Security In The Software Development Lifecycle

Hala Assal & Sonia Chiasson
School of Computer Science, Carleton University
Ottawa ON, Canada
HalaAssal@scs.carleton.ca

Why?

- Vulnerabilities persist
- Increasing and evolving threats
- Developers are *not* the enemy

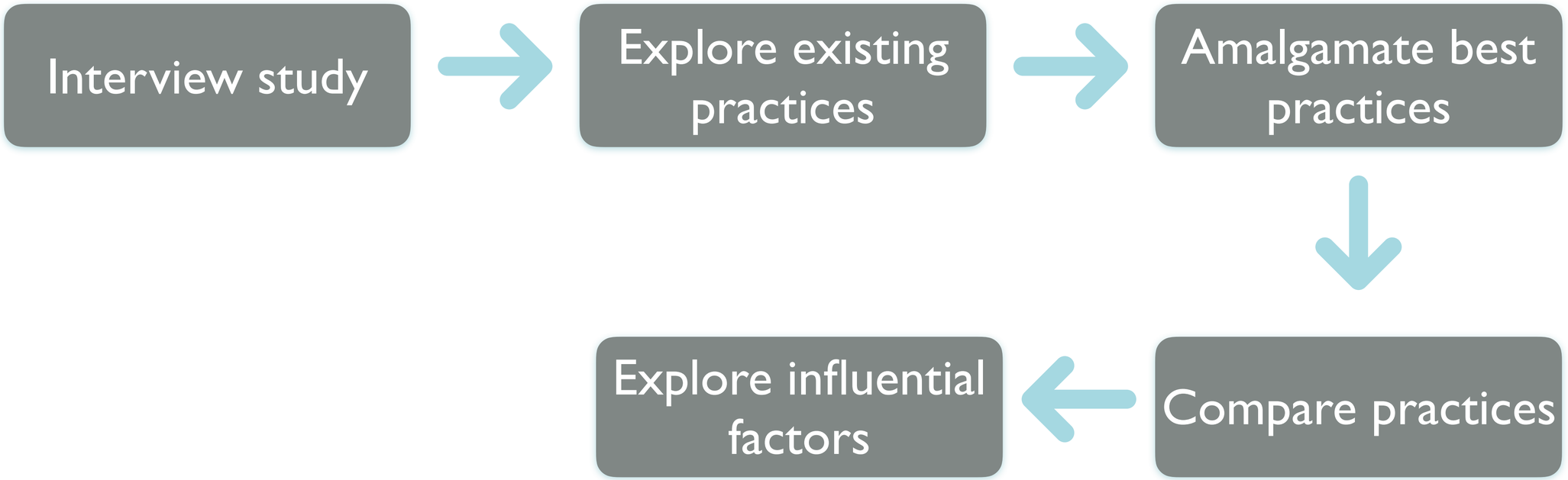


Related Work

- Security tools' adoption
  - E.g., Witschey et al., 2014; Xiao et al., 2014; Xie et al., 2011
- Proposing and improving new tools and methodologies
  - E.g., Smith et al., 2018; Nguyen et al., 2017; Xie et al., 2011
- Developers' abilities and experience
  - E.g., Smith et al., 2015; Oliveira et al., 2014; Baca et al., 2009

The overall security process
Existing practices compared to best practices

Approach


Interview study
Explore existing practices
Amalgamate best practices
Compare practices
Explore influential factors

