CERIAS

The Center for Education and Research in Information Assurance and Security

# Machine Learning Supply Chain Security

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

## Software Supply Chain Security

SoK: Analysis of Software Supply Chain Security by Establishing Secure Design Properties. Proceedings of the 1st ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED) 2022.

### Defining Software Supply Chains

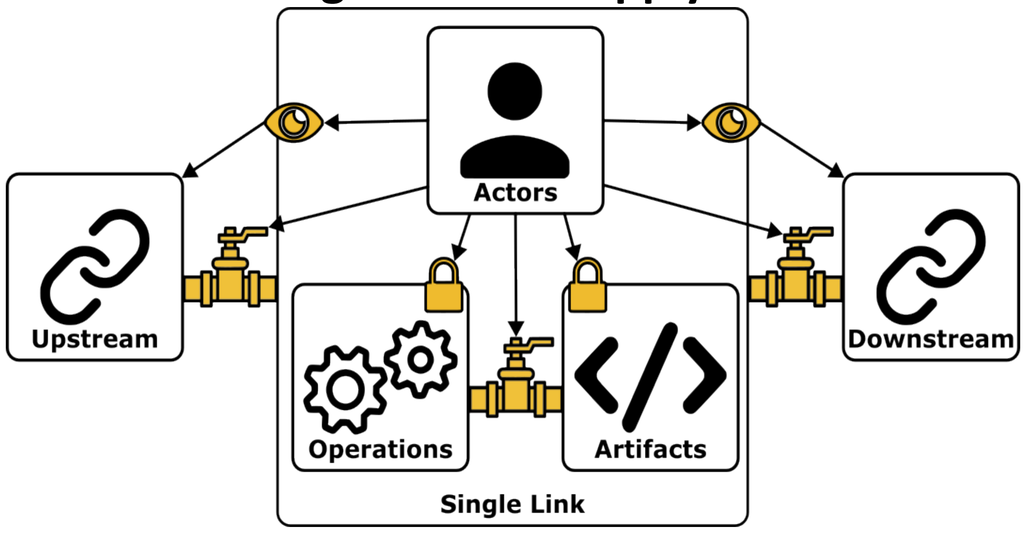


**Figure 1**. Relationship between components (Actors, Artifacts, and Operations) in the supply chain and security principles.

### Attacks Against Software Supply Chains

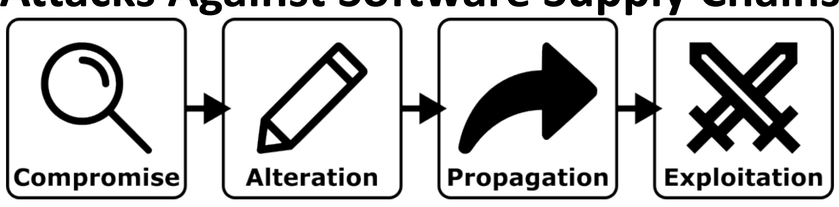


**Figure 2**. Four-stage software supply chain attack pattern.

### 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

| Techniques | Transparency | | | Validity | | | Separation | | |
|---|---|---|---|---|---|---|---|---|---|
| | Artifacts | Operations | Actors | Artifacts | Operations | Actors | Artifacts | Operations | Actors |
| SBOM | ✓ | ✓ | | | | | | | |
| npm-audit | ✓ | | | ✓ | | | | | |
| Code scanning | ✓ | | | ✓ | | | | | |
| Dependabot features | ✓ | | | ✓ | | | | | |
| GitHub Actions | | ✓ | | ✓ | ✓ | | | ✓ | |
| Git Commit Signing | | | ✓ | ✓ | | | | | |
| Scope | | | | ✓ | | | ✓ | | ✓ |
| Multi-Factor Authentication | | | | | | ✓ | | | |
| In-toto | ✓ | ✓ | | ✓ | ✓ | | | ✓ | ✓ |
| Containerization | | | | | | | ✓ | ✓ | ✓ |
| Version Locking | | | | | | | ✓ | | |
| Sigstore | ✓ | ✓ | ✓ | ✓ | ✓ | | | | |
| Mirroring and Proxies | ✓ | | | ✓ | | | ✓ | ✓ | |

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

### More Information

| Frameworks | | SCIM | SLSA 4 | CNCF |
|---|---|---|---|---|
| Transparency | Artifacts | ✓ | ✓ | ✓ |
| | Operations | ✓ | ✓ | ✓ |
| | Actors | | ✓ | ✓ |
| Validity | Artifacts | ✓ | ✓ | ✓ |
| | Operations | ✓ | ✓ | ✓ |
| | Actors | | ✓ | ✓ |
| Separation | Artifacts | | ✓ | ✓ |
| | Operations | | ✓ | ✓ |
| | Actors | | | ✓ |

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

## Machine Learning Supply Chains

An Empirical Study of Artifacts and Security Practices in the Pre-trained Model Supply Chain. Proceedings of the 1st ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED) 2022.

