SECURE-IC
THE SECURITY SCIENCE COMPANY

TELECOM Paris

Embedded France
L'EMBARQUÉ MADE IN FRANCE

IP PARIS

EMBEDDED CYBER-SECURITY: FROM REQUIREMENTS TO TECHNOLOGICAL SOLUTIONS

Prof. Sylvain Guilley

CTO & Co-founder

Université Bretagne Sud

master Cyberus

CYBERUS SUMMER SCHOOL

version: 1.5 July 2023

SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

1. EMBEDDED CYBER-SECURITY
2. THREATS
3. CERTIFICATION SCHEMES
4. PROTECTIONS, AND MAPPING TO THREATS
5. CONCLUSIONS

SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

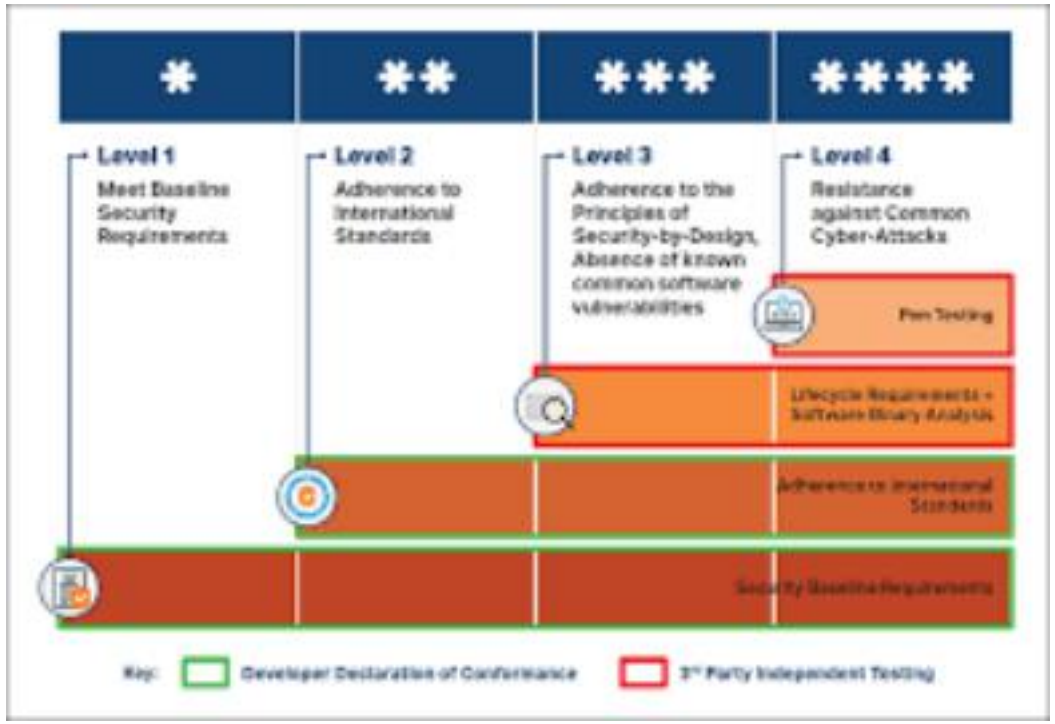
1. EMBEDDED CYBER-SECURITY
2. THREATS
3. CERTIFICATION SCHEMES
4. PROTECTIONS, AND MAPPING TO THREATS
5. CONCLUSIONS

EMBEDDED CYBER-SECURITY

Ubiquitous, from IoT end points to datacenters.

In such open and broad ecosystem, the protection of data is a major concern

Short Name	Long Name	Level of Confidence
EAL 1	Functionally tested	Lowest
EAL 2	Structurally tested	
EAL 3	Methodically tested and checked	
EAL 4	Methodically designed, tested and reviewed	Medium
EAL 5	Semiformally designed and tested	
EAL 6	Semiformally verified design and tested	
EAL 7	Formally verified design and tested	Highest



THREATS

LOCAL THREATS

REMOTE THREATS
(GPS, 3G/4G/5G, DSRC)

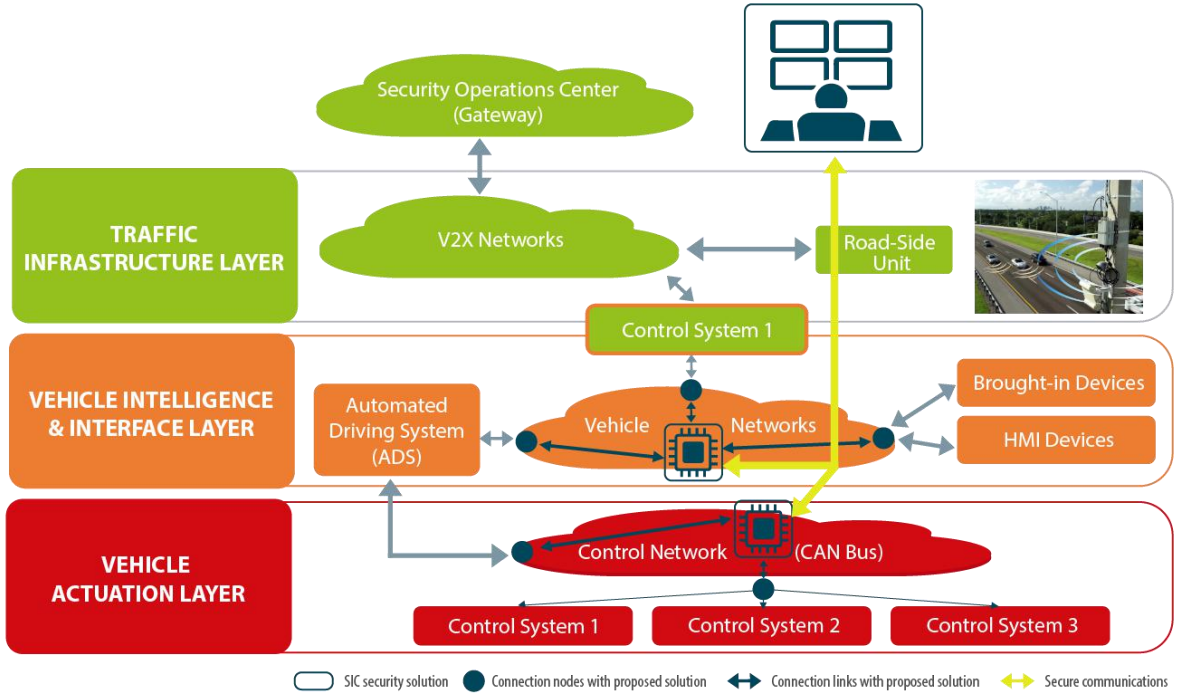
VEHICLE= TARGET

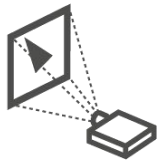
MALWARE FROM INTERNET
(corrupted PDF attached files, etc.)

JAMMER ON DRONES

INTENSE LIGHT
= BLIND CAMERAS

USB STICK
left on the ground





FAKE SCENES BY PROJECTORS

MAINTENANCE PERSONNEL
ACCESSING OBD PORT

JAMMER ON PARKING

Overview of the overall security Plug&Play solution using TR68's layer repartition

SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

1. EMBEDDED CYBER-SECURITY
2. THREATS
3. CERTIFICATION SCHEMES
4. PROTECTIONS, AND MAPPING TO THREATS
5. CONCLUSIONS

SECURE-IC
THE SECURITY SCIENCE COMPANY

THREATS

CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1274	Improper Access Control for Volatile Memory Containing Boot Code
CWE-1277	Firmware Not Updateable
CWE-1300	Improper Protection of Physical Side Channels

THREATS

Logo	Vuln. ID	Description
	CVE-2020-8694 CVE-2020-8694	With PLATYPUS, we present novel software-based power side-channel attacks on Intel server, desktop and laptop CPUs. We exploit the unprivileged access to the Intel RAPL interface exposing the processor's power consumption to infer data and extract cryptographic keys.
	CVE-2022-23823	Hertzbleed is a new family of side-channel attacks: frequency side channels. In the worst case, these attacks can allow an attacker to extract cryptographic keys from remote servers that were previously believed to be secure.
	CVE-2019-11090	They are practical. A local adversary can recover the ECDSA key from Intel fTPM in 4-20 minutes depending on the access level. We even show that these attacks can be performed remotely on fast networks, by recovering the authentication key of a virtual private network (VPN) server in 5 hours.
	CVE-2019-15809 CVE-2019-13627 CVE-2019-13627 CVE-2019-13629 CVE-2019-14318	This page describes our discovery of a group of side-channel vulnerabilities in implementations of ECDSA in programmable smart cards and cryptographic software libraries. Our attack allows for practical recovery of the long-term private key.
	CVE-2020-0549	We present CacheOut, a new speculative execution attack that is capable of leaking data from Intel CPUs across many security boundaries. SGAxe is an evolution of CacheOut, specifically targeting SGX enclaves.

