Enabling the Arm Morello Platform

Mark Nicholson: Technology Manager
Arm Central Engineering: OSS
mark.nicholson@arm.com
Introduction

- Morello and software security
  - Morello introduces hardware support for Capabilities
    - Pointers with associated limitations on allowable address ranges and functionality
    - Enables development of fine grained memory protection using Compartments
  - Based on the CHERI architecture developed by the University of Cambridge
    - University Cambridge Morello extended FreeBSD stack under development

- https://developer.arm.com/architectures/cpu-architecture/a-profile/morello

Morello is a prototype architecture

- Morello specific software will not be upstreamed, but will be maintained for the lifetime of the project

- Arm are creating an experimental Morello platform implementation
  - Enables eco system research on viability of future Capability architectures and approaches to security
  - A software model (FVP) and development board will be produced

- Open Source Software is being developed to support the platform

Arm and consortium Partners funded by UKRI (https://www.ukri.org/) grant
Overview – Arm software enablement activities

Platforms and milestones

- **October 2020**
  - FVP model
- **October 2021**
  - Development board

General platform Enablement

- **AArch64 platform software stacks**
  - Platform ports for firmware. Operating System support.
- **Hardware bring up**
  - FPGA, SoC, development board. SBSA compliance testing.

Morello Architecture Enablement

- **Morello architecture support**
  - Toolchain, libraries, Kernel development. Prototype userspace examples

Linaro and ecosystem access

- **Ecosystem software access**
  - Infrastructure provision, future engineering support and maintenance
A Morello Platform (FVP: Fixed Virtual Platform) model will be available to support ecosystem software development.

Arm FVP models use binary translation technology to deliver fast simulations of Arm-based systems:
- Providing a functional (programmer’s view) model of the hardware platform IP implementation
- FVPs are an integral part of Arm’s software development process for pre-silicon IP

### Morello FVP Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free to access - not subject to hardware availability</td>
<td>Does not provide timing/cycle count information</td>
</tr>
<tr>
<td>Supported by same software stacks as hardware platform</td>
<td>Modelling of some peripheral components is limited or abstracted</td>
</tr>
<tr>
<td>Models same mix of IP as hardware</td>
<td>Typically impacts 3rd party peripherals (PCIe, USB, memory controllers etc)</td>
</tr>
<tr>
<td>• Functional register level modelling of Morello CPU, and interconnect implementations</td>
<td>• Memory and interrupt maps and system architecture aligned with hardware</td>
</tr>
<tr>
<td>• Ethernet support</td>
<td></td>
</tr>
</tbody>
</table>
Platform software stacks

- Arm will provide platform ports of firmware based on standard open source software projects
- Enables boot of standard (AArch64) Operating System hosting development environments – providing a basis for security architecture research
  - Linux-based Android and Distro environments (e.g. Ubuntu). WinPE boot testing
Software components for the Morello architecture

- Morello is a prototype architecture (not available to license for product development)
- Support for the C64 instruction set and ABI will be maintained in forks and not upstreamed

October 2020
- FVP model

October 2021
- Dev board

Linux Kernel (Morello ABI 128bit syscall interface)
- Early limited interface
  - Reliant on BIONIC library “shim”
- Generic Kernel ABI definition
  - Developed alongside library support

C Library
- BIONIC Android C lib
  - Early “shimmmed” syscall implementation
  - static linkage only
- BIONIC and glibc development
  - glibc enables Distro environments

Toolchain support
- LLVM toolchain
  - ABI compliant primary toolchain and utilities. (+ gas support for Kernel)
- GNU/GCC toolchain
  - Evolving support
Planned release features

2020 FVP, software feature targets

- Android focused MVP (Minimum Viable Product) release
- LLVM toolchain for Android development
- Android “shimmed” BIONIC C library (static linkage only)
- Initial userspace ports of specific Android framework components
  - e.g. logd, servicemanager
  - Basic compartment manager example

Predominately targets console based “nano Android” development

2021 Dev Board, software feature targets

- Kernel and BIONIC evolution
- Initial GCC toolchain and glibc support
- Initial Distro support
- Graphics enablement

Specific timelines and commitments still being identified
Ecosystem access to Morello software

• Arm are working with Linaro to provide access to Morello software
  - Linaro will provide the infrastructure to deliver and maintain Morello software for the life time of the project
    - Code repositories, issue tracking, patch submission management
    - Engineering maintenance

• How will Morello Software be delivered?
  - Software and toolchain support for Morello will be hosted in public code repositories (git projects).
    - New Morello specific repositories for forked components
    - Firmware support may exist as platform ports in upstream projects

• A platform repository will support configuration of a development environments, this will include:
  - A manifest (or Yocto recipe) for each stack configuration
    - Defines a set of tagged releases of component projects - tested together as an integrated software stack
  - Instructions and scripting
    - Describing how to download/configure a suitable workspace and build the stack
Cambridge University CheriBSD stack

- Parallel DARPA/UKRI sponsored work undertaken by Cambridge University
  https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/cheri-morello.html

- Morello-extended FreeBSD and third-party applications
  - Full memory-safe OS implementation including kernel and userspace, with support for multiple CHERI compartmentalization models, by October 2020

DARPA software prototype stack on Morello

- Complete hybrid software stack from bare metal up: compilers, toolchain, debuggers, operating systems, applications

- Open-source application suite
  (WebKit, Wayland, Python, OpenSSH, nginx, PostgresQL …)

- CheriBSD/Morello (DARPA)
  - FreeBSD kernel + userspace, application stack
  - Kernel spatial and referential memory protection
  - Userspace spatial, referential, and temporal memory protection
  - Intra-process compartmentalization

- Android (Arm)

- CHERI-extended Google Hafnium hypervisor

- CHERI Clang/LLVM compiler suite, LLD, LLDB, GDB

- Focused on deploying CHERI incrementally, rather than clean-slate
Questions ?
Thank you

Accelerating deployment in the Arm Ecosystem