Fully External Toolchains

Brooks Davis
SRI International / The CHERI project

May 17, 2023
BSDCan FreeBSD Developers Summit

Rust is coming

- Not immediately, but soon
- Linux allowing Rust going forward
- Google moving new Android development to Rust
  - With great results
- Microsoft rewrote in-kernel TrueType bits

Security-by-design and -default

Recent guidance by US CISA and 10 other security agencies from 7 countries

- **Memory safe programming languages (SSDF PW.6.1):** Prioritize the use of memory safe languages wherever possible. The authoring agencies acknowledge that other memory specific mitigations, such as address space layout randomization (ASLR), control-flow integrity (CFI), and fuzzing are helpful for legacy codebases, but insufficient to be viewed as secure-by-design as they do not adequately prevent exploitation. Some examples of modern memory safe languages include C#, Rust, Ruby, Java, Go, and Swift. Read NSA's memory safety information sheet for more.

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

FreeBSD is at risk if there is no Rust in 15

- Obviously, a bold claim
- External sources:
  - Driver cores
  - Crypto implementations
  - Frameworks (think OFED)
- Internal:
  - I hear developer interest from multiple sources

- `rustc` is too big at add to src
  - Contains a fork of LLVM

Fully integrated toolchains

- Single source tree
  - No worries about syncing versions
- Single source of truth
  - No questions about which tools were used*
- The way we've always done it

But…

- Build times are long
  - Compilers aren't getting smaller…
- Doesn't help architecture bringup
  - or cross build from non-FreeBSD
- *host tools leak in…
  - We don't trust build isolation for releases…

Fully external toolchain questions

- Bootstrapping
  - Where does the compiler (or compilers) come from?
  - What about pkg for pkgbase?
- Reproducibility
  - Recording source versions
  - Binary tool repos?
  - What about cross OS releases?
- What stays?
- What goes?
- What have I missed?