THREATS

Logo	Description
CLKSCREW	In this work, we present the CLKSCREW attack, a new class of fault attacks that exploit the security-obliviousness of energy management mechanisms to break security.
PLUNDER VOLT	Modern processors [...] offer the user the opportunity to modify the frequency and voltage through priviledged software interfaces. With Plundervolt we showed that these software interfaces can be exploited to undermine the system's security. We were able to corrupt the integrity of Intel SGX on Intel Core processors by controling the voltage when executing enclave computations.
VOLT PILLAGER	Previous work such as Plundervolt has shown that software-based undervolting can induce faults into Intel SGX enclaves and break their security guarantees. However, Intel have addressed this issue with microcode updates. With VoltPillager, we show that hardware-based undervolting can achieve the same (and more) as Plundervolt, and bypass all currently available countermeasures for SGX.
VoltJockey	In this paper, we propose an innovative software-controlled hardware fault-based attack, VoltJockey, on multi-core processors that adopt dynamic voltage and frequency scaling (DVFS) techniques for energy efficiency.

SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

1. EMBEDDED CYBER-SECURITY
2. THREATS
3. CERTIFICATION SCHEMES
4. PROTECTIONS, AND MAPPING TO THREATS
5. CONCLUSIONS

COMMON CRITERIA – A ROBUST SECURITY TOOL

IT Security Challenges

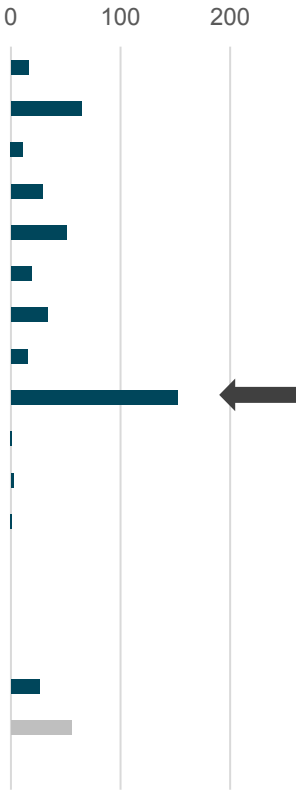
- Growing market size with different functional & therefore security functional requirements
- Growing number of IT security devices/products
- Growing number of threats and vulnerabilities
- Need to rationalize how security protections are specified and sized
- Complex mix of HW & FW

Common Criteria Solutions

- Increasing number of Protection Profiles (PPs) fine tuned to growing market needs
- Most PPs of EAL4+ assurance level for enhanced threat coverage and protection
- Evolving evaluation requirements through various revisions to capture
- Fine tuning of evaluation methods and activities
- Composition for allowing flexibility in product development

COMMON CRITERIA – PP RECOGNITION BY EAL

Protection Profiles by Assurance Level and Certification Date																											
EAL	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Basic	0	0	0	0	0	0	0	2	7	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	4	0	16
EAL1	0	0	0	0	0	0	0	5	0	1	0	2	0	0	0	4	4	6	10	3	0	12	2	9	5	1	64
EAL1+	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	4	0	3	1	0	0	0	11
EAL2	1	1	1	3	1	0	0	5	3	0	1	0	1	2	1	0	1	4	1	0	0	1	2	0	0	0	29
EAL2+	1	0	2	1	2	0	0	1	7	12	2	0	6	0	1	0	2	4	1	3	0	1	2	1	1	1	51
EAL3	2	4	1	0	0	0	0	0	0	0	2	2	1	0	0	0	1	1	0	0	4	1	0	0	0	0	19
EAL3+	0	0	0	1	3	0	2	0	0	2	9	1	1	3	0	0	1	3	0	0	2	1	2	2	0	0	33
EAL4	0	0	2	1	1	0	0	1	0	1	2	1	0	4	1	0	0	0	1	0	0	0	0	0	0	0	15
EAL4+	0	8	1	11	7	7	0	3	3	5	9	14	15	4	5	4	4	7	10	8	7	6	4	7	3	0	152
EAL5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EAL5+	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	2
EAL6	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EAL6+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL7+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Medium	0	0	0	1	0	1	1	1	4	15	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	26
None	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	5	7	11	2	4	5	4	6	0	4	0	55
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Totals:	**4**	**16**	**7**	**19**	**14**	**8**	**3**	**18**	**24**	**39**	**26**	**23**	**26**	**15**	**12**	**13**	**20**	**36**	**25**	**22**	**19**	**29**	**19**	**19**	**17**	**2**	**475**



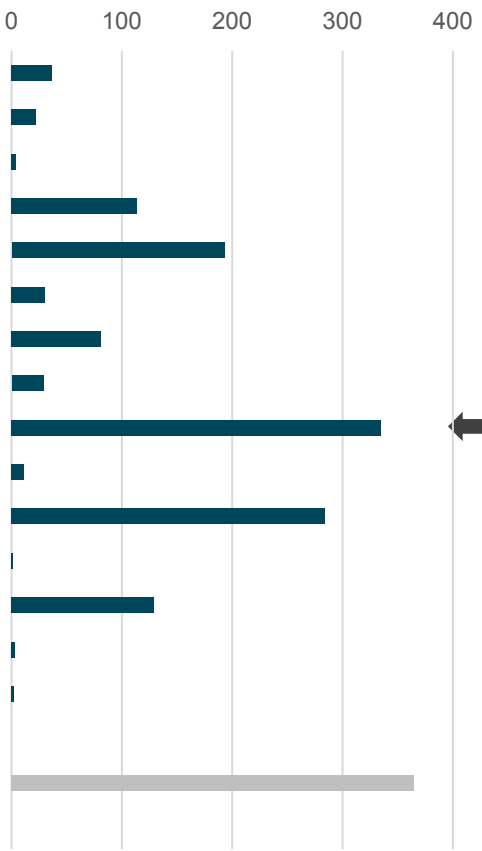
EAL4+
(Methodically designed, tested & reviewed with high degree of vulnerability and threat coverage)

Increasing cumulation of Protection Profiles

Source: https://www.commoncriteriaportal.org/pps/stats/

COMMON CRITERIA – CERTIFIED PRODUCTS

Certified Products by Assurance Level and Certification Date															
EAL	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Basic	0	0	0	0	0	0	0	0	0	0	1	5	28	3	37
EAL1	0	0	0	0	0	2	0	1	6	4	4	3	2	0	22
EAL1+	0	0	0	0	0	1	0	0	1	0	1	0	1	0	4
EAL2	0	0	0	0	1	2	2	8	12	20	17	39	12	1	114
EAL2+	0	0	0	0	0	6	4	7	32	32	42	35	30	5	193
EAL3	0	0	0	0	0	2	0	0	4	10	9	5	0	0	30
EAL3+	0	0	0	0	0	4	2	0	7	5	12	18	29	4	81
EAL4	0	0	0	0	0	0	3	0	7	8	5	3	3	0	29
EAL4+	1	0	0	1	1	7	11	12	34	48	63	69	74	14	335
EAL5	0	0	0	0	0	0	1	0	3	1	2	0	4	0	11
EAL5+	0	0	0	0	2	5	5	18	38	48	69	48	43	8	284
EAL6	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
EAL6+	0	0	0	1	0	1	0	0	15	21	20	31	33	7	129
EAL7	0	0	0	0	0	0	0	0	1	0	1	0	1	0	3
EAL7+	0	0	0	0	0	0	0	0	1	0	0	1	0	0	2
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	25	61	48	115	90	26	365
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Totals:	**1**	**0**	**0**	**2**	**4**	**30**	**28**	**46**	**186**	**258**	**294**	**372**	**351**	**68**	**1640**



EAL4+
(Most certified products under EAL)

