the software supply chain

CHAINS project
https://chains.proj.kth.se/
Software Supply Chain
Software Supply Chain
Software Supply Chain
Attacks on the Supply Chain

- Infect a downstream dependency
  - Inject a vulnerability in an open source package and let it propagate until target
  - Examples: event-stream, log4shell
Attacks on the Supply Chain

* Infect the build system
  - Trusting trust attack: compromise the compiler or other tool involved in the build
  - Example: Solarwinds, codecov
Attacks on the Supply Chain

* Infect the package registry
  - **Typosquatting:** publish packages which names are very similar to popular packages and let the malicious packages propagate into applications
  - **Example:** PyPI typosquatting
Software Bill of Materials

+ List all components used to build an application
+ White House Executive Order 14028
+ SPDX and CycloneDX
+ Balliu et al. "Challenges of Producing Software Bill Of Materials for Java", 2023

```
{ "bomFormat": "CycloneDX",
 "specVersion": "1.4",
 "version": 1,
 "components": [ 
  { 
   "bom-ref": "org.apache.ant:ant:1.10.12",
   "type": "library",
   "group": "org.apache.ant",
   "name": "ant",
   "version": "1.10.12",
   "hashes": [
     { "alg": "SHA-256",
       "content": "5c6a438c3eb8a306e6a452b95f3a07b6e6031426177920bca896c4a504ea5f6"
     }
   ],
  },
  { 
   "bom-ref": "commons-fileupload:commons-fileupload:1.4",
   "type": "library",
   "group": "commons-fileupload",
   "name": "commons-fileupload",
   "version": "1.4",
   "hashes": [
     { "alg": "SHA-256",
       "content": "a4ec02336f49253ea5045698b79232b8c5cb02cb60df3a674d77e749a1def7"
     }
   ],
  }
  ]
}
```

Automatic Dependency Updates

- Automatically scan the dependency tree and suggest changes for updates
- Dependabot, Renovate

Update dependency com.nimbusds:nimbus-jose-jwt to v9.28

renovate[bot] committed on Jan 5

Showing 1 changed file with 1 addition and 1 deletion.

<table>
<thead>
<tr>
<th>Line</th>
<th>Status</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>218</td>
<td>-218,7</td>
<td></td>
</tr>
<tr>
<td>219</td>
<td>+210,7</td>
<td></td>
</tr>
<tr>
<td>220</td>
<td></td>
<td></td>
</tr>
<tr>
<td>221</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>221</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>222</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

https://github.com/chains-project/flink/commit/fe13136ed148638672082a3ef3f5735c3945ab4
Reproducible Builds

+ Deterministic behavior of the whole build pipeline
+ Nix and guix

https://github.com/rust-lang/rust/issues/34902
Diverse Double Compilation

+ Countering trusting trust attacks
+ Wheeler, David A. "Countering trusting trust through diverse double-compiling." 2005

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

https://doi.org/10.1145/358198.358210
Dependency Debloating

+ Remove unnecessary dependencies, reduce maintenance and security risks
+ Depclean, for Java
Conclusion

- The software supply chain spans the vast amount of dependencies and tools that are necessary to build modern applications
- The software supply chain is a target for malicious actors
- Industry and academia develop solutions to address the risks of the software supply chain