06 April 2026

BT's engagement with CHERI Technology

With thanks to: Robert Watson, Jessica Clarke, Mark Johnston, CHERI-BSD and the CHERI Alliance.
& Elena Masterson and Laurence Forgiel @ BT

Sam Cater
Research Technical Manager & Accomplished Engineer @ BT

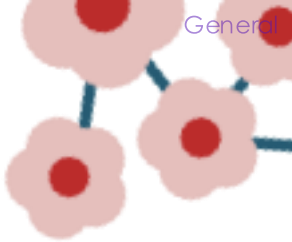
About Me

- Leading BT's engagement with CHERI
- Secure and Resilient Compute Researcher @ BT
  - Background in secure-by-design, consultancy, policy & practice, start-up relationships and showcasing.
  - Accomplished Engineer, BT Tech Fellowship
- CHERI Alliance Ambassador
- Innovate UK Grant Assessor

To be covered

- Why is BT interested in CHERI?
- Our work to date:
  - Understanding the lie of the land.
  - Trial and Error - evaluation
  - Building a Router demonstrator
- Moving forward?

Why is BT interested in memory-safety technology?

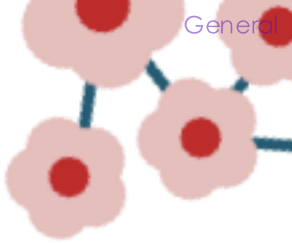


Why is BT interested in memory-safety?

- Memory Safety a strategic priority for the business
  - Supported by Chief Security Authority, MD of Research, and Security Directors.
  - Driving forward the use of memory-safe languages internally
  - Focusing on reduction of memory-safety vulnerabilities ***in our supply chain***.
- Use Case #1 – Use of memory safe hardware across our network estate.
  - Protecting the control plane and administrative functions (e.g. Web Admin, CLI).
- Use Case #2 – Downstream sales and market leadership in memory safety.
  - Strong likelihood of specialised customers pursuing memory safety.
- Alignment to UK Government priorities and strategy.

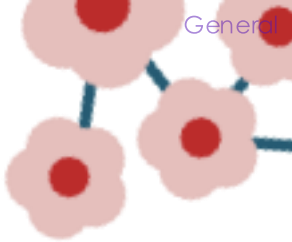
Use Case #1 – Networking Hardware

- Our network estate inherits risk through the supply chain. Risk which is not our fault.
- We are beholden to receiving patches from vendors
  - Assuming they are not behind a paywall…
- We are expected to accept the overhead, management, downtime, remediation cost, and residual risk.



Around a year ago…

- Questions to answer (“*Through the lens of CHERI newbies*”):
  - What is the maturity and availability of CHERI hardware?
  - Does it deliver on its promises?
  - What is the performance like compared to SOTA?
  - How can we best make use of/commercialise CHERI as quickly as possible?



What we found (~one year ago)

- No CHERI-enabled telecoms hardware.
- No telecoms organisations in the CHERI Alliance (we fixed that)
- Fragmented documentation. Unstable Builds. Difficulty with onboarding.
- Cyclical scenario
  - Nobody is manufacturing at scale due to little perceived demand.

How can we support this technology?

How can we support this technology?

- Public Endorsement
  - BT joined CHERI Alliance, April 2025
  - Aligning ourselves to, and supporting NCSC/DSIT priorities (Sovereign Tech, DSBD, Protecting CNI)
  - Promoting wherever possible
- But also…

Leading by example.

Let's see if we can build something…

CHERI

Building a CHERI-Enabled Router

- Why bother? Surely a ‘CHERI-enabled Router’ is easy?
- Shopped around, reviewed hardware, chose Morello.
  - CHERI-BSD - comes with prebuilt CHERI64 packages!
  - No ‘compile and hope’ build cycle.
  - Experience like a Router OS (a’la OpenWRT/PFsense).
  - Hardware extensible (PCIe slots). Some PCIe NICs caused Kernel Panics when enabled.
  - Good up-to-date documentation.
  - Easily accessible *real-time and free* support community (via Slack).
- No Packet-Firewall (PF) (Tried using IPFW….)
- NAT for legacy IPv4 = Instant Crash. IPv6 always worked!
- Got the patch! Compiled a fresh Kernel 👍

CTSRD-CHERI / cheribsd Public

Notifications | Fork 77 | Star 207

Code | Issues 150 | Pull requests 53 | Actions | Projects | Wiki | Security | Insights

pf: Fix a regression #2556

New issue

Merged markjdb merged 1 commit into CTSRD-CHERI:dev from markjdb:dev 3 weeks ago

Conversation 0 | Commits 1 | Checks 23 | Files changed 2 +3 −1

Changes from all commits | File filter | Conversations

Filter changed files

- sys
  - net
    - pfvar.h
  - netpfil/pf
    - pf.c

pf: Avoid using a zero-length array when copying headers

Fix an instance of the problem addressed by commit 0759493 ("pf: pass the correct hdr pointer") which came in via an upstream merge of commit 5e92724 ("pf: fold pf_test_state_{tcp,udp,other} into one pf_test_state").

