Carnegie Mellon University

# Securing the Software Supply Chain

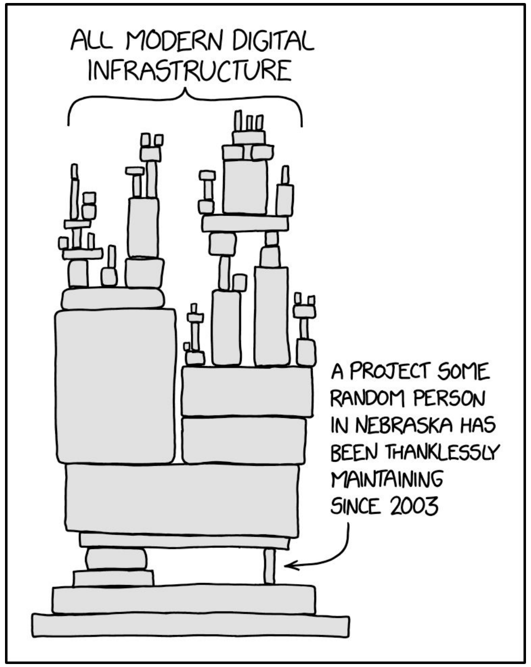
**Team Watchdogs**

- Sid Goparaju
- Wenyi Qian
- Sree Pragna Machupalli
- Surya Togaru

# Introduction

Aspects of Software Supply Chain:

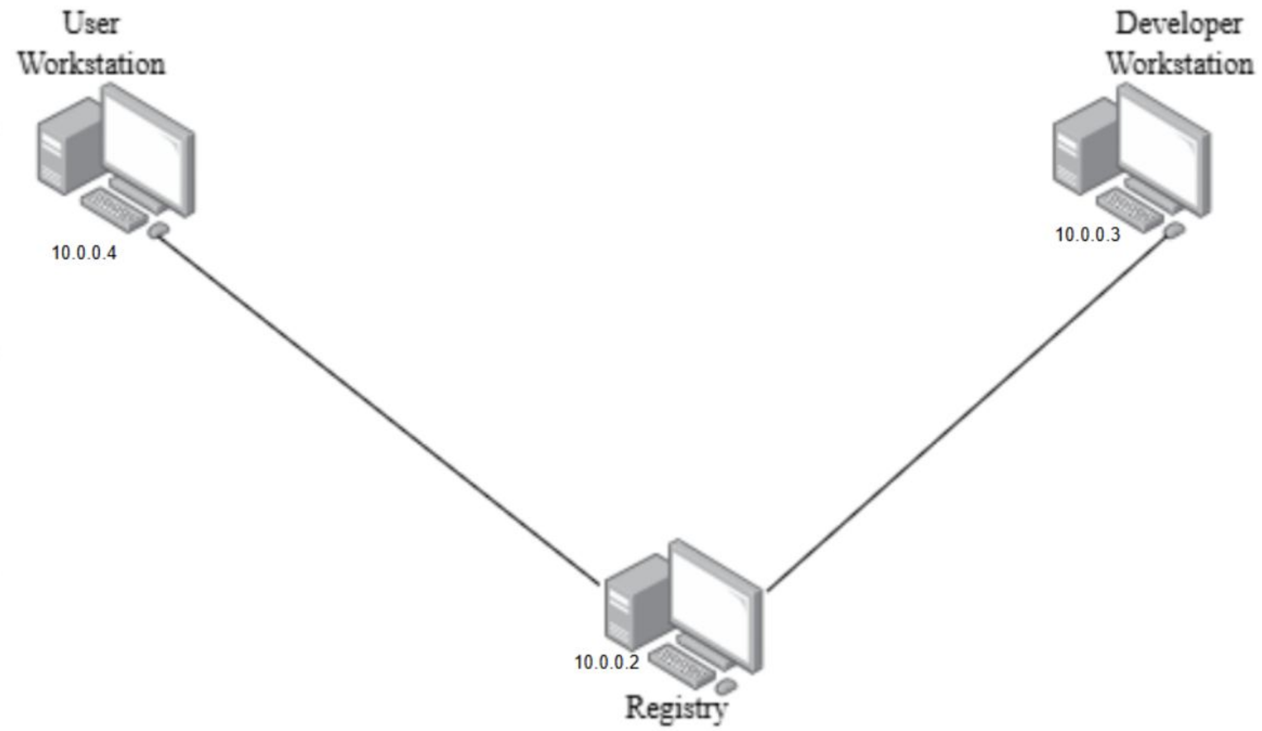
1. **Static Analysis** to identify issues early in the code and prevent their propagation,
2. **Verifying Software Authenticity** to prevent tampering and unauthorized modifications,
3. **Tracking Dependencies** to identify and quickly patch potential vulnerabilities in them.


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

# Learning Goals

1. Identify and remediate code vulnerabilities using static analysis tools like **SonarQube** and **Semgrep**.
2. Package secure applications into **Docker** images, providing a consistent deployment environment.
3. Sign and verify Docker images using **Cosign** to ensure secure distribution and maintain authenticity.
4. Detect and patch vulnerabilities in third-party packages using tools like **Syft** and **Trivy**.
5. Generate, sign, and verify SBOMs to enhance transparency and accountability in software dependencies within the supply chain.

# Lab Network Diagram



# Background Scenario

- Congrats! After countless applications and sleepless nights, you've landed an internship at Gr8scope.
- **Gr8scope's Mission**: To revolutionize assignment workflows with an open-source, cost-effective grading tool for students and faculty.
- **Challenges Await**: The only developer left abruptly (rumor has it, to join the competitor), leaving you to wrap up the development for beta launch.
- **Startup Life**: Officially an SDE intern, but you're also the security engineer, DevOps specialist, and a problem solver.
- **Perks of the Grind**: It's $100/hour!

# Demo Time!

Carnegie Mellon University