My name is Marno van der Maas and thank you very much for being interested in Sonata! This handout is made for the State of Open Con 2024. My talk was on Tuesday, 6 February from 13:30 to 14:00 (including questions and changing speakers). More information can be found at this URL: https://sched.co/1X143.
Sonata
Introduction

Putting CHERIoT hardware in the hands of embedded systems engineers

The Sunburst project aims to put CHERI hardware in the hands of embedded system engineers. Find out more on our website: https://www.sunburst-project.org/. We have regular technical interest group meetings.

We are doing so by creating two boards: Sonata and Symphony. Sonata is a low-cost system that is built for ease of development and accessibility. Symphony is a more comprehensive design which is more realistic but also more expensive. This talk focuses on Sonata.
Here’s a render of an initial version of the Sonata board! The goal here is to make a fully open source platform to get CHERI hardware in the hands of embedded systems engineers. Creating this platform in the open source takes CHERI to the next level on the path to commercialization. Sonata is easy to use, for example USB provides power, allows programming the FPGA and can be used as a serial UART terminal.
lowRISC is in a unique position to make this a reality. We are celebrating our tenth anniversary this year and have coordinated the OpenTitan project for a large chunk of that time. OpenTitan is the first production-ready chip that is open source. Last June we hit the important milestone of RTL freeze.

We also recently acquired NewAE which has vast experience creating PCBs that are easy to use along with support and training material.

- https://www.lowrisc.org
- https://www.opentitan.org
- https://www.newae.com
First let’s take a step back and talk about what CHERI is all about. CHERI stands for capability hardware enhanced RISC instructions. It is a way to address memory vulnerabilities in unsafe languages like C and C++. CHERI does this by using capabilities instead of pointers. This means that, as well as addresses, bounds and permissions are used during memory accesses as well as a validity tag that can only be manipulated by hardware.

On the slide you see what a capability could look like for an embedded 32-bit processor:

- **perms**: 6-bit compressed permissions field
- **ot**: 3-bit 'object type' used for sealing capabilities (important for compartmentalization)
- **bounds**: compressed encoding for the base and the top bounds of the capability
- **address**: 32-bit address of the capability

All of this is based on more than a decade of research at the University of Cambridge and SRI International: [https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/](https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/)
Microsoft Security Response Center analyzed all the vulnerabilities they responded to in 2019 and determined that CHERI would have deterministically mitigated at least two thirds of them. This has huge potential to improve the security of our computing systems and alleviate the huge economic costs that are associated with patching these vulnerabilities.

CHERIoT is a variant of CHERI specifically designed for embedded systems and with a strong focus on compartmentalization and temporal safety. The capability format I showed earlier is actually a CHERIoT capability. David Chisnall is giving a talk on Wednesday 7 February, where he will talk about CHERIoT as a platform for secure IoT devices. Please go along to his talk to get a better understanding of the platform as a whole and the details of CHERIoT. Talk link: https://sched.co/1Xl3T

A lot of research has been done on CHERI (steps 1-3 of TRL). Recently development has gotten more attention (steps 4-6). We want to push CHERI and CHERIoT technology further up the development stages and into the deployment stages.

There has been some work in the development stages, for example Arm Morello has proposed an initial version of CHERI in the Arm ISA including shipping a number of demonstration boards. However, we believe a RISC-V platform based on open hardware/silicon will improve accessibility to this platform. This is especially true for embedded systems and thus a good way forward in the long run.
A lot of the initial CHERI research was done on application class processors and proving that the technology could work with rich operating systems, third party applications, a large codebase and modern compilers. This was important to prove the technology.

We believe in the step towards commercialization, embedded systems may be a better place to start because vendors usually have more control over the whole software stack and can recompile everything to use pure capability. Sonata can provide the open source platform to make this happen.
Sonata is all about being usable, debuggable, connectable, extendable and interactive. To achieve all of this, we need a balance of IP blocks which you can see in this block diagram. There is also a big focus on configurability. For example the pinmux can be used to drive an LED by a PWM instead of a GPIO. And the number of I2C, SPI and UART devices is configurable.
We support many standard interfaces to connect embedded systems. It is important for Sonata, as a development board, to be connectable to as many systems as possible.

- I2C: inter-integrated circuit
- SPI: serial peripheral interface
- UART: universal asynchronous receiver and transmitter
- GPIO: general purpose input and output
And any niche use-cases can be achieved using any of the extension headers provided. You can buy off the shelf boards to for example add wireless functionality. The hat, shield and click have connectors on the top of the board. QWIIC uses I2C to daisy chain boards together (two connectors on the side). There are two PMOD connectors on the bottom as well as RS-232 and RS-485 connectors.
The CHERI research benefited from open source projects such as FreeBSD and LLVM. CHERIoT
Ibex exists because of open architecture (RISC-V, CHERI ISAv9 and CHERIoT ISA) and open
silicon (Ibex core).
The fully open nature of Sonata (RTL, DV, Board layout, software etc) will in turn provide many
opportunities for others to continue building on this work. Open source can work well to drive
innovation and Sonata is playing its part in the CHERI story here.

- https://github.com/microsoft/cheriot-ibex
The idea for Sonata is to be the open source platform that can bring all these efforts together. This means taking the work done on open standard instruction set architectures, CPU implementations, compilers, operating systems and software to put them together in an open source platform for embedded systems.
Through our partnership with UKRI we are providing 100 free Sonata boards to enable embedded hardware development with CHERI. Our project has the following UKRI/DSbD grant number: 107540. The boards will also be commercially available afterwards. The picture on the slide shows our prototype board running an LCD demo.

As part of this effort we will also be providing training and documentation to help propel the use of CHERI technology forward.
lowRISC’s motto is “open to the core”. Therefore everything is open source from the documentation to the RTL design and to the PCB design. The PCB is being manufactured by NewAE technologies, which is a company part of the lowRISC family. Here are some links:

- https://github.com/lowRISC/sonata-system
- https://github.com/newaetech/sonata-pcb
- https://lowrisc.org/sonata-system/
As an example here is part of the PCB schematic published on: https://github.com/newaetech/sonata-pcb
Please feel free to contact me about this project. We also have a working group that you can join. More detailed information can be found on our website. Scan the QR code for the handout.

Official website: https://www.sunburst-project.org/