In Hardware We Trust
Enriching the World with Hardware Security

JV Rajendran

Texas A&M University

Hack@DAC2018: Overview

- Deep dive into hardware bugs and detection techniques

Hack@DAC2018: Overview

- Deep dive into hardware bugs and detection techniques

- A RISC-V SoC testbed with injected bugs constructed in collaboration with Intel hardware security professionals

- 54 teams from industry & academia participated

Hack@DAC2018: Overview

- Deep dive into hardware bugs and detection techniques
- A RISC-V SoC testbed with injected bugs constructed in collaboration with Intel hardware security professionals
- 54 teams from industry & academia participated
- Own investigation of the effectiveness of approaches used

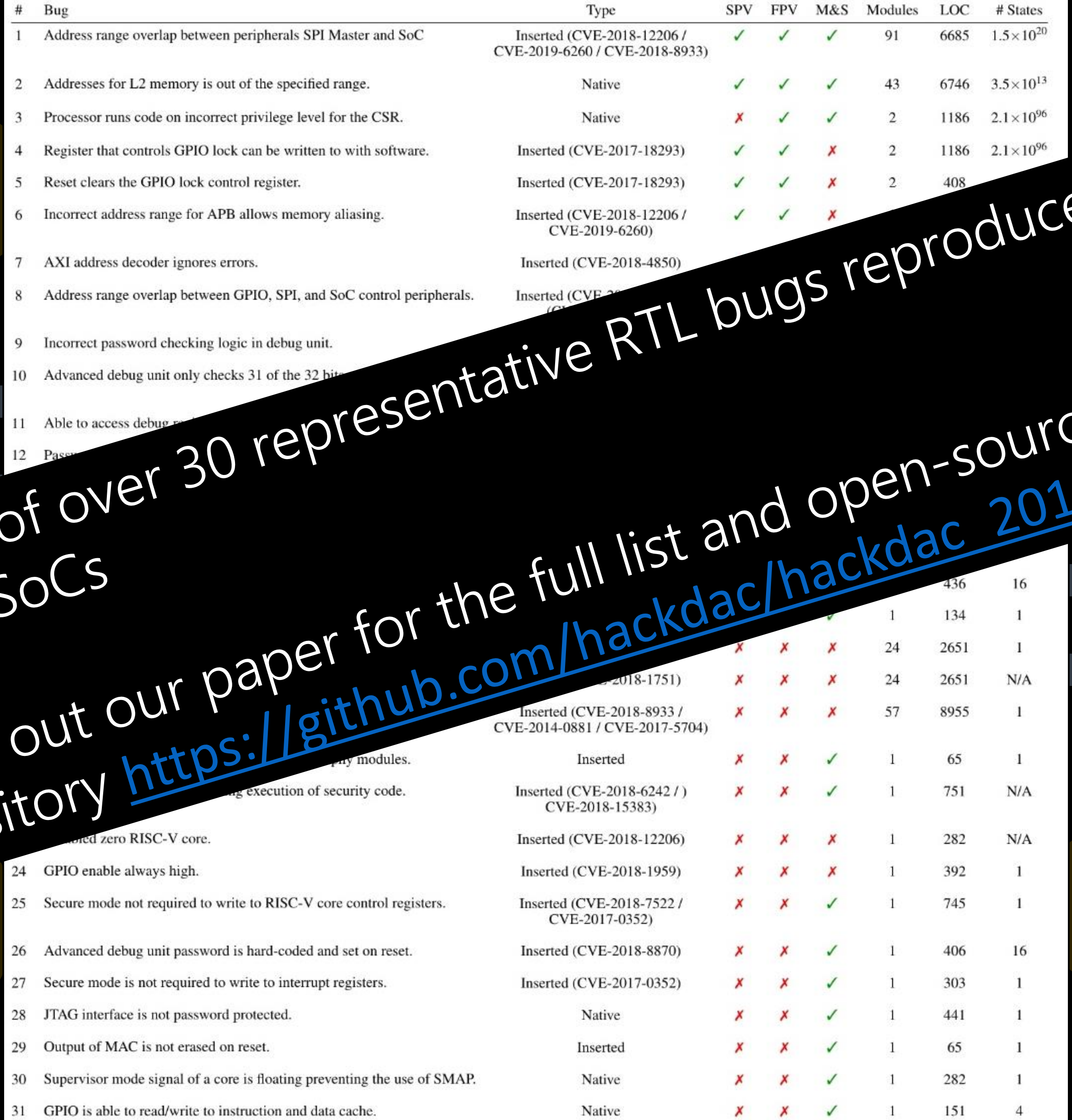
Systematic RTL Bugs Construction

denial-of-service

sensitive
mation leakage

privilege escalation

software
exploitability



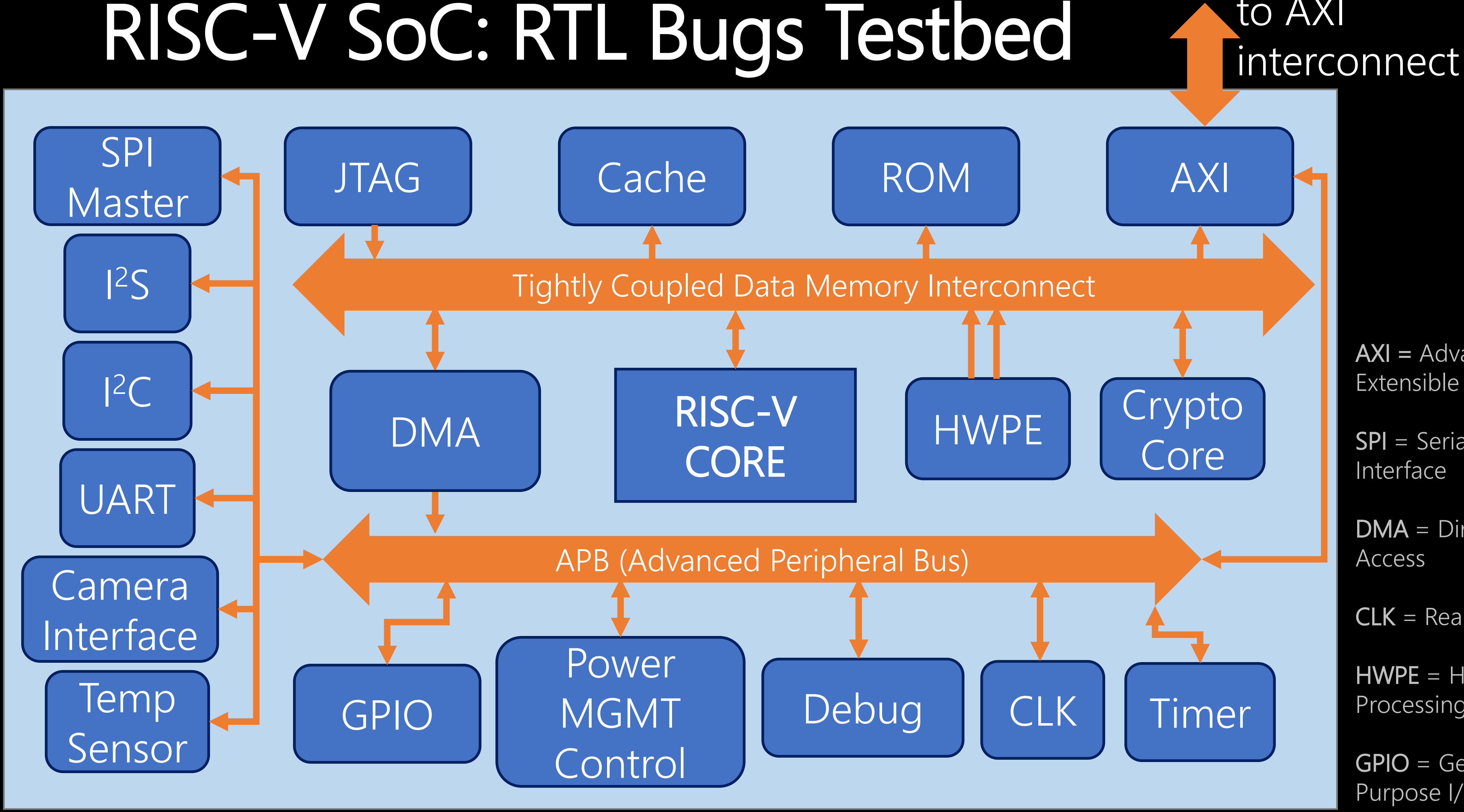
#	Bug	Type	SPV	FPV	M&S	Modules	LOC	# States
1	Address range overlap between peripherals SPI Master and SoC	Inserted (CVE-2018-12206 / CVE-2019-6260 / CVE-2018-8933)	✓	✓	✓	91	6685	1.5×10^{20}
2	Addresses for L2 memory is out of the specified range.	Native	✓	✓	✓	43	6746	3.5×10^{13}
3	Processor runs code on incorrect privilege level for the CSR.	Native	✗	✓	✓	2	1186	2.1×10^{96}
4	Register that controls GPIO lock can be written to with software.	Inserted (CVE-2017-18293)	✓	✓	✗	2	1186	2.1×10^{96}
5	Reset clears the GPIO lock control register.	Inserted (CVE-2017-18293)	✓	✓	✗	2	408	
6	Incorrect address range for APB allows memory aliasing.	Inserted (CVE-2018-12206 / CVE-2019-6260)	✓	✓	✗			
7	AXI address decoder ignores errors.	Inserted (CVE-2018-4850)						
8	Address range overlap between GPIO, SPI, and SoC control peripherals.	Inserted (CVE-20						
9	Incorrect password checking logic in debug unit.							
10	Advanced debug unit only checks 31 of the 32 bit							
11	Able to access debug r							
12	Pass							
							436	16
					✓	1	134	1
			✗	✗	✗	24	2651	1
		2018-1751)	✗	✗	✗	24	2651	N/A
		Inserted (CVE-2018-8933 / CVE-2014-0881 / CVE-2017-5704)	✗	✗	✗	57	8955	1
	ply modules.	Inserted	✗	✗	✓	1	65	1
	g execution of security code.	Inserted (CVE-2018-6242 /) CVE-2018-15383)	✗	✗	✓	1	751	N/A
	bled zero RISC-V core.	Inserted (CVE-2018-12206)	✗	✗	✗	1	282	N/A
24	GPIO enable always high.	Inserted (CVE-2018-1959)	✗	✗	✗	1	392	1
25	Secure mode not required to write to RISC-V core control registers.	Inserted (CVE-2018-7522 / CVE-2017-0352)	✗	✗	✓	1	745	1
26	Advanced debug unit password is hard-coded and set on reset.	Inserted (CVE-2018-8870)	✗	✗	✓	1	406	16
27	Secure mode is not required to write to interrupt registers.	Inserted (CVE-2017-0352)	✗	✗	✓	1	303	1
28	JTAG interface is not password protected.	Native	✗	✗	✓	1	441	1
29	Output of MAC is not erased on reset.	Inserted	✗	✗	✓	1	65	1
30	Supervisor mode signal of a core is floating preventing the use of SMAP.	Native	✗	✗	✓	1	282	1
31	GPIO is able to read/write to instruction and data cache.	Native	✗	✗	✓	1	151	4

Testbed of over 30 representative RTL bugs reproduced in RISC-V SoCs

Check out our paper for the full list and open-source repository https://github.com/hackdac/hackdac_2018_beta