Study Design

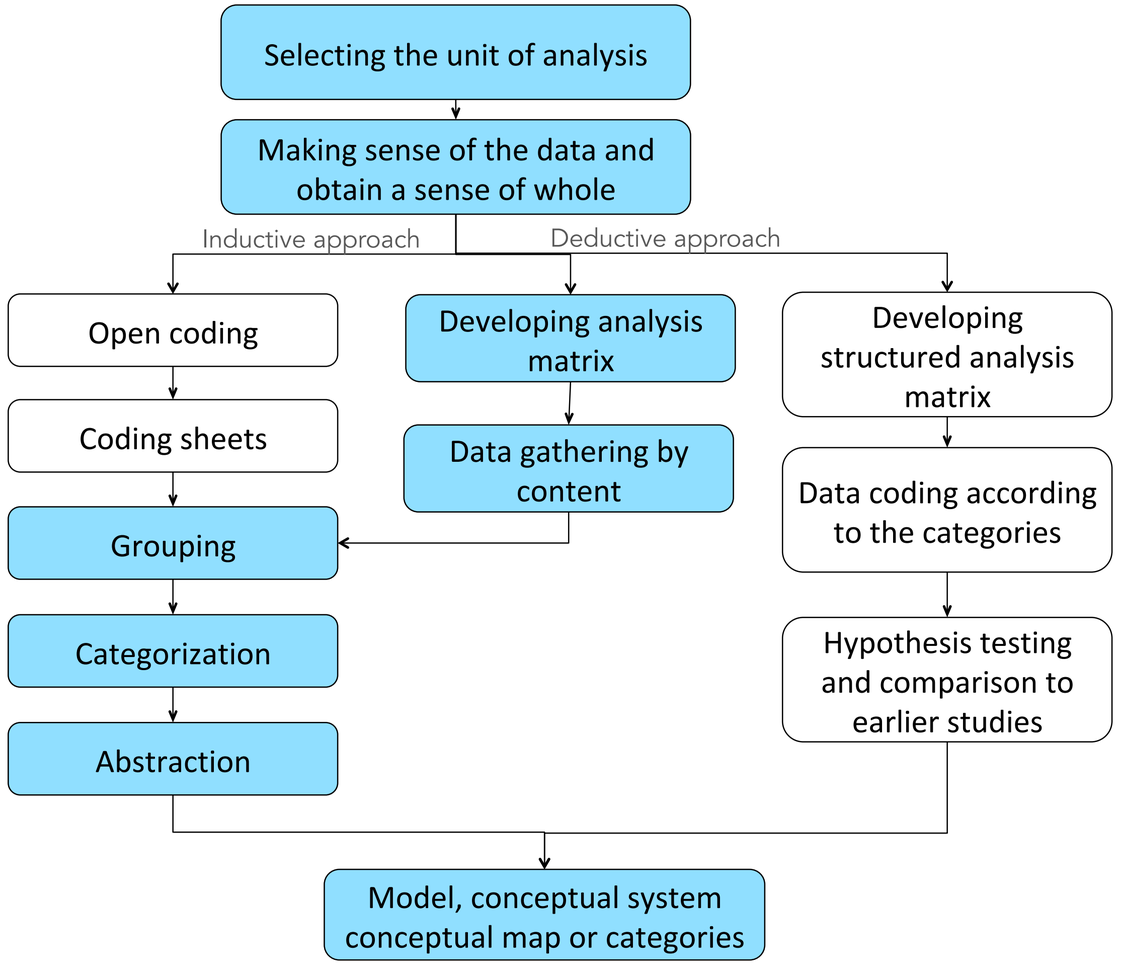
- Semi-structured interview
  - Software engineering + security topics
  - ~1hr sessions
  - Audio recorded and transcribed

Participants

- 13 professional developers
  - Avg. experience = 9.35 years (*Md*=8)
  - 15 teams in 15 different companies
  - 7 SMEs and 8 large enterprises

