Behind the fog in the Cybersecurity

TEAs on the Noel-V platform

Gianluca Furano[2], Elia Lazzeri[1 3], Luca Cassano[1]

[1]Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Italy

[2]European Space Research and Technology Centre, Europeran Space Agency, The Netherlands

[3]IONION, Milano, Italy

RISC-V in Space, Gothenburg, Sweden

What is Cybersecurity ?

What is Cybersecurity?

It is not only about cryptography and quantum/post-quantum stuff


Worrying today about
quantum threats is like
buying furniture before
you have decided to buy a house.
CHANGE MY MIND
imgflip.com

So what is it?

What is Cybersecurity?

Why should we worry about the other side?

Space data systems:

- it’s (part of) a critical infrastructure
- it’s becoming “open” to third party users
- its security perimeter is getting far bigger

Stuxnet worm 'targeted high-value Iranian assets'

Top stories

LIVE Plans to reform welfare system and cut benefits bill being announced in Parliament

BBC Sign in | Home | News | Sport | Business | Innovation | Culture | Travel | ... | Search BBC

NEWS

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | Asia | UK | Business | Tech | More

Tech

Stuxnet worm 'targ
Iranian assets'

The New York Times

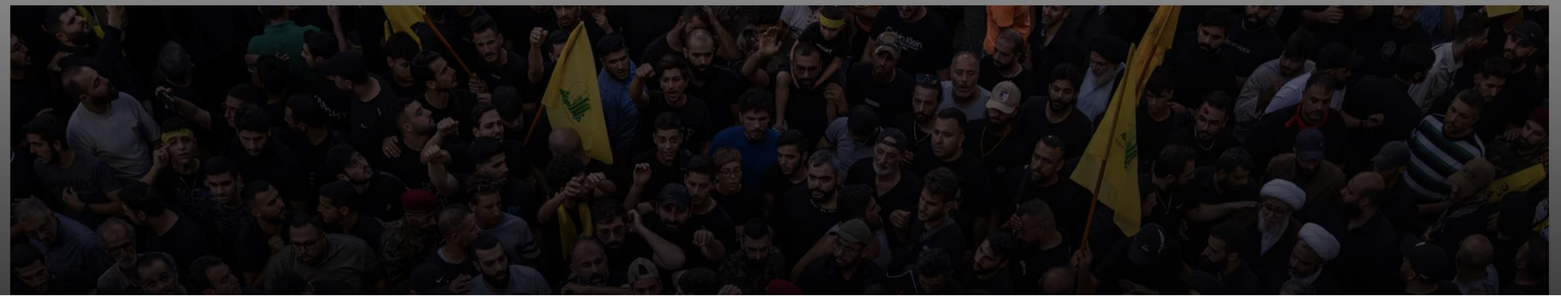
SUBSCRIBE FOR $0.

Middle East Tensions | LIVE Updates 5m ago | Deaths of Hostages | Israel-Lebanon Border Talks | Israeli Aid Block in Gaza | Syrian Druse Pilgrims Visit Israel

How Israel Built a Modern-Day Trojan Horse: Exploding Pagers

The Israeli government did not tamper with the Hezbollah devices that exploded, defense and intelligence officials say. It manufactured them as part of an elaborate ruse.

Listen to this article · 8:05 min Learn more | Share full article | 2.6K



We need to worry about the whole Cybersecurity picture to protect space assets from powerful actors or foreign governments

Let’s now talk about

Transient Execution Attacks (TEAs)

Background

Timing Attacks

Sophisticated side-channel attacks that exploit the time to access specific data or execute instructions to infer sensitive information.

