RESEARCH INSTITUTE FOR
SECURE HARDWARE &
EMBEDDED SYSTEMS

RISE – Hardware Security and the latest R&D

Philip Hodgers

IoTSF Conference, London 2019

QUEEN'S UNIVERSITY BELFAST

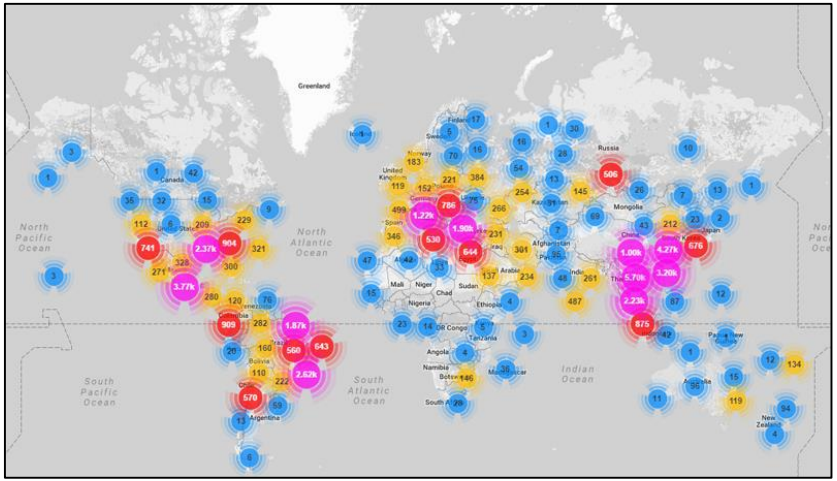
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

in association with National Cyber Security Centre

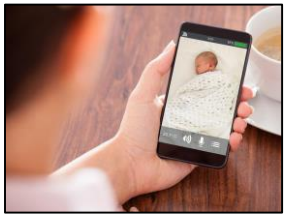
EPSRC Engineering and Physical Sciences Research Council

Insecure Connected Devices

The IoT Security challenge…



Breaking down Mirai: An IoT DDoS Botnet Analysis www.incapsula.com, Aug 2017



Adapted from https://www.techrepublic.com/pictures/photos-the-11-least-secure-connected-devices/

Vulnerabilities affecting Hardware devices

Meltdown

Spectre

FORESHADOW

"10s of more micro-architectural attacks to be expected"

… Daniel Gruss, co-author of Meltdown and Spectre attacks, March 2018

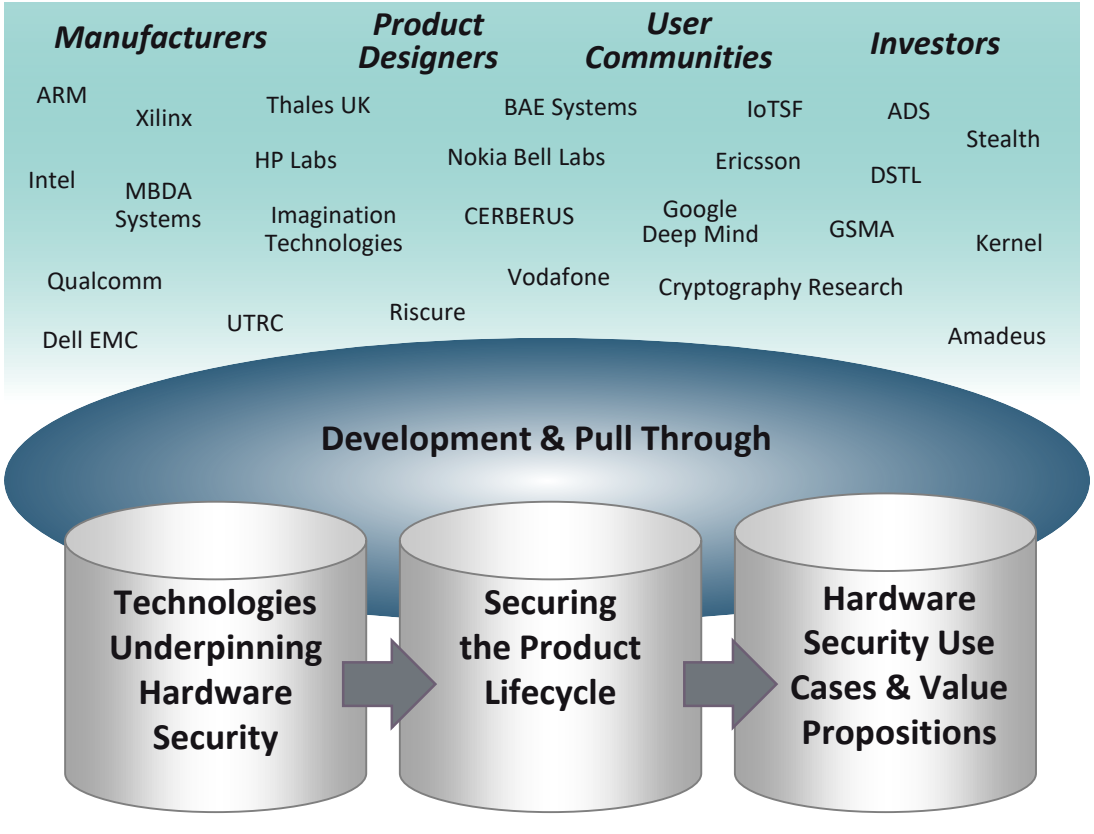
Research Institute for Secure Hardware & Embedded Systems

