NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE | TEMASEK LABORATORIES @ NTU

Cyber-Hardware Forensics & Assurance Evaluation R&D (CHFA) Programme

Grant Call 1

Prof Gan Chee Lip

Office of Research & Technology for Defence & Security (ORTDS);
Temasek Labor*atories (TL@NTU)*

18 Nov 2019

Agenda

- Introduction to Programme & Its Thrusts
- Information about Grant Call Launch
- Briefing for the Research Offices

Programme Structure

Cyber-Hardware Forensics & Assurance Evaluation R&D Programme

Lead PI: Prof. GAN Chee Lip

Use Case 1:
Rapid Recovery Forensics R&D

THRUST i: Data Recovery via Advanced Failure Analysis Techniques
Co-PI: Dr. LIU Qing

THRUST ii: Computer Aided Data Analysis of Recovered Data
Co-PI: Assoc Prof. GWEE Bah Hwee

Use Case 2:
Evaluating Modern Processors and Hardware for Security, Privacy and Assurance

THRUST iii: Research for Advanced Hardware Evaluation Techniques for Modern Systems with Security and Privacy Features
Co-PI: Dr. BHASIN Shivam

THRUST iv: Advanced Side-Channels to Evaluate Security and Privacy Features of Modern Processors
Co-PI: Assoc. Prof. CHATTOPADHYAY Anupam

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Rapid Recovery Forensics R&D

Thrust (i)
Data Recovery via Advanced Failure Analysis Techniques
PI: Dr Liu Qing (Temasek Lab@NTU)

Thrust (ii)
Computer Aided Data Analysis of Recovered Data
PI: A/P Gwee Bah Hwee (School of EEE)

Rapid Recovery Forensics R&D

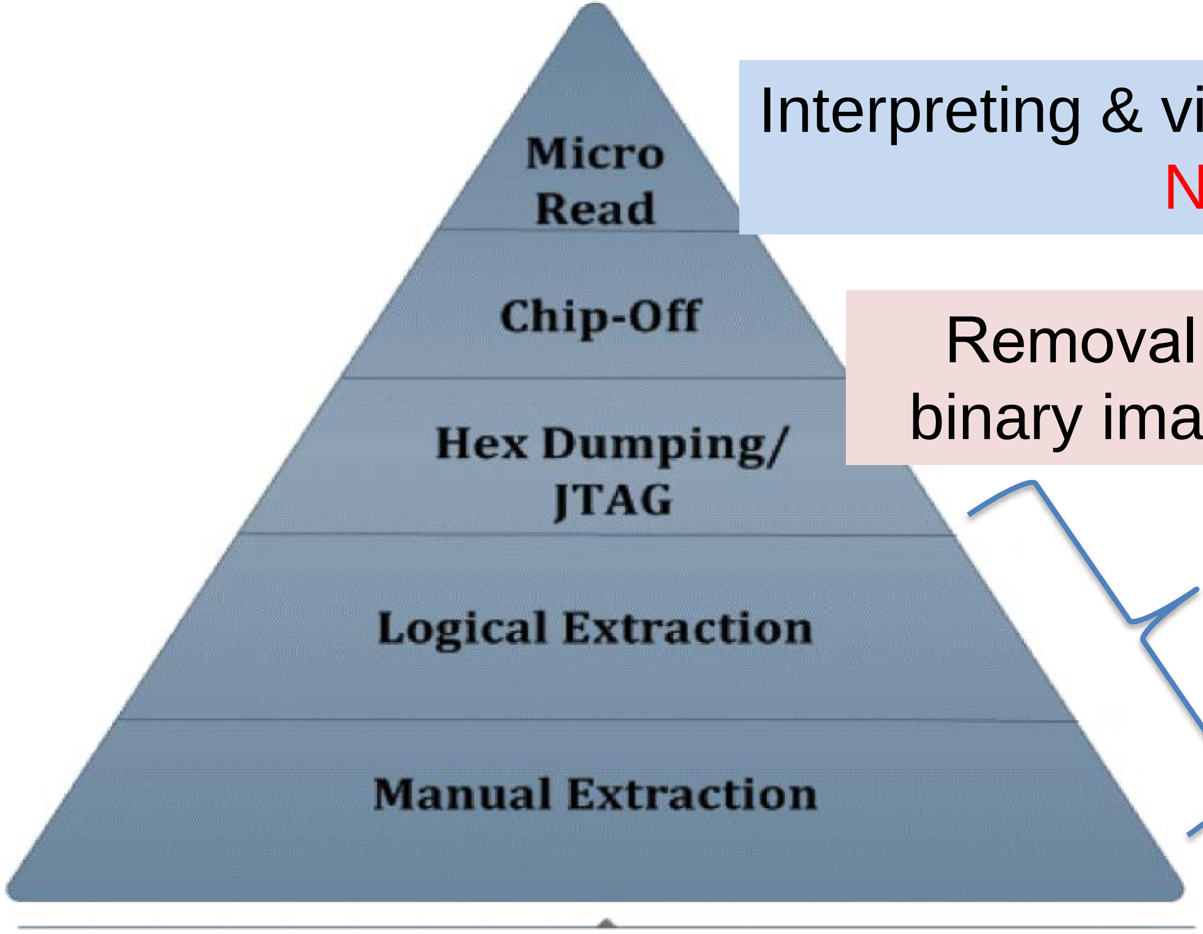
Project Scope:

1. Investigation of device level physical failure analysis and chip off techniques for data extraction from advanced memory devices.

