06 April 2026

All-Caps!

Extending Capabilities Across the Whole SoC

Samuel W Stark, Theo Markettos, Simon W Moore
University of Cambridge

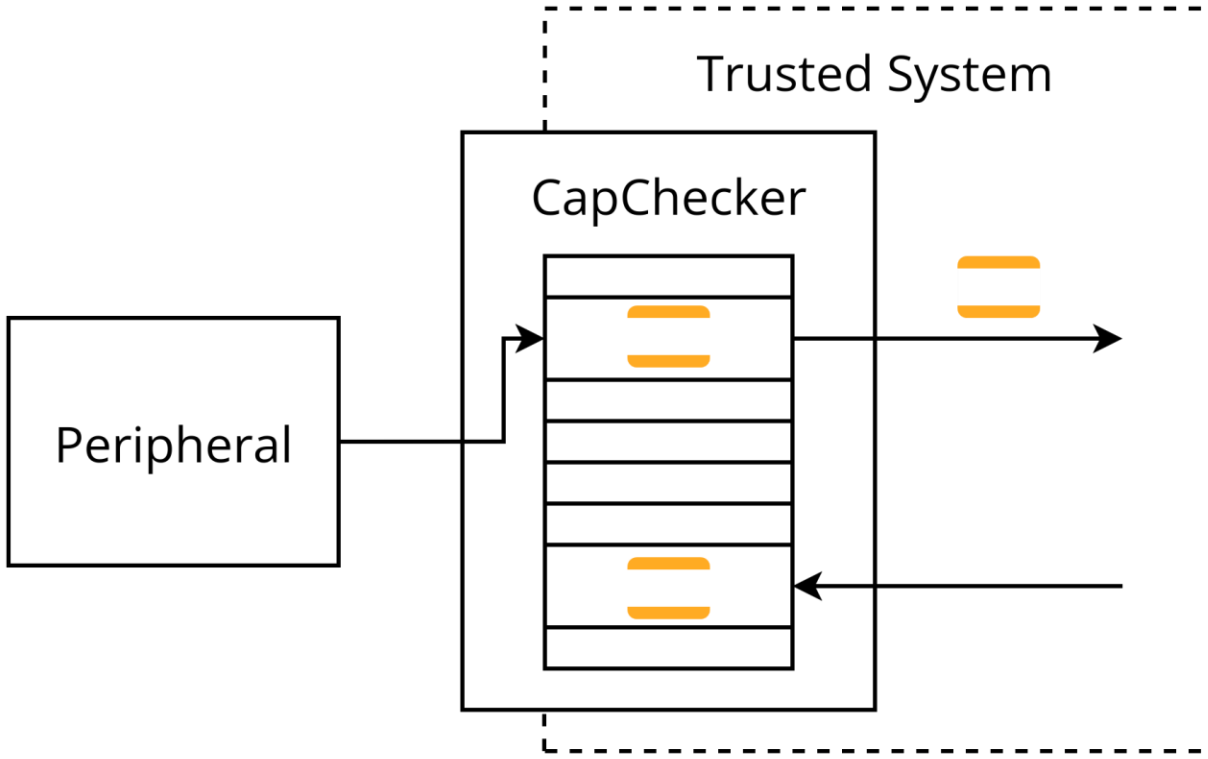
A Capability System that isn't CHERI

- CHERI works in many places!
  - Embedded single-address-space (CHERIoT)
  - Kernel and Userspace (CheriBSD)
  - Trusted peripherals (CHERI-SIMT)

- But CHERI _needs **trusted hardware**
  - Not all peripherals are trusted

Untrusted Hardware

- CapChecker is a harness around untrusted peripherals



Tagged Ticket (e.g. CHERI)

Can be used & stored directly

Unbounded(ish :)

Delete by searching for copies

User must be **TRUSTED**

C-List (e.g. CapChecker)