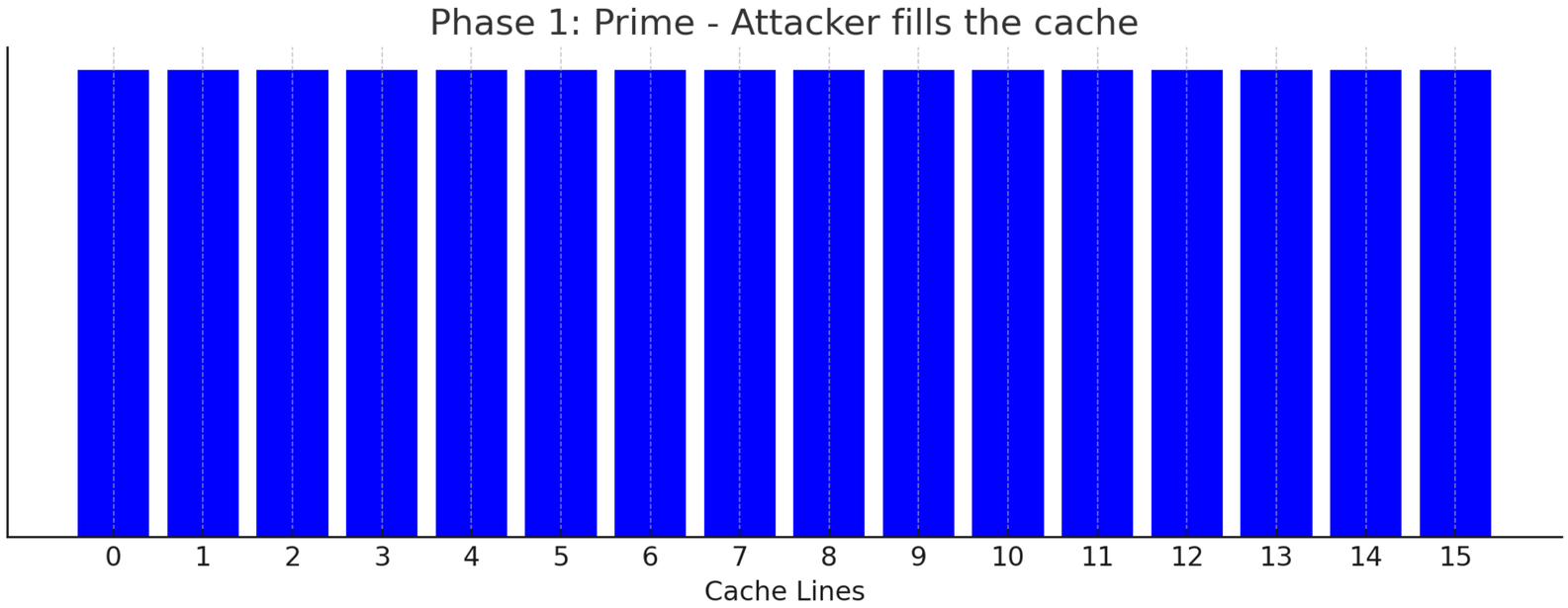
Examples:

- Prime+Probe
- Flush+Reload
- Evict+Reload
- Flush+Flush

Prime+Probe

Detailed Explanation

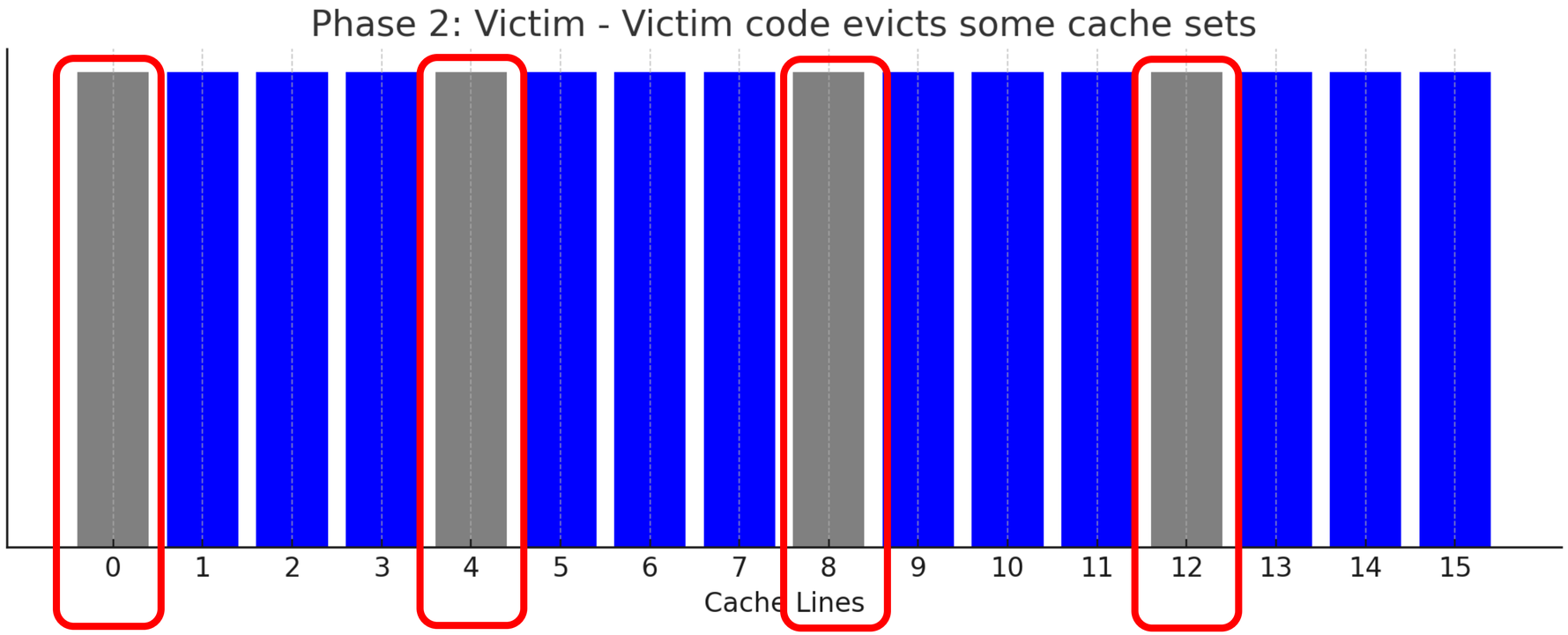
Attacker code in execution



Prime+Probe

Detailed Explanation

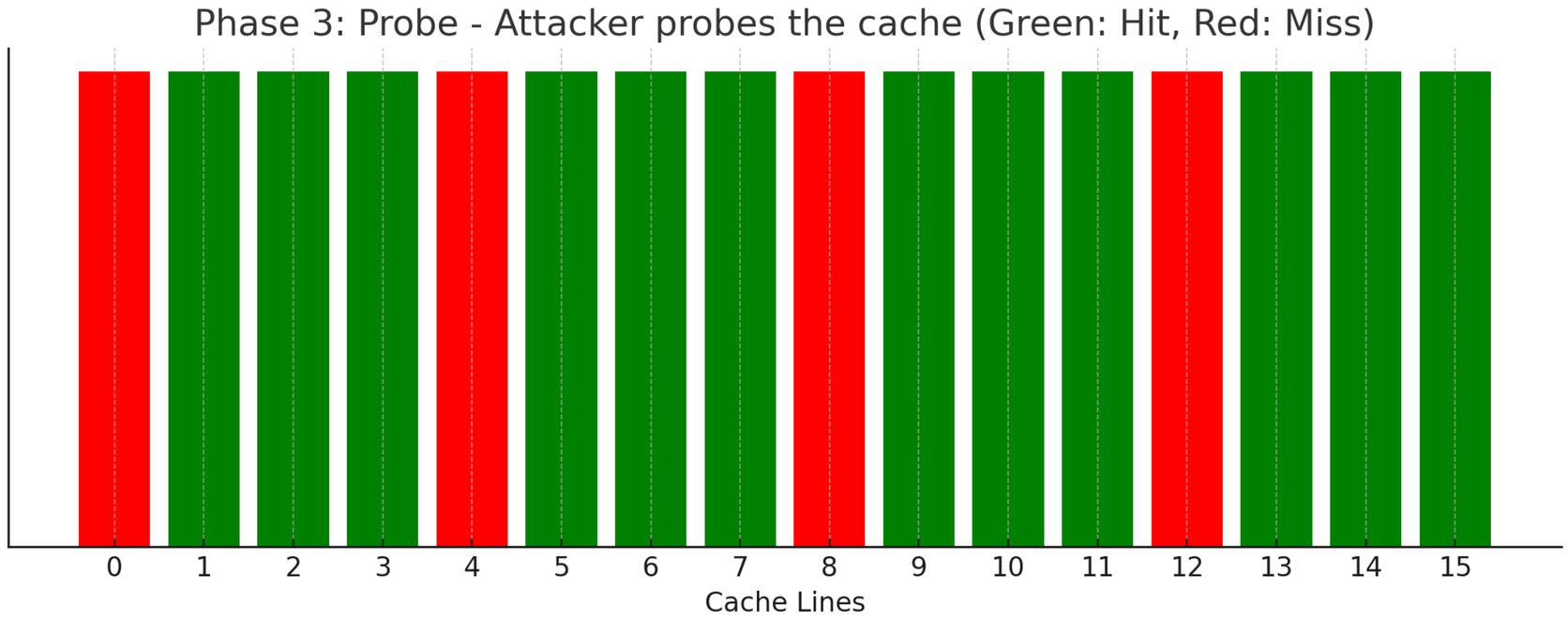
Victim code in execution



Prime+Probe

Detailed Explanation

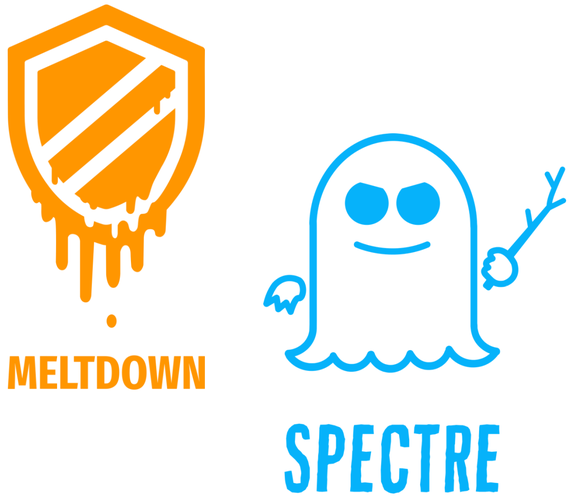