Dive In

RISC-V SoC: RTL Bugs Testbed



AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

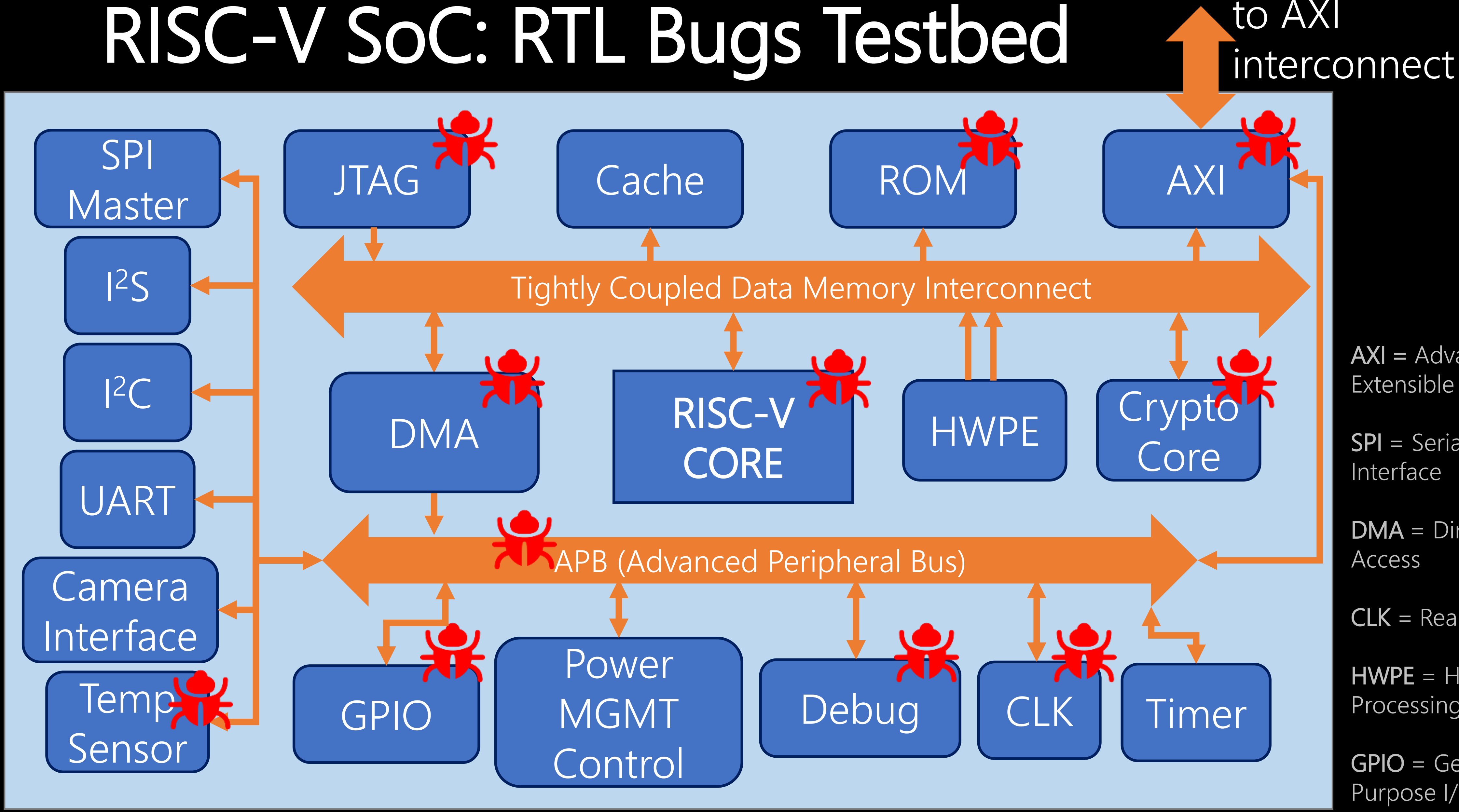
CLK = Real-Time Clock

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

RISC-V SoC: RTL Bugs Testbed



AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

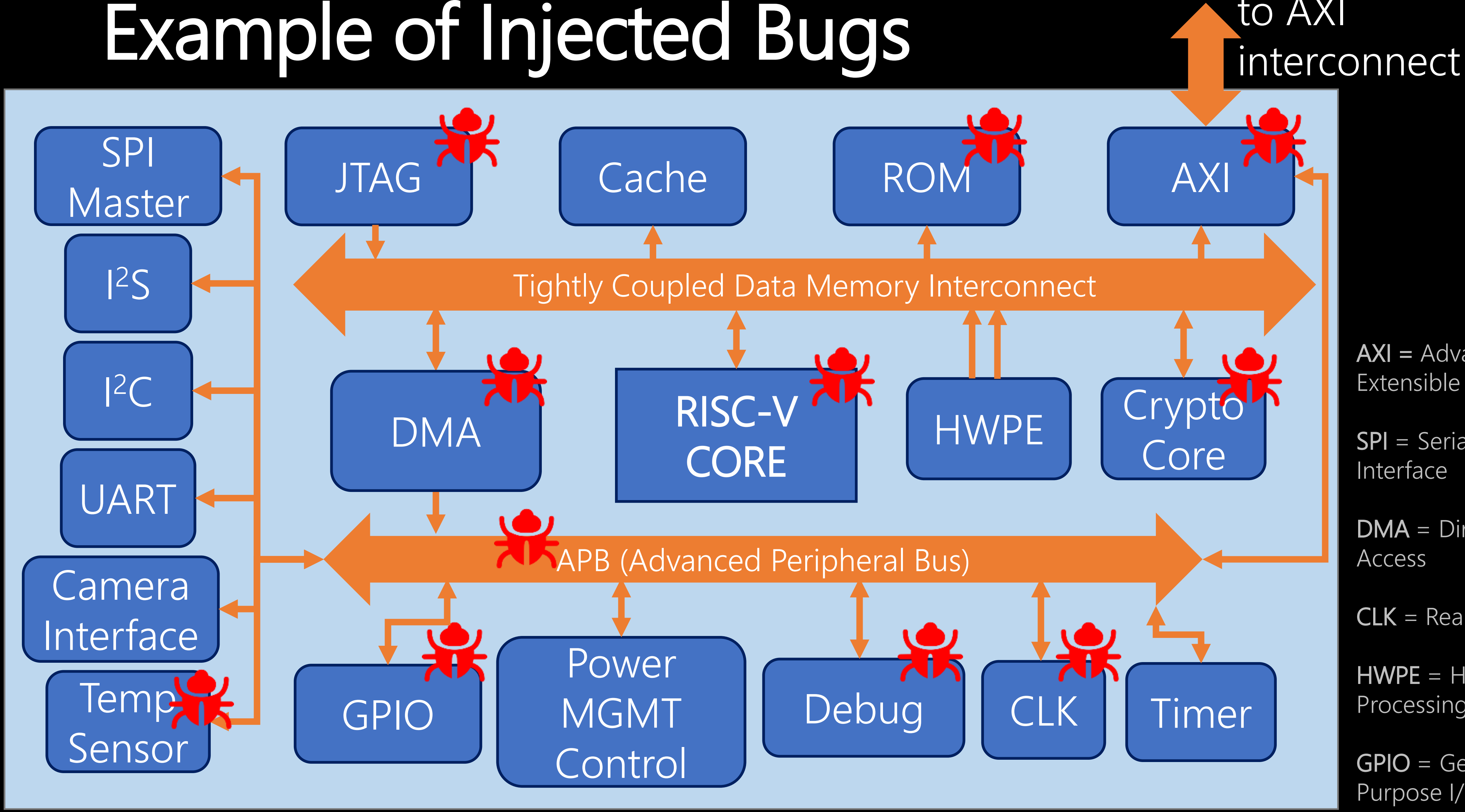
CLK = Real-Time Clock

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

Example of Injected Bugs



AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

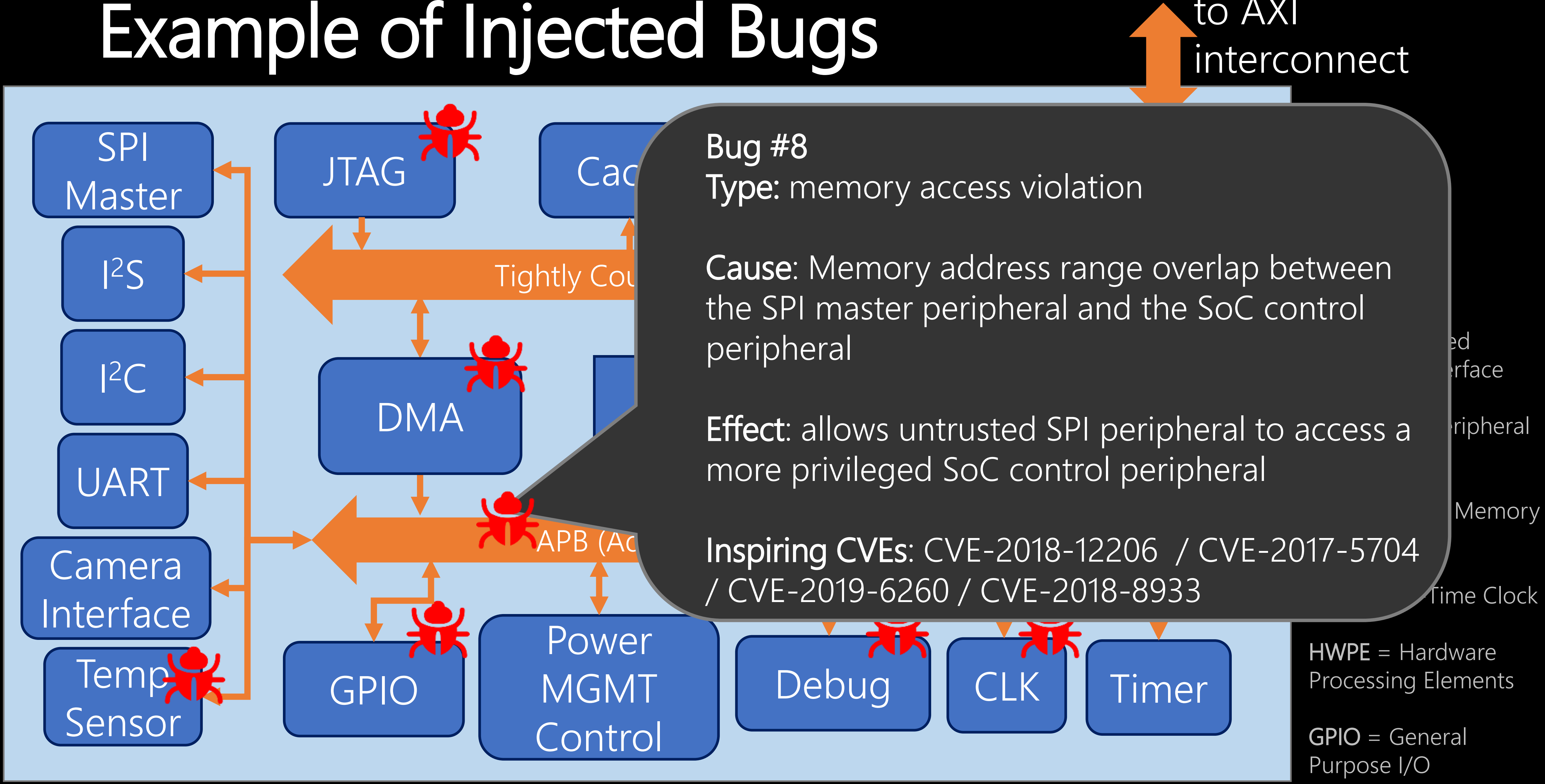
CLK = Real-Time Clock

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

Example of Injected Bugs



Bug #8
Type: memory access violation

Cause: Memory address range overlap between the SPI master peripheral and the SoC control peripheral

Effect: allows untrusted SPI peripheral to access a more privileged SoC control peripheral

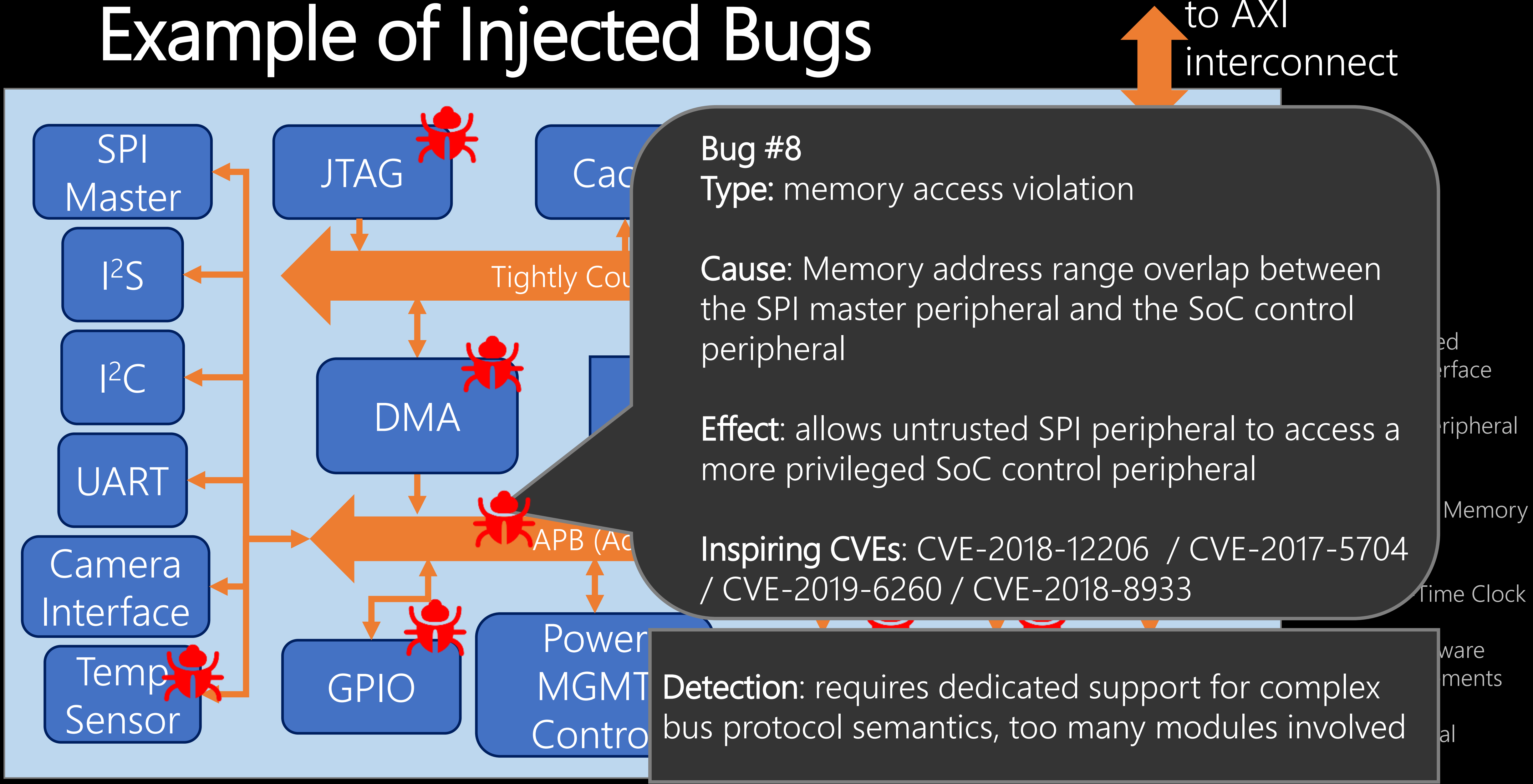
Inspiring CVEs: CVE-2018-12206 / CVE-2017-5704 / CVE-2019-6260 / CVE-2018-8933

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

Example of Injected Bugs



Bug #8
Type: memory access violation

Cause: Memory address range overlap between the SPI master peripheral and the SoC control peripheral

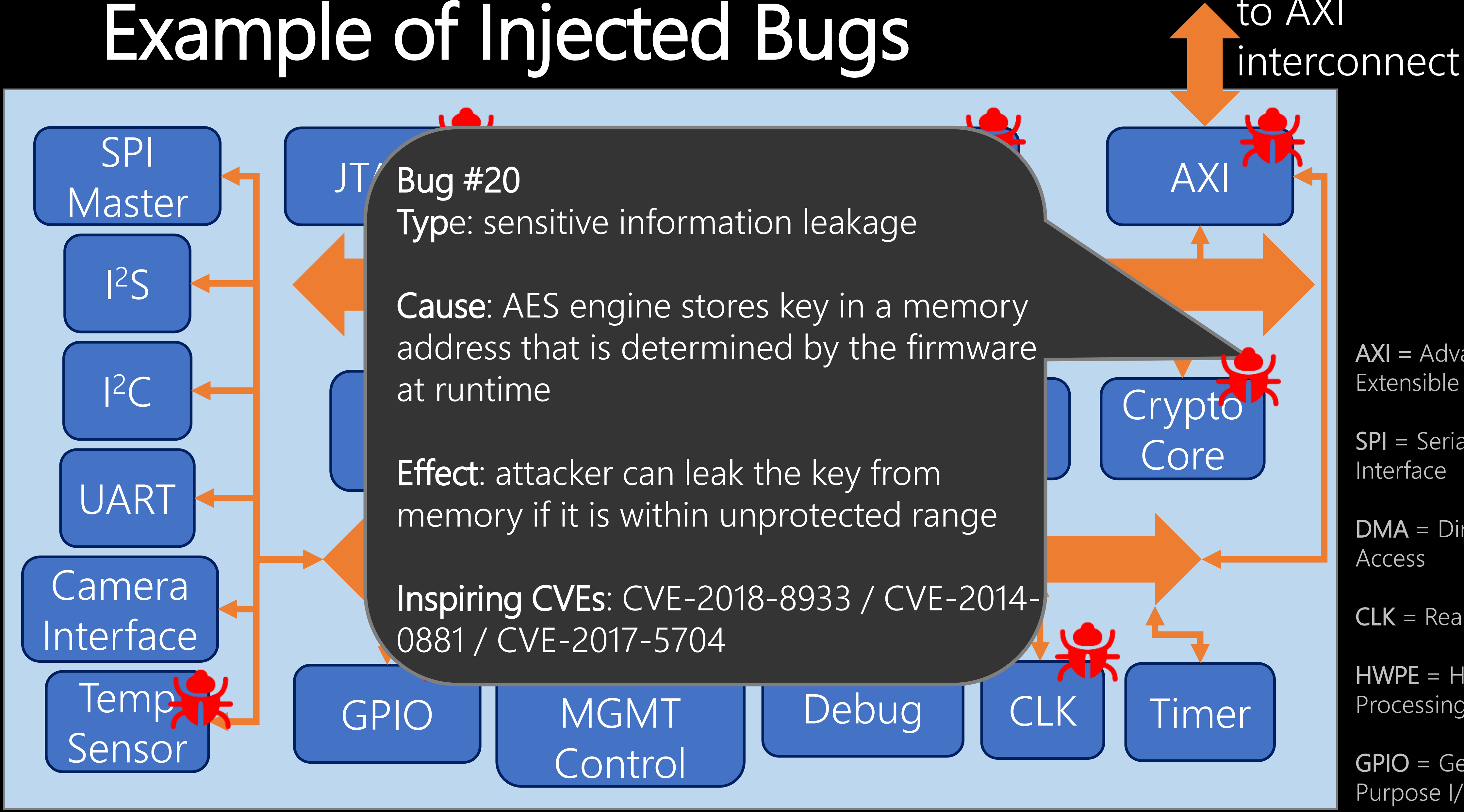
Effect: allows untrusted SPI peripheral to access a more privileged SoC control peripheral

