A Cross-role and Bi-national Analysis on Security Efforts and Constraints of Software Development Projects

Fumihiro Kanei, Ayako Akiyama Hasegawa, Eitaro Shioji, Mitsuaki Akiyama

NTT, JAPAN

ACSAC 2021, 9 December 2021.

Background and Motivation

Background

- It is important to detect and fix vulnerabilities in the development phase
- Software security tends to be less prioritized than other explicit requirements in development projects

Motivation

- Understand the obstacles that prevent the adoption of secure software development practices
- Utilize the findings to design security measures that can be easily adopted in development projects

Research Questions

RQ1: How do software development characteristics impact developers' security behavior and awareness?

RQ2: Are there any gaps between developers and managers regarding security behavior and awareness?

RQ3: Do security behavior and awareness of software development professionals follow the same tendency in the United States and Japan?

Survey design: overview

Questions in our survey

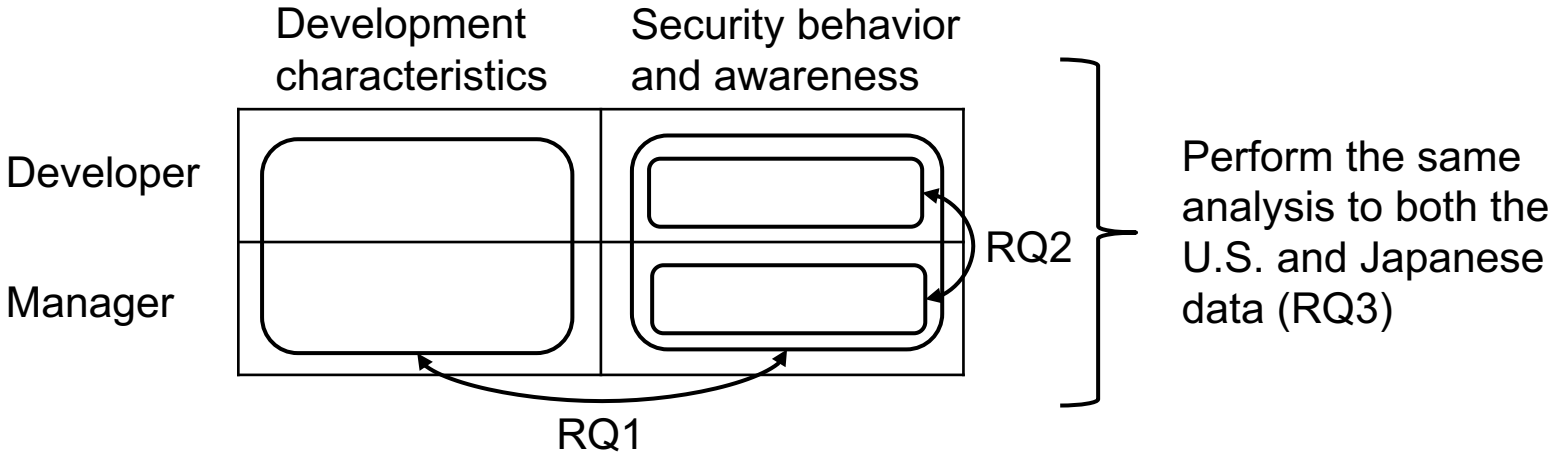
1. Demographics (e.g., age, gender)
2. Development characteristics
3. Security behavior and awareness

Target roles of participants

- Developers / Managers

Countries

- The U.S. / Japan



Survey design:

Questions about development characteristics

characteristics	Format	Options
Contractual relationship	Choice	• In-house development • Contracted development
User scope	Choice	• General public user • Limited to specific users
Development method	Choice	• Waterfall • Agile • Hybrid (e.g., Spiral)
Industry	Choice	• Public services • Finance and insurance, • Information • Medical and health-care, etc.

Survey design:
Questions about security behavior and awareness

Type	# of Questions	Format	Example of question
Resources spent on security	1	Numeric (0 to 100)	• What is the percentage of the resource directed towards security [...] in your development project?
Security awareness	5	5-point Likert (Strongly agree - Strongly disagree)	• I think software security is an important issue for our project.
Security Efforts	15	5-point Likert* (Strongly agree - Strongly disagree)	• Our project uses a tool to check whether secure coding practices are incorporated. • Our project has an in-house security assessment team.
Security Constraints	11	5-point Likert (Strongly agree - Strongly disagree)	• Our project does not have enough time to ensure software security. • I do not have the authority to decide to introduce security measures.