Use by searching/indexing list

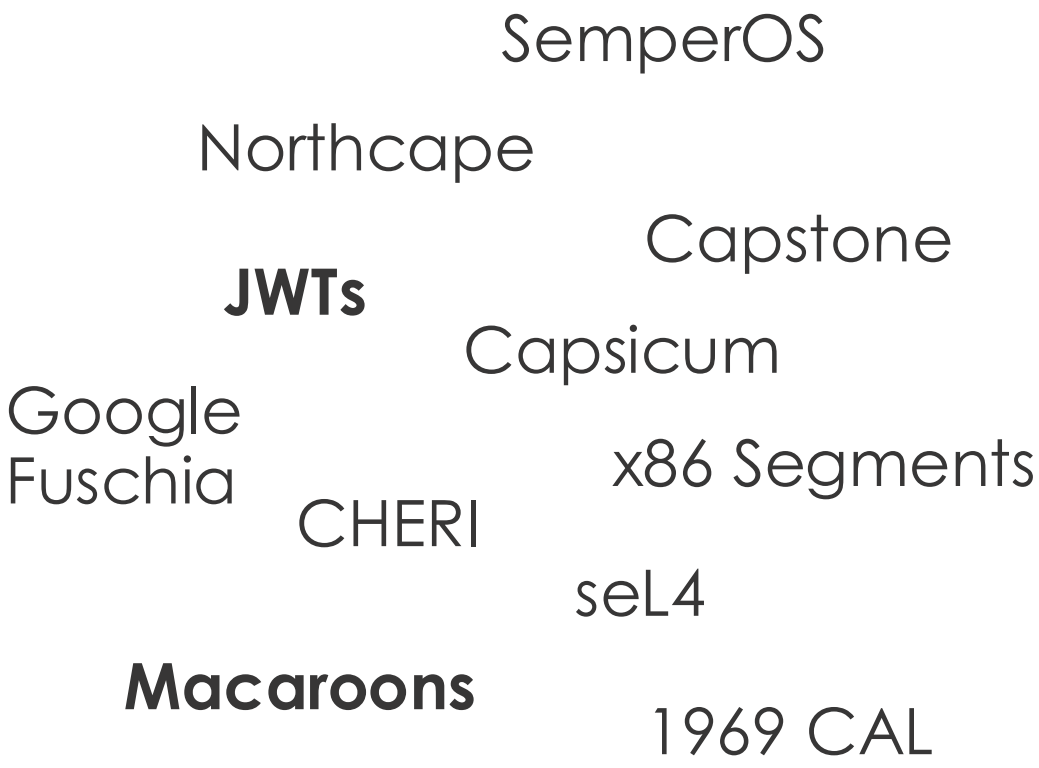
Fixed-size

Delete list elements

User can be **UNTRUSTED**

What can we do?

- Many capability systems out there
- Different pros and cons
- We can make new ones!