2. Exploration of data extraction techniques for damaged non-volatile memory devices.

3. Exploration of artificial intelligence techniques for software aided rapid recovery of forensic data, including automatic data identification, classification and restoration.

Tools & Techniques for Mobile Device Forensics



Interpreting & viewing of data on memory chips
No tool available yet

Removal of phone’s chips & creating its binary image by directly extracting its data

Device is functioning well

Figure 1: Mobile Device Tool Classification System

https://resources.infosecinstitute.com/category/computerforensics/introduction/mobileforensics/common-mobile-forensics-tools-and-techniques/

Chip-Off Approach

- The approach is highly dependent on the details of device damage.
- Failure analysis on the device level is critical to determine subsequent extraction methods.
  - Remove the memory chip from the damaged device, connect it to the reader and extract the data
  - Remove the chips from the damaged device, install them on the donor device, “on” and extract the data

Chip-Off Approach

- Remove the memory chip from the damaged device, connect it to the reader and extract the data
  - Typically used to extract unencrypted data
  - Feasible to extract the encrypted data, if the encryption key and algorithm have been well analyzed
- Remove the chips from the damaged device, install them on the donor device, “on” and extract the data
  - Fully understand the device
  - Accurately identify the chip to be mounted
  - Highly dependent on the circumstances (the chips to be mounted must be functional, availability of the donor device, passwords or techniques to bypass the secure start-up, *etc.*)

Chip-Off Data Recovery Flow

- Physical data
  - Read physical data from flash devices
- Virtual data
  - Organize physical data into virtual data
- Logical data
  - Map virtual data into logical data
- User data
  - Interpret logical data into user files

Micro-Read Approach

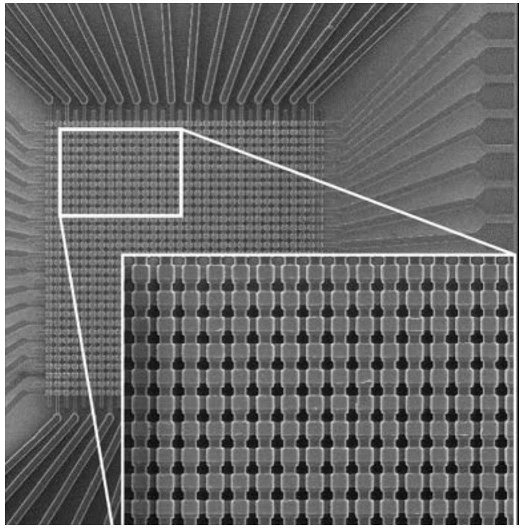
- Damaged but functional microchips
- Challenging for sample preparation to fulfil the requirements of extraction techniques
- Investigation of techniques and optimization of the recipes to extract the data
- Data analysis (signals or images)
  - Naturally used to extract unencrypted data (such as master keys)
  - Possible for encrypted data, if the encryption key and algorithm have been well analyzed

Micro-Read Approach

- Pre-data
  - Obtain chip info and take chip images
- Binary data
  - Read bit values from images
- Physical data
  - Organize and interpret binary data into physical data

Computer Aided Data Analysis of Recovered Data

- Automatic binary data extraction from microscopic images
- Automatic data analysis & classification
- Automatic data repair & restoration