*For participants unaware of what security efforts were in place, these questions includes the option of “Not sure”.

NTT

Survey design:

Recruitment

Screening conditions:

1. Working on software development in a team of multiple people
2. The role in the development project is ...
   - › Developer (with development tasks such as implementation, testing, and reviewing)
   - › Manager (with management tasks such as scheduling and resource management)

Number of participants:

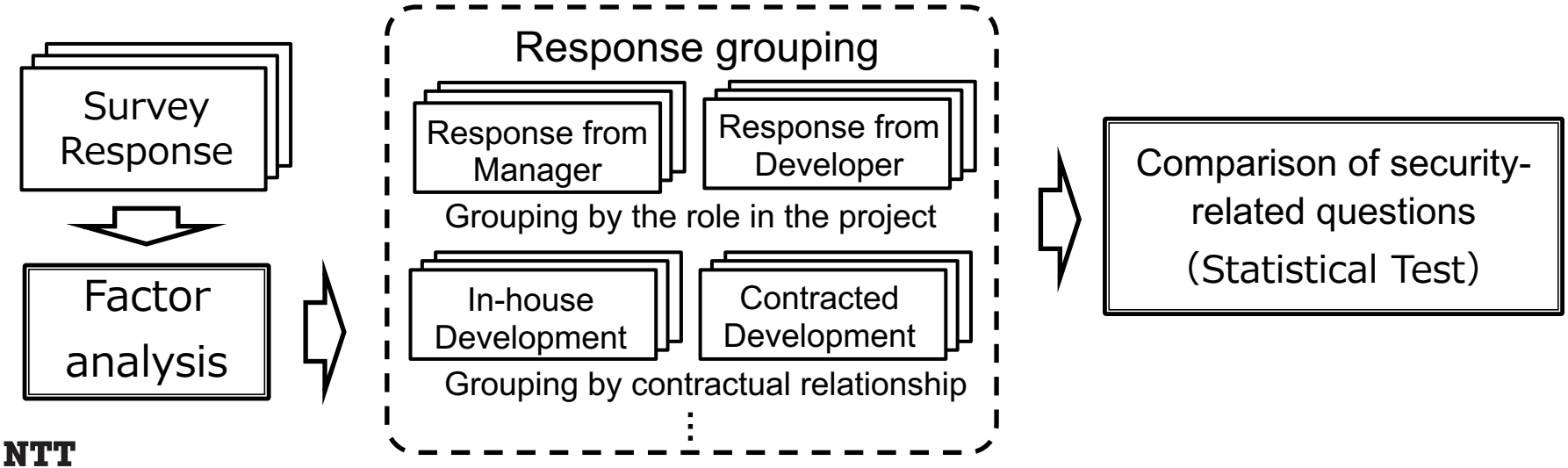
- The U.S. : 307 (162 developers, 149 managers)
- Japan : 357 (184 developers, 173 managers)

Web panels: a paid service offered by a survey company

Participation reward: US$10

Analysis Procedure

1. Grouping security-related questions by **exploratory factor analysis**
2. Response grouping by analysis perspective
   (e.g., developer or manager, in-house or contracted development ...)
3. Comparison of security-related questions by statistical test



