CIST

CIST Game: A Serious Game for Hardware Security Supply Chain

CIST Threat Model & Serious single player Game to teach threats, vulnerabilities and countermeasures to the IC Supply Chain

Stephen Hart

Basel Halak, Vladimiro Sassone

University of Southampton

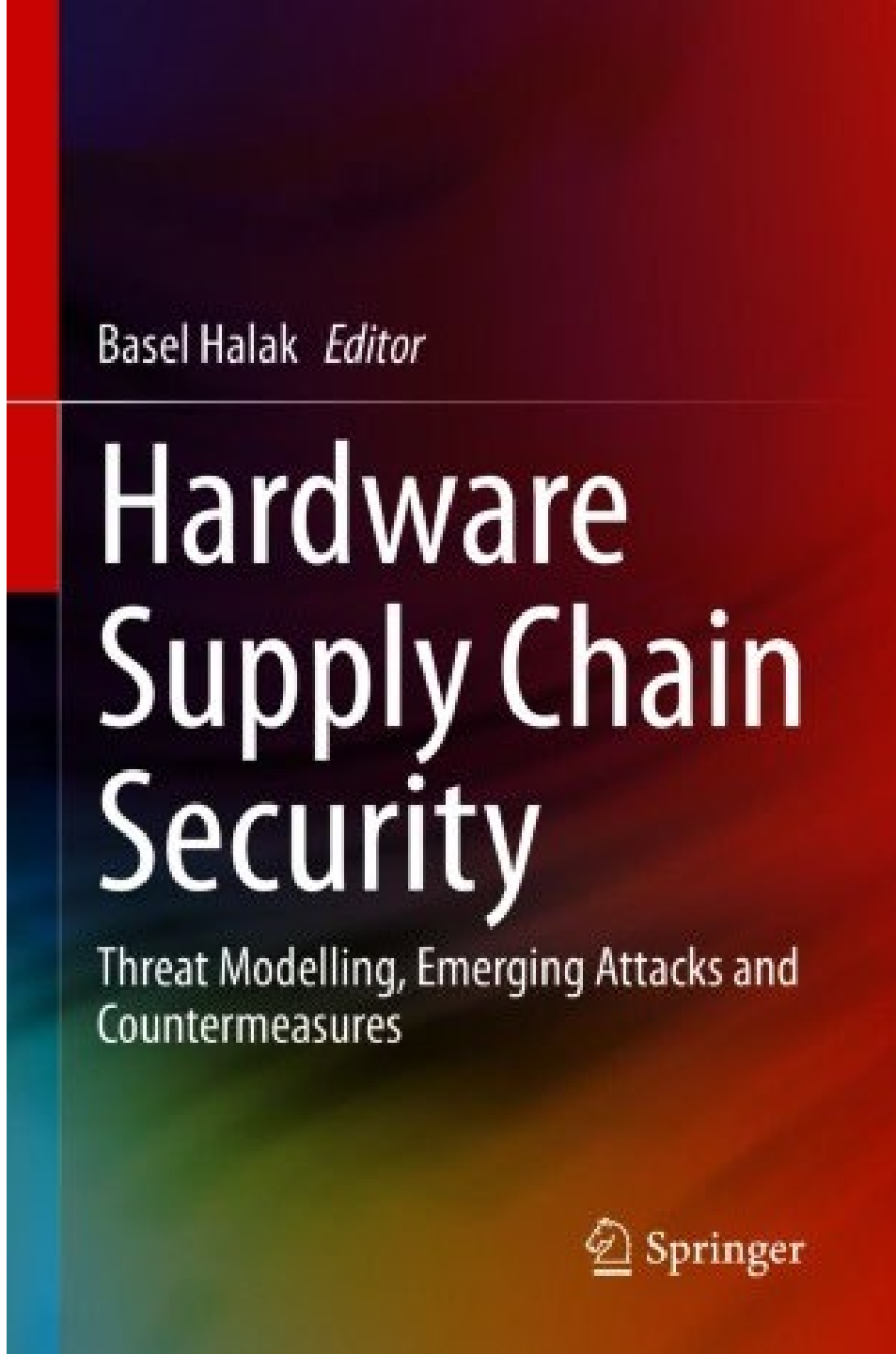
May 2021

CIST

CIST Threat Model

- Hardware-Specific Threat Modelling Approach
- Hardware-related risks throughout the life cycle of the IC from design to recycle
- Defines the desired hardware security properties, summarised as Counterfeiting, Information Leakage, Sabotage and Tampering (CIST)