Memory Microscopic Image

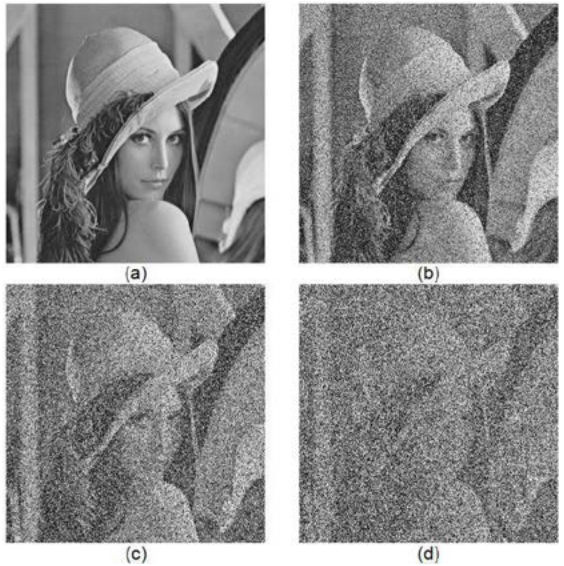


Image Restoration

Device-level FA – What can we do

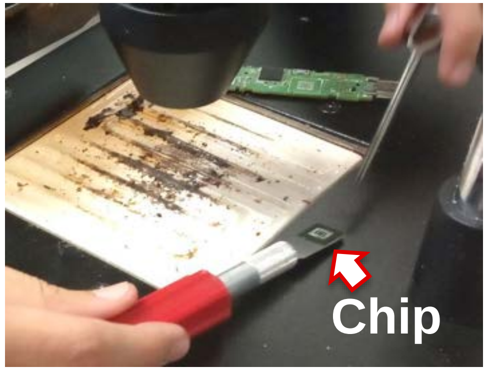
Device teardown

Mobile fix kit

Hardware extraction

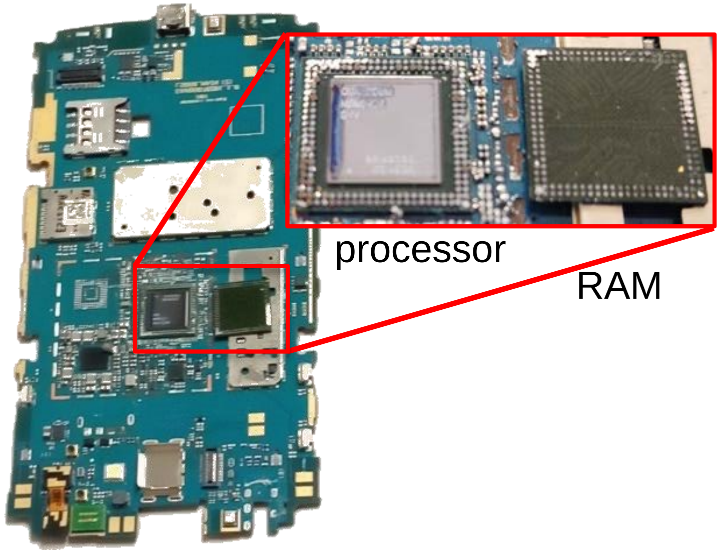
Mechanical

Thermal



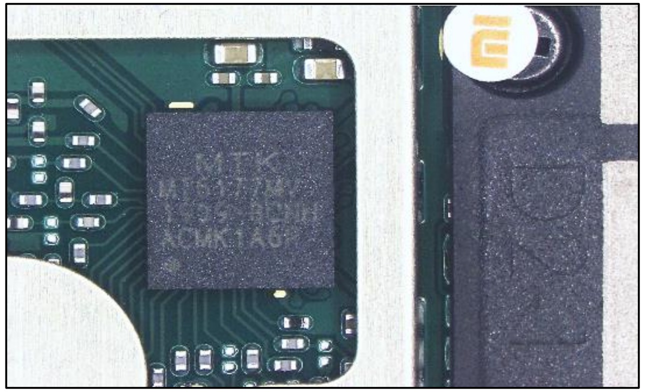
Package separation

Tools and solder



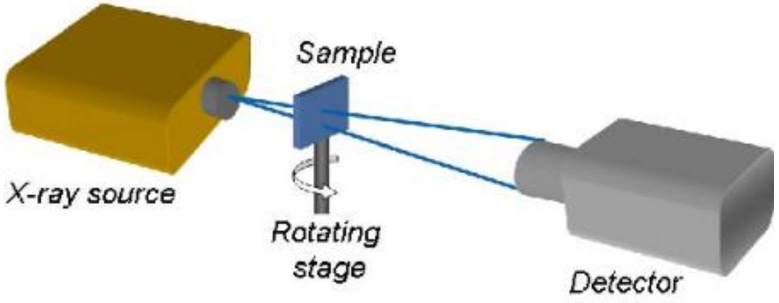
Device-level FA – What can we see

Optical

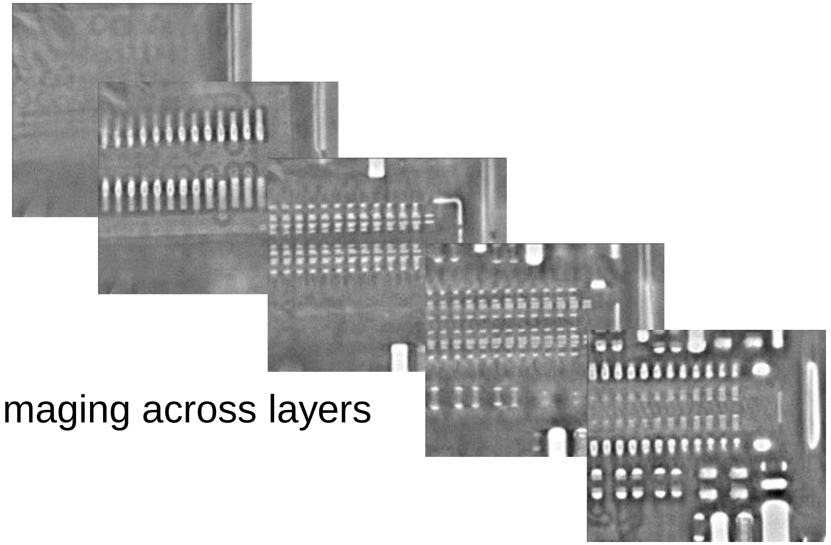


Board inspection

X-ray (2D/3D mode)

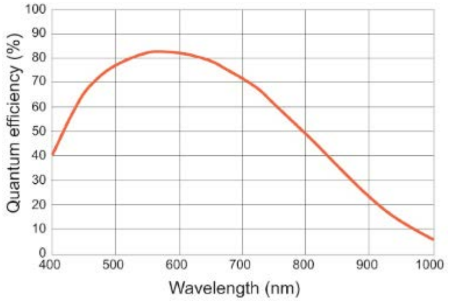


Pacheco, et al, *2010 IEEE International Reliability Physics Symposium* (2010)

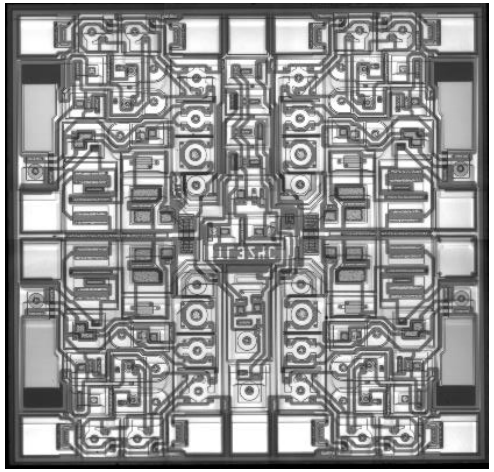


Imaging across layers

IR



IR microscope



Circuit layout

T1: Identified Mobile Device

Redmi 6/6A

- 12 nm Mediatek chipset
- 16-64 GB NAND memory
- 147.5 mm x 71.5 mm x 8.3 mm
- > Android 8.1

