Embedded workshop – Information Security

Introduction

The Embedded workshop on information security is one of the special initiatives during ISCAS 2024, and is perfectly aligned with the overall theme of ISCAS 2024 – "INTELLIGENT CYBER SECURITY SYSTEMS".

The overall aim of this Embedded workshop is to advance the ICT community's understanding of the role of circuits and systems in supporting the information security requirements of hot and emerging technologies. The workshop intends to discuss four key areas: Quantum Computing, Artificial Intelligence, Smart End Devices and Cloud Computing.

Each of these technologies has advanced enormously over the past few years and expected to expand even further with years to come, eventually driving billions of devices and systems arounds us. All the four technologies face significant security and privacy challenges that will naturally have a direct impact on their adoption rate. Since, these technologies are vividly different in their core components and modus operandi, the security (and privacy) issues they face are very different. Thus, one size might not fit all solutions are ineffective and encourage tailor-made solutions.

Quantum computing poses risks to current cryptographic methods and securing quantum communication is a concern. AI systems need robust privacy measures, especially when handling sensitive data. Smart end devices are vulnerable to hacking, and cloud computing requires secure data storage and transmission.

The workshop will discuss the key security challenges for each of these technologies. Further, it will highlight how innovations from circuits and systems perspective have supported these technologies in their sustainable growth and development.

Despite their differences, these technologies share common security concerns such as authentication, encryption, and secure communication protocols. The workshop aims to identify and discuss these common components to encourage the development of optimized and innovative security solutions applicable across the spectrum of emerging technologies. Identification of such common security components will be a great motivator for circuits and systems people as they can focus on providing optimised (low-area, low-power etc) and innovative designs.

The workshop is designed to be *complementary* to the other contents of ISCAS related to climate and to sustainable development – while the special thematic sessions will present current research on the theme, the workshop will provide a space for collective reflection.

Outcomes

The workshop aims to give the following outcomes:

- An overview of security challenges in emerging technologies: Quantum Computing, Artificial Intelligence, Smart End Devices and Cloud Computing.
- Existing circuit level security solutions which are used to mitigate such security challenges.
- Finding coherence in security issues from these heterogenous technologies
- Identifying common components to encourage the development of optimized and innovative security solutions applicable across the spectrum of emerging technologies.

All these will be documented in the form of a white paper. This paper will be widely disseminated within CASS and IEEE, to inform and inspire other researchers.

Organiser

The workshop is being organised by Shivam Bhasin, PhD.

Dr. Shivam Bhasin is a Principal Research Scientist and Programme Manager (Cryptographic Engineering) at Centre for Hardware Assurance, Temasek Laboratories, Nanyang Technological University Singapore. He received his PhD in Electronics & Communication from Telecom Paristech in 2011, Advanced Master in Security of Integrated Systems & Applications from Mines Saint-Etienne, France in 2008. Before NTU, Shivam held position of Research Engineer in Institut Mines-Telecom, France. He was also a visiting researcher at UCL, Belgium (2011) and Kobe University (2013). His research interests include embedded security, trusted computing and secure designs. He has co-authored several publications at recognized journals and conferences. Some of his research now also forms a part of ISO/IEC 17825 standard.

Programme

The workshop will take place on 20/21 May 2024. The programme of the workshop is as follows.

Embedded Workshop on Climate Change 20/21 May 2024; 1.30pm – 5.00pm
1.30pm – 1.45 pm: Opening remarks by organiser - Importance of this workshop and structure
1.45 pm – 3.00pm: Circuits and Systems Solutions for Security of Emerging Technologies **Framing presentations by 3 speakers (25 mins each)** **Topics: Quantum, IoT, Artificial intelligence**
3.00pm – 3.30pm: Break
3.30pm – 3.55pm: Circuits and Systems Solutions for Security of Emerging Technologies **Framing presentations by 1 speakers (25 mins each)** **Topics: Cloud/Confidential Computing**
3.55pm – 4.50pm: Panel Discussion o Guiding question – Finding coherence in security issues from these heterogenous technologies o Identifying common components to encourage the development of optimized and innovative security solutions applicable across the spectrum of emerging technologies.
4.50pm – 5.00pm: Conclusions and closing - Encouragement for White paper - Next steps and closing

Framing presentations

The framing presentations will be delivered by experts in their respective fields with focus on information security. Speakers from the region will be prioritised, in order to optimise

expenditure. These could include Singapore (NTU, NUS and the Singapore government), India and Taiwan.

Participants

The target public for this workshop includes a subset of ISCAS 2024 attendees, who have strong interest and/or some experience in adapting ICT for information security. This public would be a mix of early- and late-career researchers . The workshop will be open to all ISCAS participants.