https://doi.org/10.1007/978-3-030-62707-2_1



CIST Threat Model

Category	Security Property We Want?	Attack
Counterfeiting	Authenticity	Fraudulently imitating an original IC
Information Disclosure	Confidentiality	Exposing sensitive design information or secret data stored on chip
Sabotage	Availability	Deliberately damage or destroy an IC or obstruct its production
Tampering	Integrity	Maliciously change the data associated with the IC

Overview Game

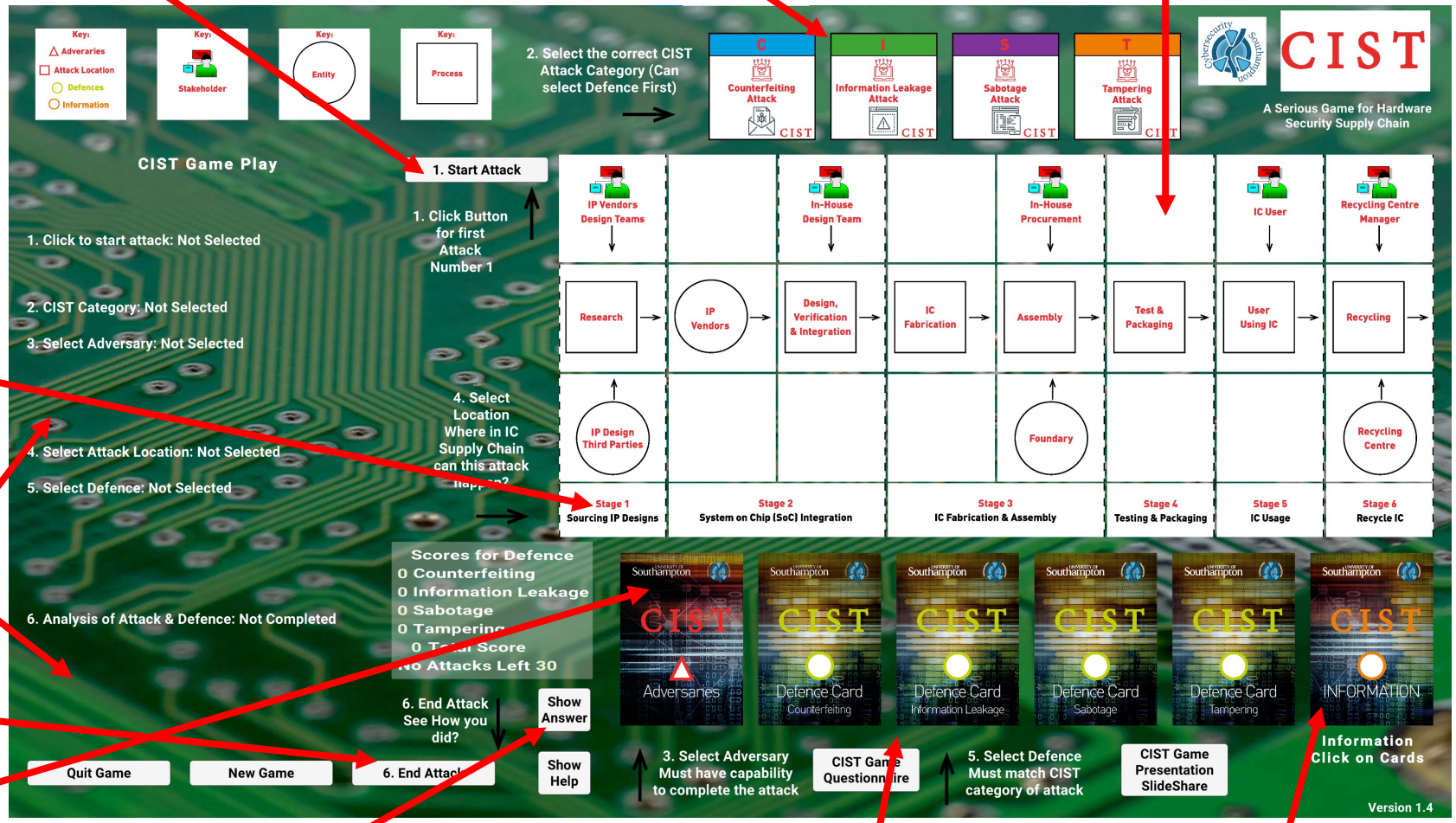
You must defend from Attacks to IC Supply Chain