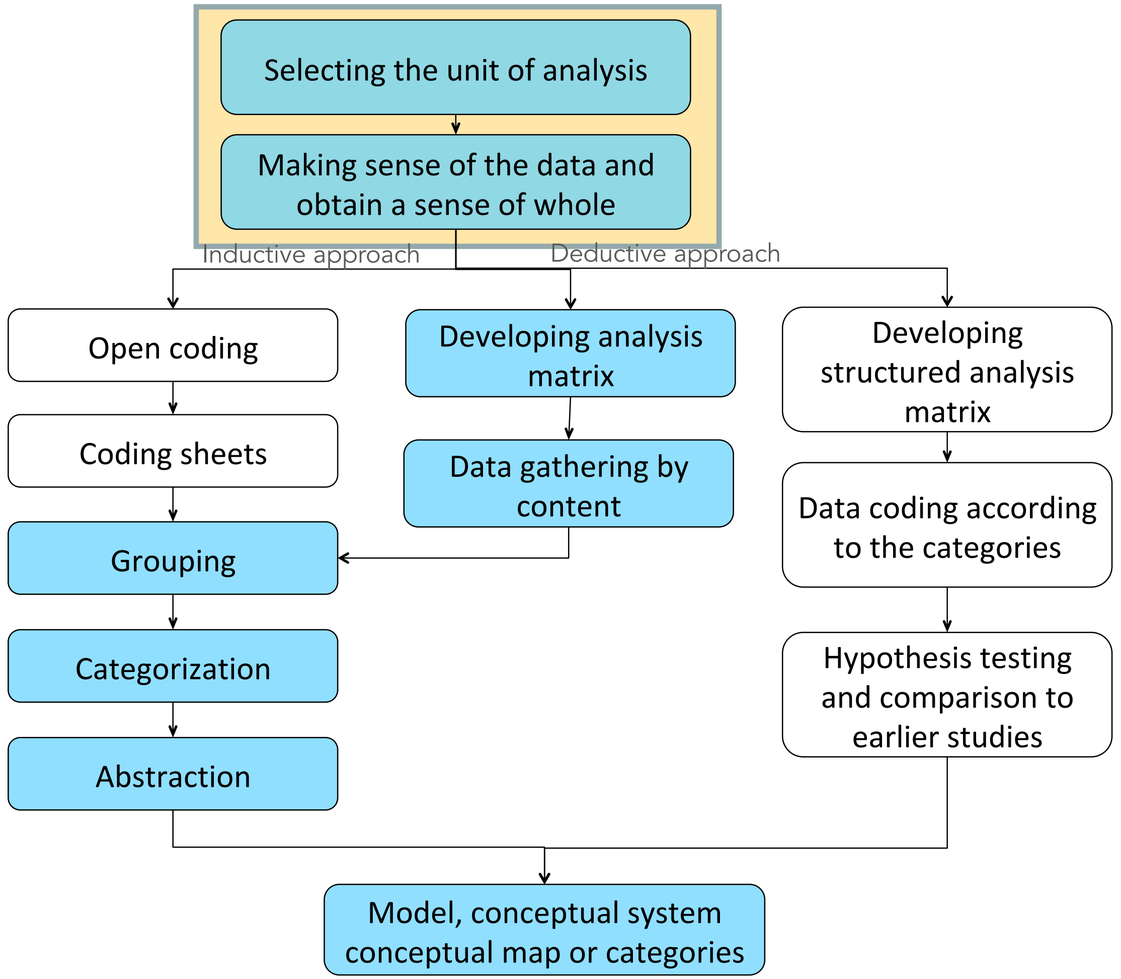
Analysis Methodology

- Qualitative Content Analysis
  (Elo & Kyngäs, 2008)
  - Deductive and inductive approaches
  - Analysis Matrix of development activities
    - 264 unique excerpts