£5M Research institute, with funding from NCSC and EPSRC

Launched Nov 2017, Prof. Maire O'Neill Centre for Secure Information Technology

Aim: To create a global centre for research and innovation in hardware security

RISE Ecosystem



RISE Research Challenges

- State-of-the-art HW security primitives: TRNGs, PUFs
- Novel HW analysis toolsets & techniques
- Attack-resilient HW platforms, HW IP building blocks

- Confidence in Developing Secure HW Devices
- Supply Chain Confidence
- Modelling of HW Security

- Combining hardware roots of trust (e.g. TPM, TEEs) with advanced cryptographic techniques, e.g. identity- or attribute-based encryption to offer data-centric security (e.g. FIDO)

RISE Research Projects

Research challenges of RISE to be delivered through a series of projects

Core Projects

SCARV: a side-channel hardened RISC-V platform.
University of Bristol, Dr Daniel Page.

IOSEC: Protection and Memory Safety for Input/output Security.
University of Cambridge, Dr Robert Watson, Prof Simon Moore, Dr Athanasios Markettos.

User-controlled hardware security anchors: evaluation and designs.
University of Birmingham, Prof Mark Ryan, Dr Flavio Garcia and Dr David Oswald.

Deep Security: investigating the application of deep learning in SCA and HT detection, with the ultimate goal of utilising deep learning.
Queen's University Belfast, Prof Máire O'Neill.

Tranche 2 Projects

SafeBet: Memory capabilities to enable safe, aggressive speculation in processors.
University of Cambridge, Prof Simon Moore.

GUPT: A Hardware-Assisted Secure and Private Data Analytics Service.
University of Edinburgh, Dr Pramod Bhatotia and Dr Markulf Kohlweiss.

TimeTrust: Robust Timing via Hardware Roots of Trust and Non-standard Hardware, with Application to EMV Contactless Payments.
University of Surrey, Dr Ioana Boreanu, Dr Tom Chothia, Prof Liqun Chen.

rFAS: Reconfigurable FPGA Accelerator Sandboxing.
University of Manchester, Dr Dirk Koch.