Increasing number of certified products

Source: https://www.commoncriteriaportal.org/pps/stats/

COMMON CRITERIA V4

§ Structural differences between V3 and V4 (new, pub. 2022) of the CC

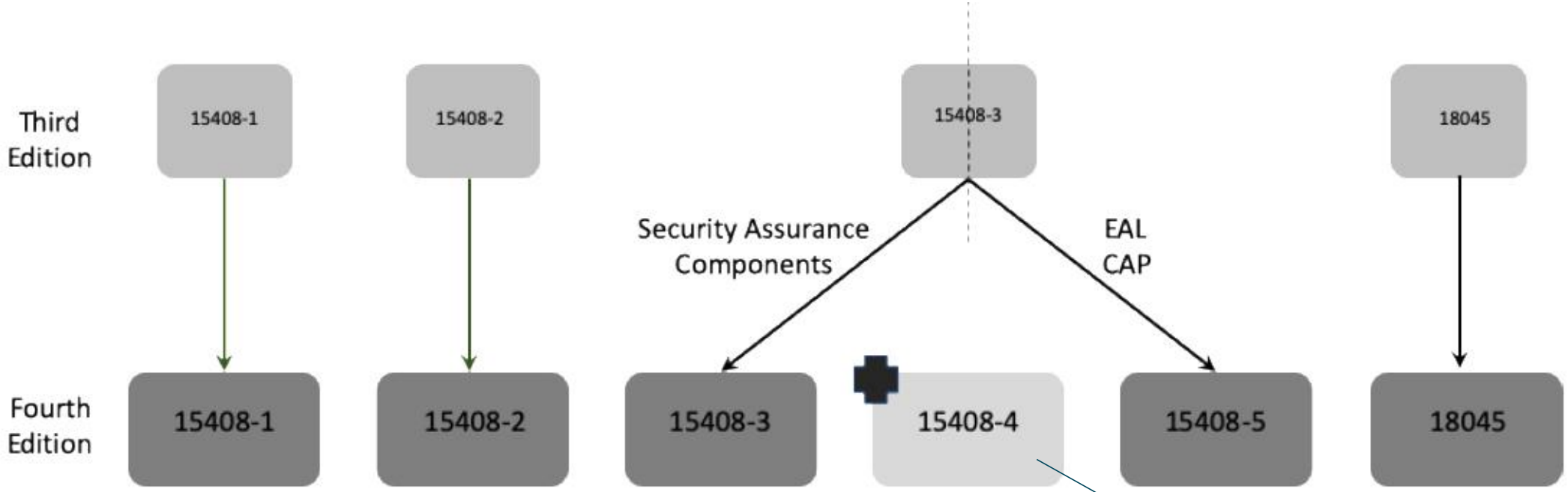
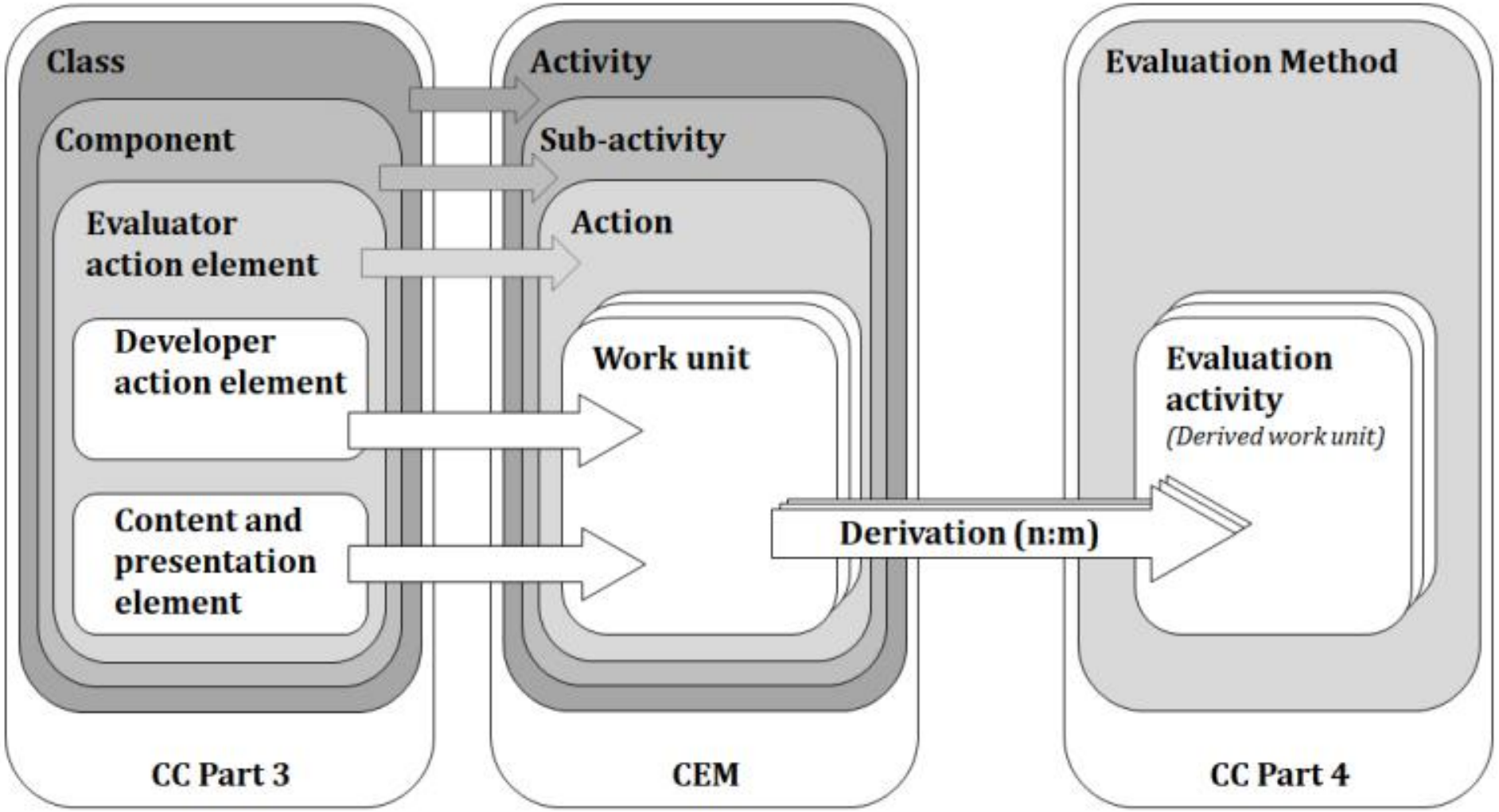


Figure 1 — Mapping between the third and fourth editions

Standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities

COMMON CRITERIA PART 4



COMMON CRITERIA V4

§ Evaluation differences between V3 and V4 (new, pub. 2022) of the CC

Benefits:

All the tests are known beforehand

No need for tailored test plan during evaluation

Even if relevant attack scenarios that were not considered by the risk owner in the PP are not tested

New approach (reduce evaluator efforts)