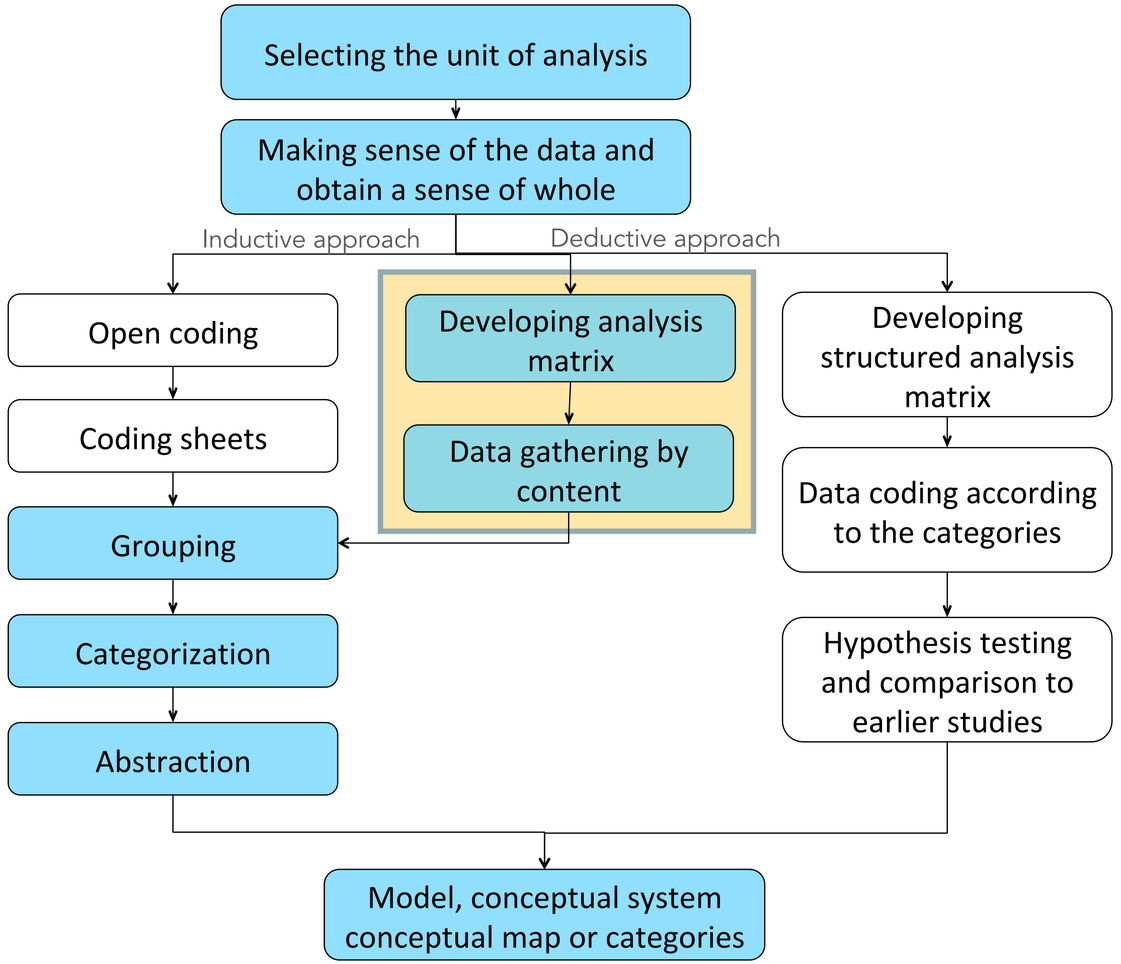
Analysis Methodology

- Qualitative Content Analysis
  (Elo & Kyngäs, 2008)
  - Deductive and inductive approaches
  - Analysis Matrix of development activities
    - 264 unique excerpts



