystem in different but connected ways—a thriving innovation ecosystem would enhance the germination of ideas as well as accelerate the technology transfer and industry

adoption of research results, which in turn supports the building and maturing of cybersecurity capabilities in the region.

**Future Research Areas**

Our R&D for the advancement of a secure smart nation does not end here. We will continue to focus R&D on security and the healing of software stacks in autonomous vehicles and the IoT, including curtailing attacks coming from nonfunctional domains. Future research areas will also focus on safe and dependable interactions between the physical worlds of sensors, motors, actuators, and robotics, and the cyber world of data processing, artificial intelligence, networking, and control systems to better protect interests and enabling the resilience of businesses and services in a digital economy of IoT and actions.

**References**


1. Anquan Capital, 2019; https://www.anquancapital.com/.
2. Böhme, M., Pham, V-T and Roychoudhury, A. Coverage-based Greybox fuzzing as Markov Chain. In *Proceedings of the 2016 ACM SIGSAC Conf. Computer and Communications Security*, 1032-1043.
3. Innovation Cybersecurity Ecosystem at Block 71—ICE71; https://ice71.sg/.
4. Lean Launchpad Singapore. Past projects, 2019; https://nus.edu/2T9k7zd.
5. Luu, L. et al. A Secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conf. Computer and Communications Security,* 17–30.
6. Monetary Authority of Singapore, SGX, and Deloitte. Delivery versus Payment on Distributed Ledger Technologies, 2018; http://bit.ly/2Qsw15a.
7. National Cybersecurity R&D Laboratories, 2019; https://ncl.sg/.
8. National Research Foundation. National Cybersecurity R&D Program, 2019; https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme/.
9. Scantist. Vulnerability management. Simplified, 2019; https://scantist.com/.
10. Sergey, I., Kumar, A. and Hobor, A. Scilla: A Smart Contract Intermediate-Level Language, 2018; https://arxiv.org/abs/1801.00687.
11. Shrivastava, S. Virtual and mixed reality for security of critical city-scale cyber-physical systems. *iTrust Times* 1, (Apr–Jun 2019). Singapore University of Technology and Design.
12. Singapore Cybersecurity Consortium, 2019; https://sgcsc.sg/.
13. Singapore International Cyber Week, 2019; https://www.sicw.sg/.
14. Singapore University of Technology and Design. iTrust Labs Home; https://itrust.sutd.edu.sg/itrust-labs-home/.

15. Taormina, R. and Galelli, S. Deep-learning approach to the detection and localization of cyber-physical attacks on water distribution systems. *J. Water Resources Planning and Mgmt 144*, 10 (2018), 04018065.
16. Zalewski, M. American fuzzy lop (2.52b), 2017; http://lcamtuf.coredump.cx/afl/.

**Karen Teh** is Senior Deputy Director of Cybersecurity R&D at the National Research Foundation, Singapore.

**Vivy Suhendra** is Executive Director of the Singapore Cybersecurity Consortium.

**Soon Chia Lim** is the director of the Cybersecurity Engineering Centre for the Cyber Security Agency of Singapore.

**Abhik Roychoudhury** is a professor at the National University of Singapore.

PQ
Innovation is fostered through cross-sector R&D discussions and partnerships and fast-tracked by national testbeds for safe and repeatable cybersecurity experiments.