EW3: ISCAS 2024 Embedded Workshops on Hardware Security

Where: Leo 1, Resorts World Convention Centre
When: Tuesday, May 21, 2024

Objective: This workshop aligns with special 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 like Side-channel analysis and Artificial Intelligence, Hardware trojan and Hardware root-of-trust.

Distinguished Speakers

Prof. Maire O'Neill
Queens University Belfast
Director, UK RISE

Prof. Trevor E. Carlson
NUS, Singapore

SCAN ME

Expression of Interest

Prof. Stjepan Picek
Radboud University, Netherlands

Prof. Saibal Mukhopadhyay
Georgia Tech, USA

Prof. Anupam Chattopadhyay
NTU, Singapore

Schedule

Morning Session		
08:30-08:40	Dr. Shivam Bhasin	Opening Remarks
08:40-09-20	Prof Maire O'Neill	Machine Learning and Hardware Security: A deeper look into Hardware-Based Threats
09:20- 10::00	Prof. Stjepan Picek	AI-based Side-channel Analysis: Lessons Learned and Open Challenges
Afternoon Session		
16:00- 16:30	Prof. Saibal Mukhopadhyay	Side Channel and Hardware Security: A Threat and a Defensive Tool
16:30- 17:00	Prof. Anupam Chattopadhyay	Securing Binarized Neural Networks via PUF-based Key Management in Memristive Crossbar Arrays
17:00- 17:30	Prof. Trevor E. Carlson	Side-Channels in Modern Processors: What Should Be Done To Protect Our Systems Next?

Organizer:
Dr. Shivam Bhasin
NTU, Singapore.
sbhasin@ntu.edu.sg

75 YEARS CAS

ISCAS 2024

EW3: ISCAS 2024 Embedded Workshops on Hardware Security

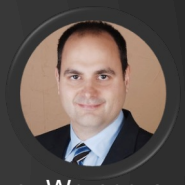
Where: Leo 1, Resorts World Convention Centre

When: Tuesday, May 21, 2024

Title: Machine Learning and Hardware Security: A deeper look into Hardware-Based Threats

Abstract: With the globalisation of supply chains the design and manufacture of today's electronic devices are now distributed worldwide, for example, through the use of overseas foundries, third party intellectual property (IP) and third party test facilities. Many different untrusted entities may be involved in the design and assembly phases and therefore, it is becoming increasingly difficult to ensure the integrity and authenticity of devices. The supply chain is now considered to be susceptible to a range of hardware-based threats, including hardware Trojans, IP piracy, reverse engineering, IC cloning and side-channel attacks. These attacks are major security threats to military, medical, government, transportation, and other critical and embedded systems applications. This talk will explore the role machine learning has to play in both hardware-based threats and in improving hardware security.

Speaker Bio: Professor Máire O'Neill is Regius Professor in Electronics and Computer Engineering and Director of the Centre for Secure Information Technologies (CSIT) at Queens University Belfast, N.Ireland. She is also Director of the UK Research Institute in Secure Hardware and Embedded Systems (RISE: www.ukrise.org), serves on the Responsible AI UK (RAI UK: www.rai.ac.uk/) leadership team and Chair of the IEEE Circuits and Systems for Communications Technical Committee. She has received numerous awards which include a 2024 Royal Irish Academy Gold Medal, a Blavatnik Engineering and Physical Sciences medal, 2019, and a Royal Academy of Engineering Silver Medal, 2014. She has authored two research books, 6 book chapters and over 200 peer-reviewed conference and journal publications. She is a Fellow of the Royal Academy of Engineering, a member of the Royal Irish Academy and Fellow of the Irish Academy of Engineering.



Title: Side-Channels in Modern Processors: What Should Be Done To Protect Our Systems Next?

