



Defend Against Modern Cyber Threats

What is CHERI?

CHERI (Capability Hardware Enhanced RISC Instructions) is a revolutionary computer architecture improving software security while keeping performance intact.

Why does CHERI matter?

- Prevents ~ 70% of the causes of cyberattacks (memory safety issues)
- Hardware protection to secure software – can even protect existing code!
- Adds security with minimal impact and costs

How It Works

CHERI replaces traditional pointers with secure “capabilities,” enforcing memory access rules and permissions to keep programs safe, and brings strong isolation between software functions

Key Benefits

1. Memory Safety: Stops bugs and attacks like buffer overflows
2. Precision Control: Assigns specific permissions for data access
3. Compatibility: No need to rewrite code!

Where It Helps

CHERI can be applied to any system, from tiny embedded IoT devices to large data centres, and everything in between. It immediately brings a much higher level of security, by design.

Join the CHERI Revolution!

Explore safer computing and built-in security at cheri-alliance.org

