Hardware Root of Trust for Internet of Video Things

Abstract: Vision sensors are ubiquitous. It is predicted that by 2030, there will be around 13 billion cameras and 1 exabyte of data generated every day. With the rapid growth of the Internet of Things (IoT), more smart applications are anticipated to be evolved around the intelligent integration of smart visual sensing and pervasive networking. The networking and accessibility of video things also pose new challenges in digital forensic, on-device data security and privacy protection in edge and fog computing. Provably secure cryptographic algorithms secure mainly the communication channels, which are inadequate against the emerging AI-assisted data fabrication, backdoor and side-channel attacks that exploit the anonymity and implementation vulnerabilities of vision-enabled endpoints. Device identification based on cryptographic primitives requires the safekeeping of an on-device secret binary key. The latter is vulnerable to various kinds of invasive, semi-invasive and side channel attacks, particularly when the device is physically accessible. Existing trust credentials also provide no link between the data and its provenance. Physical Unclonable Function (PUF) is a key-less hardware security primitive. The secret is built intrinsically into the device structure by the uncontrollable manufacturing process variations of nano-scale integrated circuits. PUFs offer promising new opportunities to assure end point security against the imminent risk of sensor and data analytic attacks. This talk will present some solutions to derive non-repudiable provenance proof from the unification of PUF responses and biometrics or other data analytic based security parameters. The three presented end-point authentication schemes of PUF-based user-device hash, data-device hash and event-driven hash show that PUF can be endowed with the capability to not only identifying the device (e.g., camera for video surveillance), but also assuring the integrity of the data that it generated or acquired, and authenticating the users who have privileged access to the device and its data.

Speaker Brief Biography: Chip Hong Chang is an Associate Professor at the Nanyang Technological University (NTU) of Singapore, and have held concurrent appointments at NTU as Assistant Chair of Alumni of the School of EEE from 2008 to 2014, Deputy Director of the Center for High Performance Embedded Systems from 2000 to 2011, and Program Director of the Center for Integrated Circuits and Systems from 2003 to 2009. He has coedited five books, and have published 13 book chapters, more than 100 international journal papers (>70 are in IEEE), more than 180 refereed international conference papers (mostly in IEEE), and have delivered over 40 colloquia and invited seminars. HIs current research interests include hardware security and trustable computing, low-power and fault-tolerant computing, residue number systems, and application-specific digital signal processing algorithms and architectures. Dr. Chang currently serves as the Senior Area Editor of IEEE Transactions on

Information Forensic and Security (TIFS), and Associate Editor of the IEEE Transactions on Circuits and Systems-I (TCAS-I) and IEEE Transactions on Very Large Scale Integration (TVLSI) Systems. He was the Associate Editor of the IEEE TIFS and IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD) from 2016 to 2019, IEEE Access from 2013 to 2019, IEEE TCAS-I from 2010 to 2013, Integration, the VLSI Journal from 2013 to 2015, Springer Journal of Hardware and System Security from 2016 to 2020 and Microelectronics Journal from 2014 to 2020. He also guest edited eight journal special issues including IEEE TCAS-I, IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE TCAD and IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS). He has held key appointments in the organizing and technical program committees of more than 60 international conferences (mostly IEEE), including the General Co-Chair of 2018 IEEE Asia-Pacific Conference on Circuits and Systems and the inaugural Workshop Chair and Steering Committee of the ACM CCS satellite workshop on Attacks and Solutions in Hardware Security. He is the 2018-2019 IEEE CASS Distinguished Lecturer, a Fellow of the IEEE and the IET.