Inspiring CVEs: CVE-2018-12206 / CVE-2017-5704 / CVE-2019-6260 / CVE-2018-8933

Detection: requires dedicated support for complex bus protocol semantics, too many modules involved

2 RISC-V SoCs used: PULPino & PULPissimo

Example of Injected Bugs



Bug #20
Type: sensitive information leakage

Cause: AES engine stores key in a memory address that is determined by the firmware at runtime

Effect: attacker can leak the key from memory if it is within unprotected range

Inspiring CVEs: CVE-2018-8933 / CVE-2014-0881 / CVE-2017-5704

AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

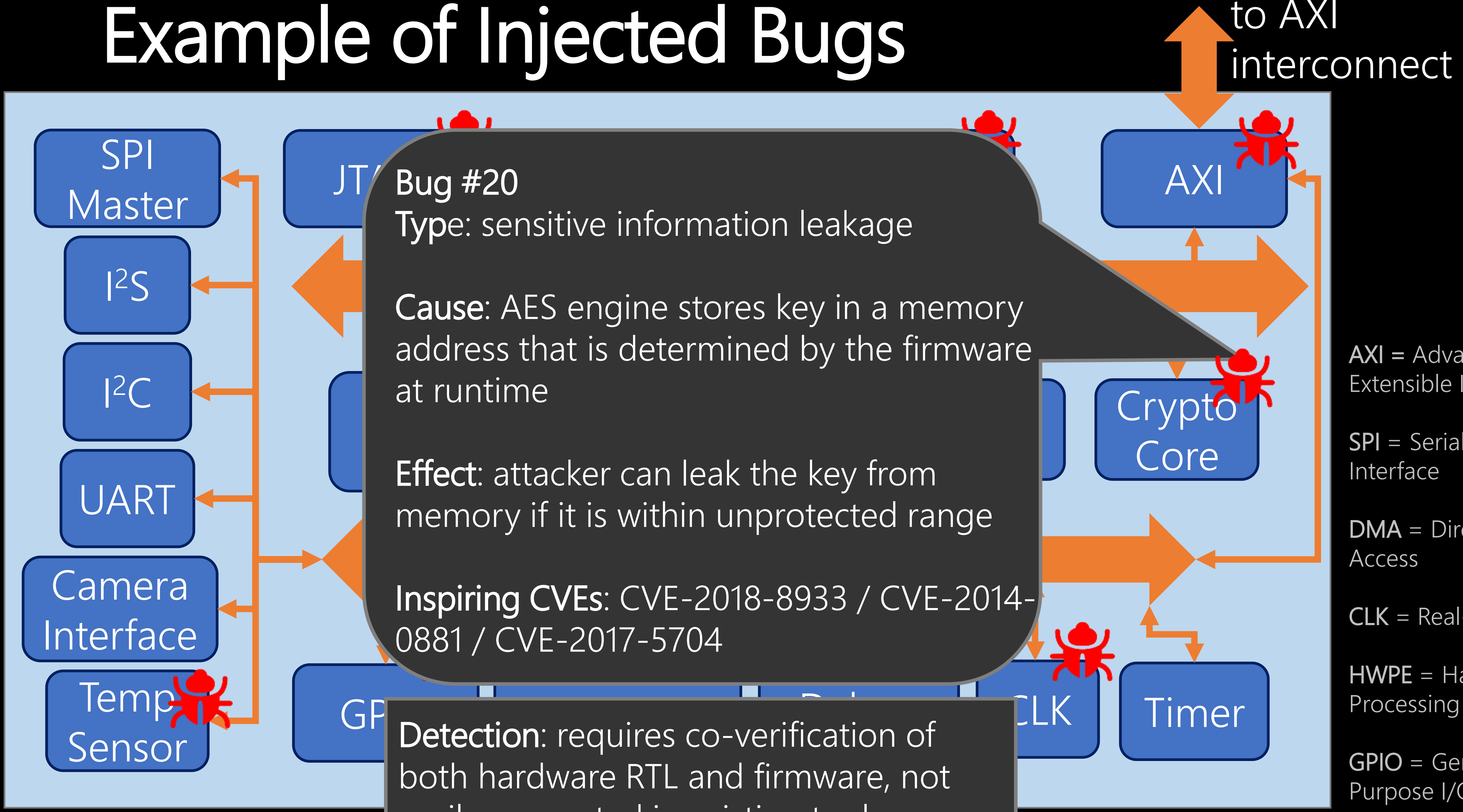
CLK = Real-Time Clock

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

Example of Injected Bugs



Bug #20
Type: sensitive information leakage

Cause: AES engine stores key in a memory address that is determined by the firmware at runtime

Effect: attacker can leak the key from memory if it is within unprotected range

Inspiring CVEs: CVE-2018-8933 / CVE-2014-0881 / CVE-2017-5704

Detection: requires co-verification of both hardware RTL and firmware, not easily supported in existing tools

AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

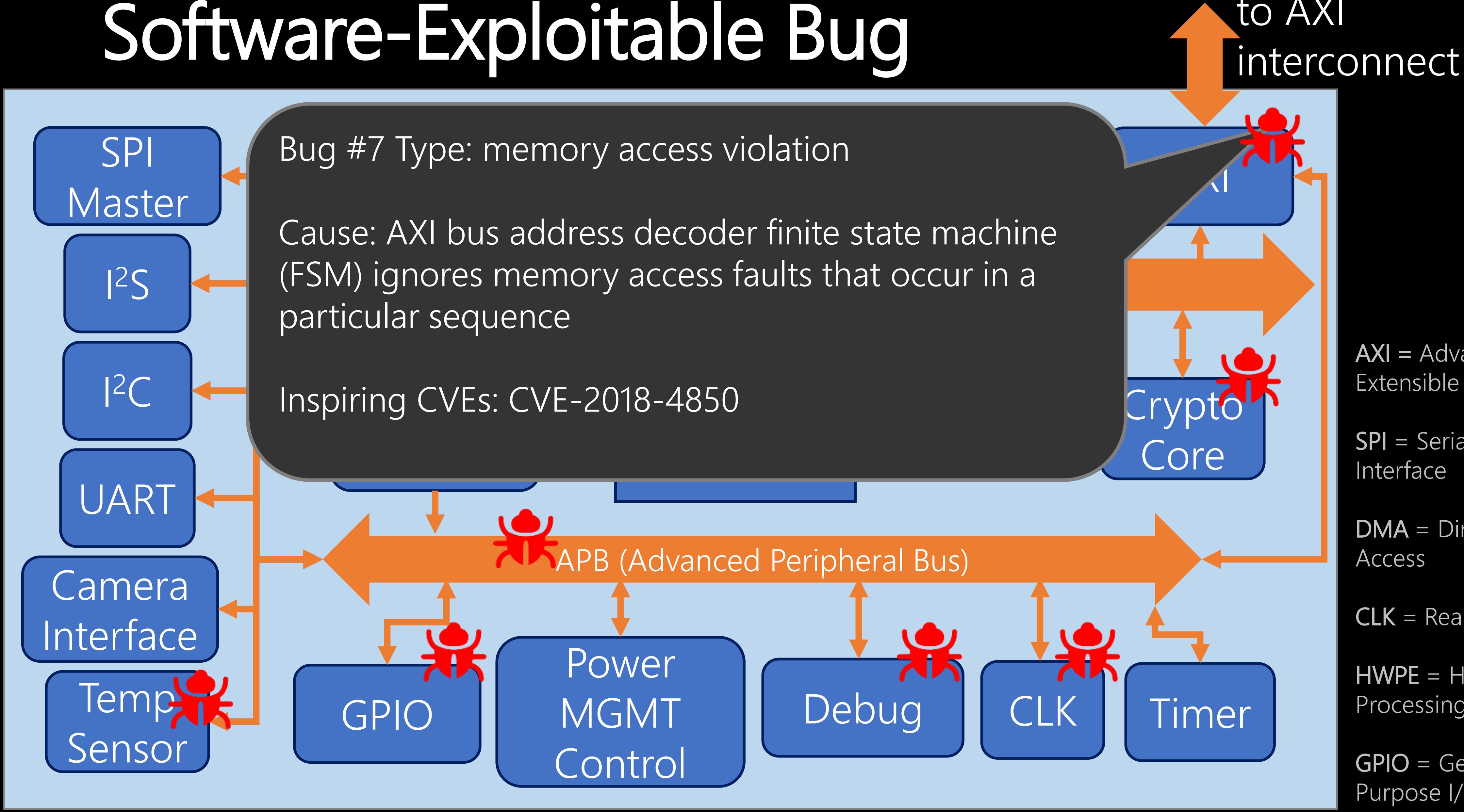
CLK = Real-Time Clock

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

Software-Exploitable Bug



Bug #7 Type: memory access violation

Cause: AXI bus address decoder finite state machine (FSM) ignores memory access faults that occur in a particular sequence

Inspiring CVEs: CVE-2018-4850

AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

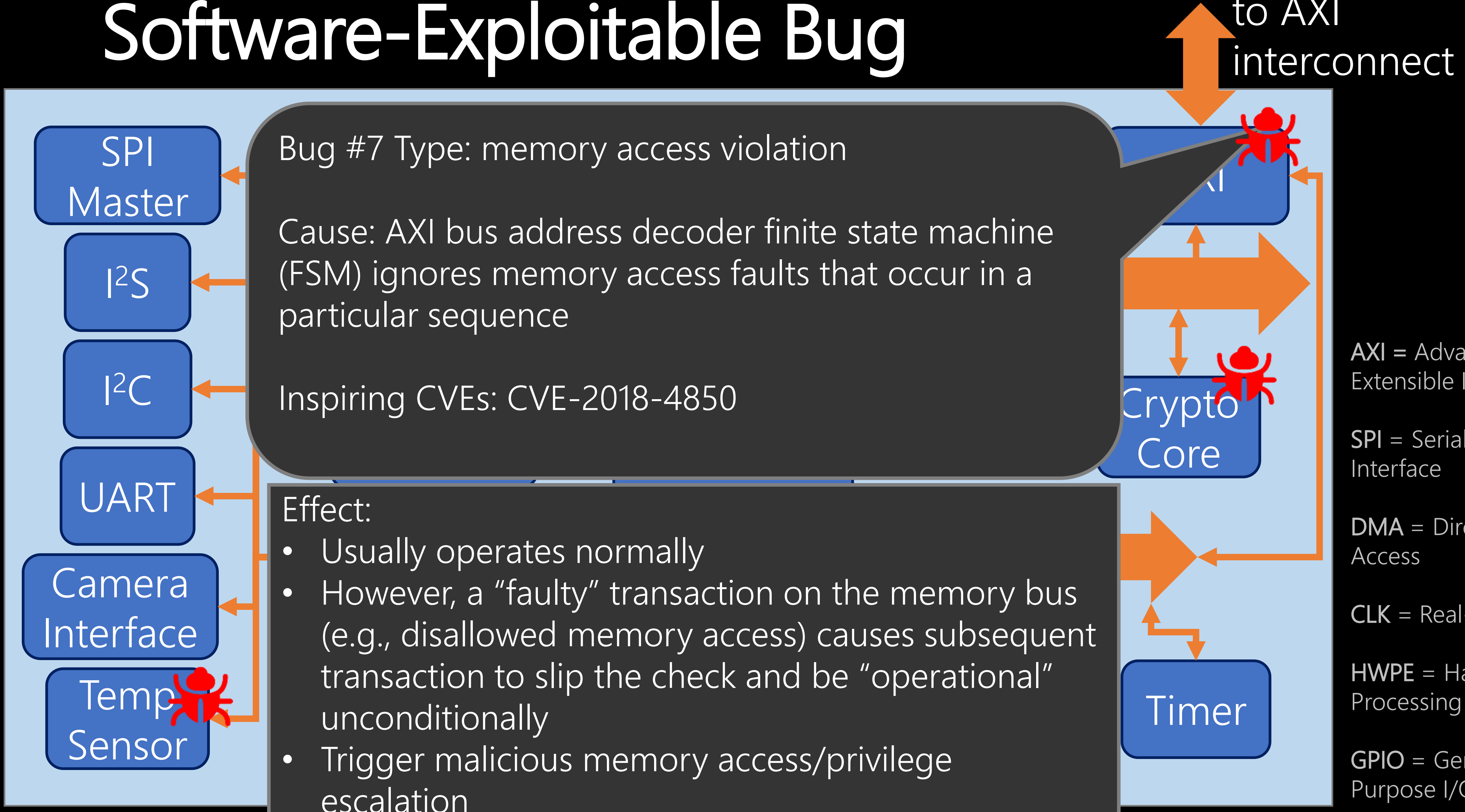
CLK = Real-Time Clock

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

Software-Exploitable Bug



Bug #7 Type: memory access violation

Cause: AXI bus address decoder finite state machine (FSM) ignores memory access faults that occur in a particular sequence

Inspiring CVEs: CVE-2018-4850

Effect:

- Usually operates normally
- However, a "faulty" transaction on the memory bus (e.g., disallowed memory access) causes subsequent transaction to slip the check and be "operational" unconditionally
- Trigger malicious memory access/privilege escalation

AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

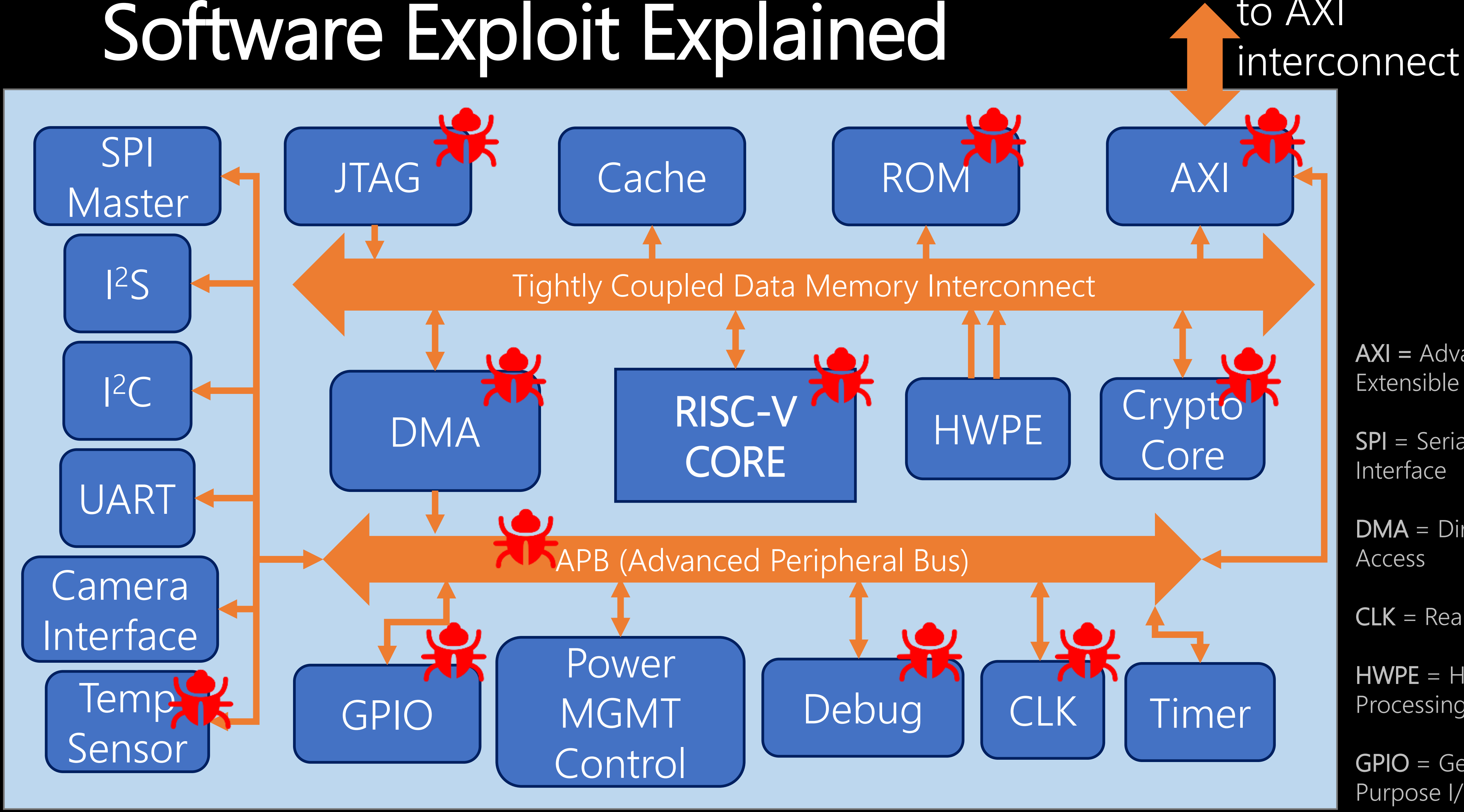
CLK = Real-Time Clock

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

Software Exploit Explained



AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

CLK = Real-Time Clock

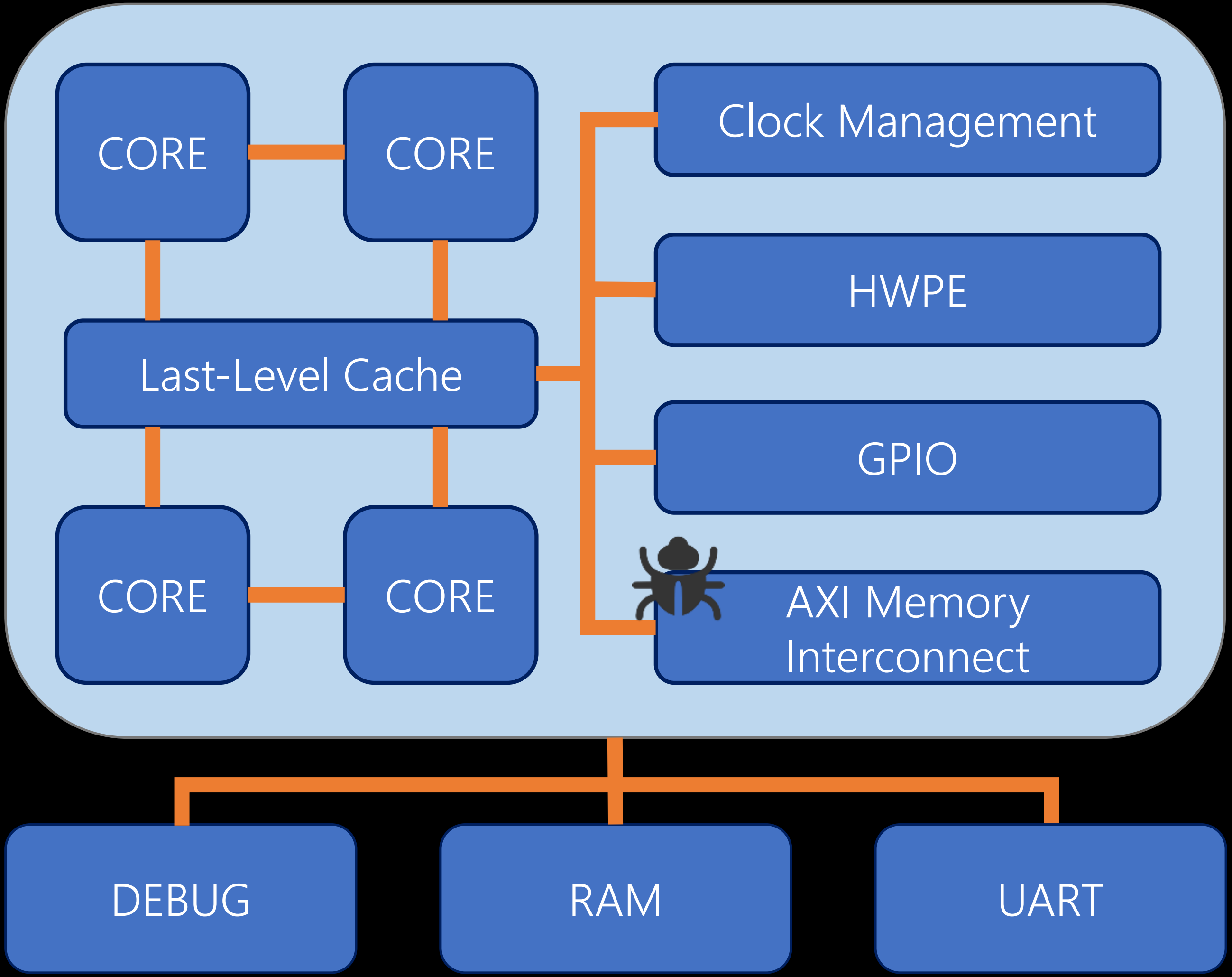
HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

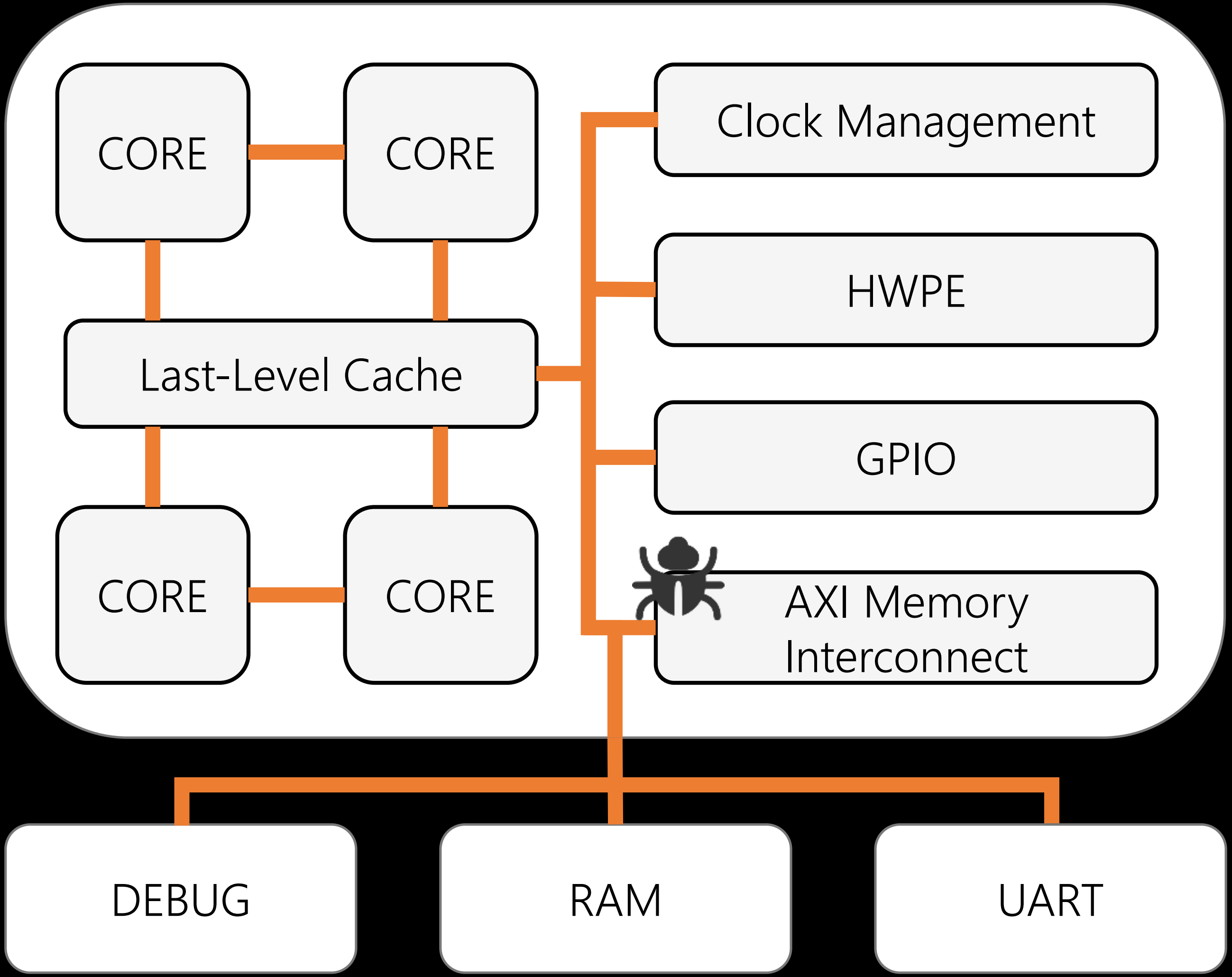
2 RISC-V SoCs used: PULPino & PULPissimo

Software Exploit Explained

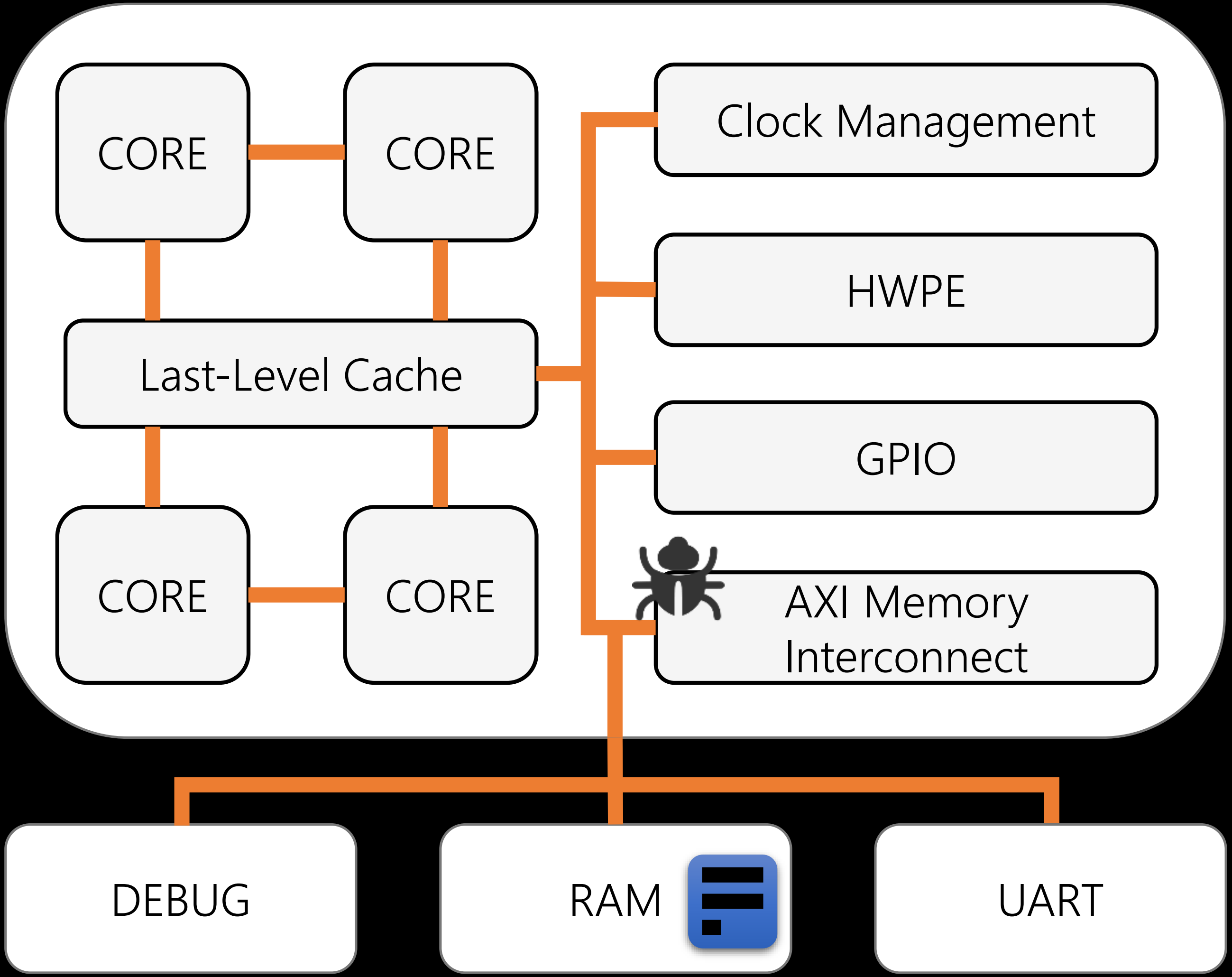
Abstracted SoC to simplify!