Abstract: Modern processors today continue to leak data, in both speculative and non-speculative ways. We see a variety of new attacks, almost every week. But, while new attacks continue to be found, we have not seen significant proposals to change current systems to improve their security. Instead, we have seen one-off fixes by many CPU vendors as larger, more comprehensive changes could lead to significant performance penalties for common workloads. In this talk, we will discuss a number of our recent attacks, such as GadgetSpinner, PrefetchX and AfterImage. These attacks provide insight into the complexity of modern processors, but also their potential for new leaks in the systems we use every day. While we continue to look at one-off fixes for many of these issues, a new, systematic methodology is needed to help move the needle to significantly reduce the number and severity of these attacks.

Speaker Bio: Professor Trevor E. Carlson is an Assistant Professor at the National University of Singapore. He has received his Bachelors and Masters degrees from Carnegie Mellon University, his PhD from Ghent University in Belgium, and completed a postdoc at Uppsala University in Sweden. His interests include building efficient processors, security solutions and simulation and modeling methodologies. His processor and security works have been selected to appear in top computer architecture, security and design automation conferences (such as ASPLOS, DAC, ICCAD, ISCA, HPCA, MICRO, MICRO Top Picks, and USENIX Security). He is currently working to standardize and help to deploy the Capstone (USENIX Security 2023) work to allow for a new class of flexible, high-performance and trustless memory protection mechanisms. He has recently been awarded Amazon, Intel and VMWare Research Awards and Grants, and his work has received six Best Paper Awards or Best Paper Nominations in conferences such as the International Symposium on Microarchitecture (MICRO) and the International Symposium on Performance Analysis of Systems and Software (ISPASS).

Organizer:
Dr. Shivam Bhasin
NTU, Singapore.
sbhasin@ntu.edu.sg

ISCAS 2024

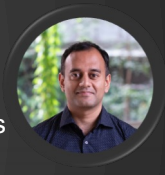
EW3: ISCAS 2024 Embedded Workshops on Hardware Security

Where: Leo 1, Resorts World Convention Centre
When: Tuesday, May 21, 2024

Title: AI-based Side-channel Analysis: Lessons Learned and Open Challenges

Abstract: Side-channel attacks (SCAs) are powerful attacks based on information obtained from the implementation of cryptographic devices. Profiling side-channel attacks have received significant attention as this attack defines the worst-case security assumptions. The most explored profiling attacks in the last few years are based on deep learning techniques. Such attacks are very powerful as they can break targets protected with countermeasures. They are also "easier" to deploy as they do not require pre-processing and feature selection. In this talk, we will cover the developments in the last eight years, starting with simple multilayer perceptron architectures and finishing with language-based models for SCA. The talk will concentrate not only on successful stories but also on open challenges like AI explainability and SCA, non-profiled deel learning attacks, large language models and SCA, and countermeasures against machine learning-based SCAs.

Speaker Bio: Stjepan Picek is an associate professor at Radboud University, The Netherlands. His research interests are security/cryptography, machine learning, and evolutionary computation. Prior to the associate professor position, dr. Picek was an assistant professor at TU Delft, and a postdoctoral researcher at MIT, USA and KU Leuven, Belgium. Dr. Picek finished his PhD in 2015 with a topic on cryptology and evolutionary computation techniques. He also has several years of experience working in industry and government. Up to now, dr. Picek has given more than 40 invited talks and published more than 150 refereed papers. He is a program committee member and reviewer for a number of conferences and journals, and a member of several professional societies. His work has been featured in the mainstream media and popular technology blogs. He received the Vera Johanides Award for young scientists in 2018, the Rikard Podhorsky Award for outstanding scientific contributions in 2023 (both awards by the Croatian Academy of Engineering), and the IEEE Croatia section award for outstanding engineering contributions in 2023. Dr. Picek received several best paper awards, most recently the NDSS 2023 Distinguished Paper Award.