IOSEC: Protection and Memory Safety for Input/Output Security

A. Theodore Markettos, Simon W. Moore, Robert N. M. Watson

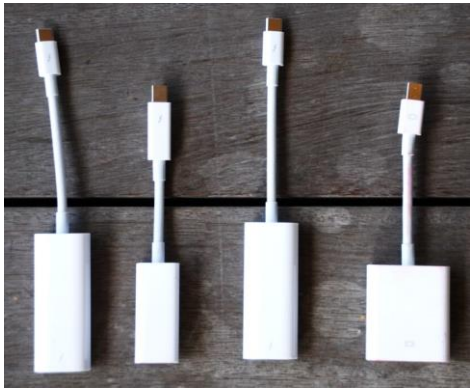
Second Annual RISE Conference

London, 21 November 2019

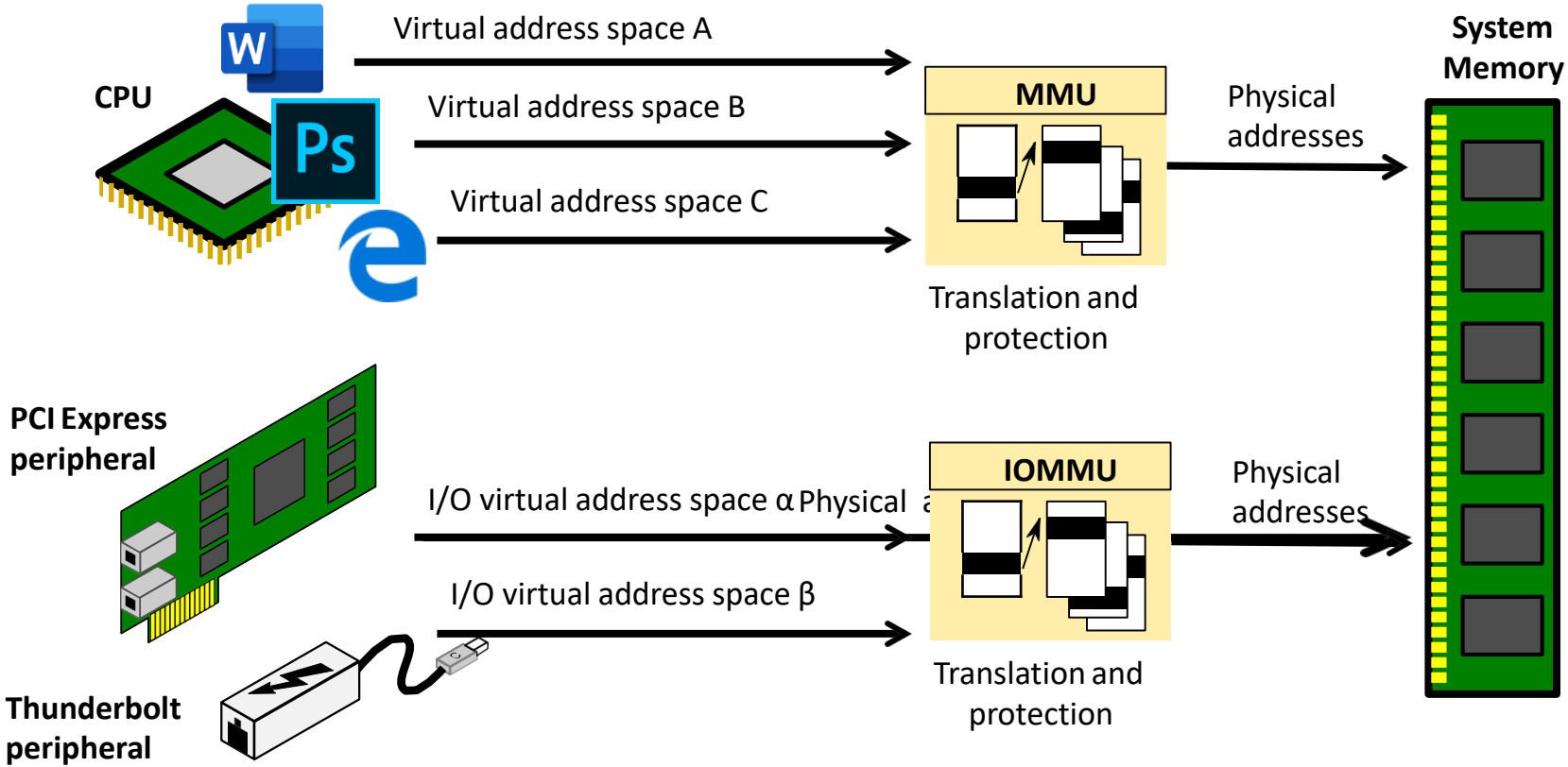
Funded by EPSRC under the RISE initiative (ref: EP/R012458/1)

Smaller laptops, more external peripherals

- Laptops getting smaller, more devices are going external
  - Chargers, dongles,docking stations
  - Common to borrow external peripherals (power, dongles, displays) from others
- Performance is increasingly more of a constraint. Security?