markjdb committed 3 weeks ago commit 5be2bd1efb2d3e1a9ce7c23f98702c85ac4f3a33

2 sys/net/pfvar.h

```
@@ -1626,7 +1626,9 @@ struct pf_pdesc {
1626 1626  #ifdef INET6
1627 1627                  struct icmp6_hdr        icmp6;
1628 1628  #endif /* INET6 */
     1629 + #ifndef __CHERI_PURE_CAPABILITY__
1629 1630                  char any[0];
     1631 + #endif
1630 1632          } hdr;
1631 1633
1632 1634          struct pf_addr   nsaddr;        /* src address after NAT */
```

2 sys/netpfil/pf/pf.c

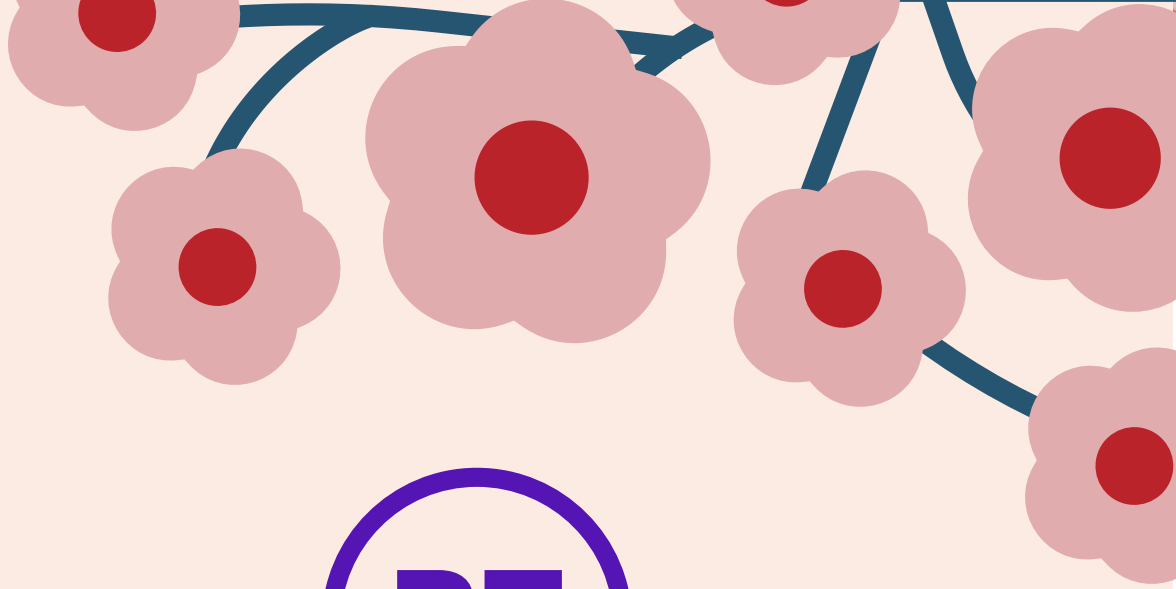
```
@@ -7102,7 +7102,7 @@ pf_test_state(struct pf_kstate **state, struct pf_pdesc *pd, u_short *reason)
7102 7102          }
7103 7103
7104 7104          if (copyback && pd->hdrlen > 0)
7105      -                m_copyback(pd->m, pd->off, pd->hdrlen, pd->hdr.any);
     7105 +                m_copyback(pd->m, pd->off, pd->hdrlen, (caddr_t)&pd->hdr);
7106 7106
7107 7107          return (action);
7108 7108  }
```

Router Demonstrator Today

- Lives in evaluation environment at Adastral Park.
- Carrying real user traffic since 23rd February. ~300GB transferred.
- 1Gb/s uses approx. 25% CPU
- Articles/Press hoping to be released in coming months.
- Praised by BT stakeholders – but where to next?

Next steps

- Verify memory safety vulnerability mitigation.
- Scale up – more ports, more traffic.
- Explore other vendors – new hardware/software expected soon.
- Separate CHERI demo to be presented at major internal conference in London - senior audience.
- Understand and appreciate Fail-Open Fail-Closed.
  - Understand compartmentalisation properly.
- Focusing on commercialisation potential.
- ***Open to collaboration with partners and other Telcos***



CHERI

THANK YOU

BT

Contact sam.cater@bt.com

Web Research and development - BT | BT Plc