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Evaluating Modern Processors and Hardware for Security, Privacy and Assurance

Thrust (iii)
Research for Advanced Hardware Evaluation Techniques for Modern Systems with Security and Privacy Features
PI: Dr Shivam Bhasin (Temasek Lab@NTU)

Thrust (iv)
Advanced Side-Channels to Evaluate Security and Privacy Features of Modern Processors
PI: A/P Anupam Chattopadhyay *(School of SCSE)*

Evaluating Modern Processors and Hardware for Security, Privacy and Assurance

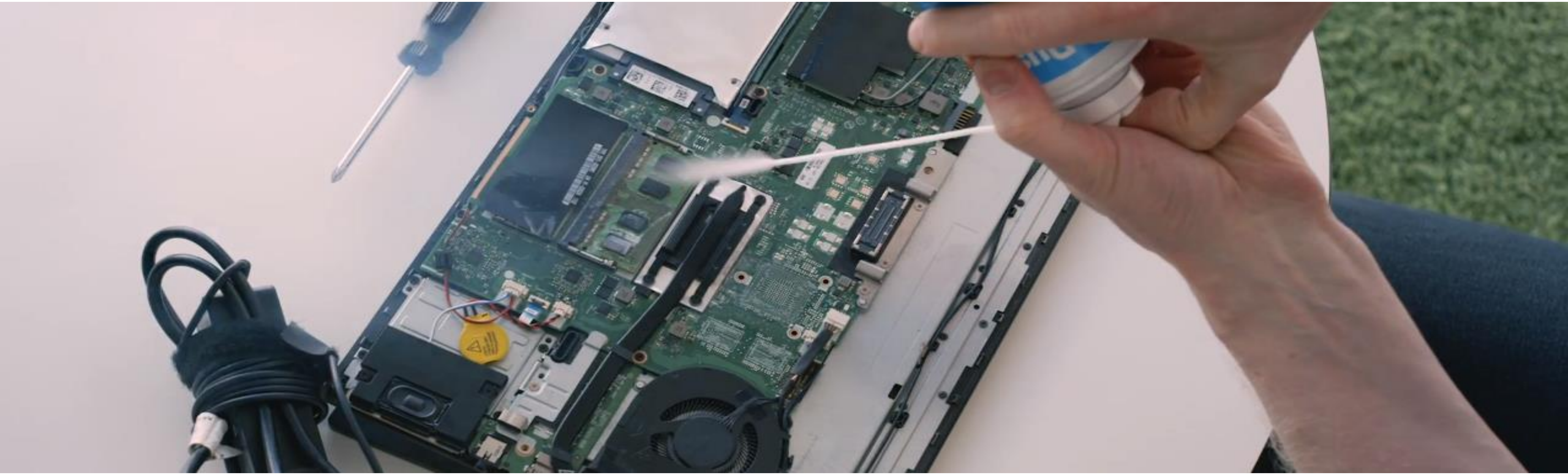
Project Scope:

1. Investigation on susceptibility of representative state of the art systems against cold boot attacks for security evaluation.

2. Investigation on susceptibility of representative state of the art systems against fault attacks (e.g. laser, electromagnetic and glitching) to bypass secure boot.

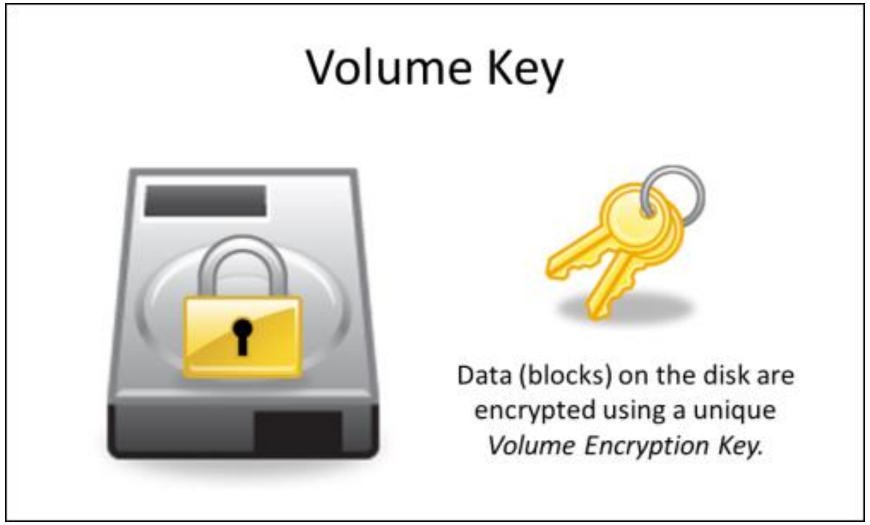
3. Investigation on the vulnerabilities of address space partitioning (e.g. data boundaries, access pattern).