Software Exploit Explained



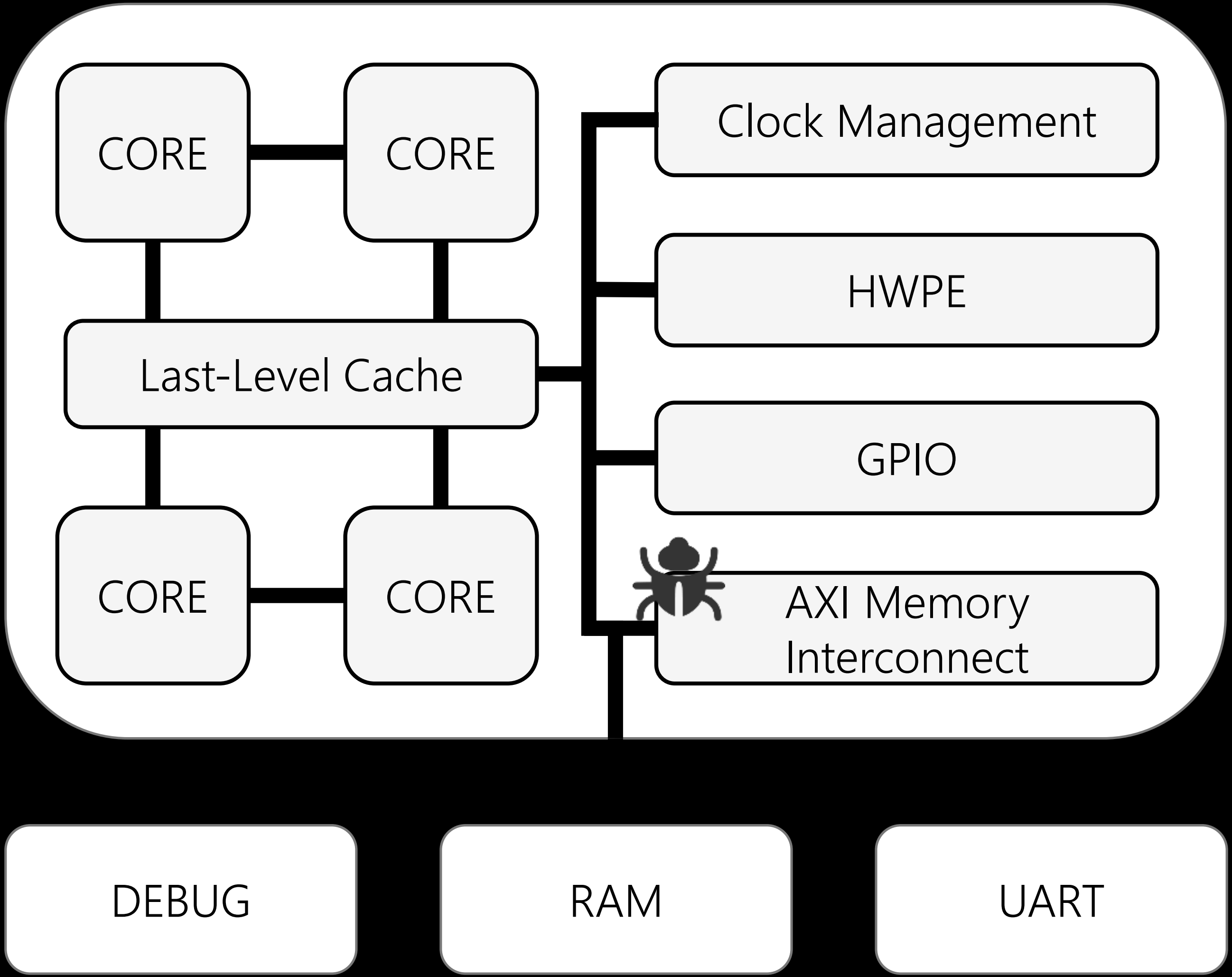
Software Exploit Explained



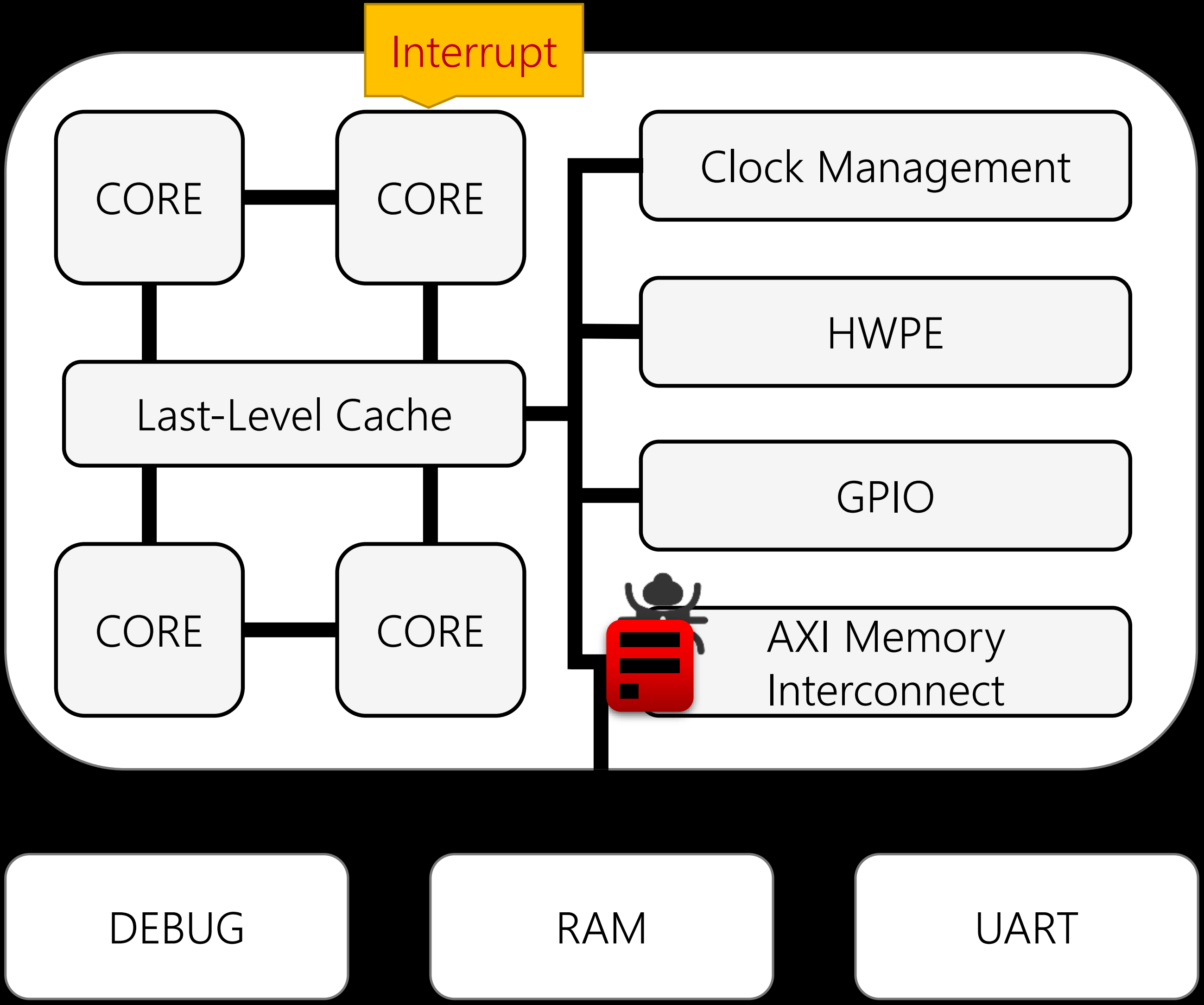
Memory access requests are usually sanitized by the page table walker in the CPU core and at the AXI memory interconnect to check whether the memory access is allowed.

✓

Software Exploit Explained

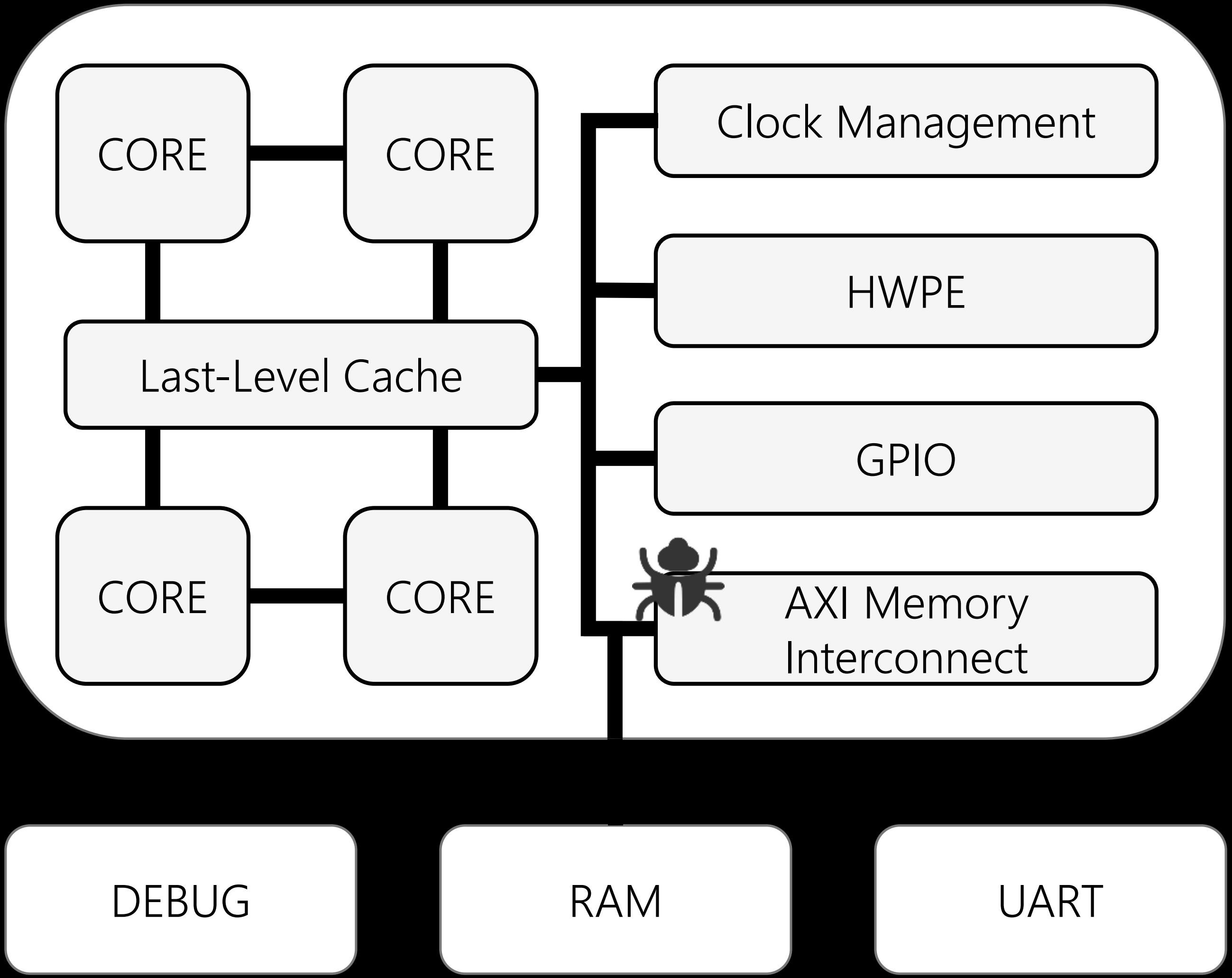


Software Exploit Explained

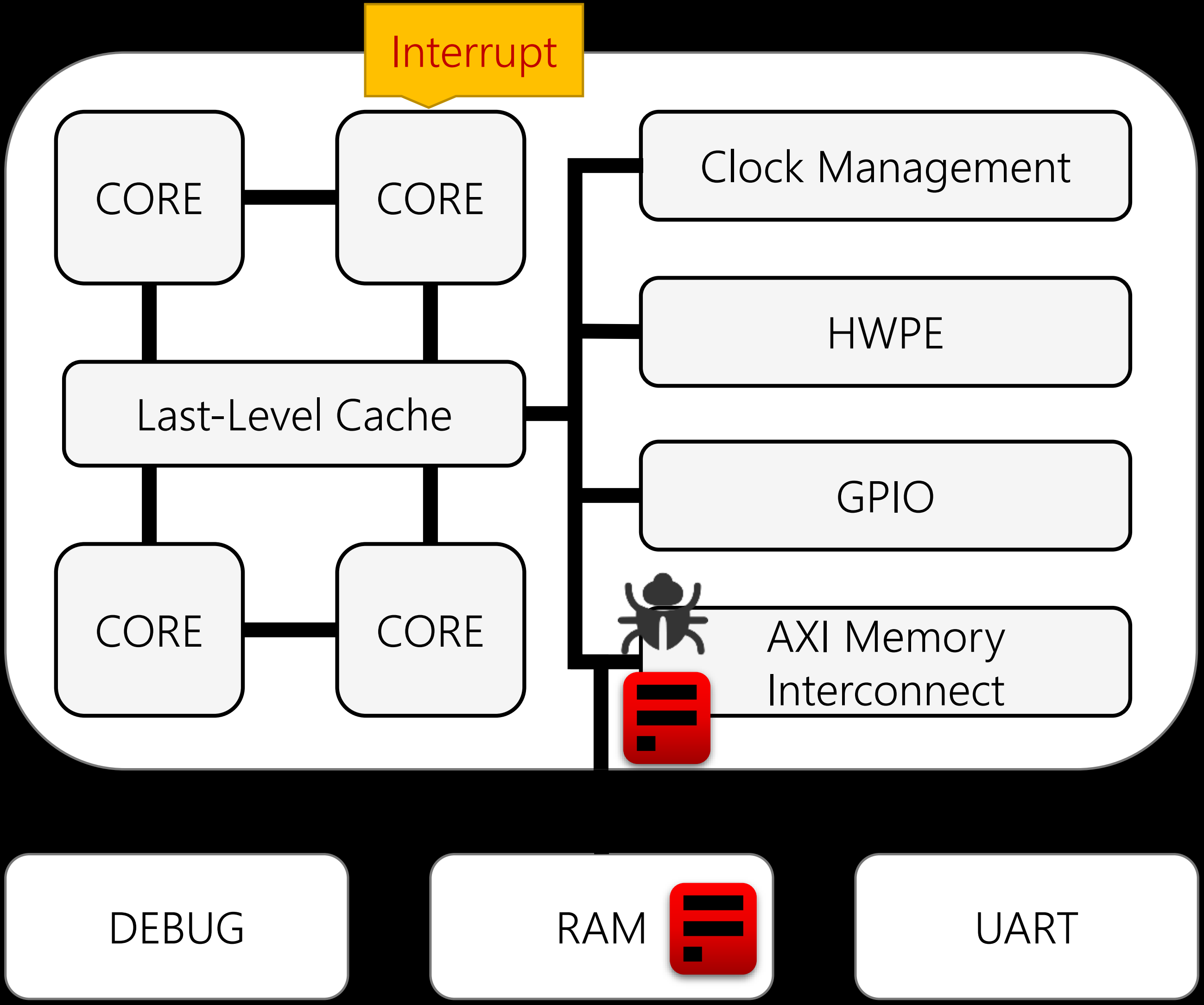


If a faulty/illegal access is detected, an interrupt is generated (even with the injected bug).

