National Cyber Security Centre
a part of GCHQ

CYBERUK 2023

Stream C

Securing foundations for technology advantage

Sponsor: ULTRA

Digital Security by Design
The imperative of change…..the past, present and future.

Siân John MBE

Senior Director
Microsoft Security Business Development

Digital Security by Design is an initiative supported by the UK Government to transform digital technology and create a resilient, and more secure foundation for a safer future.

Challenge Aim

By 2025, DSbD aims to overcome the market failures and radically update the foundation of the insecure digital computing infrastructure that underpins the entire economy.

How, why and when did **Microsoft** get involved in DSbD ?

National Cyber Security Centre
a part of GCHQ
CYBERUK 2023

UKRI
Delivered by Innovate UK, EPSRC and ESRC

CHERI Research – Microsoft engagement

- Mitigates vulnerabilities in existing code and provides tools to build new security models
- Gives much stronger security than traditional methods (privilege levels and a memory protection unit) with similar hardware requirements
- Safe languages such as Rust or Verona improve availability but not confidentiality or integrity.
  - Unsafe code still exists in Rust codebases.
  - CHERI makes code memory safe and limits impact of bugs
- Microsoft developed CHERIoT – implementation of CHERI for IoT ecosystem
- Open sourced CHERIoT and encouraging external collaborators to contribute.

Digital Security by Design

Why Google Likes CHERI

Ben Laurie

Principal Engineer
Google Research

Agenda

- Memory Safety
- Compartmentalisation
- Better, Simpler Security

Memory Safety

70% of security vulnerabilities are caused by buffer overflows.

We all know we should be using memory safe languages. But for systems programming there’s really only one game in town: Rust.

But…

Memory Safety

Rust is memory-safe … except for when it isn't - realistically, you can't write useful code without at least some unsafe code.

And probably some assembler, too.

And…

Memory Safety

We have billions of lines of system code that is in C or C++ and there is no way we can (or will) rewrite it all in Rust.

Porting most C/C++ code to CHERI is quite simple - <.03% of code changes and almost all of those changes are trivial.

Once ported, we get memory safety almost for free

Compartmentalisation

Even with memory safety, we still need to isolate processes from each other. In fact, we get a lot of benefit from splitting single applications into multiple compartments.

But traditional memory management makes this expensive. CHERI makes it cheap

Better, Simpler Security

Finally, the complexity of modern computers and their TCBs is a significant challenge.

CHERI promises a radical simplification of the lower layers of future generations of computer, as illustrated by Microsoft’s fantastic CHERIoT experiment, which has a TCB of less than 300 instructions.

Thank You

Ben Laurie

Principal Engineer

benl@google.com