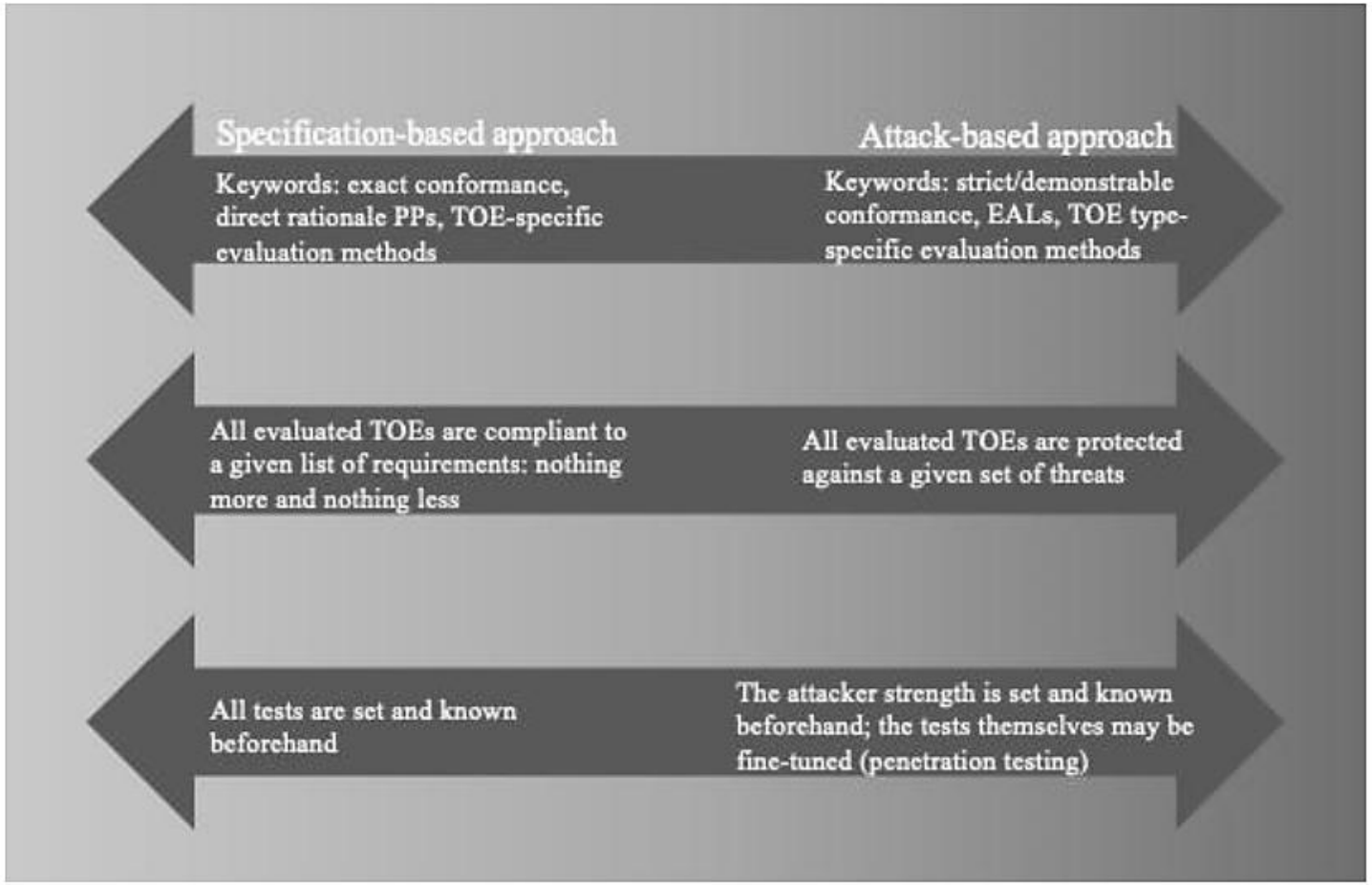


Figure 2 — Specification-based and attack-based approaches

Benefits:

Investigative approach

Follows EALs strictly

Existing approach

COMMON CRITERIA: A QUANTITATIVE MEASUREMENT

§ Common Criteria offer assurance through vetted practices:

- Documentary:
  - ASE: SECURITY TARGET EVALUATION
  - ADV: DEVELOPMENT
  - AGD: GUIDANCE DOCUMENTS
  - ALC: LIFE-CYCLE SUPPORT
- Experimental:
  - ATE: TESTS
  - AVA: VULNERABILITY ASSESSMENT

§ It is usually admitted that **AVA** is ruling the pratical security level:

- Quantitative notion of **EAL**
- Levels **1 to 7**

SECURITY LEVELS

Security is quantitative

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
> four months[56]	6	10
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical	9	*
Not practical	*	*
Access to the TOE (1)		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (2)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples / Samples with known secrets		
Public/Not required	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA
Not practical (Samples with known secrets only)	*	NA

Source: EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, May 2021, V1.1.1.

SECURE-IC
THE SECURITY SCIENCE COMPANY

SECURITY LEVELS

Security is quantitative

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

Source: CEM, v3

SECURITY LEVELS

Security is quantitative

Table B.3 — Rating of vulnerabilities and TOE resistance

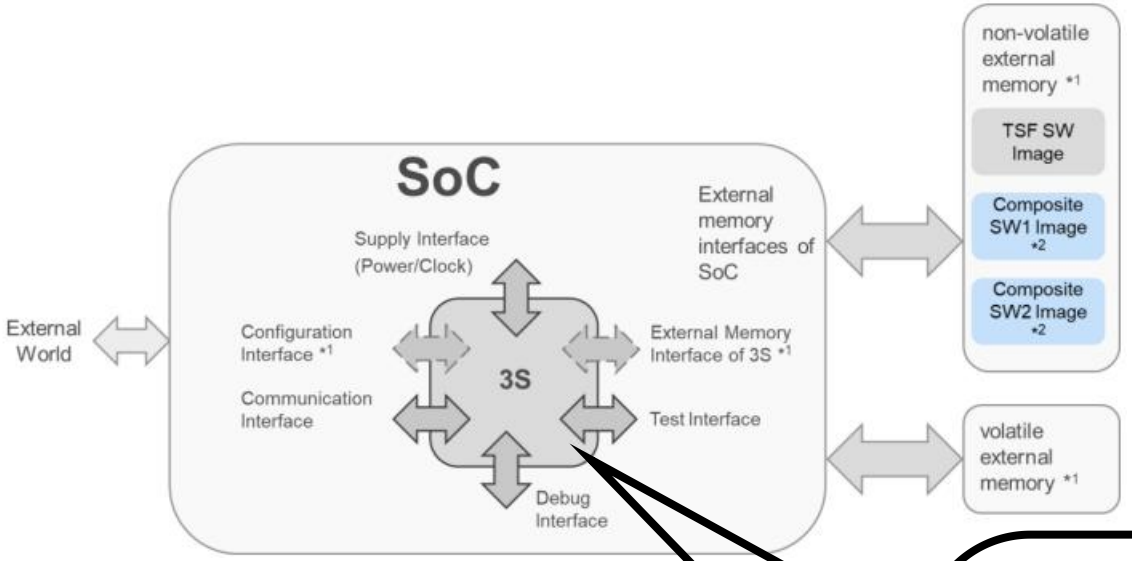
Values	Attack potential required to exploit scenario:	Meets assurance components:	Failure of components:
0-9	Basic	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Table B.2 — Calculation of attack potential

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3[a]
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**[b]
Equipment	

Source: CEM:2022

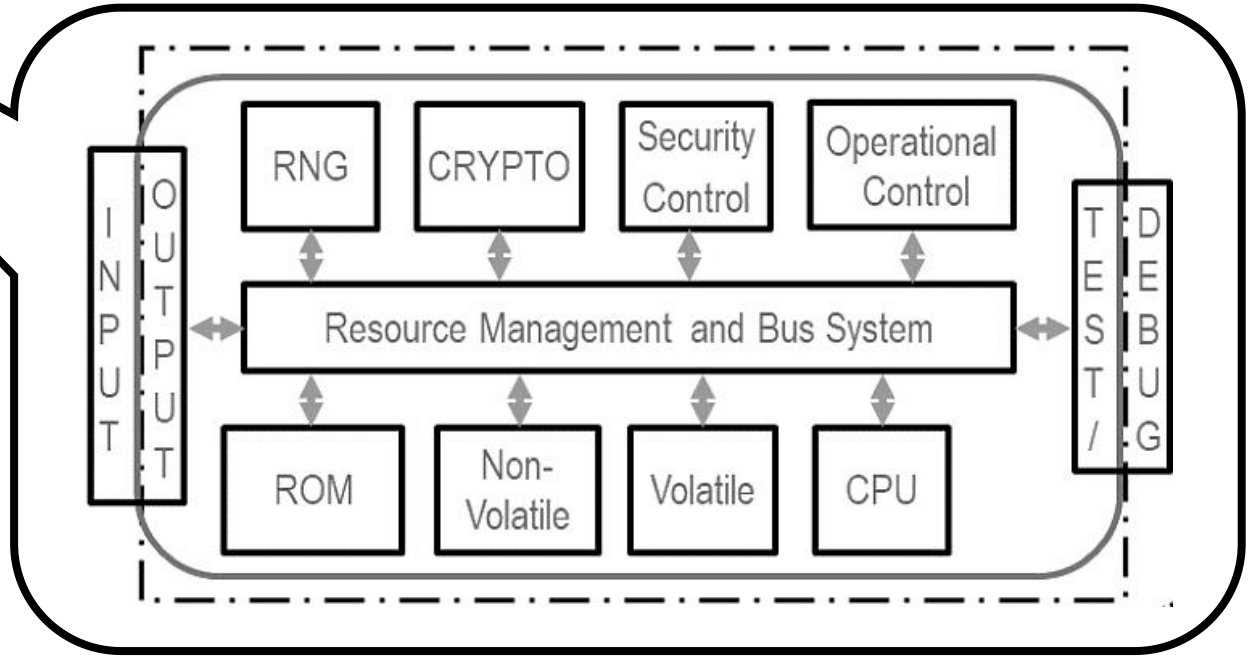
SECURITY SUB-SYSTEM (3S)



Applications:

- *User authentication and password storage*
- *Content protection*
- *Payment*
- *Subscriber Identity Module (SIM)*
- *Storage and management of digital identities*
- *Secure key storage*
- *Root of Trust (RoT)*
- *Storage of sensitive user data (e.g., healthcare records)*

Configuration interface and External Memory Interface are optional



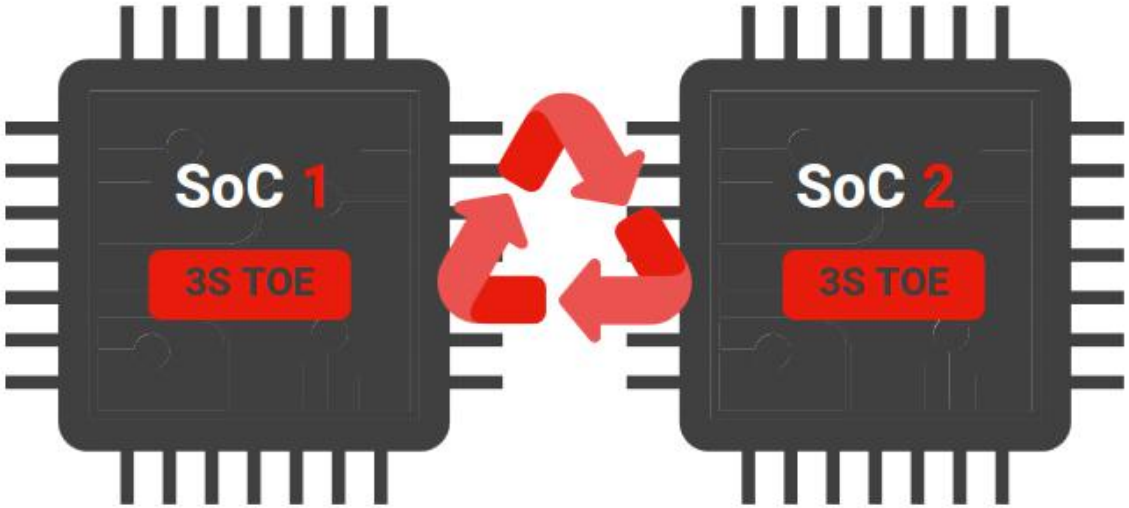
Multiple use-cases
Multiple markets

LEFT-SHIFT

Pre-certification:

§ 3S industry
- IPs: pieces of technology aiming at being reused

§ Consequence:
- Certification per product
- => Instead per project



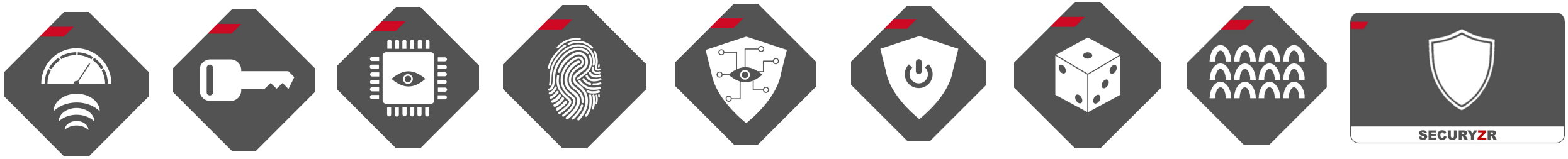
Re-use of a certified 3S TOE from one SoC to another one

Source: EUCA 2022
Rachel Menda-Shabat, Winbond, Subgroup Chair
Jean-Philippe Galvan, Qualcomm, ITSC Co-Chair

DEFENSE IN DEPTH & IN BREADTH

§ Illustration of the defense vs cost tradeoff

Countermeasure: Depth	Breadth
Digital Sensor	Number of instances (1~128)
Active Shield	One or Two (orthogonal) meshes
Error Handler	Decision rules or SVM
Side-Channel Analysis Protection using Masking	Security Order
Error-Detection Schemes	Number of detected errors
CFI: Cyber Escort Unit	Inter- or intra-procedural coverage
...	...



SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

1. EMBEDDED CYBER-SECURITY
2. THREATS
3. CERTIFICATION SCHEMES
4. PROTECTIONS, AND MAPPING TO THREATS
5. CONCLUSIONS

EXAMPLE #1: AN ATTACK ON THE OTP

CVE-2019-17391 Detail

Description

An issue was discovered in the Espressif ESP32 mask ROM code 2016-06-08 0 through 2. Lack of anti-glitch mitigations in the first stage bootloader of the ESP32 chip allows an attacker (with physical access to the device) to read the contents of read-protected eFuses, such as flash encryption and secure boot keys, by injecting a glitch into the power supply of the chip shortly after reset.

QUICK INFO

CVE Dictionary Entry:
CVE-2019-17391
NVD Published Date:
11/14/2019
NVD Last Modified:
08/24/2020
Source:
MITRE

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 4.6 MEDIUM **Vector:** CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

ESPRESSIF Products Solutions Support Ecosystem Company Join Us Contact Us 中文 Subscribe

Products > SoCs > ESP32 >

Overview Products Buy Now

Robust Design

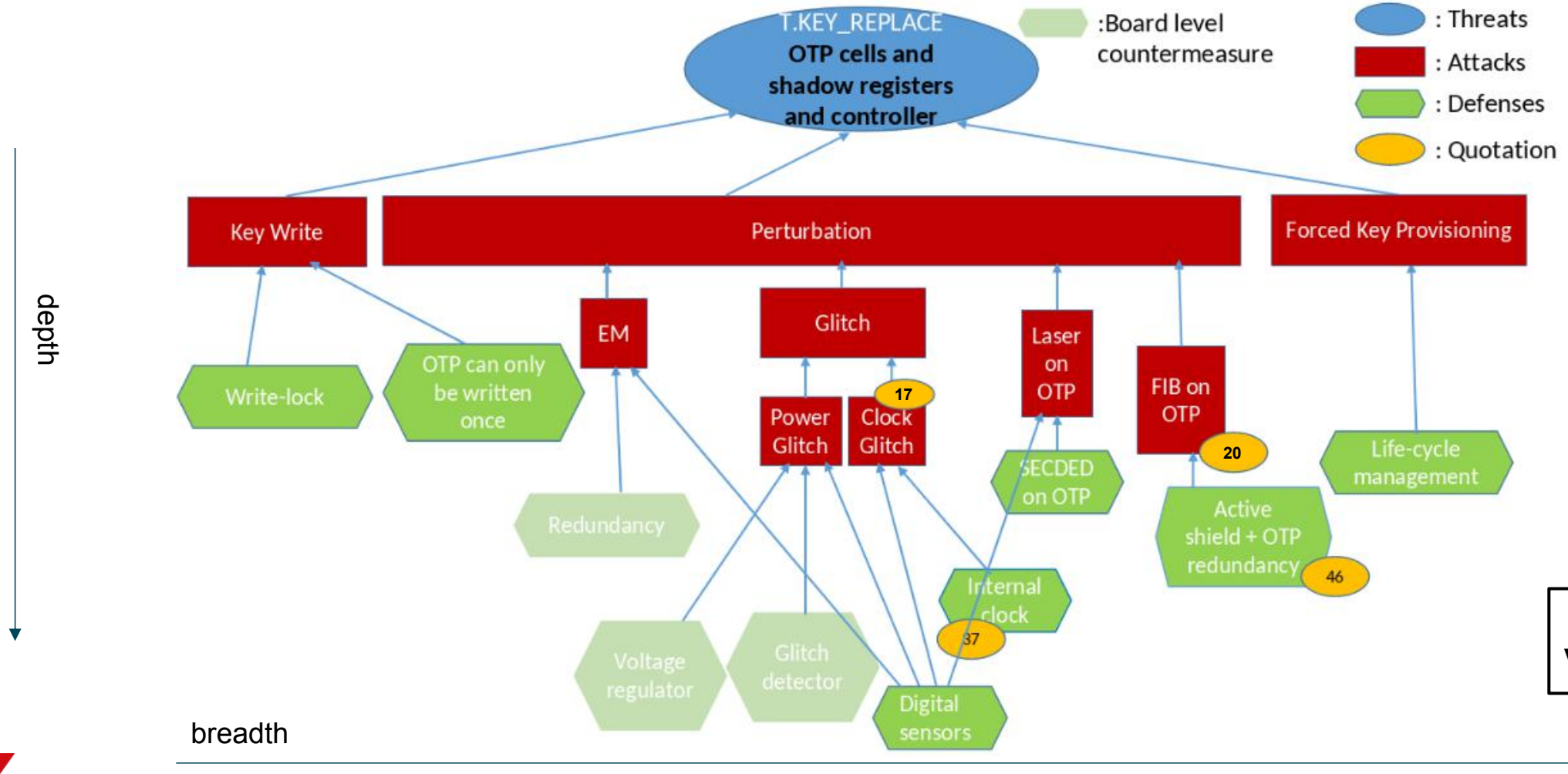
ESP32 is capable of functioning reliably in industrial environments, with an operating temperature ranging from –40°C to +125°C. Powered by advanced calibration circuitries, ESP32 can dynamically remove external circuit imperfections and adapt to changes in external conditions.