I/O Memory Management Unit: device isolation



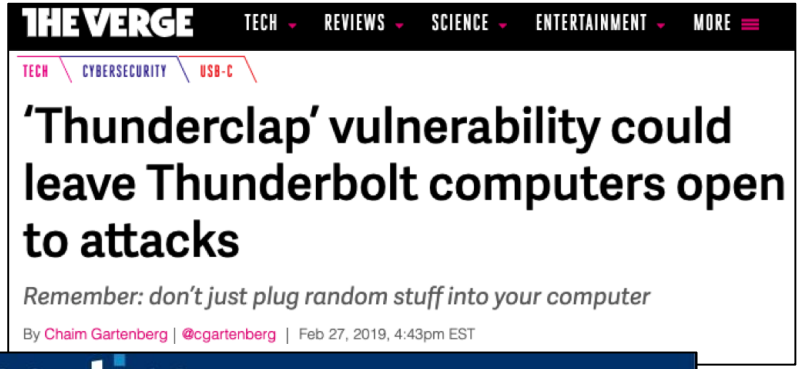
Our IOMMU attacks

- Windows10: barely uses the IOMMU, mostly unprotected from malicious devices
- MacOS: uses IOMMU since 2012 but in a limited way
  - ran a root shell
  - extracted private VPN traffic
- FreeBSD: IOMMU not enabled by default
  - when enabled, tries to properly segregate devices using IOMMU
  - root shell, private data extraction
- Linux: most distros don't enable the IOMMU by default
  - when enabled, tries to segregate devices using IOMMU
  - when enabled, could see private network traffic, kernel data, code pointers etc
  - simply set a bit in a PCIe packet to fully bypass the IOMMU!
- All exploitable from a malicious Thunderbolt dock