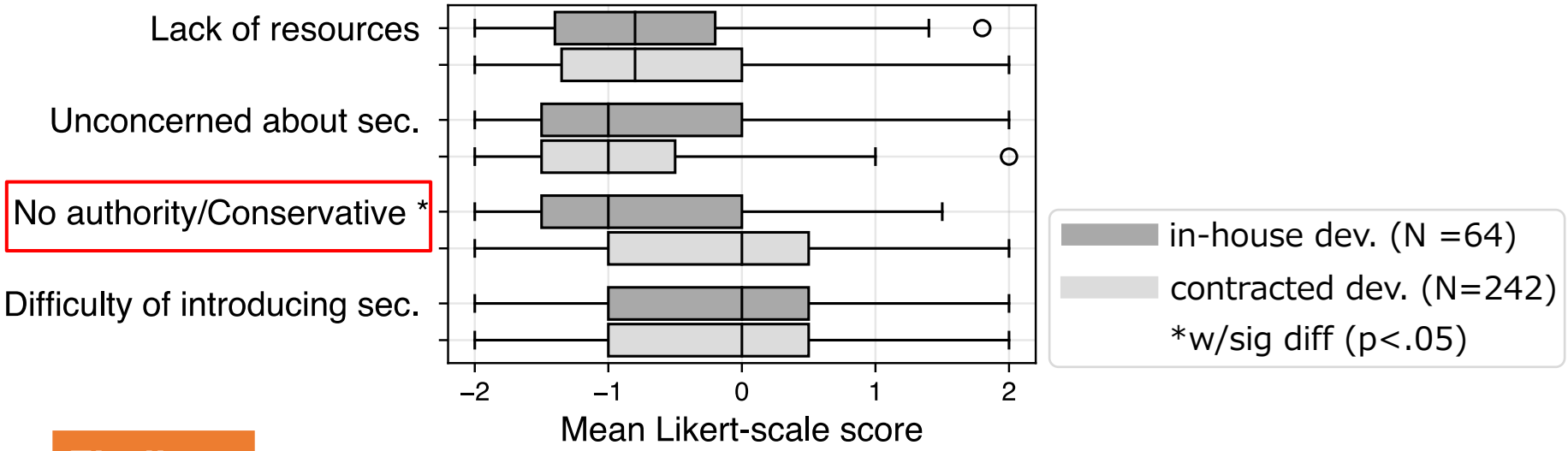
Results : Factor analysis

- **Grouping Results:**
  - Security efforts: 15 questions → 3 factors, Security constraints: 11 questions → 4 factors
- The answers to questions belonging to the same factor was averaged (-2: Strongly disagree to +2: Strongly agree)

Extracted Factors (Security constraints)

Factors	Description
Lack of Resources	Security constraints caused by a lack of various resources (time, budget, people, etc.)
Unconcerned about security	Security constraints caused by unconcern about security in development projects.
No authority / Conservative	Difficulty of changing the current development process and how lack of decision-making authority interferes with security.
Difficulty of introducing sec. measures	Difficulty of introducing new security measures into the development project.

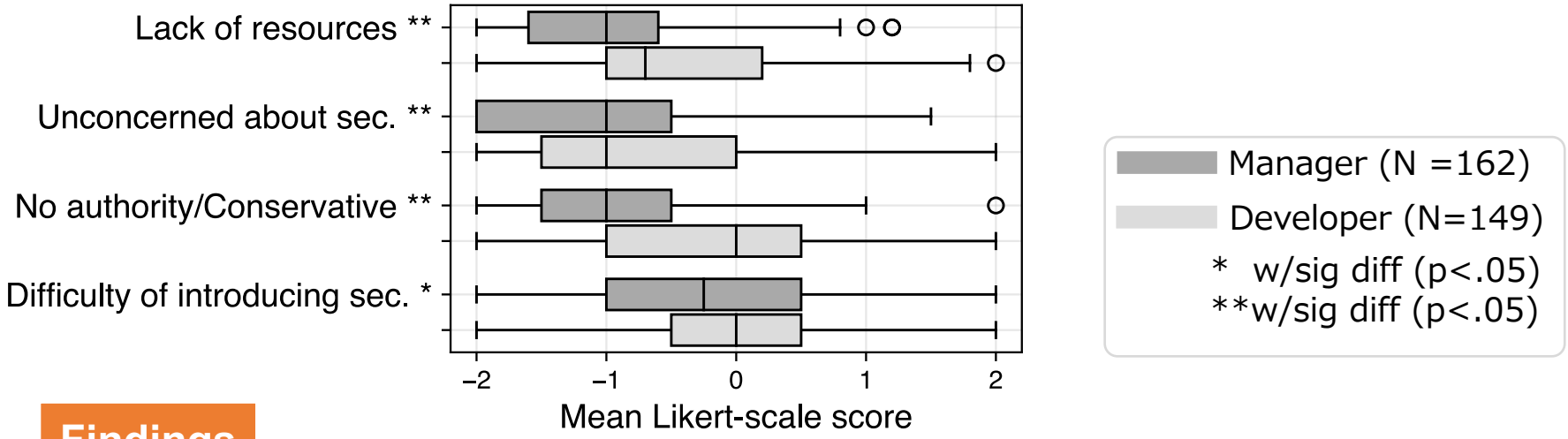
Results :
RQ1. Comparison between contractual relationships