Attacker code in execution again



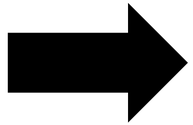
Background

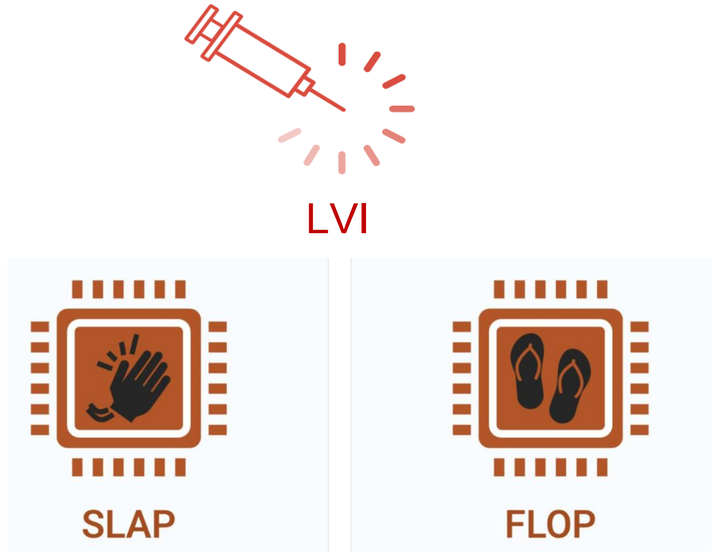
Transient Execution Attacks (TEAs)

TEAs, born with Spectre and Meltdown (January 2018), exploit speculative and out-of-order execution in modern processors.



Then





Now

What have we done?