Media interest

- NDSS publication picked up by ~70 media outlets across the world

http://thunderclap.io/thunderclap-paper-ndss2019.pdf

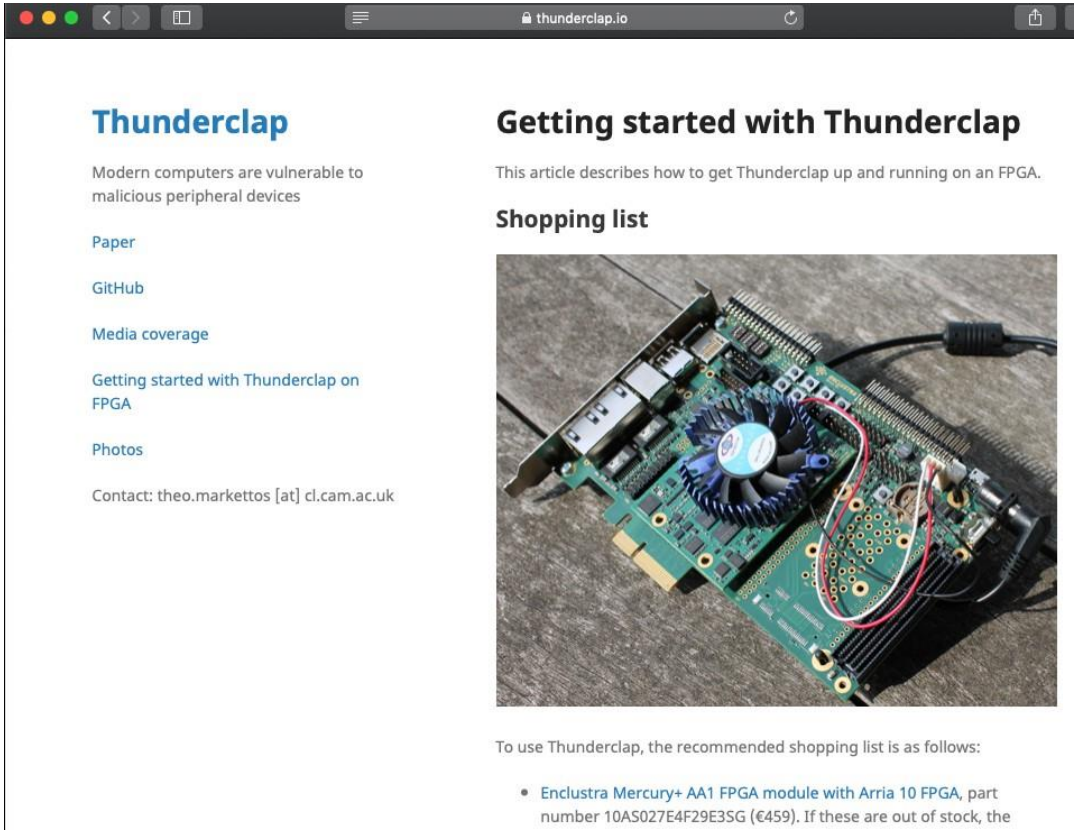


Mitigations and impact

- Collaborating with vendors since 2016
- Apple mitigated specific exploit in MacOS 10.12.4
  - encrypt the kernel pointer, hide the flags
- Microsoft shipped Kernel DMA Protection for Thunderbolt 3 in Windows 10 1803
  - IOMMU enabled for Thunderbolt devices (only)
  - Requires post-1803 firmware, ie new products only
  - Best practice guidelines for businesses: 'Standards for a highly secure Windows 10 device'
- Intel enabled IOMMU for Thunderbolt in Linux 4.21 (now 5.0rc), disabled ATS
  - Thunderbolt devices are now less trusted than internal ones
- Major laptop vendor: we won't ship Thunderbolt until we understand this attack vector better

Thunderclap.io transition to industry

- Vendors want to audit security from malicious devices, but don't have the skill set
- Our hardware and software has been open-sourced
- Worked hard to make it accessible to software folks
- Major vendors are now using it internally




CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
DEEPSECURITY: APPLYING
DEEP LEARNING TO
HARDWARE SECURITY
QUEEN'S
UNIVERSITY
BELFAST
ESTD1845

DeepSecurity: Applying Deep Learning to Hardware Security

Overall Goal

To investigate the use of **Deep Learning** for security verification in EDA tools, specifically in relation to **Hardware Trojan detection** and **Side channel analysis** to allow non-security experts to receive feedback on how to improve the security of their designs prior to fabrication.

Rambus Cryptography Research

riscure

BAE SYSTEMS

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

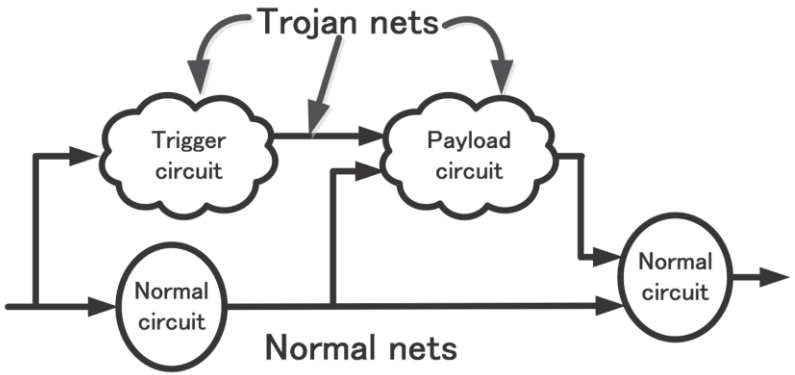
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Hardware Trojans

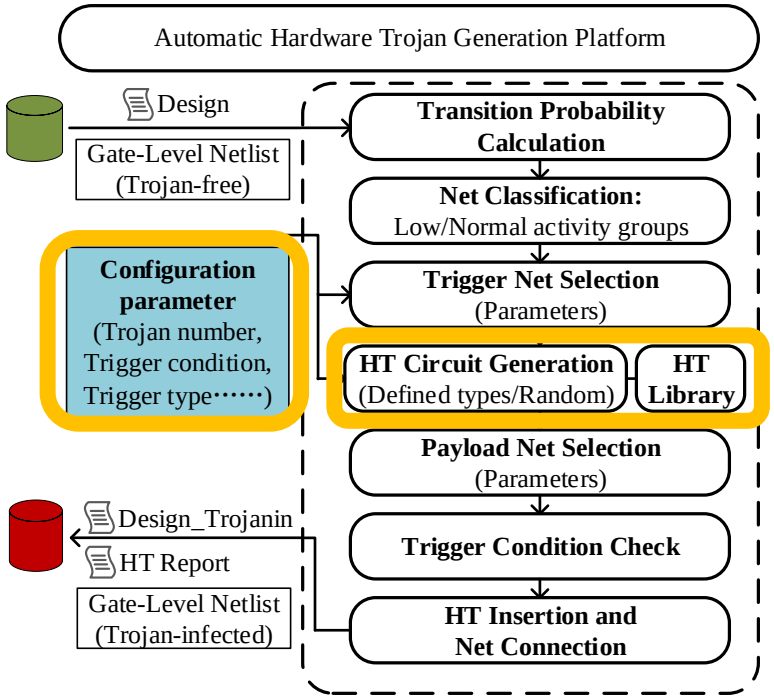
- Hardware Trojans (HTs) are malicious modifications to integrated circuits (ICs)
  - Emerging security concern in the IC industry

