

[Home](#) > [Publications](#) >

Securing the AI Software Supply Chain

Isaac Hepworth · Kara Olive · Kingshuk Dasgupta · Michael Le · Mark Lodato ·

Mihai Maruseac · Sarah Meiklejohn · Shamik Chaudhuri · Tehila Minkus ·

Google, Google, 1600 Amphitheatre Parkway, Mountain View, CA, 94043 (2024)

[Download](#)[Google Scholar](#)[Copy Bibtex](#)

Abstract

As AI-powered features gain traction in software applications, we see many of the same problems we've faced with traditional software—but at an accelerated pace. The threat landscape continues to expand as AI is further integrated into everyday products, so we can expect more attacks. Given the expense of building models, there is a clear need for supply chain solutions.

This paper explains our approach to securing our AI supply chain using provenance information and provides guidance for other organizations. Although there are differences between traditional and AI development processes and risks, we can build on our work over the past decade using Binary Authorization for Borg (BAB), Supply-chain Levels for Software Artifacts (SLSA), and next-generation cryptographic signing solutions via Sigstore, and adapt these to the AI supply chain without reinventing the wheel. Depending on internal processes and platforms, each organization's approach to AI supply chain security will look different, but the focus should be on areas where it can be improved in a relatively short time.

Readers should note that the first part of this paper provides a broad overview of

Research

“Development lifecycles for traditional and AI software”. Then we delve specifically into AI supply chain risks, and explain our approach to securing our AI supply chain using provenance information. More advanced practitioners may prefer to go directly to the sections on “AI supply chain risks,” “Controls for AI supply chain security,” or even the “Guidance for practitioners” section at the end of the paper, which can be adapted to the needs of any organization.

Research Areas

Machine intelligence



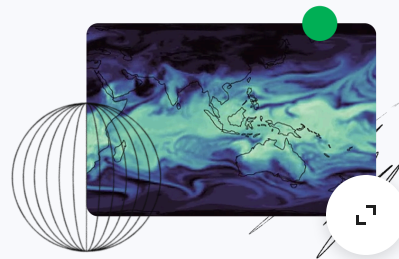
Anti abuse



Meet the teams driving innovation

Our teams advance the state of the art through research, systems engineering, and collaboration across Google.

See our teams



Follow us



Explore our other initiatives

Research

Google AI

Discover how Google AI is committed to enriching knowledge and solving complex challenges

Products

Build

Research

Responsibility

Societal Impact

About

Google Cloud

High-performance infrastructure for cloud computing, data analytics & machine learning

Overview

Solutions

Products

Pricing

Resources

Google DeepMind

Our mission is to build AI responsibly to benefit humanity

Models

Research

Science

About

Google Labs

Explore the future of AI responsibly with Google Labs

About

Experiments

Stay connected

Google

About Google

Google Products

Privacy

Terms