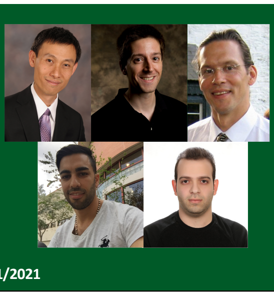
Ethnographic Study of Secure Software Development Processes in a Real Company



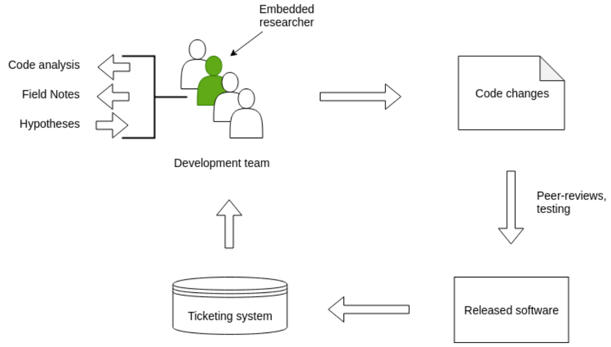
Xinming Ou(PI), Jarred Ligatti(Co-PI), Daniel Lende(Co-PI)

Ph.D. Students: Hernan Palombo, Armin Ziaie Tabari

University of South Florida

Award #1801633 SaTC: CORE: Medium: Collaborative: Understanding Security in the Software Development Lifecycle: A Holistic, Mixed-Methods Approach. $500,000, 9/1/2018-8/31/2021

We study the activities of real software development teams through anthropological fieldwork over long periods while embedded in cooperating companies. By considering large problems, working context, long-term social dynamics, incentives, and other real-world concerns, we uncover deeper, less obvious problems and opportunities for improvement.

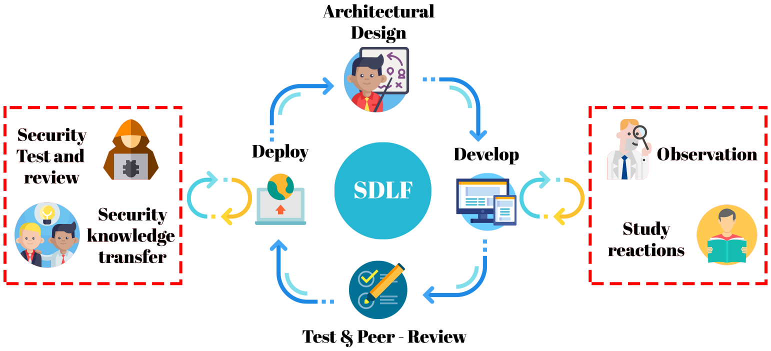


Methodology

- Researchers are embedded in real software development companies
- Researchers play the role of software developers, security analysts, and observers
- Anthropologists call this "*participant observation*"
- Theories are developed based on qualitative analysis of field notes

Motivation:

- Security vulnerabilities are often discovered too late
- Security-related bugs found by developers of commercial software are often not well-documented
- Controlled studies sometimes lack contextual information about how developers solve real-world problems in their work environments



Findings

- Secure software development practices are not standardized within small organizations
- Management often values developers' productivity over their ability to build secure software
- Developers are not trained in security

"Rationales" found

- It is unlikely that attackers will discover and exploit bugs that have existed in applications for many years.
- Fixing all security issues is too costly; focus should be on innovation.

Hypotheses

- Developers don't think as attackers
- More incentives are needed to promote better secure-software development practices

Goal

We intend to uncover generalizable patterns that (dis) incentivize security in software development, and experiment with interventions to induce positive changes of behavior.

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
October 28-29, 2019 I Alexandria, Virginia

UNIVERSITY OF SOUTH FLORIDA