### 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 hub.** They are distinguished by their contribution workflow.

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

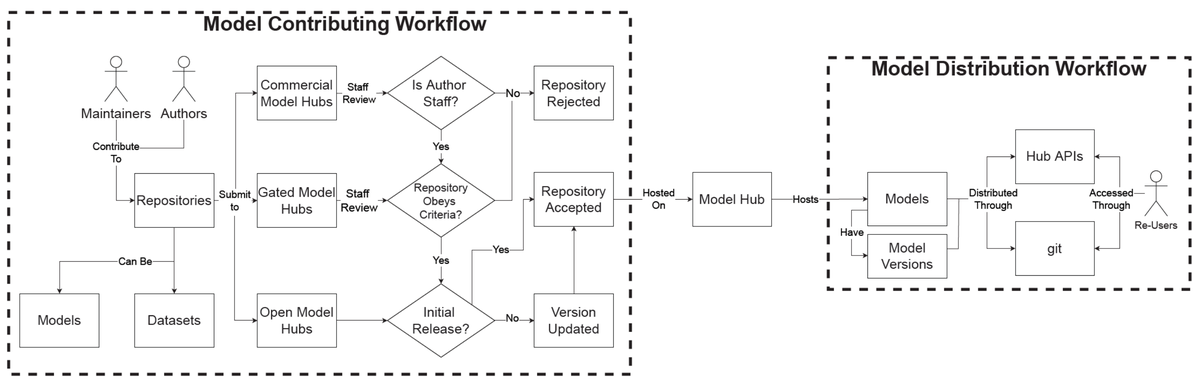


**Figure 3**. Model contribution and distribution workflow for open, gated, and commercial model hubs.

### Threats to Model Hubs

**Threat Models:**

- *Insider*
- *Outsider*

**Risks:**

- *PTM Discrepancies*
- *Maintainers Reach*

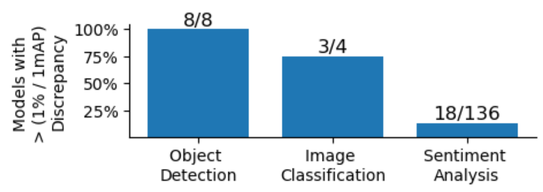


**Figure 4**. Discrepancies observed in model classes

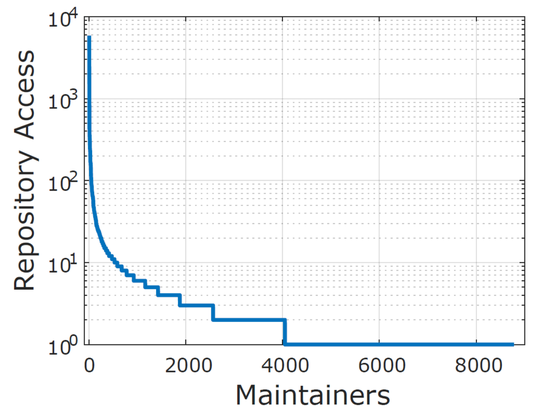


**Figure 5**. Maintainer access to PTM repositories.

Open hubs face more threats due to a lack of control features. They employ **security practices** to mitigate those threats.

1. *Permission Models*
2. *Organization Verification*
3. *Commit Signing*

## Future Work: Signing in the MLSC

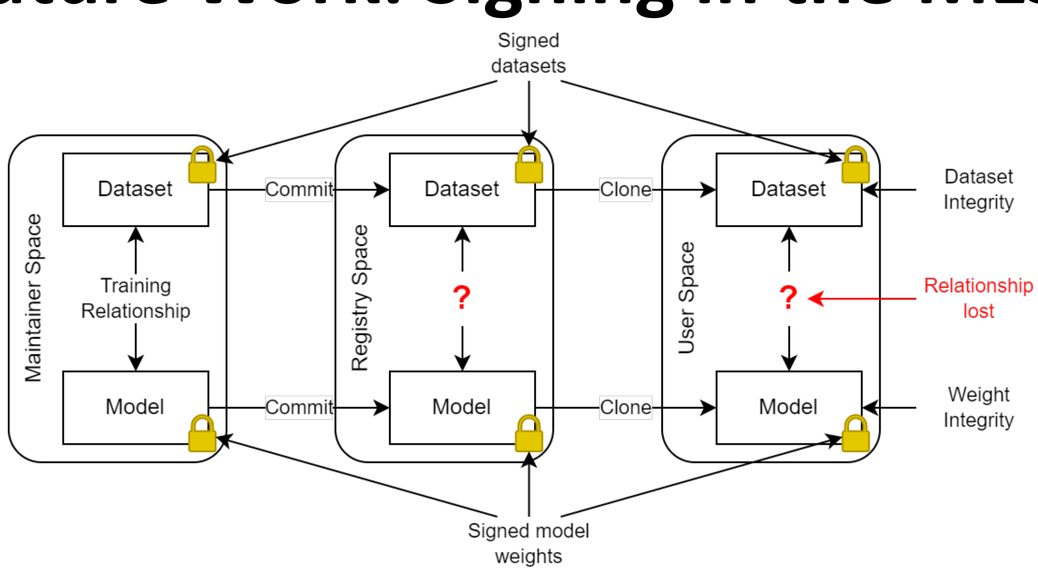


**Figure 6**. Representation of current signing protocols in the ML supply chain.

PURDUE UNIVERSITY
NSF
CISCO
CERIAS