1 point for successful defence (if correct) and 10 points to win

1. Click for First/Next Attack

2. Click tile for CIST Category (Can select defence first)

Game Board Six Stages in IC Supply Chain



4. Click on stage for this attack, remember could be more than on stage in IC supply chain

Displays options you selected

6. End Attack – Scores your answers

6. When complete click to check if you were correct

3. Click Adversaries to select attack who has capability for this attack

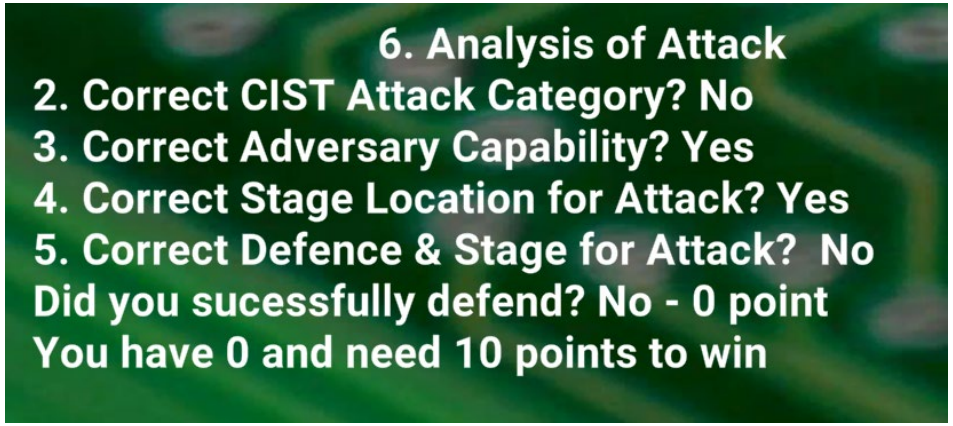
See Answer At End Attack

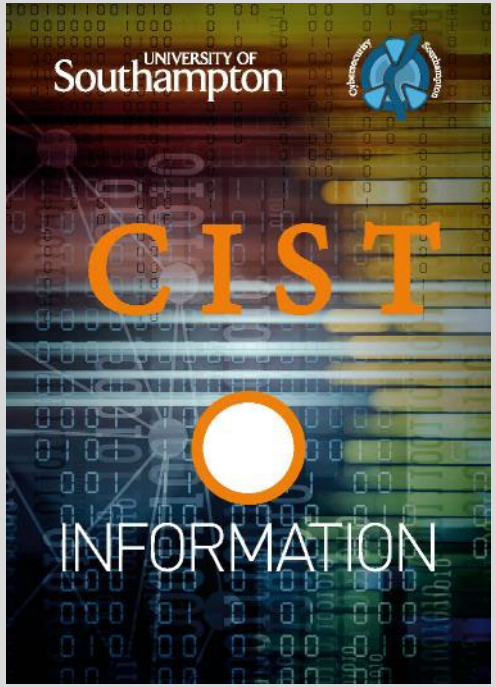
5. Click to select your Defence remember could be different depending on stage

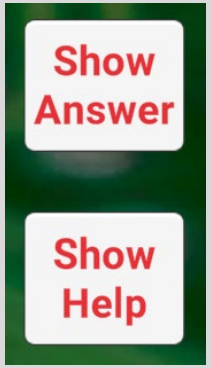
Click for Info

CIST Game Help & Feedback

- Click on Information Deck for Root of Vulnerability of current attack
- Click on any Game Board Tile for Information
- Click Show Help at any stage in the game play
- Click Show Answer after you have completed and ended your attack
- See analysis of attack after completed







CIST Gameplay

Attacks

- Attack may have more than one motive, read attack carefully

Example: Rowhammer Attack could be for Sabotage or Information Disclosure

Attack maybe possible more than one stage

Defences

- Defence could be different based on stage where attacked
- Defence can be to Protect (Stop) or Detect (Find)

