Hardening Tor in HardenedBSD

Shawn Webb
HardenedBSD

Exploit Mitigations

- Control Flow Integrity (CFI)
  - Non-Cross-DSO CFI
  - Really only covers main()
- ASLR
- RELRO
- SafeStack
- Work-in-progress: Capsicum

Current Tor Sandbox

- Tor only supports sandboxing in Linux
- Uses seccomp2
- seccomp2:
  - Filter-based
  - Uses BPF
  - Initialize filters at program init
  - “As you wish” during lifecycle

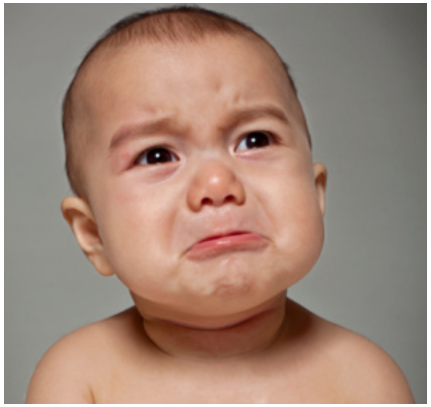
Capsicum

- Capabilities-based framework
- Once “capmode” entered, cannot create new file descriptors, sockets, etc.
- Cannot touch the global namespace (eg, no stat(2))
- Advised to pre-open file descriptors prior to entering capmode
  - Can’t do in this case

Capsicum

- Work-in-progress
- Fork child process
- Capsicumize parent
- Child process opens/creates pre-capsucmized file descriptors, passing them back to parent
- Create wrappers for “privileged” operations
  - open → sandbox_open
  - socket → sandbox_socket
  - unlink → sandbox_unlink

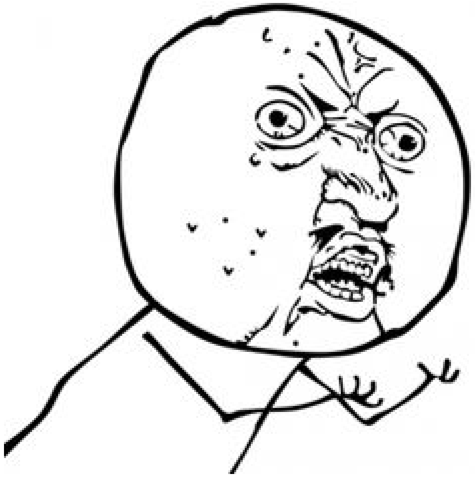
Capsicum



- Nearly every libc call touching filesystem needs to be wrapped
  - Even `close(2)`
  - Result: large diff for upstreaming patch
  - Linux will need to:

```
#define sandbox_stat(path, sb) stat((path), (sb))
```

- Parent cannot call `connect(2)`
  - Huge problem
    - YUUUUUGE
  - FreeBSD manpages say you can



Capsicum

- Long-term development:
  - Instead of calling stat() directly, call sandbox_stat()
  - Developers have to remember which APIs need sandboxing
- Remember, target audience primarily Linux
- Maintainability?
- Prediction:

Attacking Capsicum

- Modern applications expect to open descriptors at will
- Capsicumization turns into writing wrapper library
  - libcasper
  - My file descriptor passing code
- Use ret2libc style attacks
  - Return into wrapper functions

Attacking Capsicum

- No ASLR in upstream FreeBSD
  - Hardcode addresses in malicious payload
  - Copy/paste exploitation
- Takeaway: Wrapper-style Capsicumization requires ASLR to be effective
- Another takeaway: Wrapper-style Capsicumization requires ASLR + CFI to be effective
- **Conclusion: Tor Capsicumization is only effective on HardenedBSD**

Future Work

- Cross-DSO CFI in HardenedBSD
  - Opens the door to full CFI in Tor
- Port CFI and SafeStack to arm64
  - Tor on arm64 is a thing!

ADVENTURE
TIME