Ultra-Low Power Consumption

Engineered for mobile devices, wearable electronics and IoT applications, ESP32 achieves ultra-low power consumption with a combination of several types of proprietary software. ESP32 also includes state-of-the-art features, such as fine-grained clock gating, various power modes and dynamic power scaling.

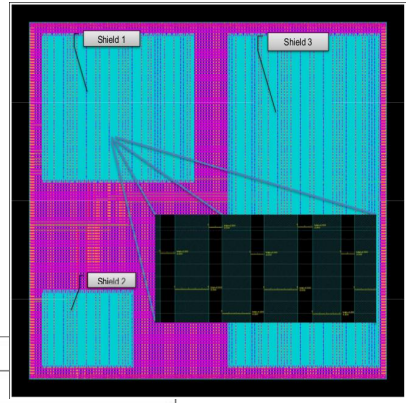
ATTACK-PROTECTION TREE

§ Example of **T.KEY_REPLACE** threat from **PP0114** C2C V2X EAL4+ on **OTP**



AVA_VAN.4
Values 20-24

QUOTATION OF ATTACKS (PP 0117)



§ Active shield: yes or no? Analysis based on **T.Phys-Probing** threat

Goal of attack	Prepare chip such that we can either read out sensitive signals or edit the chip to disable countermeasures
Assumption	Chip must be working after the experimental preparation

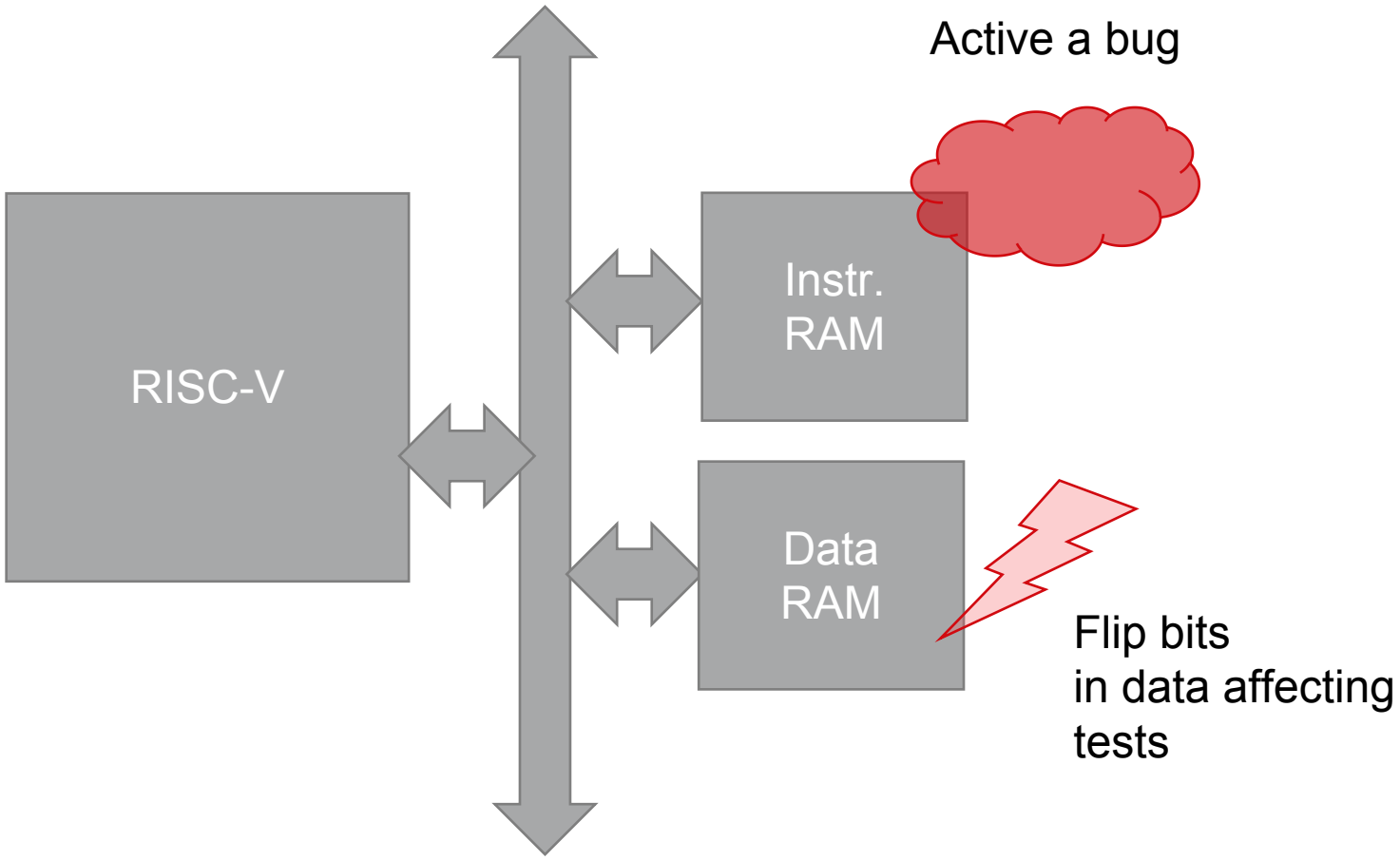
With increasing order of complexity in performing the attack –>

	A. Front side wo AS	B. Front side wo AS w Sensitive signals are routed in lower layers (not easily accessible)	C. Front side w AS	D. Back side wo AS	Comments/Remarks
Elapsed Time	7	10	13	15	Based on works of Christopher Tarnovsky BlackHat 2010 with <220nm, 4+ metals, which is old
Expertise	3	6	8	8	
Knowledge of TOE	0	11	11	11	
Window of Opportunity	4	10	10	10	
Equipment	7	7	9	9	
	21	**44**	**51**	**53**	
	AVA_VAN.4	AVA_VAN.5	AVA_VAN.5	AVA_VAN.5	

	Steps: (repeated till success)	**Comments**
0	Identification of sensitive signals	especially challenging for the cases B and D
1	Chemical preparation to access metal	very challenging for D because the substrate is thick and drilling must stop precisely at the active area (not visible)
2	Open and rewire the shield (if any)	very error prone because the shield is dense
3	Identify any access to the sensitive wire (easier wo AS or if the sensitive signal is close to chip surface)	challenging for B
4	Passive or active probing attack steps	more complex in case of D