- Globalisation of semiconductor supply chains, design and fabrication of ICs now distributed worldwide
  - use of overseas foundries,
  - third party IP,
  - third party test facilities

- Becoming difficult to ensure the integrity and authenticity of devices

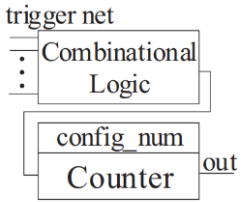


An Improved Automatic Hardware Trojan Generation Platform

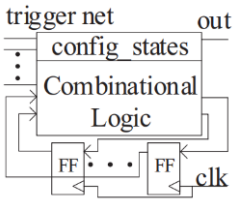


CIRCUIT TYPES IN TROJAN LIBRARY

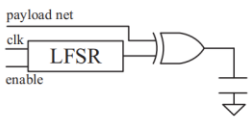
HT Part	Type Name	Description	
Trigger	comb	Combinational Trigger composed of AND gates	
	seque_CNT	Counter based sequential trigger	(a)
	seque_FSM	Finite-state machine based sequential trigger	(b)
	user_def_trig	User-defined trigger circuits	
Payload	func	XOR gate based functional error payload	
	leak_LFSR	Linear feedback shift register based information leakage payload	(c)
	leak_SHIFT	Shift register based information leakage payload	(d)
	user_def_pay	User-defined payload circuits	



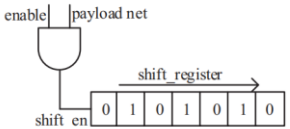
(a)



(b)



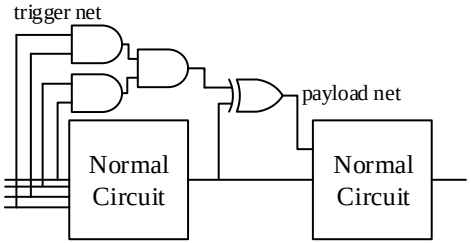
(c)



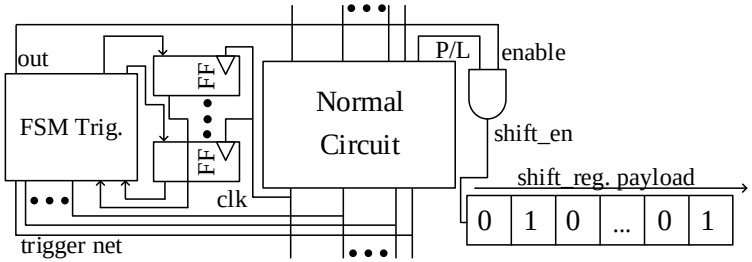
(d)

An Improved Automatic Hardware Trojan Generation Platform

Generated HT benchmark samples:



(a) Combinational Trojan with functional error payload



(b) FSM based sequential Trojan with a SHIFT based leakage circuit

When compared with the COTD detection results from [1], who proposed a dynamic Hardware Trojan benchmark.

TABLE I
COMPARISON OF COTD-BASED HT DETECTION RESULTS

Benchmarks	Trigger Conditon (Rare/Total)	Type	HTs in [1]		Generated HTs [2]	
			FPR(%)	FNR(%)	FPR(%)	FNR(%)
s13207-c5_6	5/6	comb	25	0	0.39	23
s13207-s5_6	5/6	seq	0.11	0	0.41	19
s15850-c5_6	5/6	comb	27	0	12	25
s15850-s5_6	5/6	seq	0.09	0	0.11	17
s35932-c5_6	5/6	comb	60	0	15	33
s35932-s5_6	5/6	seq	0.08	0	0.03	20