Cold Boot Attack



- Keys must be loaded to decrypt and process encrypted data
- Exploit data remanence property of DRAM to extract decryption key from post-freeze

Cold Boot Attack



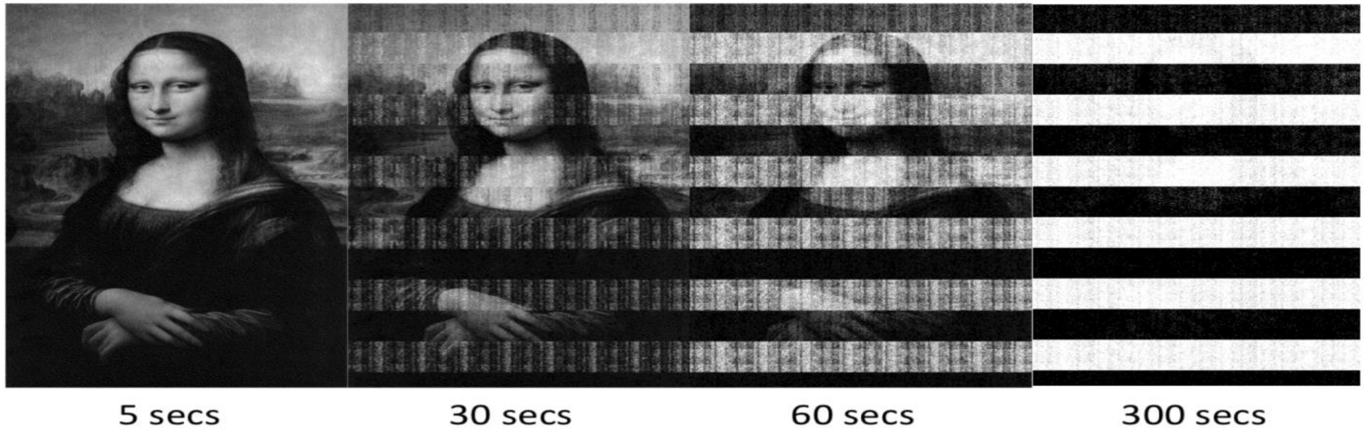
Volume Key

Data (blocks) on the disk are encrypted using a unique *Volume Encryption Key.*

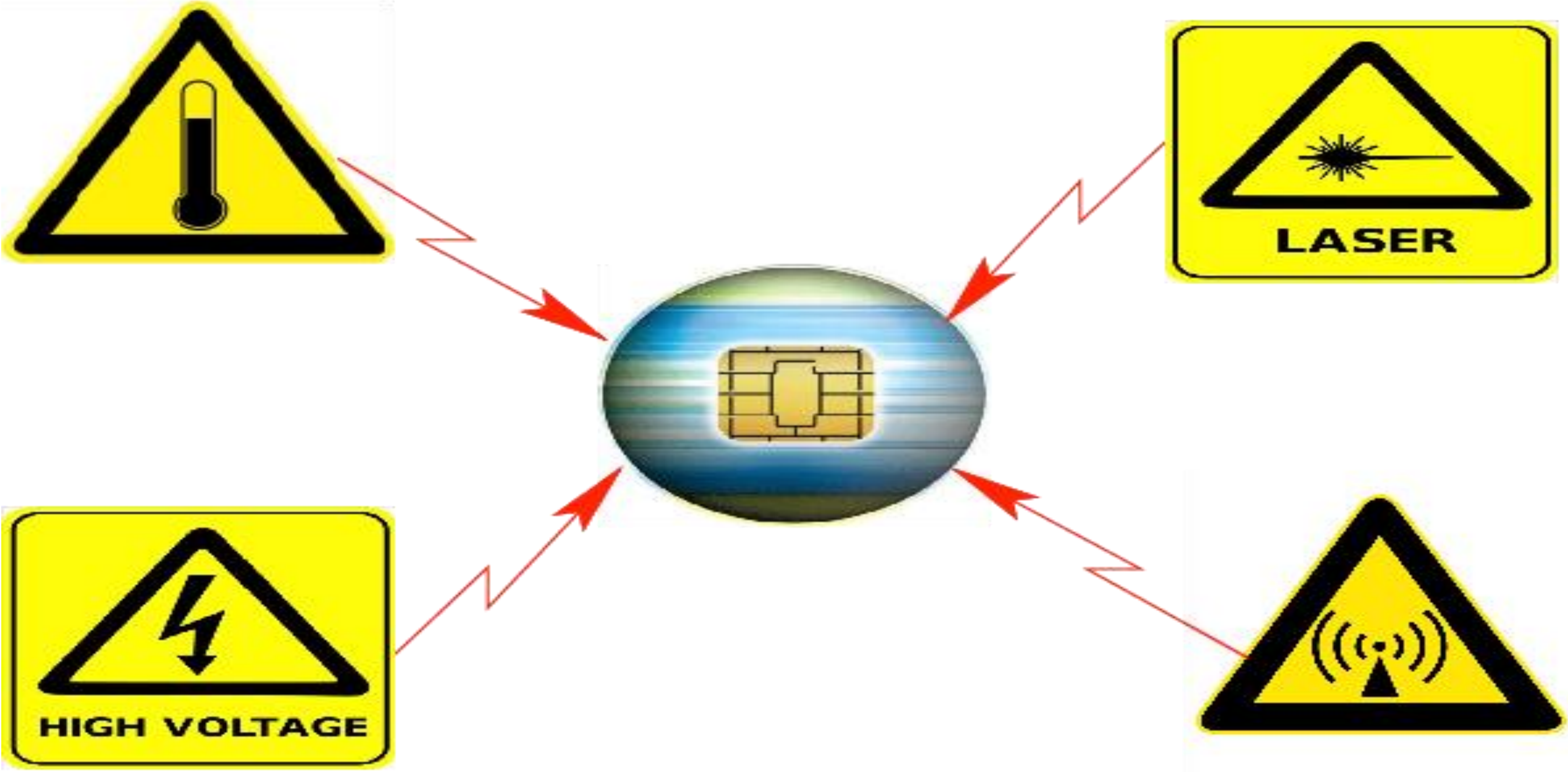
Steps of a Cold Boot Attack

1. Freeze memory at power-off
2. Extract memory content
3. Locate secret keys in memory content
4. Reconstruct decayed keys
5. Decrypt sensitive data

