(The First?)

CHERI Microkernel Workshop

Robert N. M. Watson and Simon W. Moore
University of Cambridge

Peter G. Neumann
SRI International

CHERI Microkernel Workshop – 23 April 2016
Welcome to the
Computer Laboratory

• When the building catches fire, you want to go
down the stairs and out the front door

• We are in room FW11

• Tea/coffee/food is in room FW09

• Room FW08 is also available as a breakout room

• Toilets are on the ground floor opposite the café
The (working) plan

• 10:30 start
• 12:30(ish) lunch
• Afternoon(ish) finish (15:00? 17:00?)
• Dinner if you would like to join us (tell us soon)

• Talks with discussion
• Followed by discussion, white boarding, and general schmoozing
THE WORKSHOP
Why are we here?

• CHERI is strongly influenced by historic microkernel thinking
  • E.g., HYDRA, PSOS, Mach, etc.
  • “The Machine” NewOS workshop in ETH Zurich:
    How could architectural capabilities affect microkernel design?
• CHERI brings several architectural features to the table:
  • Fine-grained memory protection within address spaces
  • Scalable software compartmentalization with efficient memory sharing
  • Strong compatibility with MMU-based VM / C-language model
• But CHERI microkernels mean different things to different people
Hybrid architecture → hybrid OS?

• **Multi-address-space OS**
  + CHERI memory protection within tasks – and kernel?
  + CHERI for kernel bypass on capability operations
  + CHERI to compartmentalize within microkernel

• **Single-address-space OS**
  + CHERI compartmentalization model – some MMU use
  + CHERI compartmentalization model – MMU for full-system virtualization only
  + CHERI compartmentalization model – no MMU use

• And what about convergence with **language runtimes**?
Goals

• Help all understand the CHERI baseline
• Identify common interests across a broad set of microkernel research communities
• Explore models for architectural capability use in microkernel and microkernel-like designs
• Discuss potential collaborations to explore those
• Ponder whether there are architectural gaps in CHERI that could/should be filled
• Think more fundamentally about capabilities
INTRODUCTIONS
## Current talklet list

<table>
<thead>
<tr>
<th>Talklet</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHERI introduction + architecture</td>
<td>Robert Watson</td>
</tr>
<tr>
<td>CHERI models</td>
<td>Simon Moore</td>
</tr>
<tr>
<td>CHERI C + compiler</td>
<td>David Chisnall</td>
</tr>
<tr>
<td>CheriBSD OS model</td>
<td>Robert Watson</td>
</tr>
<tr>
<td>CheriABI process model</td>
<td>Brooks Davis</td>
</tr>
<tr>
<td>CheriBSD compartmentalization model</td>
<td>Robert Watson</td>
</tr>
<tr>
<td>CheriOS microkernel</td>
<td>Hadrien Barral</td>
</tr>
<tr>
<td>CHERI models and proofs</td>
<td>Peter Sewell</td>
</tr>
<tr>
<td>CHERI and The Machine</td>
<td>Dejan Milojicic</td>
</tr>
<tr>
<td>L4 capability model</td>
<td>Adam Lackorzynski</td>
</tr>
<tr>
<td>SeL4 capability model</td>
<td>Matthew Grosvenor</td>
</tr>
<tr>
<td>Barrelfish capability model</td>
<td>Timothy Roscoe</td>
</tr>
<tr>
<td>Language capability models</td>
<td>Ben Laurie</td>
</tr>
</tbody>
</table>