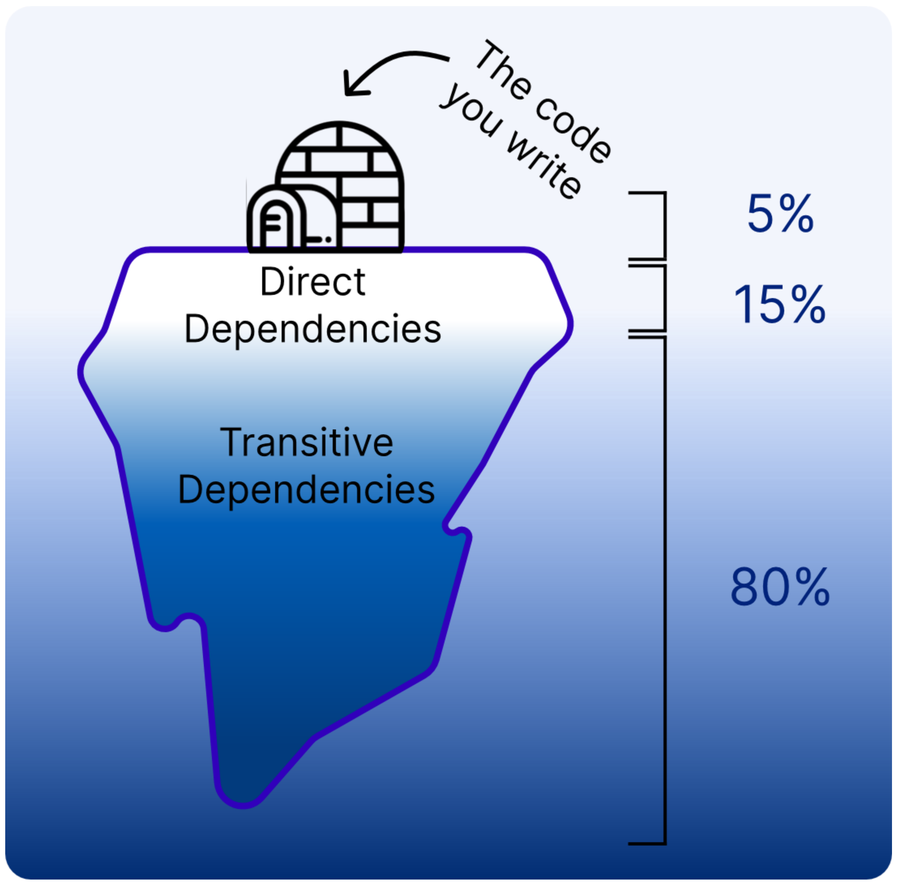
Software Bill of Materials: Ingredients of your Software

Aman Sharma
(amansha@kth.se)

CDIS Spring Conference, 25 May 2023

Martin Wittlinger
(marwit@kth.se)



Your application is a composition of in-house code and third-party components (commercial or open source).

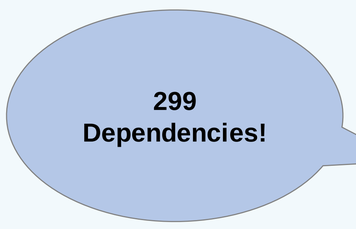
- You developed 5% of the code
- You use 15% non inhouse code
- *You are not aware of the 80% left*

⚠ Large parts of your software are out of your control!

Consequences

- Liability for failures
  SolarWinds: https://rb.gy/azc00
- Non sustainable
  LeftPad: https://rb.gy/ggoua
- More attack surface
  Coop: https://rb.gy/r5qoa
- Licensing & Export Regulation
  Akka: https://rb.gy/28a1m

Software Bill of Materials




```
{
    "bomFormat" : "CycloneDX",
    "specVersion" : "1.4",
    "metadata" : {
      "timestamp" : "2023-02-26T01:58:47Z",
      "tools" : [ {
          "name" : "CycloneDX Maven plugin",
          "version" : "2.7.5" }
      ],
      "component" : {
        "group" : "org.jenkins-ci.main",
        "name" : "jenkins-parent",
        "version" : "2.384",
        "licenses" : [ ... ],
        "externalReferences" : [ {
            "url" : "https://github.com/jenkinsci/jenkins"
        } ],
        "bom-ref" :
"pkg:maven/org.jenkins-ci.main/jenkins-parent@2.384?type=pom"
      }
    },
    "components" : [ {
        "group" : "org.jenkins-ci.main",
        "name" : "jenkins-core",
        "version" : "2.384",
        "bom-ref" :
"pkg:maven/org.jenkins-ci.main/jenkins-core@2.384?type=jar"
    } ],
    "dependencies" : [ {
        "ref" :
"pkg:maven/org.jenkins-ci.main/jenkins-core@2.384?type=jar",
        "dependsOn" : [
          "pkg:maven/com.google.guava/guava@31.1-jre?type=jar"
          ...
        ]
    } ]
}
```

I was produced at Build :D

You must know what is inside your software to protect it from the outside world!

1. Balliu, Musard, et al. *"Challenges of Producing Software Bill Of Materials for Java"*
2. NTIA *"Executive Order on Improving the Nation's Cybersecurity"* | The White House
3. State of Open Source security 2022 | Snyk