Adoption of Security Analysis Tools in Software Development

Shams Al-Amin, Nirav Ajmeri, Munindar Singh, Jon Doyle, Emily Z. Berglund

Motivation

❑Security tools guide developers to identify potential vulnerabilities in their codes

❑However, the use of security tools is not common among developers

❑Sanctions are a way to enforce adoption of security practices among developers

Research Objective

❑Research Question

Which sanctioning mechanism promotes greater adoption of security tools?

❑Research Contributions

-A model that will improve understanding of the adoption of security tools in developers

-Useful for identifying appropriate sanctioning mechanisms for increasing use of security tools

❑Novelty

-Simulates heterogeneity of developers

-Produces emergent adoption dynamics due to developer and manager decisions

Contribution

❑Simulate

-Heterogeneity in developers' skills, preferences and decisions

-Heterogeneity in project task requirements, durations, number of developers

-Developers' decision making to maximize utility

-Sanctions to increase functionality or security of product

-Dynamic interactions between developers and manager

Modeling Framework

❑Developer's Decision Making

-A developer can code, run security tests, learn to code or run security tests, or do other tasks not related to project

-A developer only receives reward for coding or testing

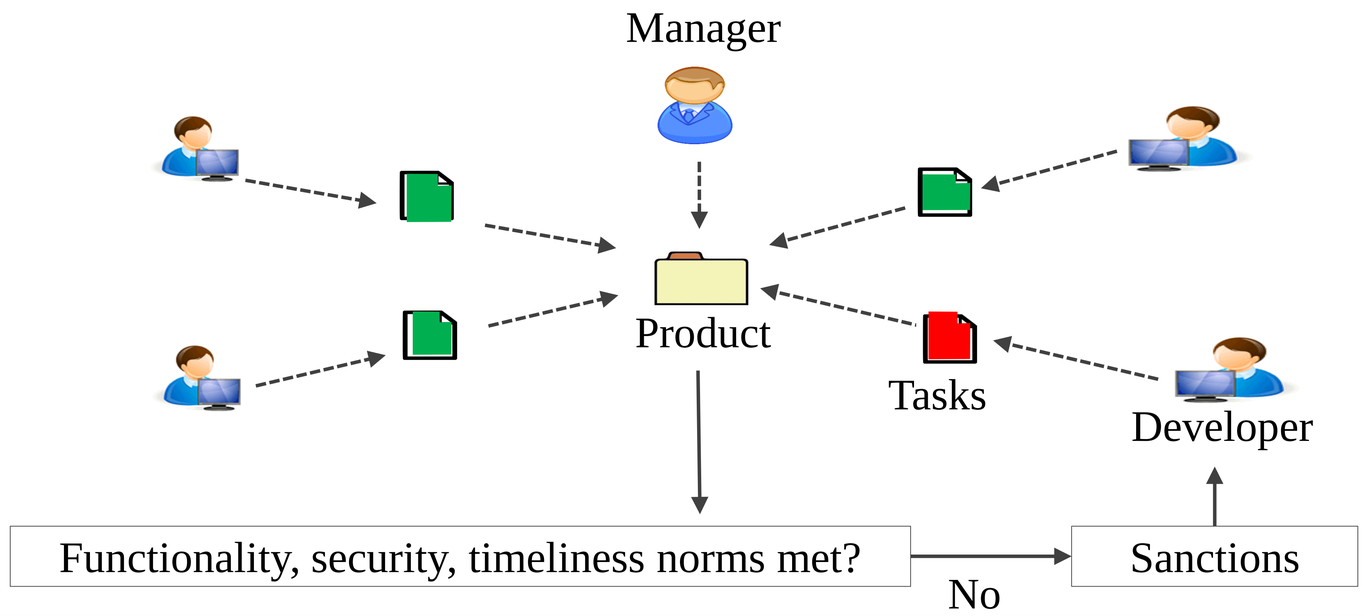
❑Manager's Sanctions: Rewards and Penalties

-Sanctions after each project completion based on timeliness, functionality, or security

-Change in developer's preference of action according to sanction

-Individual, group, and peer sanctions

-Positive and negative sanctions



Preliminary results

Performances	# Sanctions	For functionality		For security	
		Individual	Group	Individual	Group
Tasks tested (%)	19	20	19	16	**33**
Time spent on security tasks (%)	37	37	37	32	**40**
Sanctions (%)	-	20	20	46	20
Sanction efficacy (%)	-	100	100	70	**100**

Simulation description: Number of projects : 5, developers : 10, tasks/project : 50, project duration: 55, Time required to code a task : 6, time required to test a task : 5, Maximum skill : 100, Average of skill required for tasks: 50, Average skill of developers in initialization 50

❑Observation

-Group sanctioning for security promotes better adoption of security practices

Future work

❑Conduct survey to identify the attitude of people and seed the simulation accordingly

❑Extend the model to compare resilience and liveliness for sanctions

Science of Security Lablet

NC STATE UNIVERSITY