An Analysis of the Role of Situated Learning in Starting a Security Culture in a Software Company

Anwesh Tuladhar, Daniel Lende, Jay Ligatti, Xinming Ou
University of South Florida

This research is supported by the National Science Foundation NSF under Grant No. 1801633.
Introduction

● Goals
  ○ Obtain first-hand understanding of software development and security in the real world
  ○ Adopt a holistic approach to study software development – Collective effort of the whole software development team

● Anthropological research method of Participant Observation
  ○ Studying developers in their “native habitat”
  ○ Studying the problem within the context of where the process happens
  ○ Observe software engineers as a collective
The Company

- Development team
  - 5 software engineers (1 with extensive background in security)
  - 1 quality assurance (QA) engineer
- Network engineers
  - Managing internal infrastructure
- Support engineers
- Virtual application security (AppSec) team
  - At least 1 software engineer from each product team assigned
  - Responsible for security of the product

Agile S-SDLC
Months 1 - 3

- **AppSec Tasks**
  - Cybersecurity Framework (CSF)
  - Application Security Verification Standard (ASVS)
- **Sprint + AppSec tasks**
- "**Burning cycles**"
  - "I knocked off a couple of CSF tickets."
  - "My changes are in PR. I will next work on ASVS tickets while I wait for reviews."
Months 4 - 5

- Threat modelling
Months 4 - 5

- Threat modelling
- Security Scrum Poker
Sprint Tasks + AppSec Tasks

Months 4 - 5

- Threat modelling
- **Security Scrum Poker**
- Contextual analysis of security
- Inclusion of security tickets within the sprint
Sprint Tasks + AppSec Tasks

- Whole team involvement in security
- Security considerations made in other tickets
  - During design
  - Security driven code refactor
- Customer requested feature postponed as security issue was identified
- Total 20 security related tickets filed
What was Driving the Change?
The Role of Management

- Established processes S-SDLC
- Established AppSec structure
- Access to resources: Black Duck, SonarQube, ZAP
- Set security as a deliverable
The Role of Situated Learning

- Role of Subject Matter Experts (SMEs)
  - Knowledgeable developers
  - Learners
- Existence of Preferred Practices
Co-creation + Situated Learning

- Co-creation can leverage the situated learning environment to establish secure preferred practices.


Beginning of a Security Culture
Thank you!

Anwesh Tuladhar
atuladhar@usf.edu

Daniel Lende
dlende@usf.edu

Jay Ligatti
ligatti@usf.edu

Xinming Ou
xou@usf.edu