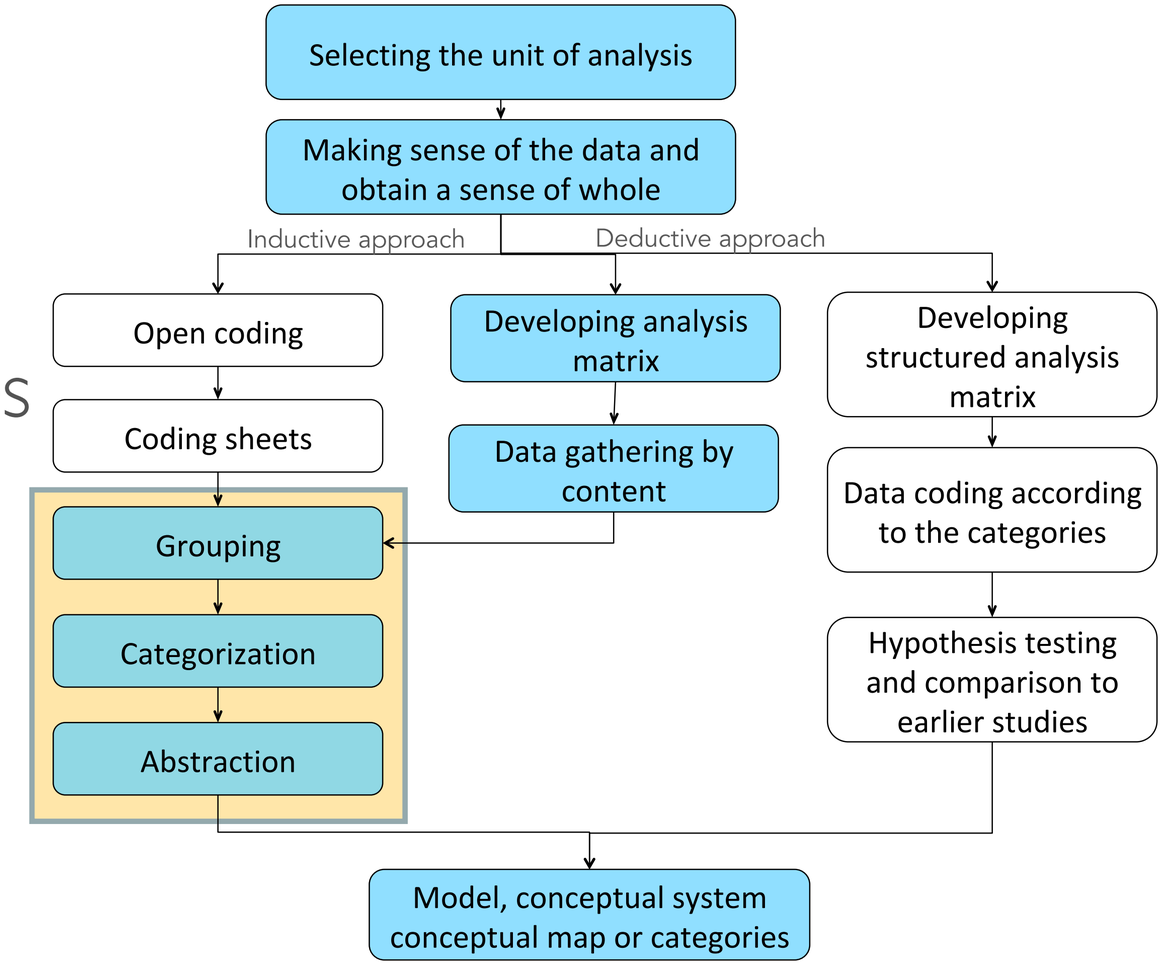
Analysis Methodology

- Qualitative Content Analysis
  (Elo & Kyngäs, 2008)
  - Deductive and inductive approaches
  - Analysis Matrix of development activities
    - 264 unique excerpts



