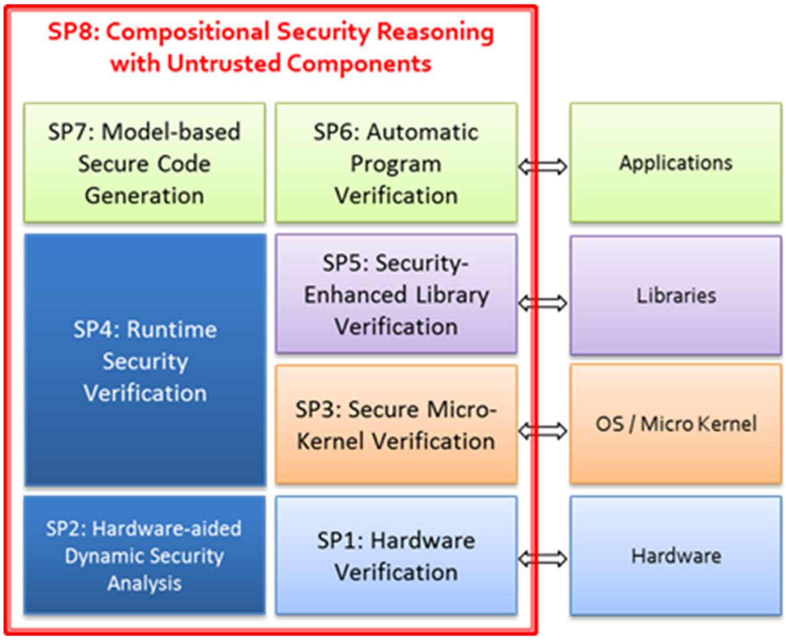
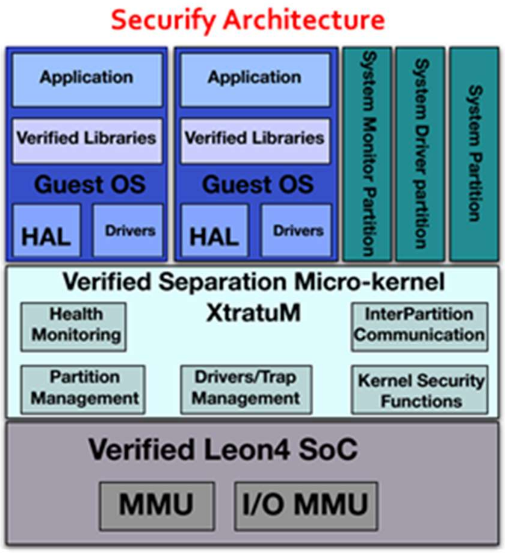
SECURIFY: A Compositional Approach of Building Security Verified System

More and more we embrace the convenience and effectiveness of the advancement of IT and the Internet in our business and personal lives. With this convenience, we have also been subjected to new dangers: cyber-attacks. Cyber-attack detection, defense and recovery are important topics in cybersecurity, but the ultimate goal of cybersecurity is to build attack-free systems. Security verification and building attack-free systems are very challenging tasks in view of the size and the complexity of the IT systems, which are fast growing with the new trends of computing: cloud computing, mobile computing, cyber-physical systems, internet of things. This is mainly because a well-developed system consists of several layers in its execution stack: hardware layer, OS/micro kernel layer, library layer and program layer. Attacks in any of the layers will lead to the security breach of the system.

Existing security verification focuses on a specific part or aspect of the system. In this proyect, we follow an approach that would allow us to build secure and verifiable systems ground-up, which has never been done before. First, we are developing an execution stack from hardware layer, OS layer to library layer (security libraries), named Securify, where each layer is formally proved to implement the specification and only the specification (to prevent the attacks like backdoor) and the system is verified to be free from vulnerabilities (to prevent advanced persistent threats (APT) and 0-Day attacks). Secondly, we are looking into software security verification and secure software development. Particularly, we aim at developing a compositional approach based on Securify and develop an automatic security reasoning tool so that developers can build applications on top of Securify, use third-party untrusted components and still be able to reason about the security of the overall system.

This project aims at a comprehensive coverage of the security at each level of the execution stack. This includes theoretical results, individual security analysis tool for each layer, and most importantly a completely verified execution stack Securify, which provides a ready platform for our collaborators to develop secure systems. We are going to work closely with ST Electronics (Info-Security) for security device development, Wincor Nixdorf Singapore to develop secure thin client computing architecture for ATM and POS Terminals and Deloitte to build finance security systems. We will continue work with Singapore Defence (D-STA and DSO) to provide R&D for secure system development. We aim at developing Securify as the world first verified execution stack, which has the potential to be commercialized with the help of NTU Venture.


SP8: Compositional Security Reasoning with Untrusted Components
SP7: Model-based Secure Code Generation
SP6: Automatic Program Verification
Applications
SP4: Runtime Security Verification
SP5: Security-Enhanced Library Verification
Libraries
SP3: Secure Micro-Kernel Verification
OS / Micro Kernel
SP2: Hardware-aided Dynamic Security Analysis
SP1: Hardware Verification
Hardware



Principal Investigators	Asst. Prof. Liu Yang *(SCSE, NTU)* Asst. Prof. Alwen Fernato Tiu *(SCSE, NTU)* Prof. Thambipillai Srikanthan *(SCSE, NTU)* Prof. Dong Jin Song *(NUS)* Assoc. Prof. Sun Jun *(SUTD)*
Researchers	Dr. David Miguel Sanan Baena Dr. Zhang Fuyuan Dr. Hou Zhe Mr. Sanjeev Kumar Das Dr. Frederic Tuong Dr. Omar Ibrahim Al Bataineh Mr. Cheng Kun
Students	Ms. Du Xiaoning
School / Department	School of Computer Science and Engineering
Collaborator	DSO National Laboratories Wincor Nixdorf ST Electronics
Source of Funding	National Research Foundation, Singapore