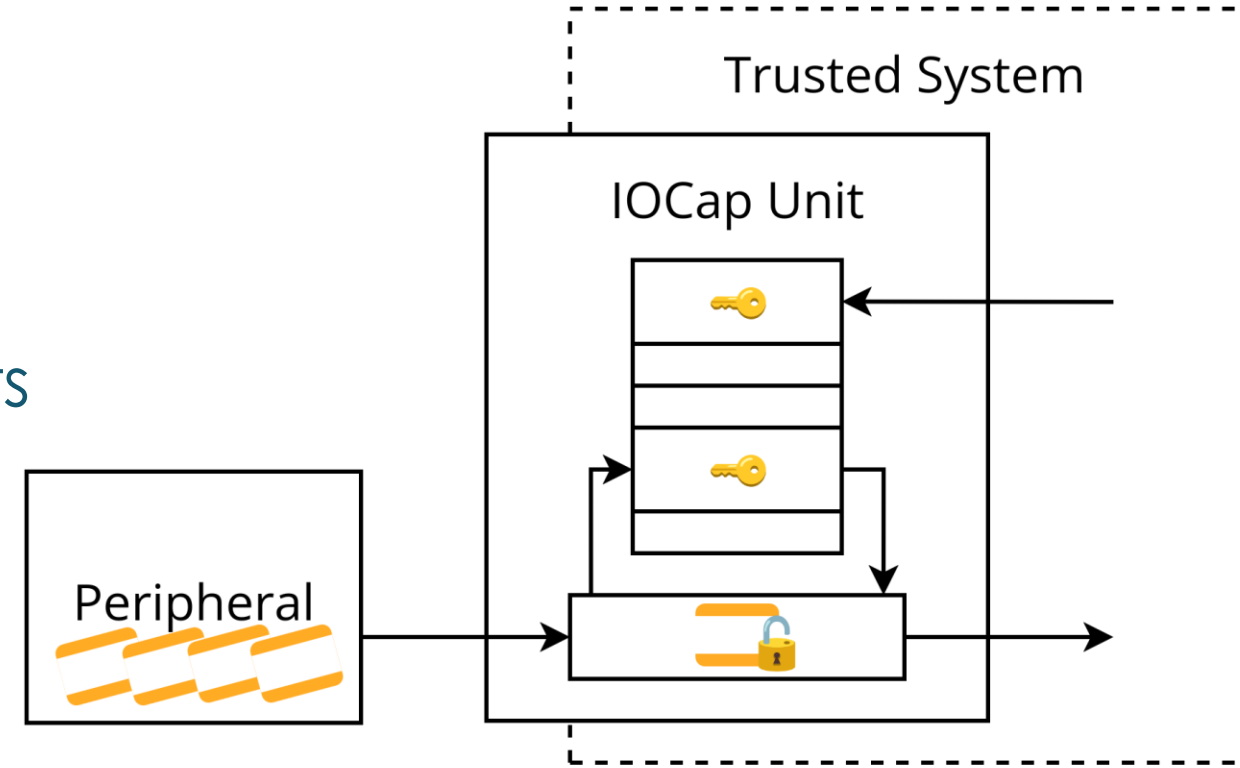


A New Kind of Capability

- Google's Macaroons are capabilities designed for the web
  - Web clients are **untrusted**
- Tickets, like CHERI
  - With support for reduction & delegation
- Use **cryptographic authentication** instead of a tag bit

Revoking a New Kind of Capability

- Authentication requires a **key**
  - Each ticket linked to a key
- Keep a list of keys,
  delete keys to revoke tickets
  - Keep key-index inside ticket
- Many-to-one ticket-to-key
  - Fixed-size key list, unbounded tickets



Tagged Ticket (e.g. CHERI)

Can be used & stored directly

Unbounded(ish :)

Delete by searching for copies

User must be **TRUSTED**

C-List (e.g. CapChecker)

Use by searching/indexing list

Fixed-size

Delete list elements

User can be **UNTRUSTED**

Cryptographic Tickets

Can be used & stored directly

Unbounded(ish :)