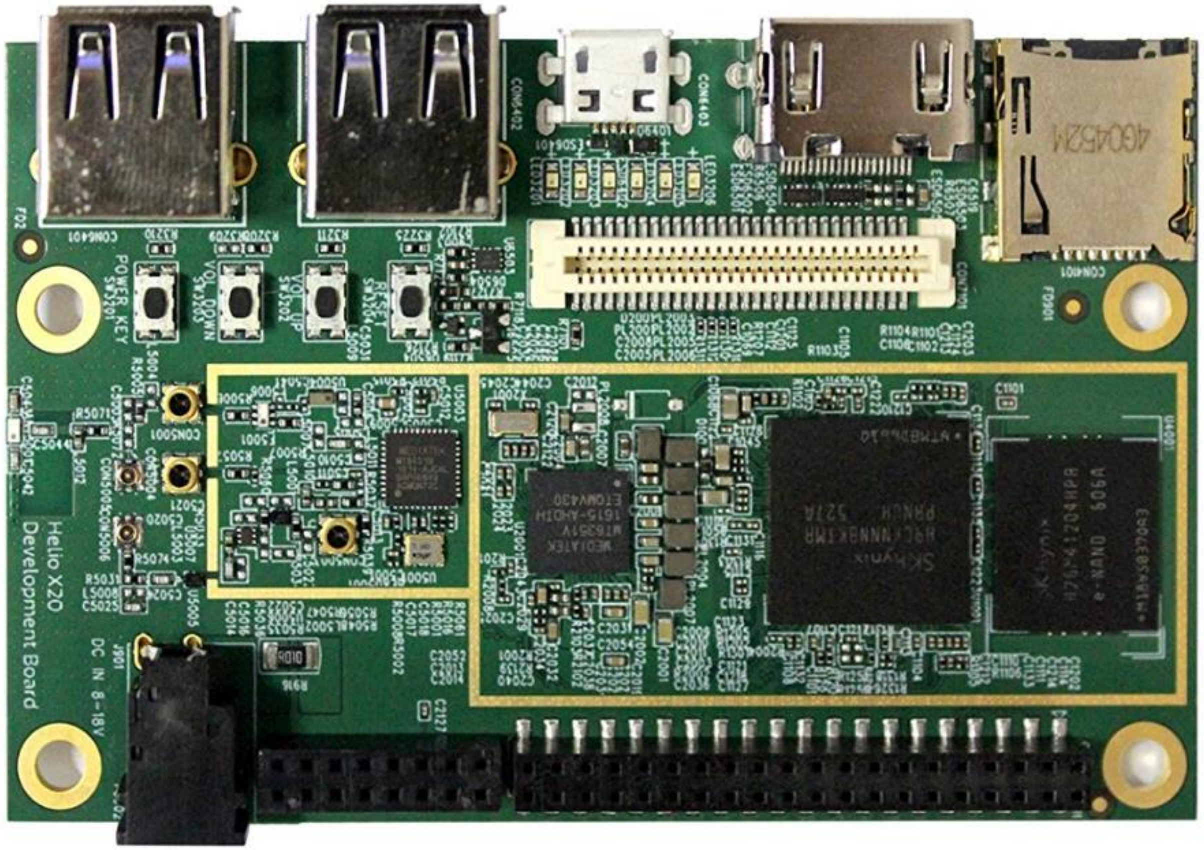
-50^{o}C
$10

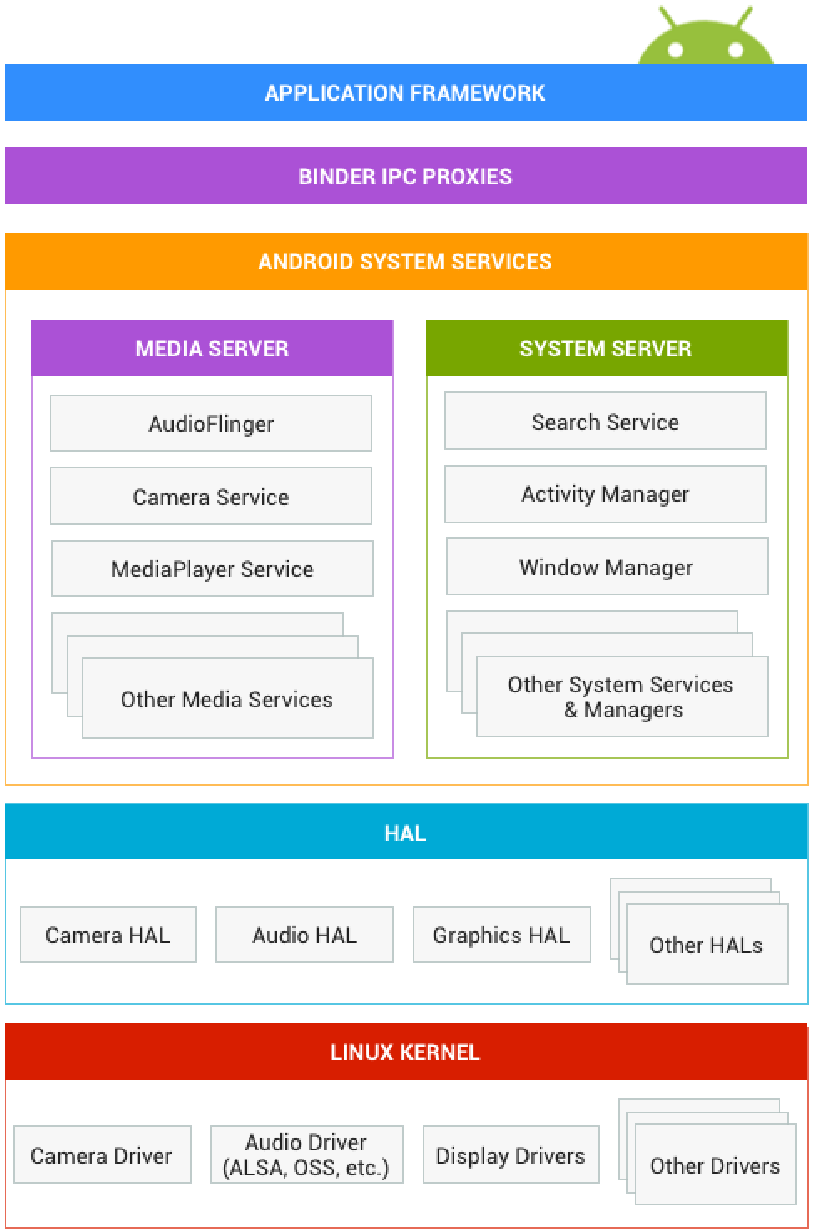


Physical Attacks: Fault Injection



T2: Mediatek x20 Board





APPLICATION FRAMEWORK

BINDER IPC PROXIES

ANDROID SYSTEM SERVICES

MEDIA SERVER

- AudioFlinger
- Camera Service
- MediaPlayer Service
- Other Media Services