AVA_VAN.5
Values =>25

EXAMPLE #2: AN ATTACK ON THE CPU



EXAMPLE #2: AN ATTACK ON THE CPU COUNTERMEASURE

1. Dual Core Lock Step

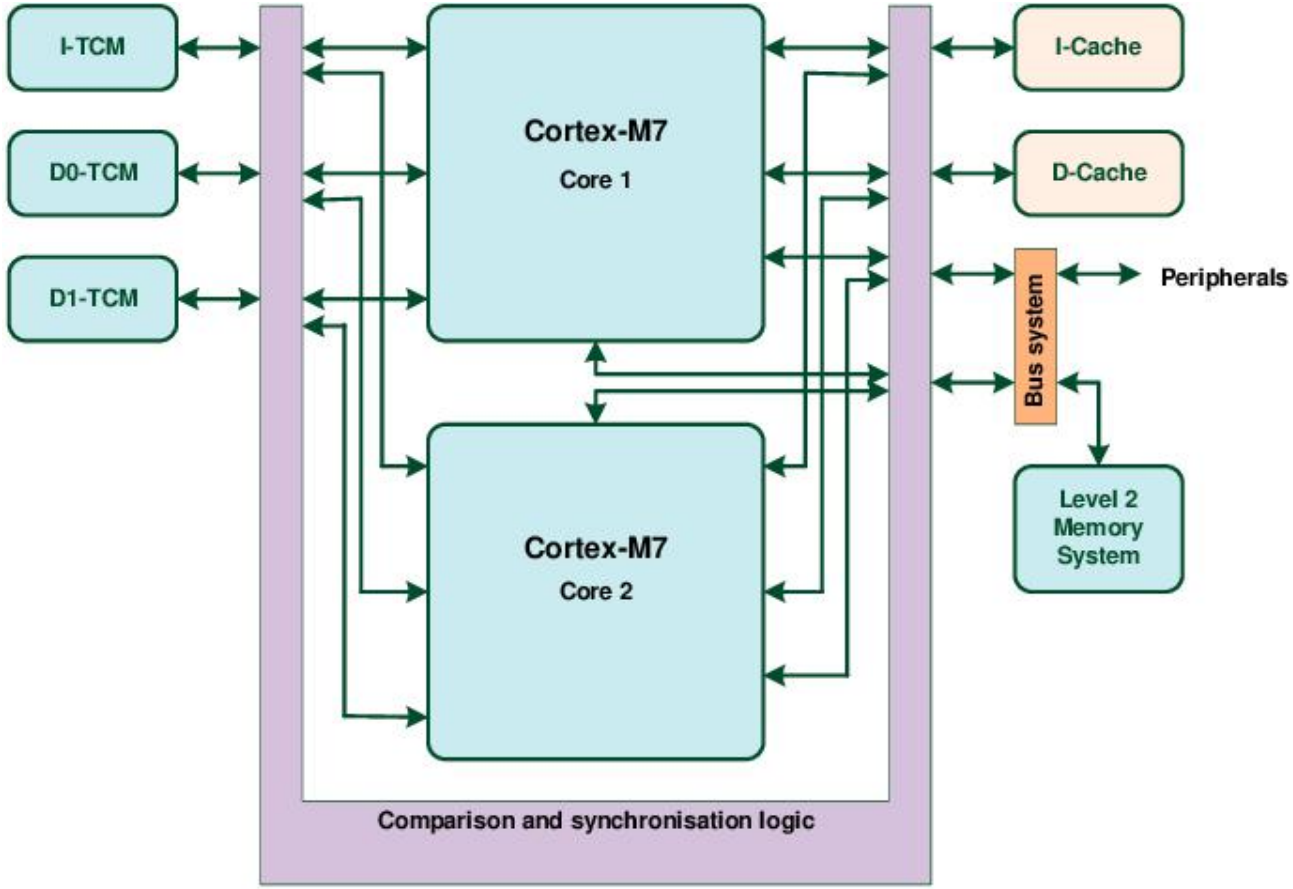
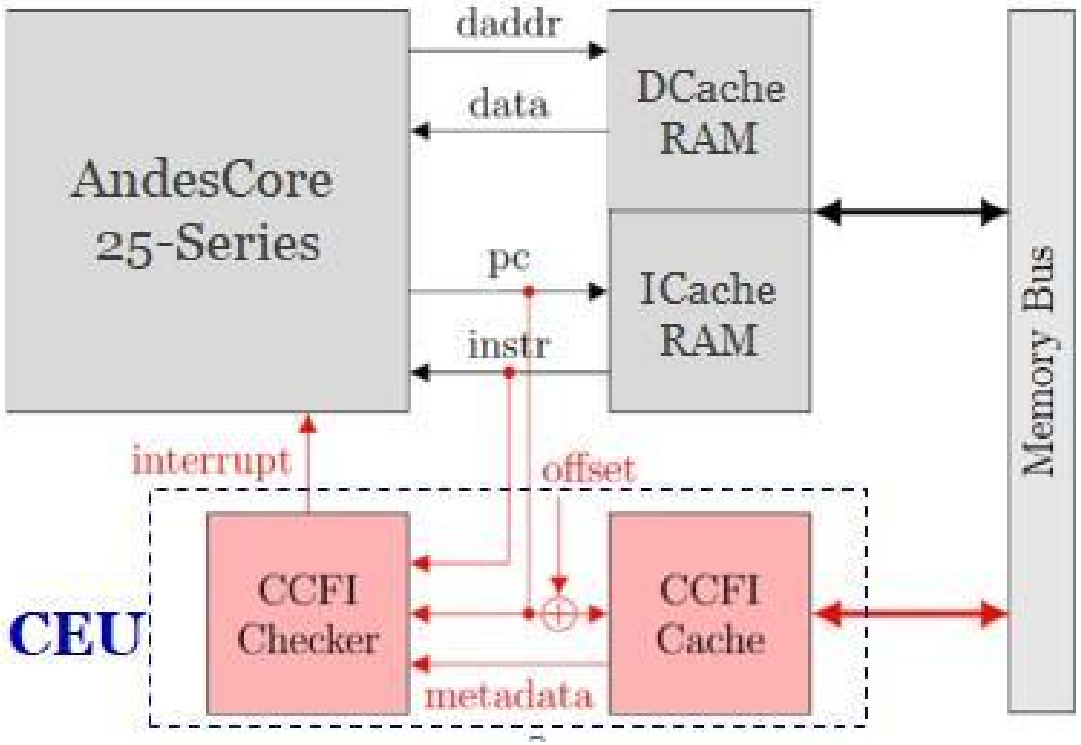


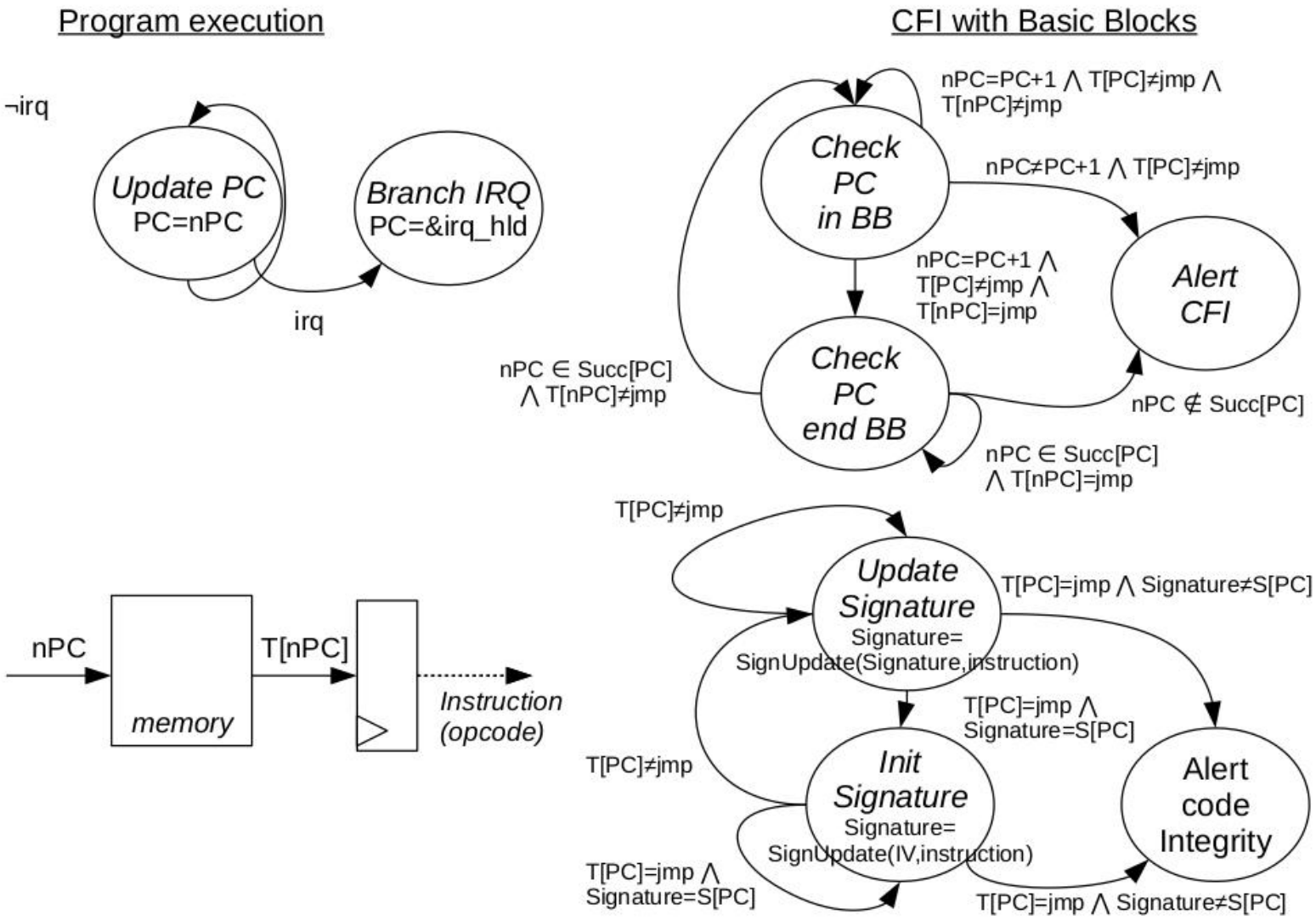
Fig. 3. Dual-Core Lock-Step configuration in the Cortex-M7 processor