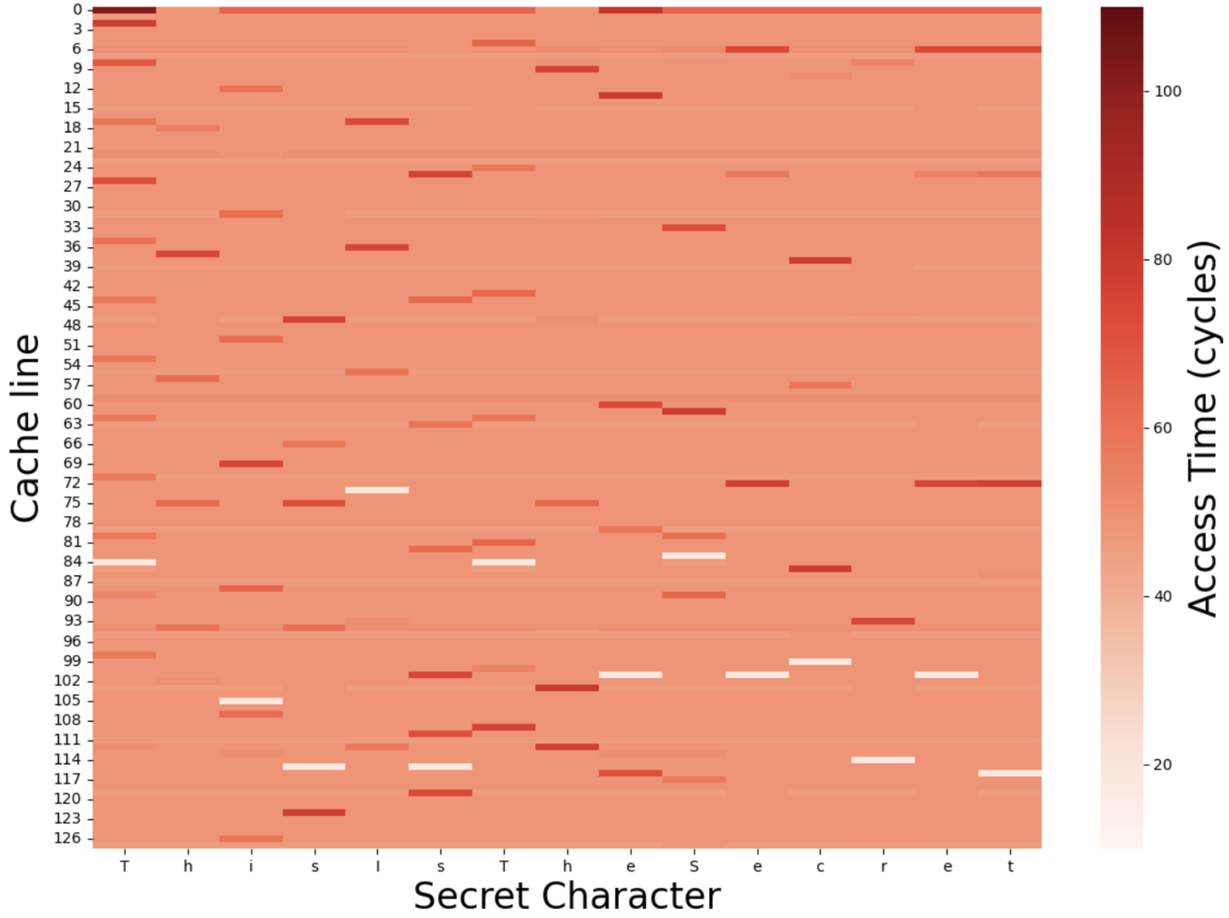
Experimental Setup

AMD Virtex UltraScale+ FPGA VCU118 Evaluation Kit

- FPGA Device: Xilinx XCVU9P-L2FLGA2104E FPGA.
- Memory: 5GB DDR4.
- PCIe Gen3 x16.