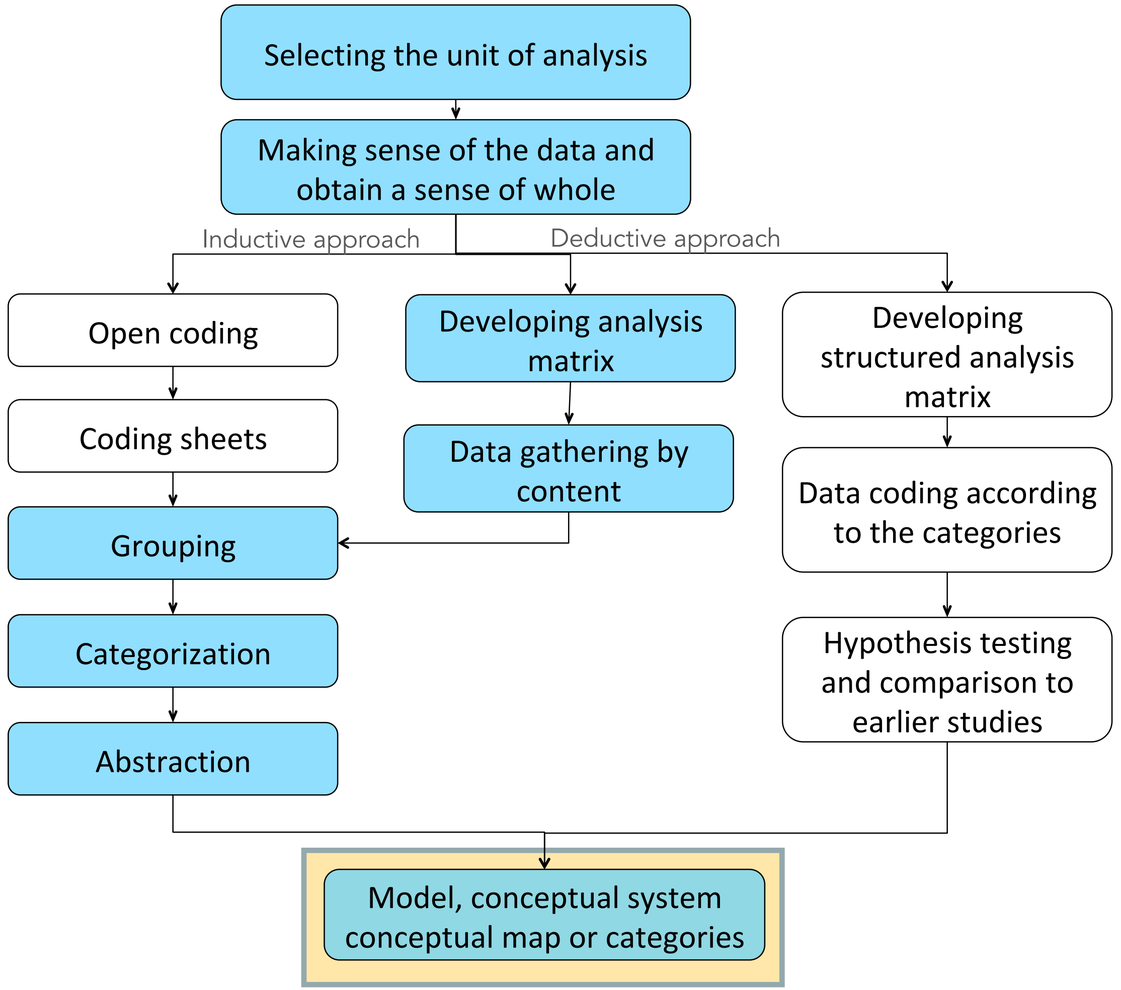
Analysis Methodology

- Qualitative Content Analysis
  (Elo & Kyngäs, 2008)
  - Deductive and inductive approaches
  - Analysis Matrix of development activities
    - 264 unique excerpts



Analysis Methodology

- Qualitative Content Analysis
  (Elo & Kyngäs, 2008)
  - Deductive and inductive approaches
  - Analysis Matrix of development activities
    - 264 unique excerpts



Security In Practice

The Security Adopters & The Security Inattentive

Security Adopters

	Design	Implementation	Developer testing	Code analysis	Code review	Post-dev testing
T1	×	●	×	●	●	●
T3	?	●	?	●	●	●
T5	●	●	○	●	●	●
T11	?	●	○	●	●	?
T12	×	●	○	●	●	●
T14	×	●	●	⊗	●	●

Security Inattentive

	Design	Implementation	Developer testing	Code analysis	Code review	Post-dev testing
T2	×	●	×	○	○	●
T4	○	○	○	⊗	○	○
T6	×	○	×	×	○	○
T7	×	×	×	⊗	×	○
T8	×	×	×	⊗	×	●
T9	●	●	○	⊗	○	○
T10	○	○	×	⊗	○	⊗
T13	×	●	×	⊗	○	●
T15	×	×	×	×	×	×

● : secure, ○ : somewhat secure, × : not secure, ⊗ : not performed, ? : no data

Security Adopters Themes	Common Themes	Security Inattentive Themes
	Design	
· Security design is very important	· Security is not considered in the design stage	· Security consideration in the design stage is adhoc
	Implementation	
	· Security is a priority during implementation · Developers' awareness of security is expected when implementing	· Security is not a priority during implementation · Developers take security for granted · Developers misuse frameworks · Developers lack security knowledge · Developers perceive their security knowledge inaccurately · Vulnerability discovery can motivate security
	Developer Testing	
· Developers test for security fortuitously · Security is a priority during developer testing	· Developers do not test for security	· Developers' security testing is feature-driven
	Code Analysis	
· Security is a priority during code analysis		· Security is a secondary objective during code analysis · Developers rarely perform code analysis, never for security · Developers vary in awareness of analysis tools
	Code Review	
· Code review is a formal process that includes security · Preliminary code review is done as a checkpoint before the formal review		· Security is not considered during code review · Security consideration in code review is minimal
	Post-development Testing	
· Security is a priority during post-development testing · Post-development testing is used to discover security vulnerabilities, or for final verification · Testers have the final approval		· Security is not considered in post-development testing · Post-development testing plans include a security dimension · Post-development security testing is feature-driven · Post-development security testing is adhoc · Post-development security testing is externally-driven