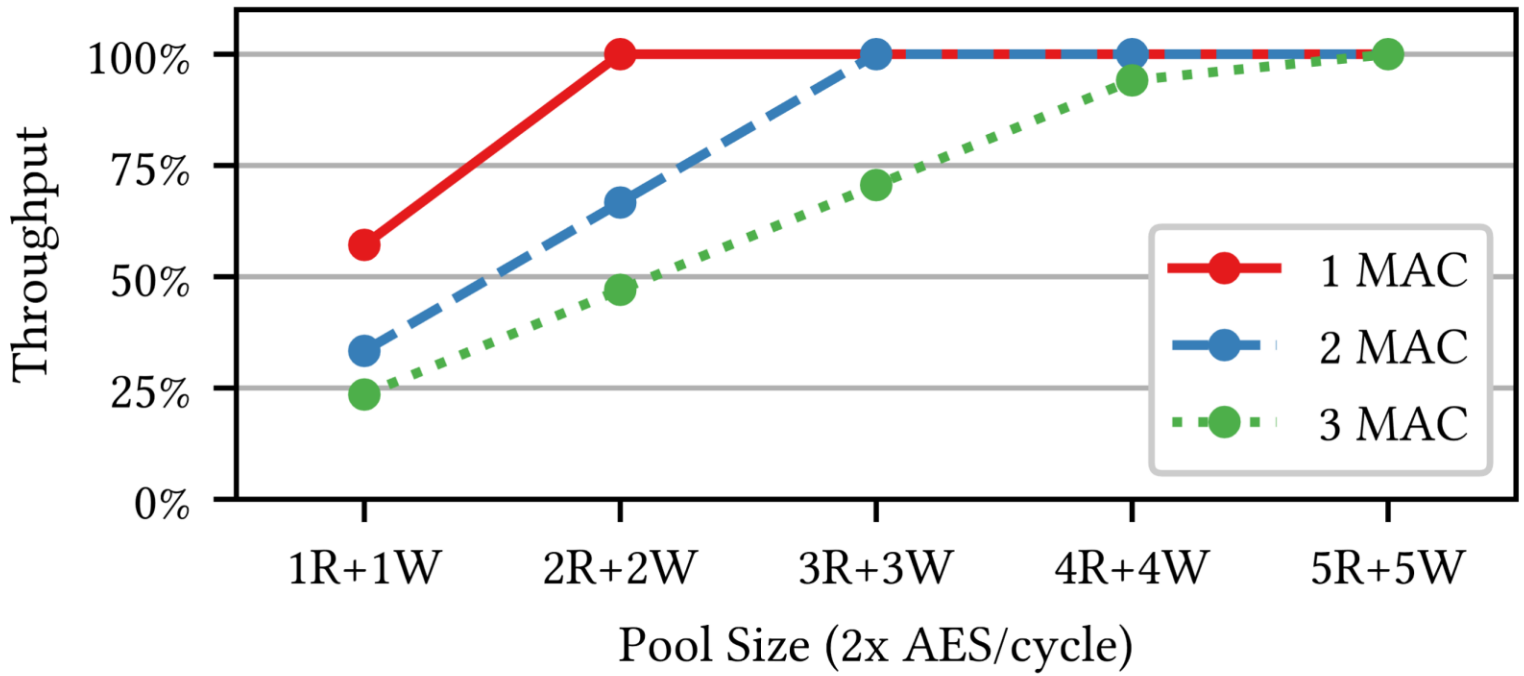
Delete keys as list elements

User can be **UNTRUSTED**

Does it work?

- Yes!
- Full OS, hardware, peripheral support
- Reaches maximum throughput

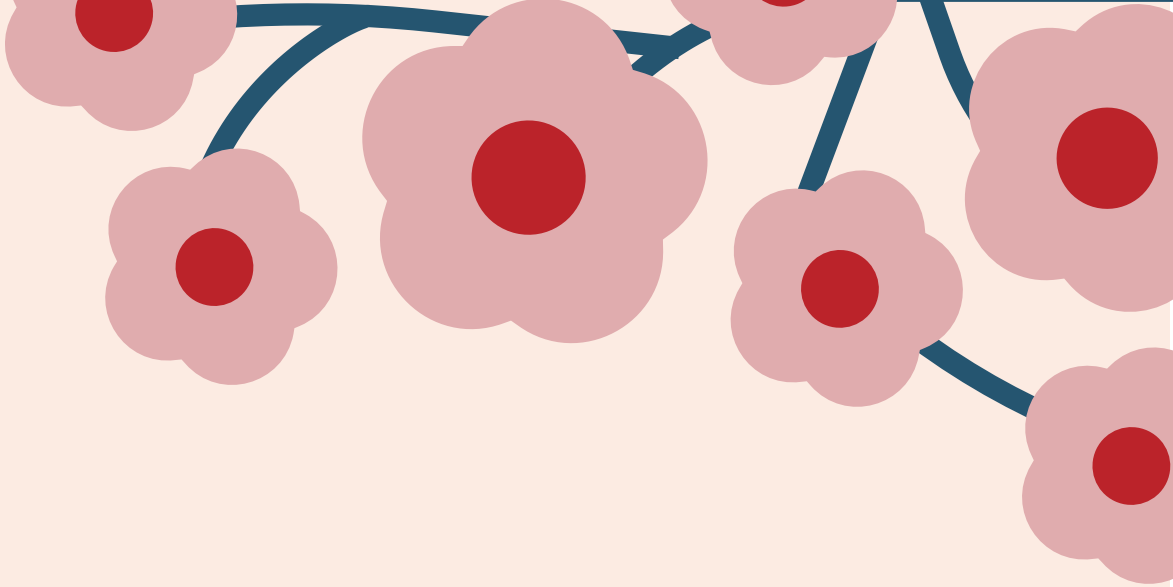
```
cap: [v: 1 | f: 0 | sealed: 0 | addr:
0x0000000010007000 | base: 0x0000000010007000 |
length: 0x0000000000001000 | offset:
0x0000000000000000 | perms: 0x000000000000000d |
otype: 0xffffffffffffffff]
virtio_queue_init_vq negotiated size 1024 for
queue 0
virtio-iocap: global keys already set up
virtio-iocap: Wrote queue_iocap text and
signature to device
virtio-iocap: stats gw  20 bw   0 gr  16 br   0
sector: 0x0
virtio-iocap: virtio_fill_desc from virtio addr:
00000000884806f0 len: 00000010 flags: 1 next: 1
success
virtio-iocap: virtio_fill_desc from virtio addr:
00000000824b61f0 len: 00000200 flags: 3 next: 2
success
virtio-iocap: virtio_fill_desc from virtio addr:
00000000822b06cf len: 00000001 flags: 2 next: 0
success
virtio_queue_notify - device 0x824a84c0, vq
0x824a84e0, old avail_idx: 0, vq->avail->idx: 1,
*current_used_idx = 0, last_used_idx = 0
```



Takeaway

CHERI's principles are great, but there are places CHERI can't reach.

Full-system protection needs new systems!



CHERI

THANK YOU

Contact samuel.stark@cl.cam.ac.uk