CHERITech'26
CONFERENCE

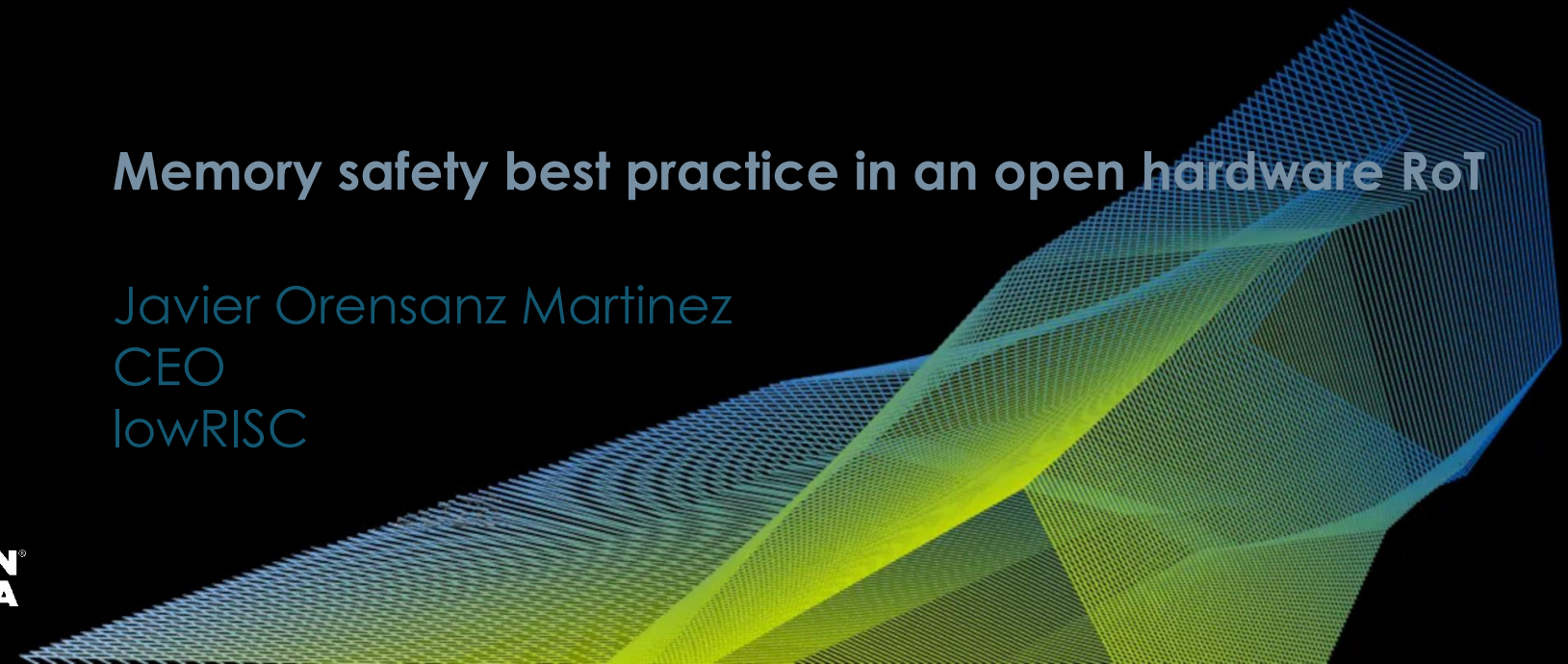
12–13 Nov 2026
Munich, DE

Located at semi | SEMICON EUROPA

CHERI in OpenTitan

Memory safety best practice in an open hardware RoT

Javier Orensanz Martinez
CEO
lowRISC



About lowRISC

Making open-source silicon a reality, commercially relevant, and widely adopted throughout the industry

- Regulated not-for-profit, established in Cambridge UK in 2014
- Neutral stewards of Ibex and OpenTitan
- 35 engineers covering security, design, verification, software
- Owners of NewAE: ChipWhisperer and ChipShouter

opentitan

RISC-V® FOUNDING

CHERI Alliance Founder

About OpenTitan

The world's most active open silicon project

- Open source - Apache 2.0
- Discrete or integrated
- Commercially proven
- Strongly backed by Google

Google Open Source Blog

The latest news from Google on open source releases, major projects, events, and outreach programs for early career developers.

OpenTitan shipping in production

Wednesday, March 4, 2026

by Cyrus Stoller & Miguel Osorio, OpenTitan

Last year, we shared the exciting news that fabrication of production OpenTitan silicon had begun. Today, we're proud to announce that OpenTitan® is now shipping in commercially available Chromebooks.

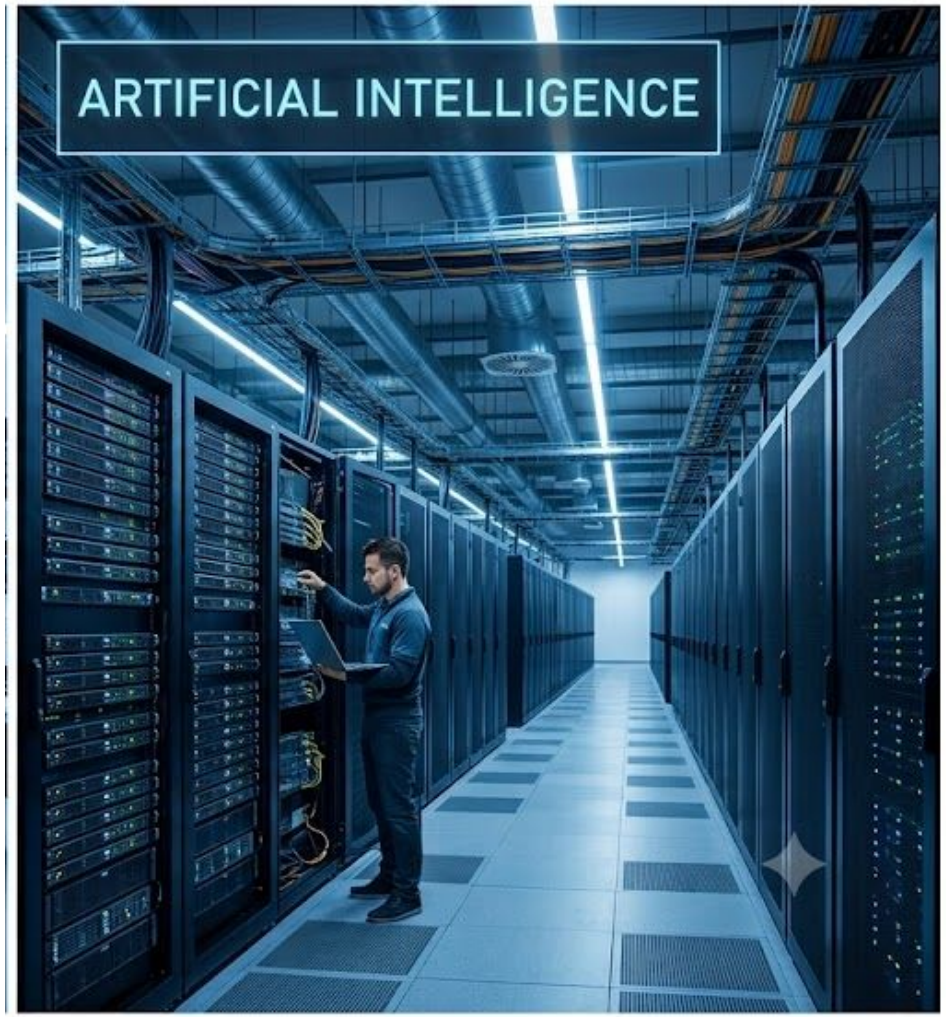
The first OpenTitan part is being produced by Nuvoton, a leader in silicon security.



Hackers have gained superpowers

AI models supercharge software attacks

- Scanning for open ports
- Cross-referencing known vulnerabilities
- Finding or creating exploitation code
- Mimicking the behaviour of normal software



Two big reasons for CHERI

Protection against memory attacks

When humans are out of the loop, memory attacks are the most common type of cyber attacks

CHERI protects any code against memory attacks **in the hardware**: you just need to rebuild it

Minimizing the damage of a hack

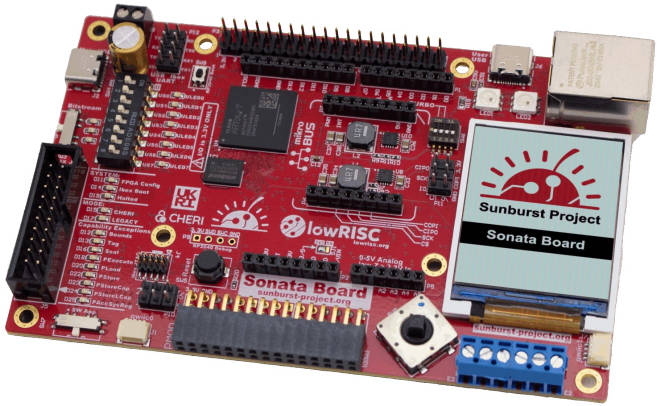
CHERI enables highly granular code compartmentalization

Even if a device or computer is compromised, the hacker cannot use it to gain access to the rest of its code

CHERI is in all of lowRISC's current projects

Sonata board

CHERIoT-Ibex reference implementation



CHERI-Mocha

CVA6-CHERI Linux-capable RISC-V processor

High-performance Secure Enclave reference design

CHERI

OpenTitan Earl Grey 2

Ibex implementation with hybrid CHERI configuration

Protected against fault injection and side-channel attacks

opentitan

Why CHERI in OpenTitan

Physical isolation is not enough

RoTs are becoming more powerful, able to run more complex software stacks

Third party code will creep in, even in discrete devices

PPA impact is negligible

CHERI performance is much higher than software protection

CHERI area is marginally higher than an ePMP, which it can replace

Detailed paper on lowrisc.org

Rust is not a solution for everyone

Can you ensure that all software running on your RoT will be secure?

Is there any Unsafe Rust code in your stack?

CHERI in OpenTitan

Security hardened version with the latest SCA and FI countermeasures

Hybrid CHERI mode

Boot in legacy RISC-V mode, switch to CHERI (you can't switch back)

Use legacy, certified software

Enable easy performance comparison between modes

Availability

Design functionally complete

RTL simulation and CW340 FPGA boards available now

RTL freeze Q1 2027



CHERI

THANK YOU

Contact contact@cheri-alliance.org

Web www.cheri-alliance.org

Located at semi | SEMICON EUROPA

CHERI™ and the CHERI logo are protected trademarks. Use of these marks is subject to the CHERI Alliance Trademark Policy – https://cheri-alliance.org/legal-and-policies/trademark/

This work © 2026 by CHERI Alliance is licensed under CC BY-SA 4.0 (Creative Commons Attribution-ShareAlike 4.0 International) – https://creativecommons.org/licenses/by-sa/4.0/