Security Adopters Themes	Common Themes	Security Inattentive Themes
	Design	
· Security design is very important	· Security is not considered in the design stage	· Security consideration in the design stage is adhoc
	Implementation	
	· Security is a priority during implementation · Developers' awareness of security is expected when implementing	· Security is not a priority during implementation · Developers take security for granted · Developers misuse frameworks · Developers lack security knowledge · Developers perceive their security knowledge inaccurately · Vulnerability discovery can motivate security
	Developer Testing	
· Developers test for security fortuitously · Security is a priority during developer testing	· Developers do not test for security	· Developers' security testing is feature-driven
	Code Analysis	
· Security is a priority during code analysis		· Security is a secondary objective during code analysis · Developers rarely perform code analysis, never for security · Developers vary in awareness of analysis tools
	Code Review	
· Code review is a formal process that includes security · Preliminary code review is done as a checkpoint before the formal review		· Security is not considered during code review · Security consideration in code review is minimal
	Post-development Testing	
· Security is a priority during post-development testing · Post-development testing is used to discover security vulnerabilities, or for final verification · Testers have the final approval		· Security is not considered in post-development testing · Post-development testing plans include a security dimension · Post-development security testing is feature-driven · Post-development security testing is adhoc · Post-development security testing is externally-driven

Security Adopters

Security Inattentive

Security Adopters Themes	Common Themes	Security Inattentive Themes
	Design	
· Security design is very important	· Security is not considered in the design stage	· Security consideration in the design stage is adhoc
	Implementation	
	· Security is a priority during implementation · Developers' awareness of security is expected when implementing	· Security is not a priority during implementation · Developers take security for granted · Developers misuse frameworks · Developers lack security knowledge · Developers perceive their security knowledge inaccurately · Vulnerability discovery can motivate security
	Developer Testing	
· Developers test for security fortuitously · Security is a priority during developer testing	· Developers do not test for security	· Developers' security testing is feature-driven
	Code Analysis	
· Security is a priority during code analysis		· Security is a secondary objective during code analysis · Developers rarely perform code analysis, never for security · Developers vary in awareness of analysis tools
	Code Review	
· Code review is a formal process that includes security · Preliminary code review is done as a checkpoint before the formal review		· Security is not considered during code review · Security consideration in code review is minimal
	Post-development Testing	
· Security is a priority during post-development testing · Post-development testing is used to discover security vulnerabilities, or for final verification · Testers have the final approval		· Security is not considered in post-development testing · Post-development testing plans include a security dimension · Post-development security testing is feature-driven · Post-development security testing is adhoc · Post-development security testing is externally-driven

Common

Security Adopters Themes	Common Themes	Security Inattentive Themes
	Design	
· Security design is very important	· Security is not considered in the design stage	· Security consideration in the design stage is adhoc
	Implementation	
	· Security is a priority during implementation · Developers' awareness of security is expected when implementing	· Security is not a priority during implementation · Developers take security for granted · Developers misuse frameworks · Developers lack security knowledge · Developers perceive their security knowledge inaccurately · Vulnerability discovery can motivate security
	Developer Testing	
· Developers test for security fortuitously · Security is a priority during developer testing	· Developers do not test for security	· Developers' security testing is feature-driven
	Code Analysis	
· Security is a priority during code analysis		· Security is a secondary objective during code analysis · Developers rarely perform code analysis, never for security · Developers vary in awareness of analysis tools
	Code Review	
· Code review is a formal process that includes security · Preliminary code review is done as a checkpoint before the formal review		· Security is not considered during code review · Security consideration in code review is minimal
	Post-development Testing	
· Security is a priority during post-development testing · Post-development testing is used to discover security vulnerabilities, or for final verification · Testers have the final approval		· Security is not considered in post-development testing · Post-development testing plans include a security dimension · Post-development security testing is feature-driven · Post-development security testing is adhoc · Post-development security testing is externally-driven