Software Exploit Explained



Software Exploit Explained

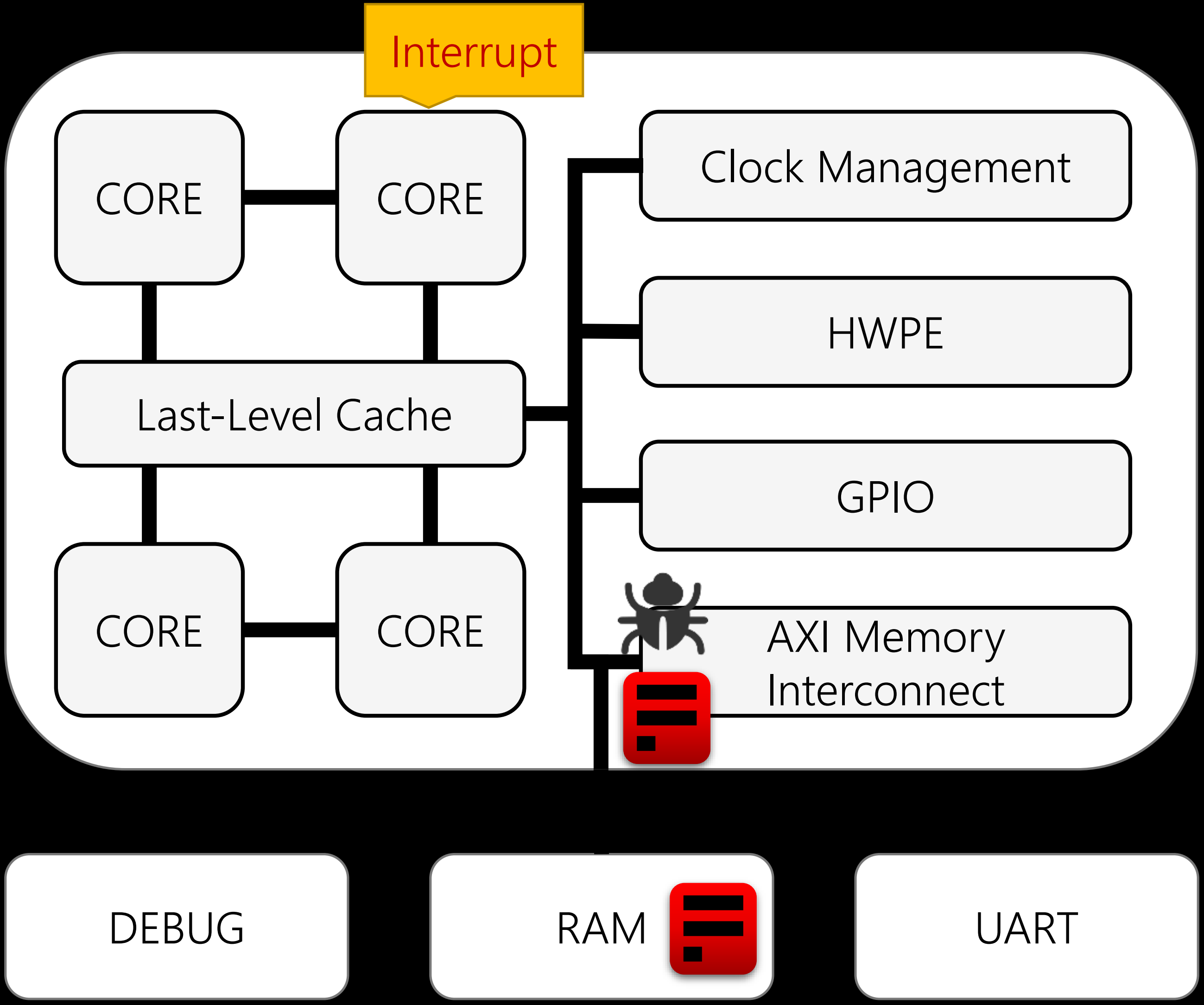


The interconnect is still processing a faulty memory access request, and another one comes in.

With this bug, the second request slips through the sanitization check and is allowed to occur even if it is illegal. ✓

Resulting in faulty (illegal) memory access.

Software Exploit Explained

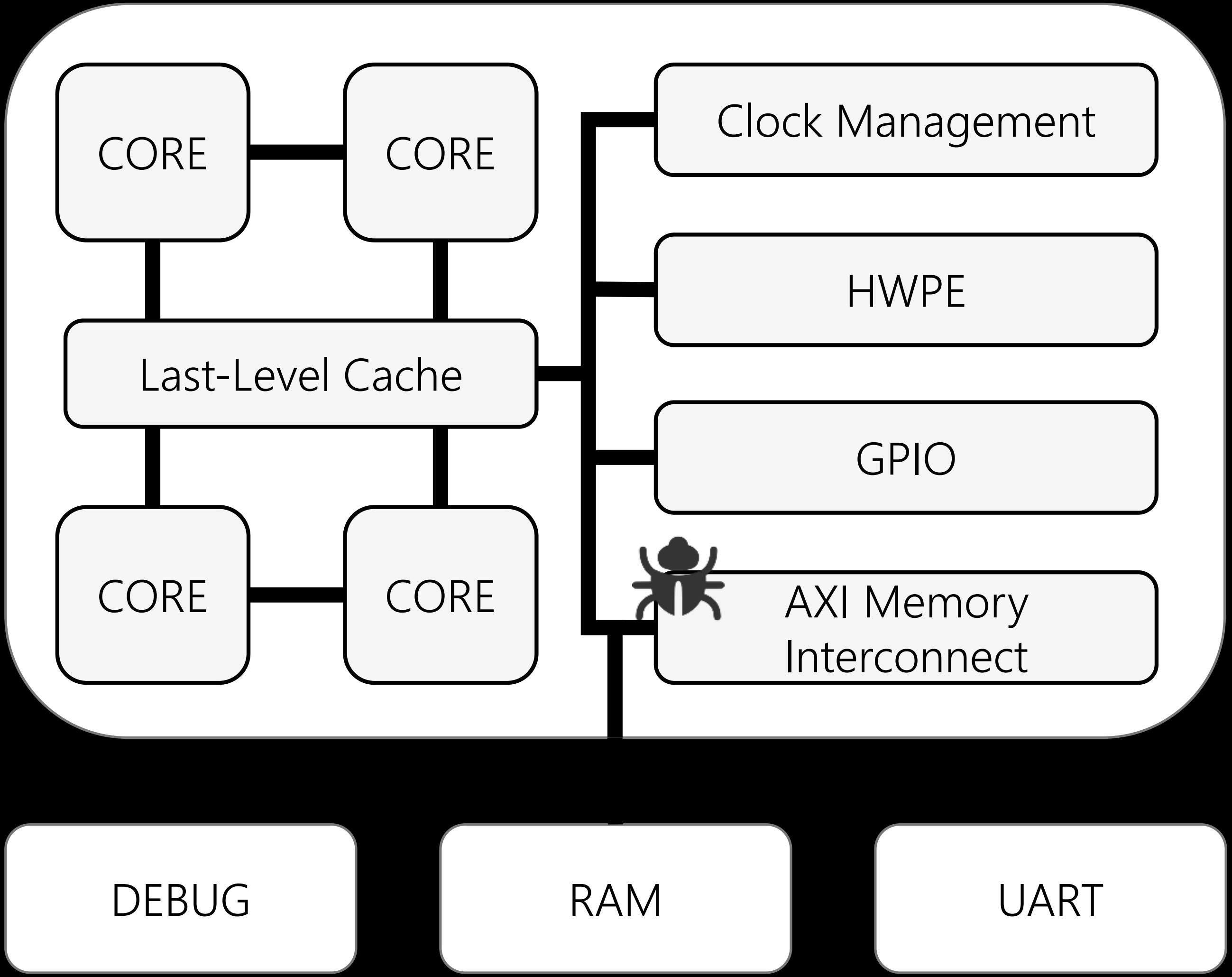


The interconnect is still processing a faulty memory access request, and another one comes in.

With this bug, the second request slips through the sanitization check and is allowed to occur even if it is illegal. ✓

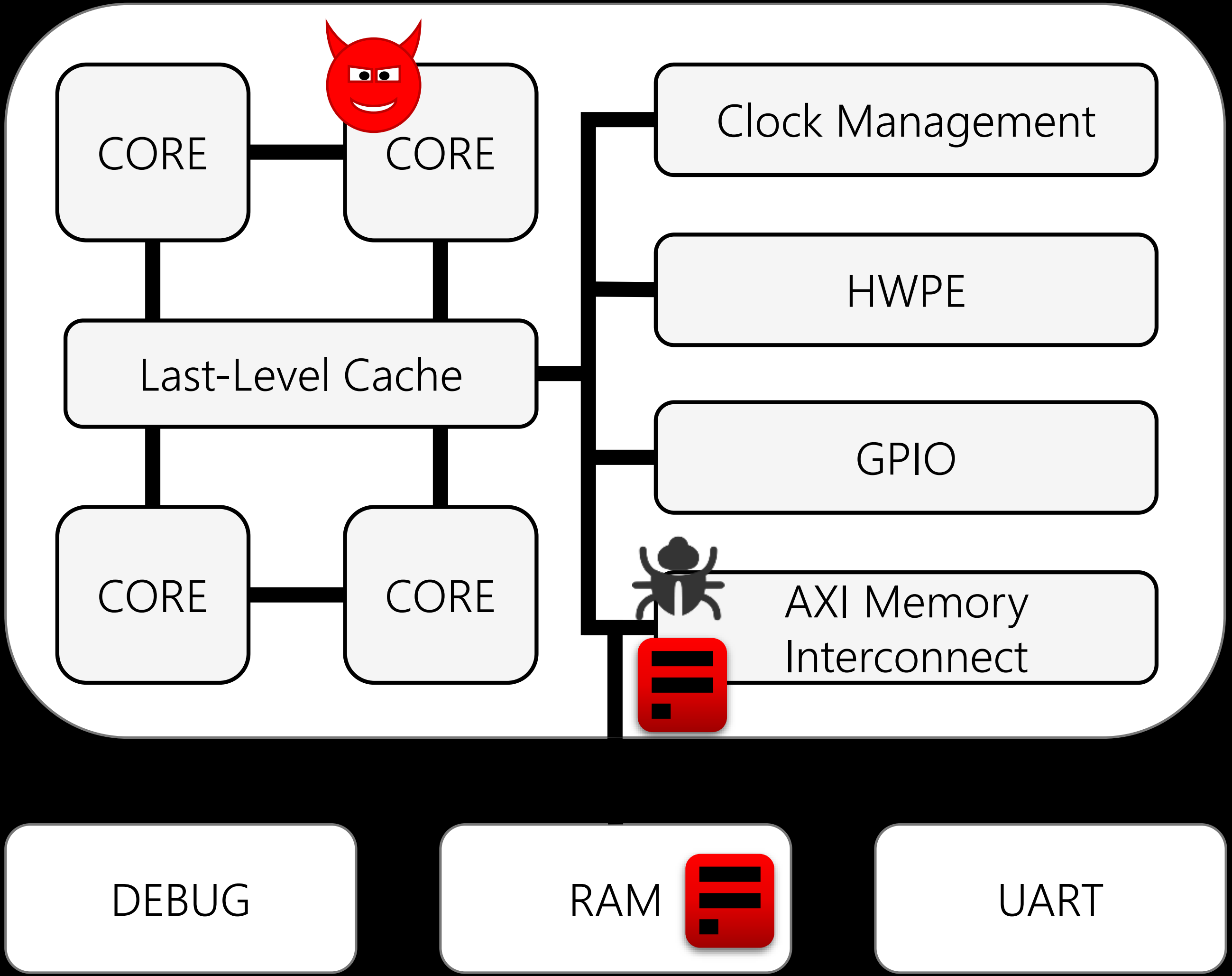
Resulting in faulty (illegal) memory access.

Software Exploit Explained



Software Exploit Explained

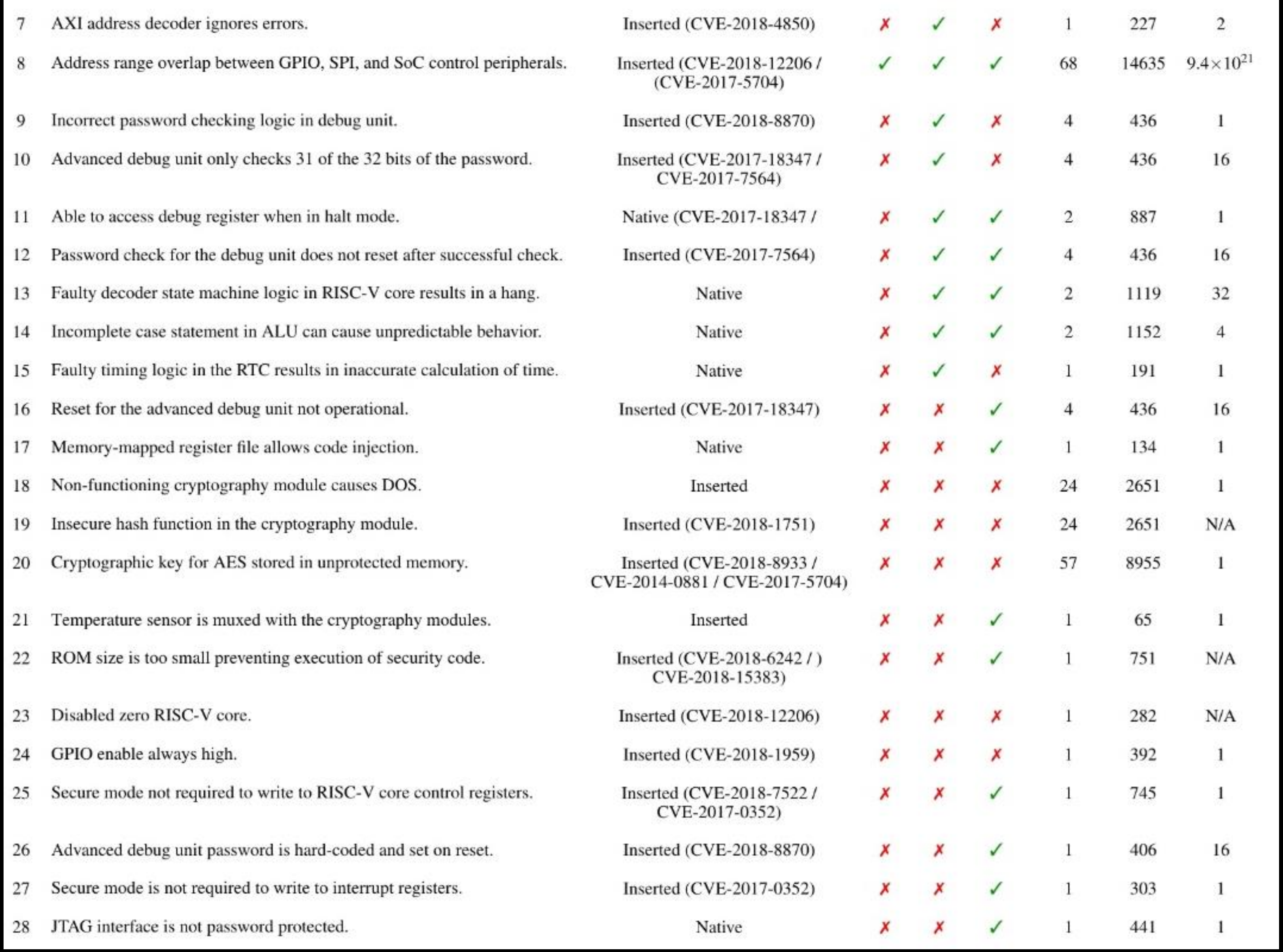
One malicious process can compromise the entire platform!