Title: Securing Binarized Neural Networks via PUF-based Key Management in Memristive Crossbar Arrays

Abstract: Binarized neural networks (BNNs) are a subset of deep neural networks proposed to consume less computational resources with a smaller energy budget. Recent studies showed that memristor-based in-memory computing architectures can be constructed to accelerate BNNs, with better performance compared to traditional CMOS technologies. The memristor non-volatility utilized for in-memory computing poses a notable threat to theft attacks in the presence of adversaries with physical access. This motivates us to introduce two novel protection methodologies to safeguard the model parameters of BNNs in the memristive crossbar. We propose to take advantage of Physical Unclonable Functions (PUFs), which can be implemented using memristor-based crossbars for protecting BNN. This feature provides superior security compared to the traditional stored-key-based schemes. We provide circuit-level hardware designs to implement our methodologies with negligible additional overhead compared to an unprotected design and detailed supporting analysis to validate our security claims.

Speaker Bio: Anupam Chattopadhyay received his B.E. degree from Jadavpur University, India, MSc. from ALaRI, Switzerland, and Ph.D. from RWTH Aachen in 2000, 2002, and 2008 respectively. From 2008 to 2009, he worked as a Member of Consulting Staff in CoWare R&D, Noida, India. From 2010 to 2014, he led the MPSoC Architectures Research Group in RWTH Aachen, Germany as a Junior Professor. Since September 2014, Anupam was appointed as an Assistant Professor in SCSE, NTU, where he got promoted to Associate Professor with Tenure from August 2019. In the past, he held visiting positions at Kyoto University, Japan; Politecnico di Torino, Italy; EPFL, Switzerland; Technion, Israel, and Indian Statistical Institute, Kolkata. His research interests are in Application-specific architecture, Electronic Design Automation, and Security. Anupam is an Associate Editor of IEEE Embedded Systems Letters and series editor of Springer Book Series on Computer Architecture and Design Methodologies. He is senior member of ACM and IEEE.

Organizer:
Dr. Shivam Bhasin
NTU, Singapore.
sbhasin@ntu.edu.sg

ISCAS 2024

EW3: ISCAS 2024 Embedded Workshops on Hardware Security

Where: Leo 1, Resorts World Convention Centre

When: Tuesday, May 21, 2024

Title: Side Channel and Hardware Security: A Threat and a Defensive Tool"

Abstract: Power and Electromagnetic (EM) emission based side-channel leakage play crucial roles in hardware security. This talk will discuss how side-channel leakage can act as threats to secure execution as well as can be used as defensive tools to enhance security against malicious attacks. The first part of the talk will discuss power/EM-based attacks to crypto engines and machine learning accelerators, and present circuit-based techniques to improve side-channel resistance. The second part of the talk will present machine learning (ML) based methods to use side-channel leakage for intrusion (malware) detection. The efficacies of ML models used in side-channel based malware detection will be discussed. The talk will conclude with future challenges and research needs in inhibiting and exploring side-channel to improve security.

Speaker Bio: Saibal Mukhopadhyay received the B.E. degree in electronics and telecommunication engineering from Jadavpur University, Kolkata, India, in 2000, and the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2006. He was a Research Staff Member with the IBM Thomas J. Watson Research Center, Yorktown Heights, NY, USA, from August 2007 to September 2007. He is currently a Joseph M. Pettit Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. He has authored or coauthored over 200 articles in refereed journals and conferences and holds five U.S. patents. His research interests include the design of energy-efficient, intelligent, and secure systems in nanometer technologies. He was a recipient of the Office of Naval Research Young Investigator Award, in 2012; the National Science Foundation CAREER Award, in 2011; the IBM Faculty Partnership Award, in 2009 and 2010; the SRC Inventor Recognition Award, in 2008; the SRC Technical Excellence Award, in 2005; and the IBM Ph.D. Fellowship Award, from 2004 to 2005.

Organizer:
Dr. Shivam Bhasin
NTU, Singapore.
sbhasin@ntu.edu.sg

ISCAS 2024