https://docs.google.com/presentation/d/1yDSew8gAhIwzNUoAU8l_h9Zc5QpA2ePDFrONq6ybY8c

SBoM contents for embedded system images

Open discussion

Arnout Vandecappelle
Mind

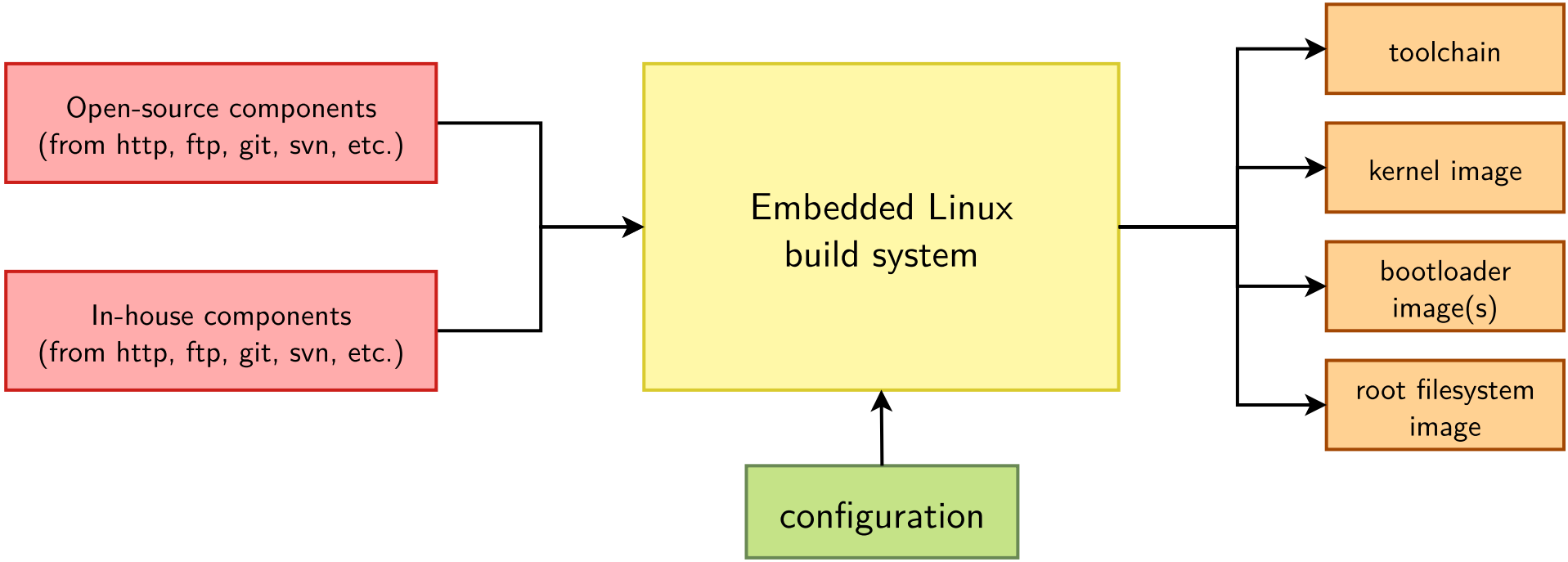
https://mind.be

Who is Arnout

- Embedded software architect
- Focus on Linux OS integration
- Mind consultant since 2008
- Worked for 40+ customers in multimedia, security, home automation, satellite, telecom, chips, …
- Buildroot maintainer (team of 4)

mind
an open source of wisdom

Embedded Linux build system



Buildroot's "SBoM"

- List of packages (separate "target" and "host")
  - Package name, version
  - Source URL
  - Downloaded tarball + hash
  - Patches (local + downloaded) + hash
  - Licenses + license files + hash
  - Dependencies (build only)
- List of files per package
- CVE information
  - Package CPE ID
  - List of CVEs that apply to current version (based on CPE ID)
    - Current information only (not reproducible)
    - Patched or N/A CVEs removed (manually maintained list)

mind
an open source of wisdom

Buildroot’s “SBoM”: what’s missing

- External files (Kconfig, device tree, Buildroot config)
- Buildroot source itself
- Version information of vendored dependencies
- Everything in one file
- SPDX format
- Manifest of source files + license
- Mapping of source → target files
- … ?

mind
an open source of wisdom

Discussion points

- Who/what are the consumers of SBoM?
  - Are there any existing tools?
  - What to they do?
- Which information is needed in the SBoM?
  - Pretty much just component name + version and dependencies…
- How is this best expressed in SPDX?
  - Shouldn't we include CPE IDs?
- How to deal with vendored dependencies
  - Directly included in source
  - Submodules
  - Cargo/go/npm/… modules
  - Vendored in by build system

mind

an open source of wisdom