Attacker can register an interrupt handler and spam the bus wtih faulty memory accesses.

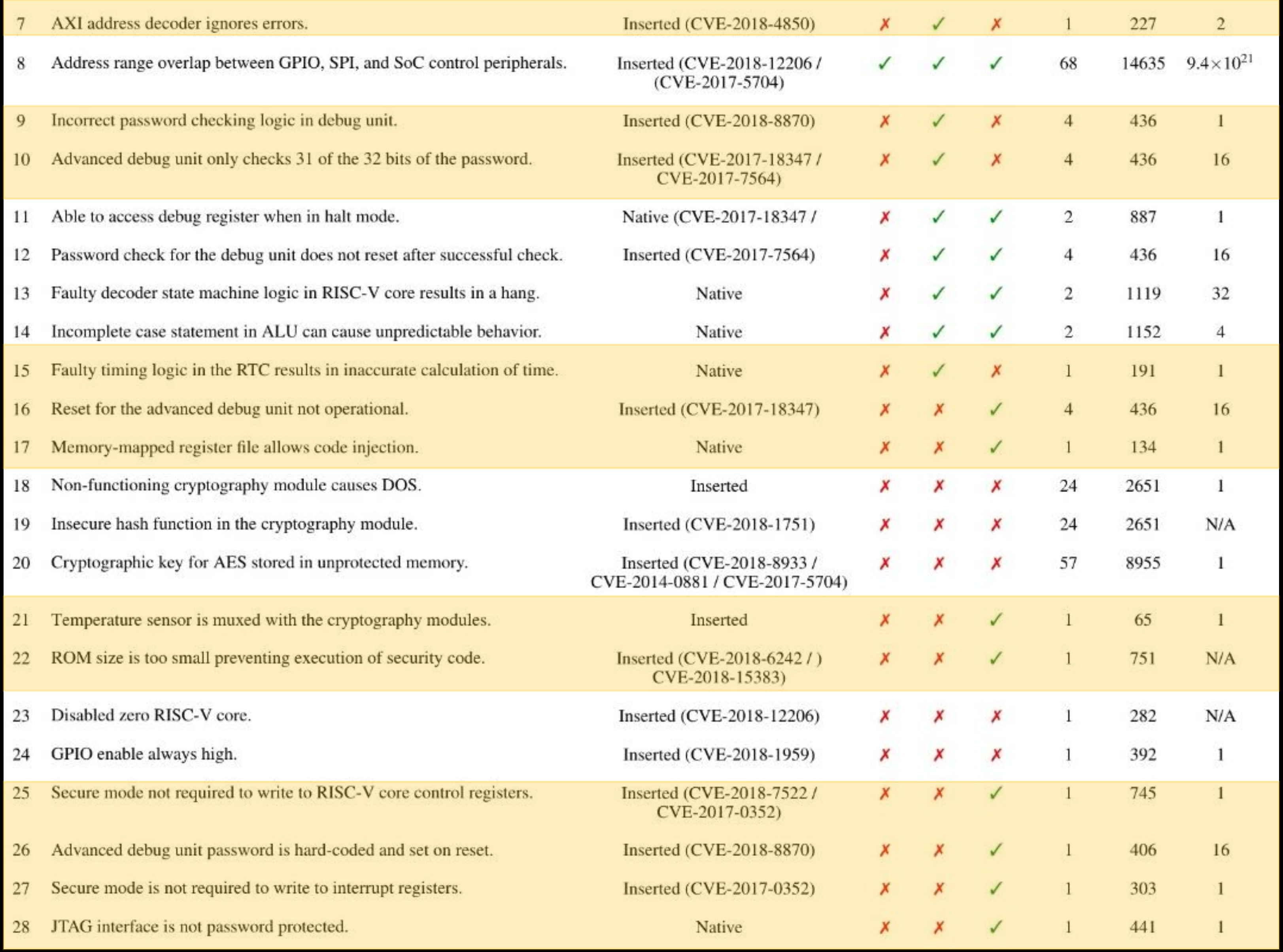
Eventually, a malicious memory access will slip through the checks and is allowed.

Results and HardFails



7	AXI address decoder ignores errors.	Inserted (CVE-2018-4850)	✗	✓	✗	1	227	2
8	Address range overlap between GPIO, SPI, and SoC control peripherals.	Inserted (CVE-2018-12206 / (CVE-2017-5704)	✓	✓	✓	68	14635	9.4×10^{21}
9	Incorrect password checking logic in debug unit.	Inserted (CVE-2018-8870)	✗	✓	✗	4	436	1
10	Advanced debug unit only checks 31 of the 32 bits of the password.	Inserted (CVE-2017-18347 / CVE-2017-7564)	✗	✓	✗	4	436	16
11	Able to access debug register when in halt mode.	Native (CVE-2017-18347 /	✗	✓	✓	2	887	1
12	Password check for the debug unit does not reset after successful check.	Inserted (CVE-2017-7564)	✗	✓	✓	4	436	16
13	Faulty decoder state machine logic in RISC-V core results in a hang.	Native	✗	✓	✓	2	1119	32
14	Incomplete case statement in ALU can cause unpredictable behavior.	Native	✗	✓	✓	2	1152	4
15	Faulty timing logic in the RTC results in inaccurate calculation of time.	Native	✗	✓	✗	1	191	1
16	Reset for the advanced debug unit not operational.	Inserted (CVE-2017-18347)	✗	✗	✓	4	436	16
17	Memory-mapped register file allows code injection.	Native	✗	✗	✓	1	134	1
18	Non-functioning cryptography module causes DOS.	Inserted	✗	✗	✗	24	2651	1
19	Insecure hash function in the cryptography module.	Inserted (CVE-2018-1751)	✗	✗	✗	24	2651	N/A
20	Cryptographic key for AES stored in unprotected memory.	Inserted (CVE-2018-8933 / CVE-2014-0881 / CVE-2017-5704)	✗	✗	✗	57	8955	1
21	Temperature sensor is muxed with the cryptography modules.	Inserted	✗	✗	✓	1	65	1
22	ROM size is too small preventing execution of security code.	Inserted (CVE-2018-6242 /) CVE-2018-15383)	✗	✗	✓	1	751	N/A
23	Disabled zero RISC-V core.	Inserted (CVE-2018-12206)	✗	✗	✗	1	282	N/A
24	GPIO enable always high.	Inserted (CVE-2018-1959)	✗	✗	✗	1	392	1
25	Secure mode not required to write to RISC-V core control registers.	Inserted (CVE-2018-7522 / CVE-2017-0352)	✗	✗	✓	1	745	1
26	Advanced debug unit password is hard-coded and set on reset.	Inserted (CVE-2018-8870)	✗	✗	✓	1	406	16
27	Secure mode is not required to write to interrupt registers.	Inserted (CVE-2017-0352)	✗	✗	✓	1	303	1
28	JTAG interface is not password protected.	Native	✗	✗	✓	1	441	1

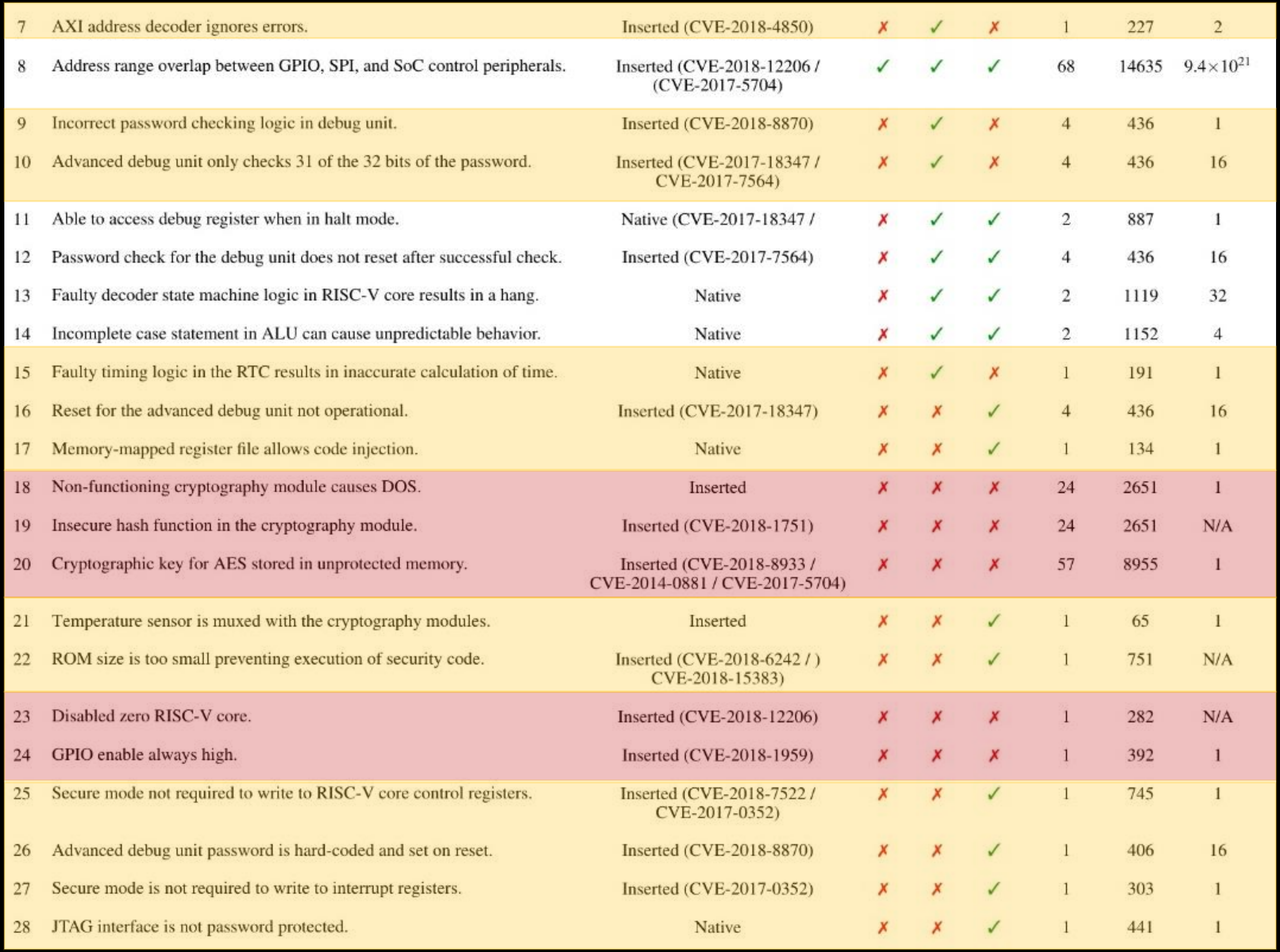
Results and HardFails



7	AXI address decoder ignores errors.	Inserted (CVE-2018-4850)	✗	✓	✗	1	227	2
8	Address range overlap between GPIO, SPI, and SoC control peripherals.	Inserted (CVE-2018-12206 / (CVE-2017-5704)	✓	✓	✓	68	14635	9.4×10^{21}
9	Incorrect password checking logic in debug unit.	Inserted (CVE-2018-8870)	✗	✓	✗	4	436	1
10	Advanced debug unit only checks 31 of the 32 bits of the password.	Inserted (CVE-2017-18347 / CVE-2017-7564)	✗	✓	✗	4	436	16
11	Able to access debug register when in halt mode.	Native (CVE-2017-18347 /	✗	✓	✓	2	887	1
12	Password check for the debug unit does not reset after successful check.	Inserted (CVE-2017-7564)	✗	✓	✓	4	436	16
13	Faulty decoder state machine logic in RISC-V core results in a hang.	Native	✗	✓	✓	2	1119	32
14	Incomplete case statement in ALU can cause unpredictable behavior.	Native	✗	✓	✓	2	1152	4
15	Faulty timing logic in the RTC results in inaccurate calculation of time.	Native	✗	✓	✗	1	191	1
16	Reset for the advanced debug unit not operational.	Inserted (CVE-2017-18347)	✗	✗	✓	4	436	16
17	Memory-mapped register file allows code injection.	Native	✗	✗	✓	1	134	1
18	Non-functioning cryptography module causes DOS.	Inserted	✗	✗	✗	24	2651	1
19	Insecure hash function in the cryptography module.	Inserted (CVE-2018-1751)	✗	✗	✗	24	2651	N/A
20	Cryptographic key for AES stored in unprotected memory.	Inserted (CVE-2018-8933 / CVE-2014-0881 / CVE-2017-5704)	✗	✗	✗	57	8955	1
21	Temperature sensor is muxed with the cryptography modules.	Inserted	✗	✗	✓	1	65	1
22	ROM size is too small preventing execution of security code.	Inserted (CVE-2018-6242 /) CVE-2018-15383)	✗	✗	✓	1	751	N/A
23	Disabled zero RISC-V core.	Inserted (CVE-2018-12206)	✗	✗	✗	1	282	N/A
24	GPIO enable always high.	Inserted (CVE-2018-1959)	✗	✗	✗	1	392	1
25	Secure mode not required to write to RISC-V core control registers.	Inserted (CVE-2018-7522 / CVE-2017-0352)	✗	✗	✓	1	745	1
26	Advanced debug unit password is hard-coded and set on reset.	Inserted (CVE-2018-8870)	✗	✗	✓	1	406	16
27	Secure mode is not required to write to interrupt registers.	Inserted (CVE-2017-0352)	✗	✗	✓	1	303	1
28	JTAG interface is not password protected.	Native	✗	✗	✓	1	441	1