2. Cyber Escort Unit

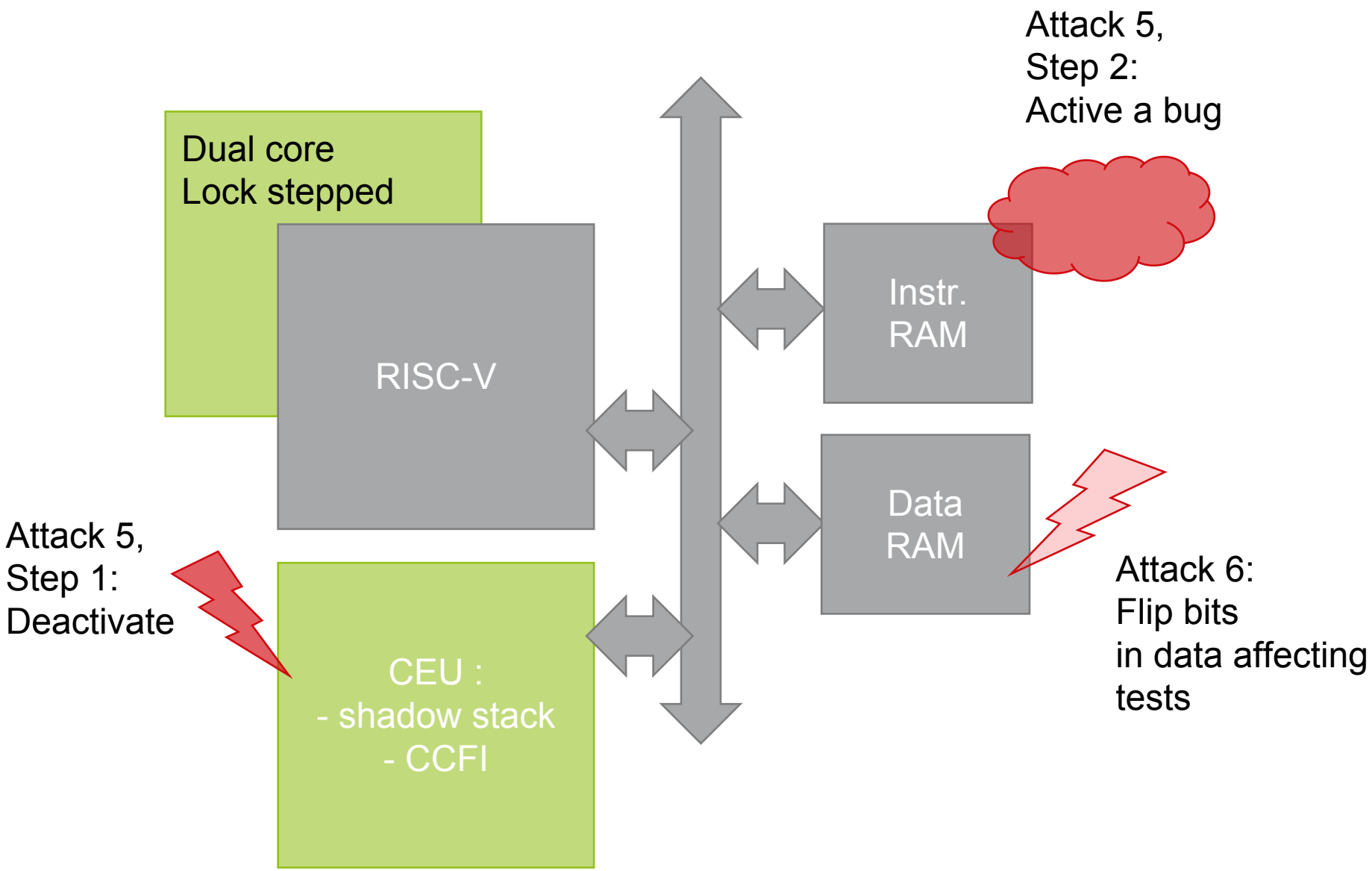


Offset by two clock periods to avoid «same effect»

EXAMPLE #2: AN ATTACK ON THE CPU COUNTERMEASURE



EXAMPLE #2: AN ATTACK ON THE CPU



EXAMPLE #2: AN ATTACK ON THE CPU

§ Threats: PP 0084

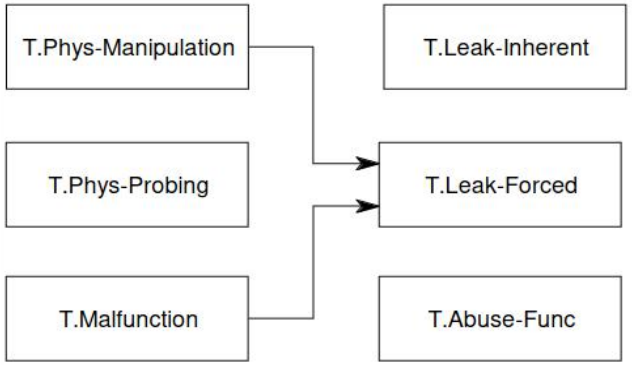


Figure 6: Standard Threats

§ Coverage

Coverage	Nature	Location	Dual Core LS	Shadow Stack	Code verification	Control Flow Integrity	Immutable	BIST
Perturbation	Physical	CPU	x			x		
		Instr. RAM			x	x		
		Data RAM						
	Cyber/ Logical	CPU					x	
		Instr. RAM			x	x		
		Data RAM		x (addresses)				
Defect	Physical	RAMs						x
	Cyber/Lo	Inst. RAM				x		

Attack #6

Attack #5

EXAMPLE #2: AN ATTACK ON THE CPU

- **[Attack 5]** Physical faults are double covered by CEU and lock step. Protection against bugs are “only” covered by CEU. Hence the attack 5 consists in disabling CEU and then to exploit a bug. The only way to disable CEU is to which it off by an accurate attack, such as FIB circuit edition or laser attack on the DFF that enables/disables it. Such attack requires a critical knwoledge of the position of elements to disable the CEU protection, but the disablement can be done whenever. Then, finding the bug can take some time, but it is eventually expected that some bug will be found, and it “suffices” for the attacker to identify inputs to activate it.
- **[Attack 6]** Faults on data leading to a security breach undetected by CEU (i.e., since the control flow will be respected) can allow to achieve an adversarial goal. But such attack has double complexity in terms of identification and in exploitation. The identification requires a deep understanding the of the code, most probably resulting in a decompilation and a mean to run the code as if it is on the target (a complete simulation equivalent, which is basically that used to design the code). Hence a leak of critical information. Then, the attacker shall devise where, when, and what value to give to the faulty variable. In terms of exploitation, the variable will spawn in memory only dynamically, hence the local and timely and accurate fault shall be triggered. This entails a multiple expertise.

	Attack 5	Attack 6	Comments/Remarks
Elapsed Time	4	7	
Expertise	3	8	
Knowledge of TOE	11	11	Code is BlackBox (attack should be accurate in space and time) --> identification and exploitation is difficult
Window of Opportunity	4	4	
Equipment	7	9	Example FIB, etc. advanced equipment
	29	39	
Scope of attack	AVA_VAN.5	AVA_VAN.5	Using CEMv3.1R5

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Table 13: Rating of vulnerabilites and TOE resistance

SECURE-IC
THE SECURITY SCIENCE COMPANY

AGENDA

1. EMBEDDED CYBER-SECURITY
2. THREATS
3. CERTIFICATION SCHEMES
4. PROTECTIONS, AND MAPPING TO THREATS
5. CONCLUSIONS

CONCLUSIONS

- Common Criteria can be applied upfront
- They allow to quantify a security level, starting from the specifications
- Such trends are encouraged by 3S PP
- Benefits: reuse of pre-certified components
- CC is not just a certification but also a framework/tool to select the depth and breadth of security IPs

SECURE-IC
THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
TAIWAN	sales-TAIWAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

FOLLOW US ON SOCIAL MEDIA