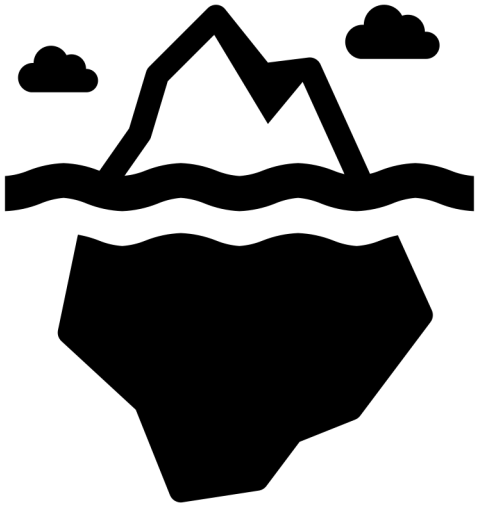
Arm64 live patching

Mark Rutland <mark.rutland@arm.com>

Where is livepatch on arm64?

- We need to enable CONFIG_HAVE_RELIABLE_STACKTRACE=y
  - But the actual unwinder is the tip of the iceberg
- Lots of preparatory work has been done, e.g.
  - FTRACE_WITH_{REGS,ARGS,CALL_OPS} for the actual patching
  - Data-driven extable fixups to avoid incorrect unwinds
  - Templated/unified entry assembly
- Several known unwinding issues to be dealt with
  - **Unwinding across exception boundaries**
  - Gaps in ftrace/kretprobe return trampolines
  - False positives with noreturn functions
  - Non-AAPCS64 assembly functions/trampolines

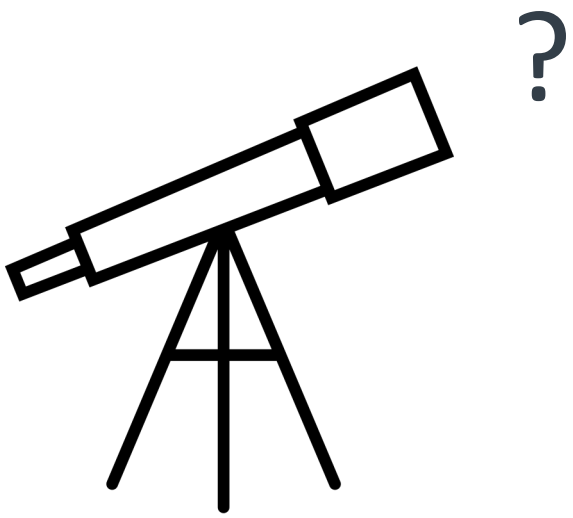


Unwinding across exception boundaries

- At exception boundaries, liveness+provenance of **LR** and **FP** is unknown
  - Always starting from **FP** has false negatives
  - Always starting from **LR** has false positives
- Unwinding across exception boundaries is important
  - Essential for proposed preemption changes
  - Faster, better forward progress
  - Useful for developers and users (e.g. panic(), perf unwinds)
- We need metadata and/or codegen restrictions
  - Reverse engineered metadata not ok
    - LPC 2021 “Objtool on arm64” - https://lpc.events/event/11/contributions/971/
  - Compiler generated metadata ok in theory
    - SFrame might be sufficient

What's the plan?

- Continue getting useful prerequisites upstream
  - Passs additional data to arch_stack_walk() callbacks
    - Opaque arch_unwind_state with accessors
    - Useful for BPF, dump_backtrace(), etc
  - Explicit identification of exception boundaries
    - Allows logging ambiguous LR values
    - Useful for humans reading backtraces
  - Fix gaps in ftrace/kretprobe return trampolines
    - Useful for humans reading backtraces
- Prototype SFrame kernel unwinder
  - Hybrid with existing FP unwinder, used for exception boundaries
  - Identify and report feedback for gaps (e.g. noreturn handling?)
  - Figure out plan for hand-written assembly



arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה