CIS 751 Project Proposal

Chuck Zumbaugh

December 2, 2025

Proposed Title: Securing the supply chain

Overview: Modern software development depends heavily on layers of abstractions such as libraries, frameworks, cloud infrastructure, and source code repositories built and maintained by others. This supply chain is an important attack vector, and several recent incidents, such as the Log4j vulnerability, highlight the scope of the fallout when this vector is exploited. This review is intended to discuss the primary attack vectors in the supply chain, security measures and practices to reduce risk, and a discussion on recent incidents.

1. Overview of the software supply chain
2. Supply chain attack vectors
   (a) Source code repositories
   (b) Software dependencies
   (c) Cloud infrastructure
   (d) Artifact registries
   (e) Build systems
3. Defending against supply chain attacks - Discussion on modern security frameworks and standards
4. Recent supply chain security incidents such as Log4j and the SolarWinds attack