SaTC: CORE: Small: Detecting Vulnerabilities and Remediations in Software Dependencies

NC STATE UNIVERSITY

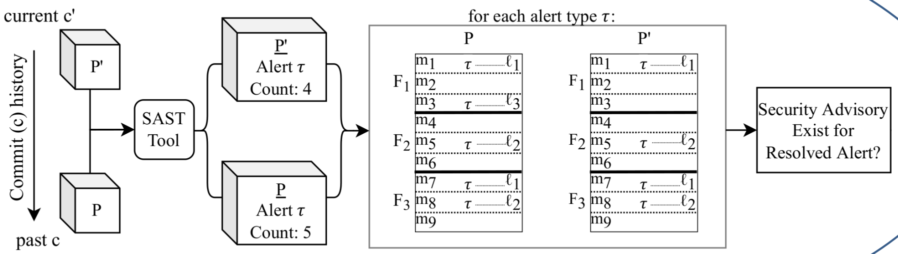
Challenge:

Software commonly relies on dozens to hundreds of open-source packages and modules written and maintained by other companies and volunteers.

Many vulnerability fixes go unannounced, preventing even diligent developers from shipping secure products.

Scientific Impact:

- Novel techniques to discover silent vulnerability fixes based on source code changes.
- Ecosystem studies to empirically demonstrate the pervasiveness of silent vulnerability fixes.



Solution:

Differential Alert Analysis (DAA) leverages knowledge embedded in Static Application Security Testing (SAST) tools rather than requiring difficult to train machine learning.

DAA is used to study broad ecosystems such as PyPI (Python), Maven (Java), NPM (JavaScript), and RubyGems (Ruby).

William Enck, Bradley Reaves,
NC State, CNS-1946273

Broader Impact and Broader Participation:

- Vulnerable dependencies impacts both open and closed source software.
- We will open source our tools and help ecosystems better manage vulnerability fixes.
- We have reported findings to SafetyDB (Python), who informed customers and the public.