SYSTEM SERVER

- Search Service
- Activity Manager
- Window Manager
- Other System Services & Managers

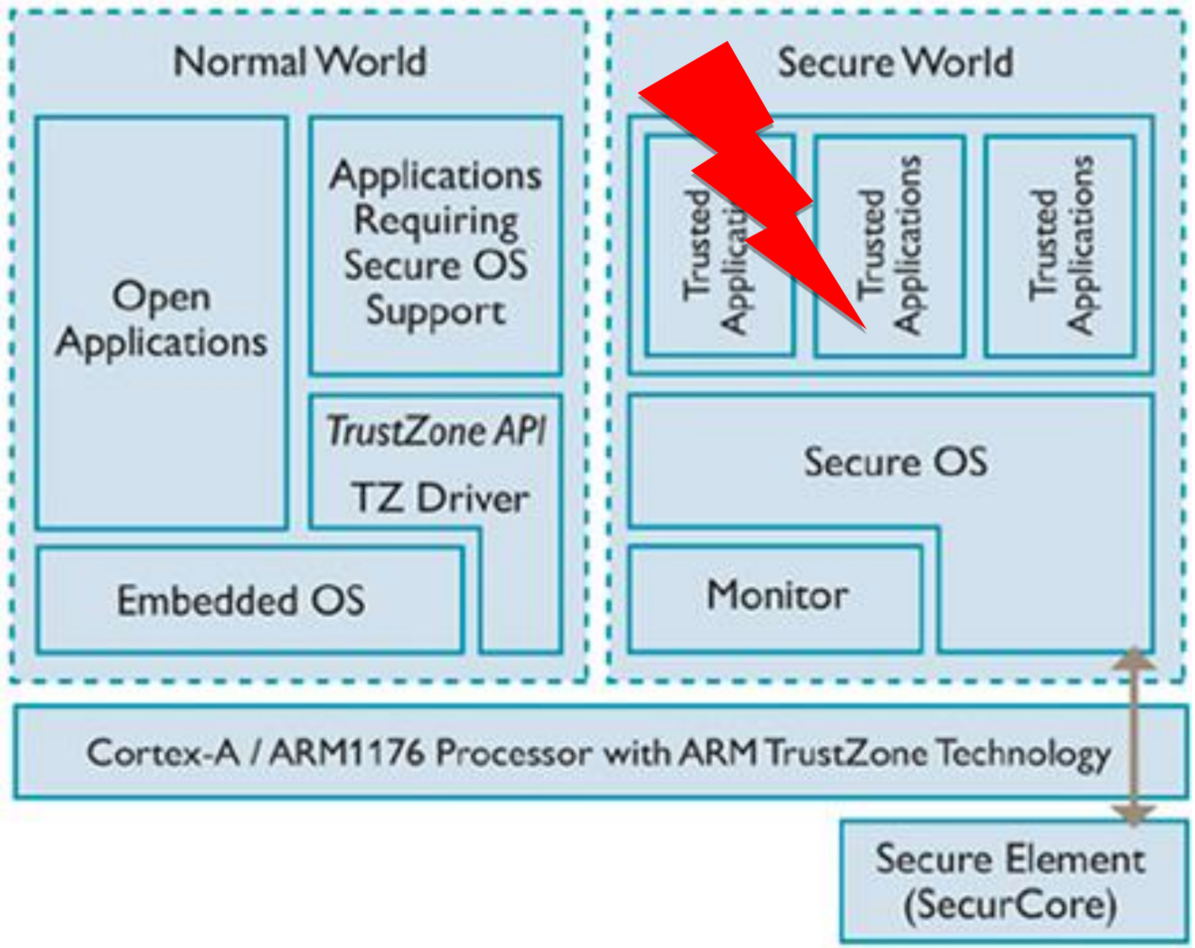
HAL

- Camera HAL
- Audio HAL
- Graphics HAL
- Other HALs

LINUX KERNEL

- Camera Driver
- Audio Driver (ALSA, OSS, etc.)
- Display Drivers
- Other Drivers