Some bugs were very difficult to detect

Results and HardFails

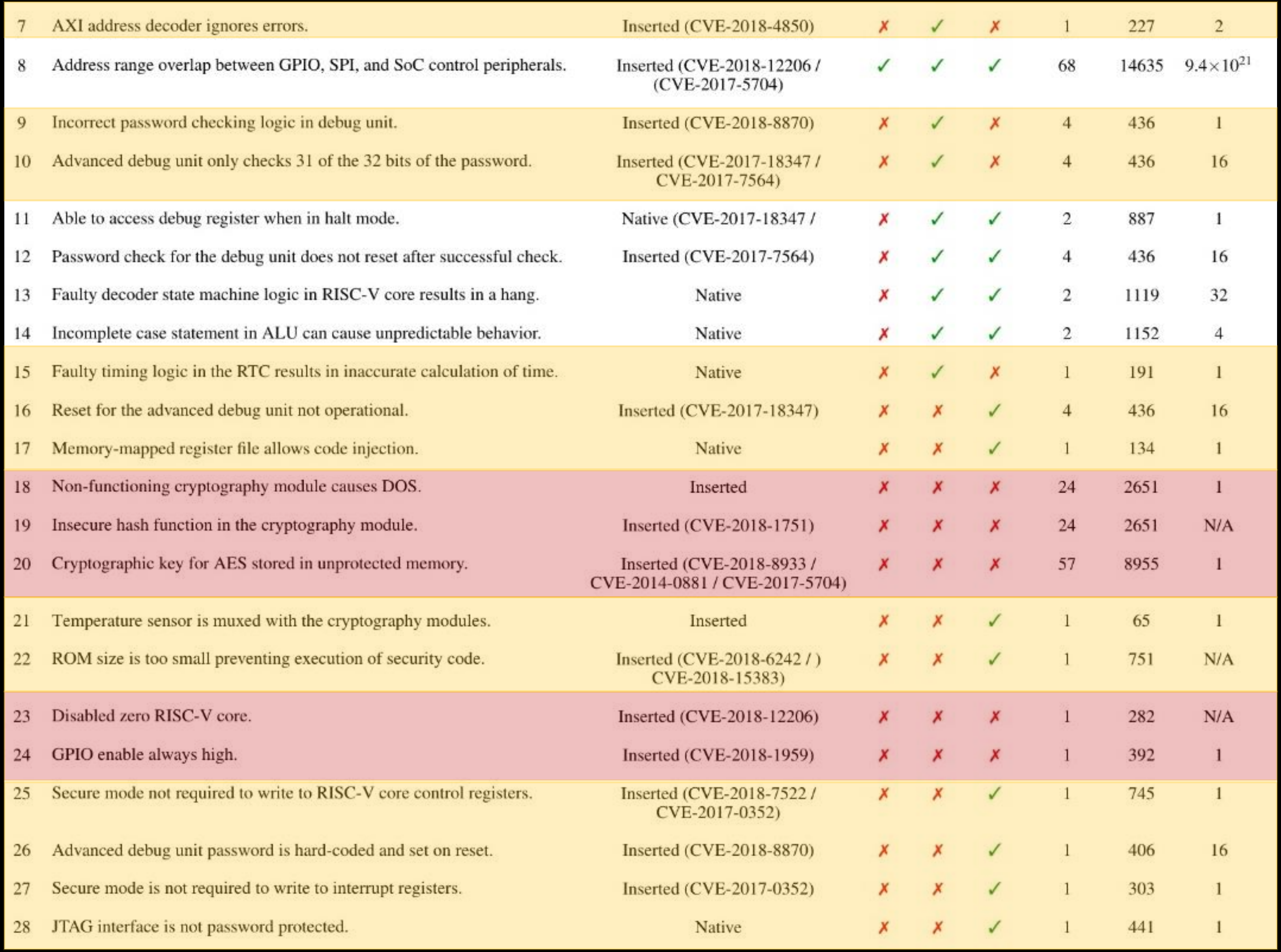


7	AXI address decoder ignores errors.	Inserted (CVE-2018-4850)	✗	✓	✗	1	227	2
8	Address range overlap between GPIO, SPI, and SoC control peripherals.	Inserted (CVE-2018-12206 / (CVE-2017-5704)	✓	✓	✓	68	14635	9.4×10^{21}
9	Incorrect password checking logic in debug unit.	Inserted (CVE-2018-8870)	✗	✓	✗	4	436	1
10	Advanced debug unit only checks 31 of the 32 bits of the password.	Inserted (CVE-2017-18347 / CVE-2017-7564)	✗	✓	✗	4	436	16
11	Able to access debug register when in halt mode.	Native (CVE-2017-18347 /	✗	✓	✓	2	887	1
12	Password check for the debug unit does not reset after successful check.	Inserted (CVE-2017-7564)	✗	✓	✓	4	436	16
13	Faulty decoder state machine logic in RISC-V core results in a hang.	Native	✗	✓	✓	2	1119	32
14	Incomplete case statement in ALU can cause unpredictable behavior.	Native	✗	✓	✓	2	1152	4
15	Faulty timing logic in the RTC results in inaccurate calculation of time.	Native	✗	✓	✗	1	191	1
16	Reset for the advanced debug unit not operational.	Inserted (CVE-2017-18347)	✗	✗	✓	4	436	16
17	Memory-mapped register file allows code injection.	Native	✗	✗	✓	1	134	1
18	Non-functioning cryptography module causes DOS.	Inserted	✗	✗	✗	24	2651	1
19	Insecure hash function in the cryptography module.	Inserted (CVE-2018-1751)	✗	✗	✗	24	2651	N/A
20	Cryptographic key for AES stored in unprotected memory.	Inserted (CVE-2018-8933 / CVE-2014-0881 / CVE-2017-5704)	✗	✗	✗	57	8955	1
21	Temperature sensor is muxed with the cryptography modules.	Inserted	✗	✗	✓	1	65	1
22	ROM size is too small preventing execution of security code.	Inserted (CVE-2018-6242 /) CVE-2018-15383)	✗	✗	✓	1	751	N/A
23	Disabled zero RISC-V core.	Inserted (CVE-2018-12206)	✗	✗	✗	1	282	N/A
24	GPIO enable always high.	Inserted (CVE-2018-1959)	✗	✗	✗	1	392	1
25	Secure mode not required to write to RISC-V core control registers.	Inserted (CVE-2018-7522 / CVE-2017-0352)	✗	✗	✓	1	745	1
26	Advanced debug unit password is hard-coded and set on reset.	Inserted (CVE-2018-8870)	✗	✗	✓	1	406	16
27	Secure mode is not required to write to interrupt registers.	Inserted (CVE-2017-0352)	✗	✗	✓	1	303	1
28	JTAG interface is not password protected.	Native	✗	✗	✓	1	441	1

Some bugs were very difficult to detect

Some bugs could not be detected at all

Results and HardFails



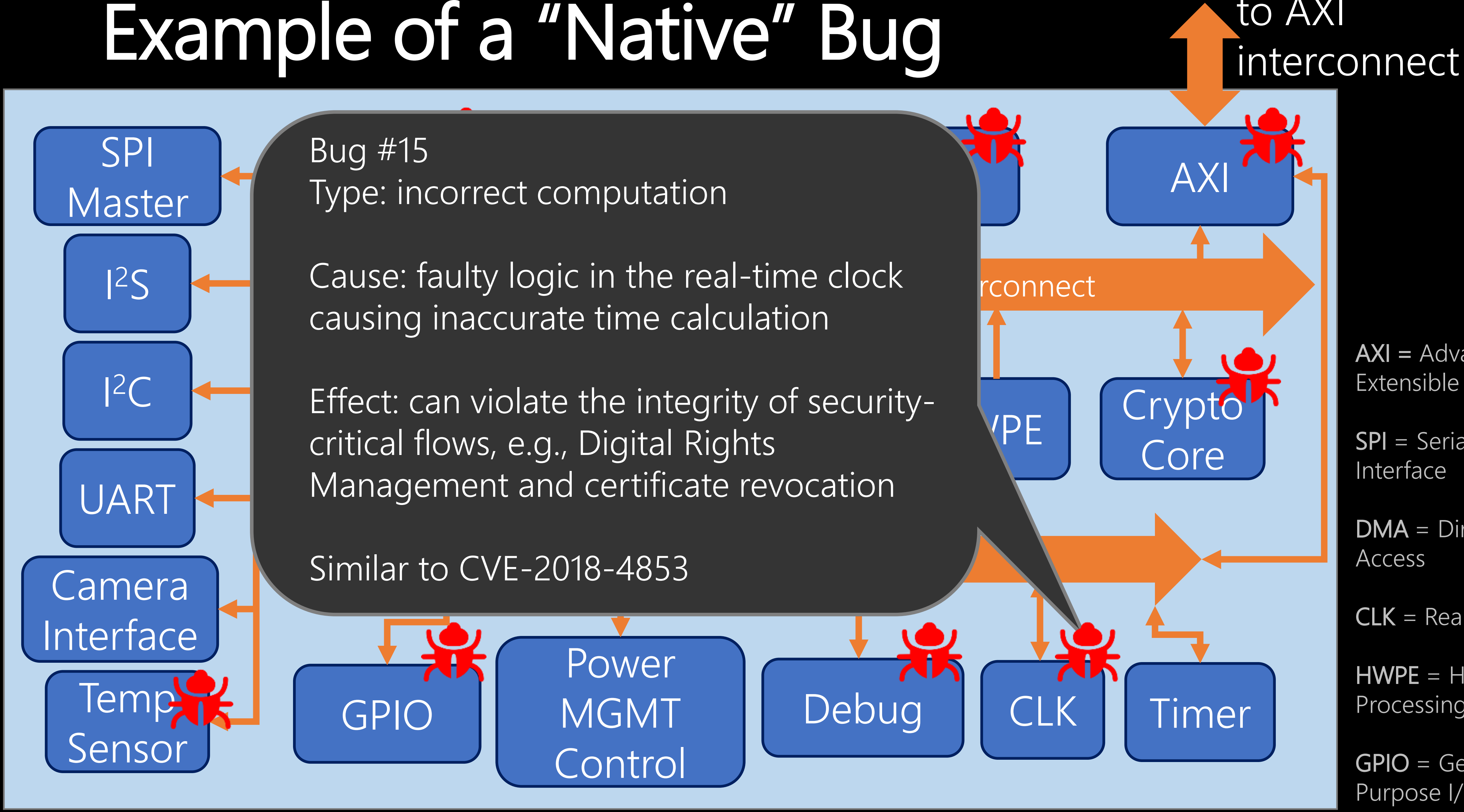
7	AXI address decoder ignores errors.	Inserted (CVE-2018-4850)	✗	✓	✗	1	227	2
8	Address range overlap between GPIO, SPI, and SoC control peripherals.	Inserted (CVE-2018-12206 / (CVE-2017-5704)	✓	✓	✓	68	14635	9.4×10^{21}
9	Incorrect password checking logic in debug unit.	Inserted (CVE-2018-8870)	✗	✓	✗	4	436	1
10	Advanced debug unit only checks 31 of the 32 bits of the password.	Inserted (CVE-2017-18347 / CVE-2017-7564)	✗	✓	✗	4	436	16
11	Able to access debug register when in halt mode.	Native (CVE-2017-18347 /	✗	✓	✓	2	887	1
12	Password check for the debug unit does not reset after successful check.	Inserted (CVE-2017-7564)	✗	✓	✓	4	436	16
13	Faulty decoder state machine logic in RISC-V core results in a hang.	Native	✗	✓	✓	2	1119	32
14	Incomplete case statement in ALU can cause unpredictable behavior.	Native	✗	✓	✓	2	1152	4
15	Faulty timing logic in the RTC results in inaccurate calculation of time.	Native	✗	✓	✗	1	191	1
16	Reset for the advanced debug unit not operational.	Inserted (CVE-2017-18347)	✗	✗	✓	4	436	16
17	Memory-mapped register file allows code injection.	Native	✗	✗	✓	1	134	1
18	Non-functioning cryptography module causes DOS.	Inserted	✗	✗	✗	24	2651	1
19	Insecure hash function in the cryptography module.	Inserted (CVE-2018-1751)	✗	✗	✗	24	2651	N/A
20	Cryptographic key for AES stored in unprotected memory.	Inserted (CVE-2018-8933 / CVE-2014-0881 / CVE-2017-5704)	✗	✗	✗	57	8955	1
21	Temperature sensor is muxed with the cryptography modules.	Inserted	✗	✗	✓	1	65	1
22	ROM size is too small preventing execution of security code.	Inserted (CVE-2018-6242 /) CVE-2018-15383)	✗	✗	✓	1	751	N/A
23	Disabled zero RISC-V core.	Inserted (CVE-2018-12206)	✗	✗	✗	1	282	N/A
24	GPIO enable always high.	Inserted (CVE-2018-1959)	✗	✗	✗	1	392	1
25	Secure mode not required to write to RISC-V core control registers.	Inserted (CVE-2018-7522 / CVE-2017-0352)	✗	✗	✓	1	745	1
26	Advanced debug unit password is hard-coded and set on reset.	Inserted (CVE-2018-8870)	✗	✗	✓	1	406	16
27	Secure mode is not required to write to interrupt registers.	Inserted (CVE-2017-0352)	✗	✗	✓	1	303	1
28	JTAG interface is not password protected.	Native	✗	✗	✓	1	441	1

Some bugs were very difficult to detect

Some bugs could not be detected at all

And some of the teams detected „native“ bugs not injected by us!

Example of a "Native" Bug



Bug #15
Type: incorrect computation

Cause: faulty logic in the real-time clock causing inaccurate time calculation

Effect: can violate the integrity of security-critical flows, e.g., Digital Rights Management and certificate revocation

Similar to CVE-2018-4853

AXI = Advanced Extensible Interface

SPI = Serial Peripheral Interface

DMA = Direct Memory Access

CLK = Real-Time Clock

HWPE = Hardware Processing Elements

GPIO = General Purpose I/O

2 RISC-V SoCs used: PULPino & PULPissimo

Study I: Competition Setup

- Phase I:
  - preliminary qualification where 54 teams participated world-wide over 12 weeks to detect the bugs
  - Pulpino SoC

Study I: Competition Setup

- Phase I:
  - preliminary qualification where 54 teams participated world-wide over 12 weeks to detect the bugs
  - Pulpino SoC

- Phase II:
  - on-site final competition at DAC over an 8-hour time-frame
  - More complex PULPissimo SoC → enabled injection of more advanced bugs

Study I: Competition Setup

- Phase I:
  - preliminary qualification where 54 teams participated world-wide over 12 weeks to detect the bugs
  - Pulpino SoC

- Phase II:
  - on-site final competition at DAC over an 8-hour time-frame
  - More complex PULPissimo SoC → enabled injection of more advanced bugs

- SoCs used are not toy examples yet not overly complex SoC designs for the teams to work with

Methods & Techniques Used by Teams

54 teams participated worldwide over 12 weeks to detect the bugs

Manual Inspection

Dynamic Verification

Formal Verification

Methods & Techniques Used by Teams

54 teams participated worldwide over 12 weeks to detect the bugs

Manual Inspection

- Most popular approach
- Prioritized high-risk areas
- Does not scale to cross-layer & complex bugs
- Relies strongly on human expertise

Dynamic Verification

Formal Verification

Methods & Techniques Used by Teams

54 teams participated worldwide over 12 weeks to detect the bugs

Manual Inspection

- Most popular approach
- Prioritized high-risk areas
- Does not scale to cross-layer & complex bugs
- Relies strongly on human expertise

Dynamic Verification

- **Assertion-based simulation** using SystemVerilog
- **Software-based testing**: running C code to try and trigger memory accesses to privileged memory

Formal Verification

Methods & Techniques Used by Teams

54 teams participated worldwide over 12 weeks to detect the bugs

Manual Inspection

- Most popular approach
- Prioritized high-risk areas
- Does not scale to cross-layer & complex bugs
- Relies strongly on human expertise

Dynamic Verification

- **Assertion-based simulation** using SystemVerilog
- **Software-based testing**: running C code to try and trigger memory accesses to privileged memory

Formal Verification

- Tried but failed
- Limited scalability
- Extensive expertise & time required to use the tools

Students

TECHNISCHE
UNIVERSITÄT
DARMSTADT

- Ghada Dessousky (Ph.D)
- Pouya Mahmoody (Ph.D)

- Rahul Kande (Ph.D)
- Chen Chen (Ph.D)
- Georges Alsankary (Ph.D)
- Bhagyaraja Adapa (Ph.D)
- Garrett Persyn (Grad)