Findings

People in a **project located in the lower part of a contractual hierarchy** feel more constrained due to their lack of decision-making authority
⇛ possibly due to requests made or priorities set by their contractor

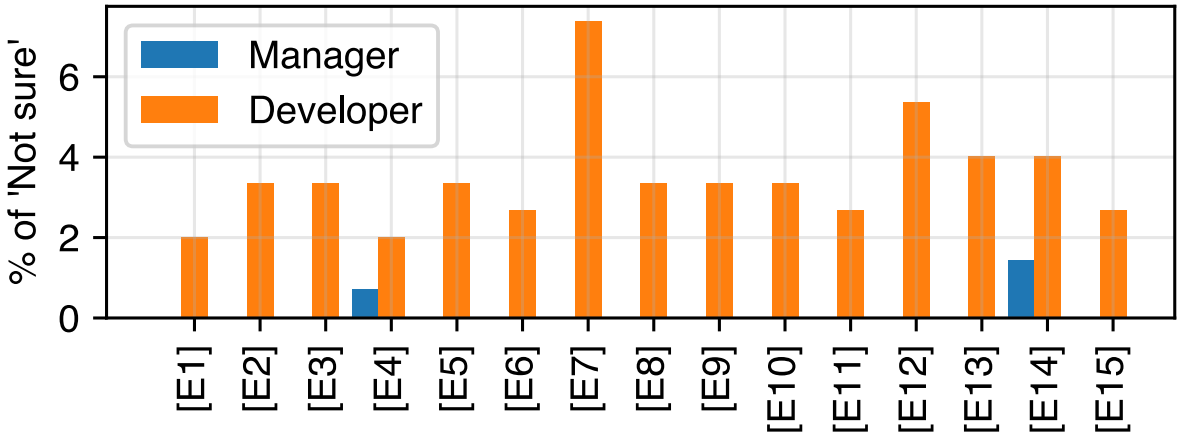
Results :
RQ2. Comparison between developers and managers



Findings

1. **Difficulty of decision-making** (e.g., introducing new sec. measures) is a strong security constraint for both developers and managers
2. There are **gaps in perception** between developers and managers
   ⇛ Managers tend to feel less constrained about security than developers
   ⇛ Developers tend not to know the overall security efforts of the project

Results :
RQ2. Comparison between developers and managers



Percentage of “Not sure” in questions about security effort

Findings

1. **Difficulty of decision-making** (e.g., introducing new sec. measures) is a strong security constraint for both developers and managers
2. There are **gaps in perception** between developers and managers
   ⇛ Managers tend to feel less constrained about security than developers
   ⇛ Developers tend not to know the overall security efforts of the project

Results :
RQ3. Comparison between the U.S. and Japan

- **Common between the U.S. and Japan**
  - Difficulty of decision-making is a strong security constraint
  - Managers tend to feel less constrained about security than developers
  - Developers tend not to know the overall security efforts of the project

- **Different between the U.S. and Japan**
  - People in projects in Japan tend to conduct less security effort and feel more constrained than people in projects in the U.S.

Implications

- **Supporting security-related decision-making**
  - Decision makers need to be assisted in the decision-making process
  - Interventions to bridge the gaps between developers' and managers' perceptions should be conducted
    - › e.g., sharing the security issues that developers are concerned about with managers

- **Designing appropriate user study**
  - To improve the ecological validity, researchers must consider the characteristics of developers and managers, and select appropriate participants who suit the purpose and content of a survey

Discussions

- **Limitations**
  - Social desirability bias
    - › The survey was conducted anonymously, and all questions were optional
  - Lack of population generalizability (only the U.S. and Japan)

- **Ethics**
  - We followed the research ethics principles stated in the Menlo Report (IRB approval)
    - › Participants were informed in advance about the content of the survey
    - › Compliance with personal information protection laws

Conclusion and future work

- **Conclusion**
  - We conducted an online survey for software development professionals, and quantitatively analyzed obstacles that prevent secure software development
  - The lack of decision-making authority and difficulty in decision-making are large obstacles that prevent secure software development
  - By comparing the answers between developers and managers, we found gaps in perception between them

- **Future work**
  - Assisting security-related decision-making in the development process
    - › e.g., design metrics that can be used as indicators for security-related decision-making

A Cross-role and Bi-national Analysis on Security Efforts and Constraints of Software Development Projects

Contact: fumihiro.kanei.sw@hco.ntt.co.jp

Thank you!