Vulnerabilities Study on Trusted Execution Environments (TEE)



Attack Techniques, Platforms

- Based on the TEE, among others, the following capabilities are provided:
  - Address Space Partitioning
  - Secure, remote attestation

- Side channel attack techniques
  - Fault attacks: Voltage, Frequency control
  - Hardware Performance Counters
  - Speculative execution modules, e.g., Branch prediction, Prefetch
    - Meltdown, Spectre, Foreshadow

- Target platforms
  - RISC-V (prototype); Intel, AMD, ARM (commercial)

Potential Topics For Grant Call

Potential Topics

1. Rapid Recovery Forensics R&D
    - Overcoming screen lock (e.g. through biometrics, fingerprint, facial) capabilities of modern mobile devices
    - Mobile data decryption for digital forensics
    - Investigation and analysis of volatile memory dump for data interpretation
    - Data recovery from damaged modern mobile devices using Universal Flash Storage (ver 2.1 and above)
    - Repair and restoration for partially corrupted or erased video data

Potential Topics

2. Evaluating Modern Processors and Hardware for Security, Privacy and Assurance
    - Data remanence of emerging memory and its implications to cold boot attacks
    - Extracting memory dump of malware protected by memory separation/isolation schemes (e.g. Software Guard eXtension (SGX), Secure Encrypted Virtualisation (SEV), System Management Mode (SMM))
    - Investigation on resistance of special status flags to semi-invasive and invasive techniques
    - Semi-invasive or invasive techniques for hardware authentication and Trojan detection in integrated circuits and embedded systems
    - Design of robust but low-cost tamper proof encasing for low-cost IoT devices to prevent physical attacks

CHFA R&D Grant Call

Funding Specifications

Duration

1. The duration of each project is up to ***3 years***.

Quantum

2. This grant will provide ***10% IRC/overheads*** above direct research costs for Singapore-based Institutes of Higher Learning and Research Institutions. The total quantum will not exceed ***$1,000,000*** (***inclusive*** of 10% IRC/Overheads).

Expenditure Guidelines

3. There will be a list of fundable and non-fundable items as determined by NRF. Please refer to the list provided in the submission package (file: *"CHFA - RnD - Grant Application Info"*)

   Please note that the list may be subjected to changes.

Eligibility

4. The grant call is open to all ***Faculty and Principal Investigators (PIs)*** from a publicly-funded Singaporean Institute of Higher Learning (IHL) or Research Institution (RI); where

Institutes of Higher Learning (IHLs):

- National University of Singapore (NUS)
- Nanyang Technological University (NTU)
- Singapore Management University (SMU)
- Singapore University of Technology and Design (SUTD)
- Singapore Institute of Technology (SIT)
- Singapore University of Social Sciences (SUSS)

Research Institutions (RIs):

- A*STAR Research Institutes/Centres/Consortia

Funding Specifications

Eligibility

5. Each proposal submission must have a Principal Investigator (PI) who is a full-time staff (or part-time with at least 75% appointment) at publicly-funded Singapore based IHL/RI.

   The PI and his research team members must not have any outstanding report(s) from other national grants.

6. Only research conducted in Singapore may be funded under the CHFA Programme.

   Researchers from Government and/or cybersecurity industry in Singapore are eligible to apply as collaborators.

   International researchers are welcomed as collaborators. Collaborators are not restricted to any category but are not eligible to receive any funding.

Funding Specifications

Eligibility

7. Proposals already funded by other funding agencies are not eligible for funding under this grant call.

Submission

8. There are ***3 templates*** in the 'Submission Package' and all must be completed; and where applicable, signed with relevant supporting documents attached.

   Submission Package
   - Info sheet
   - Annex C – Full Proposal (template)
   - Annex D – Project Budget (template)
   - Annex E – Performance Indicators (template)

   *Please note there is no Annex A & B in the submission package

9. All applications must be submitted to CHFA ***through the applicant PI's respective Research Office***. Any direct submissions will not be considered.

   All submitted proposals by the Research Offices are deemed to have its contents verified and the submission (and the Grant Call T&Cs) supported by your institute. Please ensure own internal processes are followed.

Application & Submission

Deadlines

10. All proposals must reach CHFA by 31 Jan 2020 (1200 hrs, Friday, Singapore Time). Late submissions will not be considered.

    Please abide to the ***internal submission deadline*** determined by each respective Research Offices.

Timelines

11. - Grant Call opens: **18 Nov 2019**
    - Grant Call closes: **31 Jan 2020**
    - Award announcement: **No later than 1 Apr 2020**
    - Tentative project start date: **1 May 2020**

Evaluation Criteria

Criteria & Scoring

12.
- Potential Impact & Application Significance
- Comparative Advantage
- Rigour of Approach
- Novelty
- PI Track Record
- Budget & Utilization

Evaluation Panel

13.
- PIs from CHFA
- Representatives from NRF, CSA, MINDEF, MHA
- External Reviewers

Questions?

Enquires

Please email NCR_CHFA@ntu.edu.sg.

Thank You