Machine Learning Supply Chain Security

Taylor R. Schorlemmer, Wenxin Jiang, James C. Davis

Software Supply Chain Security


Defining Software Supply Chains

Attacks Against Software Supply Chains

Security Principles for Software Supply Chains

We propose three supply chain security principles.

1. **Transparency** – knowledge about actors, artifacts, and operations should remain readily available within the supply chain.
2. **Validity** – actors, artifacts, and operations should remain correct. The connections between them should also remain correct.
3. **Separation** – Connections between actors, artifacts, and operations should only exist when necessary – compartmentalizing components of the supply chain.

Applying Security Principles

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Transparency</th>
<th>Validity</th>
<th>Separation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBOM</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>open audit</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Code scanning</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dependencies</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>GitLab Actions</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Git Commit Signing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Scope</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Multi-Feature Authentication</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>It logs</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Containerization</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Version Locking</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Sigstore</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 1. How existing security techniques embody our proposed principles with respect to different components of the software supply chain.

Model Reuse Leads to a Supply Chain

Pre-trained models (PTMs) are machine learning models that have already been trained on data.

PTMs can be reused in several ways:

1. **Fine Tuning**
2. **Pruning**
3. **Quantization**
4. **Knowledge Distillation**
5. **Transfer Learning**

Open-source PTMs are often shared on model hubs.

Model Hubs

PTMs are hosted on three types of model hubs. They are distinguished by their contribution workflow.

1. **Open**
2. **Gated**
3. **Commercial**

Threat Models:

- **Insider**
- **Outsider**

Risks:

- **PTM Discrepancies**
- **Maintainers Reach**

Future Work: Signing in the MLSC

Figure 1. Relationship between components (Actors, Artifacts, and Operations) in the supply chain and security principles.

Figure 2. Four-stage software supply chain attack pattern.

Figure 3. Model contribution and distribution workflow for open, gated, and commercial model hubs.

Figure 4. Discrepancies observed in model classes.

Figure 5. Maintainer access to PTM repositories.

Table 2. How three common software supply chain security frameworks embody our proposed principles with respect to components.

More Information


Table 2. How three common software supply chain security frameworks embody our proposed principles with respect to components.