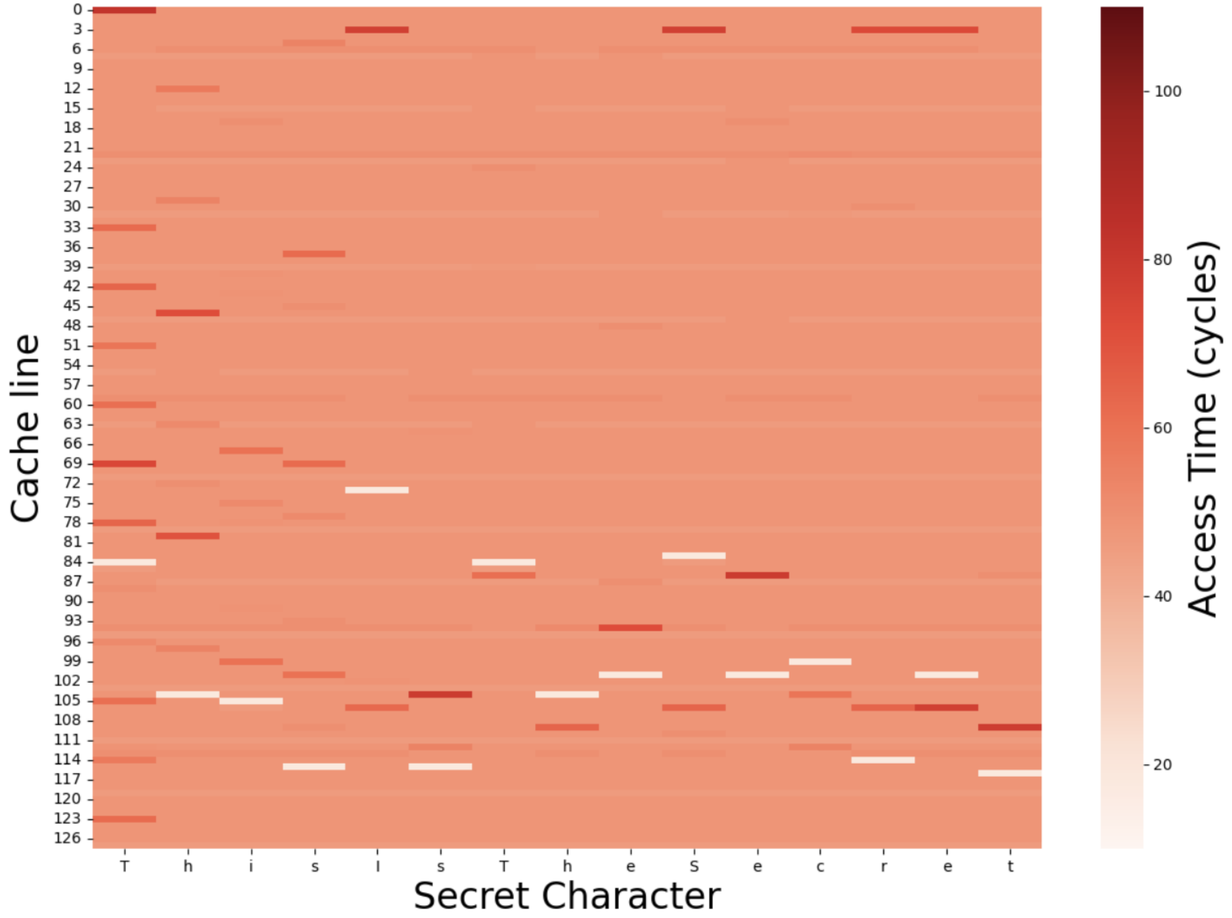
Security Assessment

Spectre V1 on the Noel-V Platform



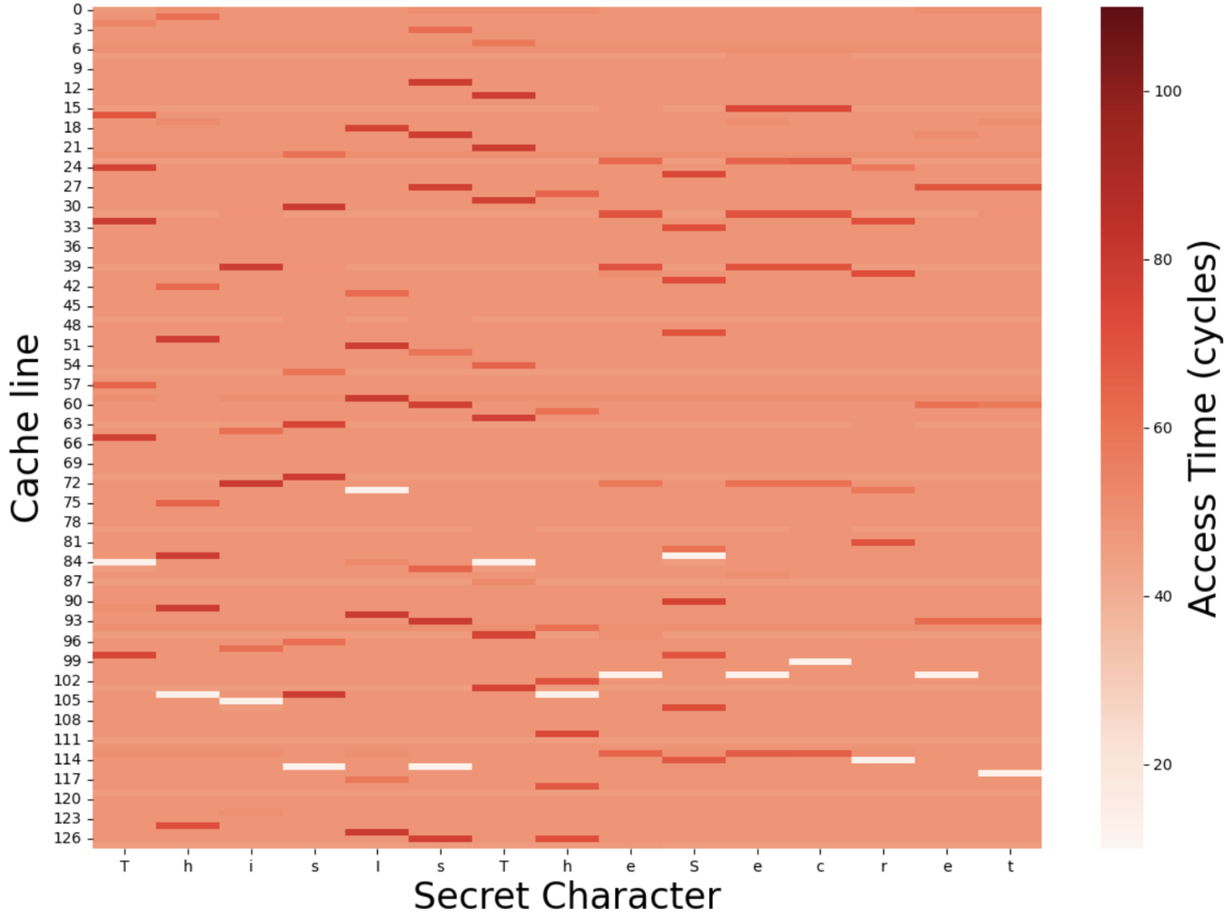
Security Assessment

Spectre V2 on the Noel-V Platform



Security Assessment

Spectre RSB on the Noel-V Platform



IT IS NOT ONLY ABOUT NOEL-V

We executed multiple TEAs even on CVA6 and BOOM, in addition we are testing multiple others (SiFive, Microchip, NaxRiscv, …..)

All the tested architectures are sensitive to TEAs

Conclusions

Conclusions

1. The mechanisms that allow TEAs are currently exploitable even in RISC-V processors

Conclusions

1. The mechanisms that allow TEAs are currently exploitable even in RISC-V processors

2. As the space field grows and opens to new user, space regulators/agencies/designers/component manufacturers should stop worrying only about cryptography and start addressing other cybersecurity problems

Conclusions

1. The mechanisms that allow TEAs are currently exploitable even in RISC-V processors

2. As the space field grows and opens to new user, space regulators should stop worrying only about cryptography and start addressing other cybersecurity problems

3. We should try to not copy the same errors that ARM and x86 (AMD and Intel) have made

Want to test your processor design against TEAs?

elia.lazzeri@polimi.it

Write us!

We would like to thank