Gameplay

Step 1 - Click Button 1. Start Attack

Step 2 – Select CIST category for given attack

Step 3 - Select Adversary capable of attack

Step 4 – Select stage where attack can happen

Step 5 – Select your Defence for this attack

Step 6 - Click on Button 6. End Attack

Review how you did and can now click to see answer, click button 1 to start next attack

CIST Game Key Terms – Part 1

- Rowhammer Attacks - This is a form of fault attack which exploits the fact that repeated accesses to DRAM rows can cause bits to flip in adjacent DRAM rows
- Trojan Insertion - malicious addition or modification to the existing circuit elements, in order to change the system functionality
- PUF - Physically Unclonable Functions that for a given input and conditions (challenge), provides a physically-defined "digital fingerprint" output (response)
- PUF Attack – Attacker attempts to spoof the challenge-response pairs (CRPs)
- Remarking ICs attack – Access to fabricated chips and remarking tools

CIST Game Key Terms – Part 2

- Side-channel analysis - Non-invasive experiments (e.g. measurement of power consumption, execution time or electromagnetic emissions)
- Speculative execution attacks - Measure execution times of various running processes
- Clkscrew attack (Pronounced Clock Screw) – Access to energy management hardware
- Microprobing - Physical access to the device and reverse engineering tools
- Cache timing attacks– Access to the computing devices to install a malware and measure execution times of various running processes
- Fault injection attack – Knowledge of system & can perform semi-invasive experiments

CIST Game Demo (30 Attacks)

Please play the game. Remember 1-point for successful defence.

10 points to win.

Welcome to CIST
A Serious Game for Hardware Security Supply Chain

Game Objective

The objective of the game is for you to defend against attacks on the Hardware Supply Chain. Each Attack can only be one CIST Category but may take place in more than one stage of the supply chain. Some attacks can have more than one motive, Sabotage or Information leakage, so read the Attack carefully. Also, the defence can be different depending on the stage of the Attack. If you successfully defend by getting all questions correct, you win 1 point and need 10 points to win the game. There are 30 possible attacks.

Game Play & Rules

Step 1: Click Button 1. Start Attack - To create a new attack for you to defend

Step 2: Click on the CIST category tile to select the correct category (Selected tile turns over)

Step 3: Click on the back of the Adversaries Deck, select which Adversary could attempt this type of attack

Step 4: Click on the stage where you think this attack can happen, and it may be in more than one stage (Red square appears on the Stage Tile when selected)

Step 5: Click on the back of the relevant Defence Deck to select your Defence for this attack

Step 6: Click on Button 6. End Attack - when you have selected all your defence options. Remember, Attack Category and Attack Defence Category must be the same

Help and Information

Information Click on supply chain tiles to see information also click on information deck to see information about the attack

Answer After you have clicked Button 6. to end the attack you can select Show Answer and then click Get Answer to see what the answer was for this attack

Key: Adveraries, Attack Location, Defences, Information

Key: Stakeholder

Key: Entity

Key: Process

CIST Game Play

1. Click to start attack: Not Selected

2. CIST Category: Not Selected

3. Select Adversary: Not Selected

4. Select Attack Location: Not Selected

5. Select Defence: Not Selected

6. Analysis of Attack & Defence: Not Completed

1. Start Att

1. Click Butto for first Attack Number 1

4. Selec Locatio Where in Supply Ch can this at happen

Scores for
0 Counterfei
0 Informatio
0 Sabotage
0 Tampering
0 Total Sc
No Attacks L

See How you did?

Show Answer

Quit Game | New Game | 6. End Attack | Show Help

3. Select Adversary Must have capability to complete the attack

CIST Game Questionnaire

5. Select Defence Must match CIST category of attack

CIST Game Presentation SlideShare

Recycling Centre Manager

Recycling

Recycling Centre

Stage 6 Recycle IC

Information Click on Cards

Version 1.4

CIST

Possible Questions

- Do you understand the Game Play?
- Do you agree to benefit of using Gamifcation to teach cyber security awareness and education?
- Do you think players will learn about IC Supply Chain threats, vulnerabilities and countermeasures playing the game?