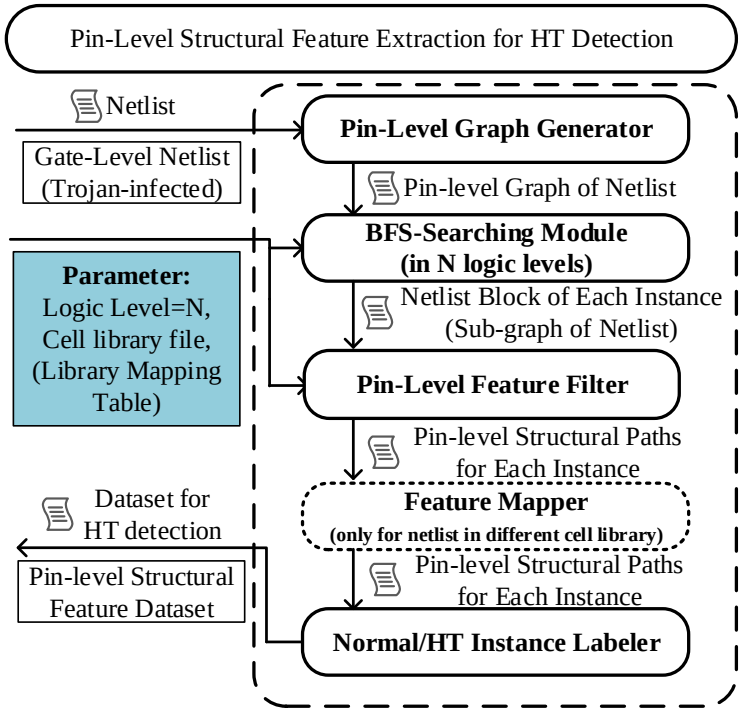
[1] J. Cruz, Y. Huang, P. Mishra, and S. Bhunia, “An automated configurable trojan insertion framework for dynamic trust benchmarks,” in Proc. Design, Automation Test in Europe Conf. Exhibition, March 2018

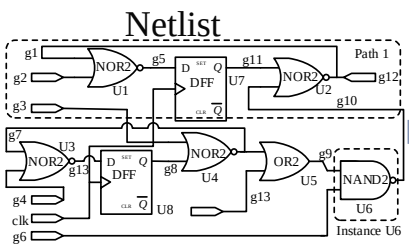
[2] Yu, S., Liu, W., & O'Neill, M. (2019). An Improved Automatic Hardware Trojan Generation Platform. In IEEE Computer Society Annual Symposium on VLSI (ISVLSI)

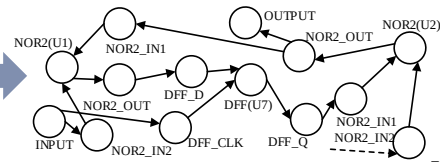
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

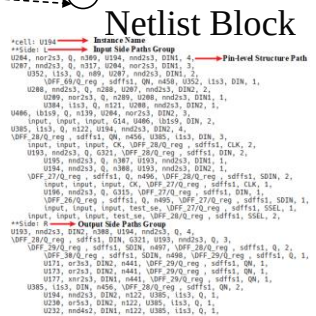
A Novel Feature Extraction Strategy for Hardware Trojan Detection

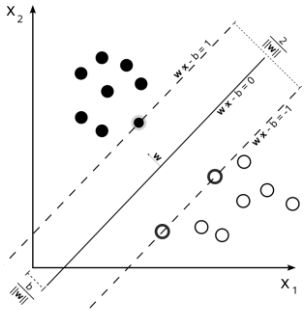
" A Novel Feature Extraction Strategy for Hardware Trojan Detection " ISCAS 2020, (Submitted)











RISE Spring School

https://www.ukrise.org/springschool/programme/

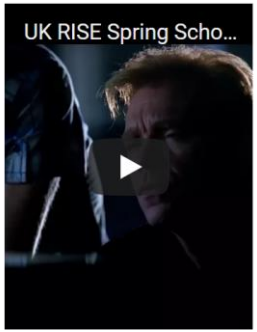
PUF: From Research to Practice
Chongyan Gu, Queen's University Belfast, UK

Winning the War in Memory
Simon Moore, University of Cambridge, UK

Perspectives on hardware security: embedding it everywhere, continuously and inexpensively
Massimo Alioto, National University of Singapore

ARM's perspective on the importance of hardware security research
Richard Grisenthwait, ARM

Software-based Microarchitectural Attacks
Dr Daniel Gruss, Graz University of Technology, Austria



Physical Attacks: Towards combined threat, protection and beyond
Shivam Bhasin, David Berend, Nanyang Technical University Singapore

Thank you

ukrise.org | info@ukrise.org | @UK_RISE

QUEEN'S UNIVERSITY BELFAST
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES
in association with National Cyber Security Centre
EPSRC Engineering and Physical Sciences Research Council