Security Adopters Themes	Common Themes	Security Inattentive Themes
	Design	
· Security design is very important	· Security is not considered in the design stage	· Security consideration in the design stage is adhoc
	Implementation	
	· Security is a priority during implementation · Developers' awareness of security is expected when implementing	· Security is not a priority during implementation · Developers take security for granted · Developers misuse frameworks · Developers lack security knowledge · Developers perceive their security knowledge inaccurately · Vulnerability discovery can motivate security
	Developer Testing	
· Developers test for security fortuitously · Security is a priority during developer testing	· Developers do not test for security	· Developers' security testing is feature-driven
	Code Analysis	
· Security is a priority during code analysis		· Security is a secondary objective during code analysis · Developers rarely perform code analysis, never for security · Developers vary in awareness of analysis tools
	Code Review	
· Code review is a formal process that includes security · Preliminary code review is done as a checkpoint before the formal review		· Security is not considered during code review · Security consideration in code review is minimal
	Post-development Testing	
vulnerabilities, or for final verification · Testers have the final approval		· Post-development security testing is feature-driven · Post-development security testing is adhoc · Post-development security testing is externally-driven

Security is a priority during post-development

Security is not considered in post-development

Security Adopters Themes	Common Themes	Security Inattentive Themes
	Design	
· Security design is very important	· Security is not considered in the design stage	· Security consideration in the design stage is adhoc
	Implementation	
	· Security is a priority during implementation · Developers' awareness of security is expected when implementing	· Security is not a priority during implementation · Developers take security for granted · Developers misuse frameworks · Developers lack security knowledge · Developers perceive their security knowledge inaccurately · Vulnerability discovery can motivate security
	Developer Testing	
· Developers test for security fortuitously · Security is a priority during developer testing	· Developers do not test for security	· Developers' security testing is feature-driven
	Code Analysis	
· Security is a priority during code analysis		· Security is a secondary objective during code analysis · Developers rarely perform code analysis, never for security · Developers vary in awareness of analysis tools
	Code Review	
· Code review is a formal process that includes security · Preliminary code review is done as a checkpoint before the formal review		· Security is not considered during code review · Security consideration in code review is minimal
	Post-development Testing	
· Security is a priority during post-development testing · Post-development testing is used to discover security vulnerabilities, or for final verification · Testers have the final approval		· Security is not considered in post-development testing · Post-development testing plans include a security dimension · Post-development security testing is feature-driven · Post-development security testing is adhoc · Post-development security testing is externally-driven

"When we go to do a further security analysis, we have a lot more context in terms of what we're thinking, and people aren't running around sort of defending threats that aren't there."

–Adopters theme: Security design is very important

"Security testing [pause] I would say less than 5%. Because we're doing embedded systems, so security [is] pretty low in this kind of work."

– Inattentive theme: Developer testing is feature-driven

Digging Deeper…

Factors Affecting Security Practices

- Division of labour
- Resource availability
- Security knowledge

- Company culture
- External pressure
- Experiencing a security incident

Factors Affecting Security Practices

- Division of labour
- Resource availability
- Security knowledge

- Company culture
- External pressure
- Experiencing a security incident

Factors Affecting Security Practices

- Division of labour
- Resource availability
- **Security knowledge**

> "Probably in the two years that I've been working, I never got feedback [on] the security of my code [...] [Developers reviewing code] don't pay attention to the security aspect and they **can't** basically make a comment about the security of your code."

- Company culture
- External pressure
- Experiencing a security incident

Factors Affecting Security Practices

- Division of labour
- Resource availability
- Security knowledge

- Company culture
- External pressure
- Experiencing a security incident

Factors Affecting Security Practices

- Division of labour
- Resource availability
- Security knowledge

- Company culture
- External pressure
- **Experiencing a security incident**

"No one had really been thinking about looking at the product from security stand-point and so the new tester we had hired, he really went at it from 'how can I really break this thing?' [..] and found quite a few problems with the product that way."

Now What?

Now What?

- Rethink best practices
- Focus on building a security company culture

"To be honest, I don't think anybody cares about [security]. I've never heard or seen people talk about security at work [...] I did ask about this to my managers, but they just said 'well, that's how the company is. Security is not something we focus on right now.'"

–Factor: Company culture