HOW DO YOU KNOW THAT A SECURITY REQUIREMENTS METHOD ACTUALLY WORK?

Dr. Federica Paci
Research Fellow
University of Trento

ITT Trust and Security Seminar (TSS)
September 26 2012

OUTLINE

- Motivation and Research Questions
- Studies Design
- Studies Execution
- Analysis and Results
- Main Findings
- Conclusions

Evaluating SRE Methods

- Security requirements methods
  - Leiter and Van Lamsweerde on anti-goals
  - Liu & Yu on i-*method (father of SI*)
  - Massacci, Mylopoulos, Zannone, Asnar on SI*
  - Mouratidis and Giorgini on SecureTropos
  - Haley, Yu, & Nuseibeh on Problem Frames
- Security methods, procedures used in industry
  - ISO 27000 series, OWASP, CLASP, COBIT, COSO ….
- Usually validated by applying them to a realistic scenario

THE NEED OF EXPERIMENTING MORE

- Survey of Condori-Fernandez et al. ESEM'09
  - 67% of Requirement Engineering papers have an "Experiment" – evaluation by the designer
  - 13% have a "Case Study"
- Examples
  - Opdahl et al.[Inf. Softw. Tech.2009] two comparative controlled experiments: misuse cases vs attack treesa
  - Gegick et al. [SIGSOFT 2005] experiments with undergraduate students to validate SAFE-T methodology
  - Yskout et al.[ICSE 2012] Controlled experiment with master students to assess the impact of using annotations on patterns selection

RESEARCH QUESTIONS

Do security requirements methods work when they are applied by someone different than their own inventor?

If Yes Why?

If Not Why Not?

STUDIES DESIGN I

- **eRISE** (Engineering **RI**sks and **SE**curity Requirements)
  - Two qualitative studies inspired to the principles of grounded theory (Glass & Strauss 1967)
- **Data collection and analysis**
  1. Questionnaires ➔ Statistical Analysis
  2. Post-it notes ➔ Affinity Analysis
  3. Focus Groups Interviews ➔Coding
  4. Participants Reports ➔Qualitative Content Analysis
  5. Audio-Video Recording ➔Coding

STUDIES DESIGN II: ACTORS

- **Designer**
  - The security requirements method inventor
- **Customer**
  - The owner of a case study on which the SRE methods are applied
- **Observer**
  - Audio-video record Participants
- **Researcher**
  - Collect and Analyze the data
- **Participant**
  - Apply an SRE method to analyze a case study

STUDIES DESIGN IV: ACTUAL NUMBERS

- Method Designers: 6 (out of 9 being invited)
- Observers: 7
- Participants: 91 participants
  - 28 Master Students in Computer Science from University of Trento
  - 63 Practioners attending a Master Course in Audit for Information Systems from Dauphine University
- Customers : 2 ATOS and SIEMENS

SRE METHODS EVALUATED

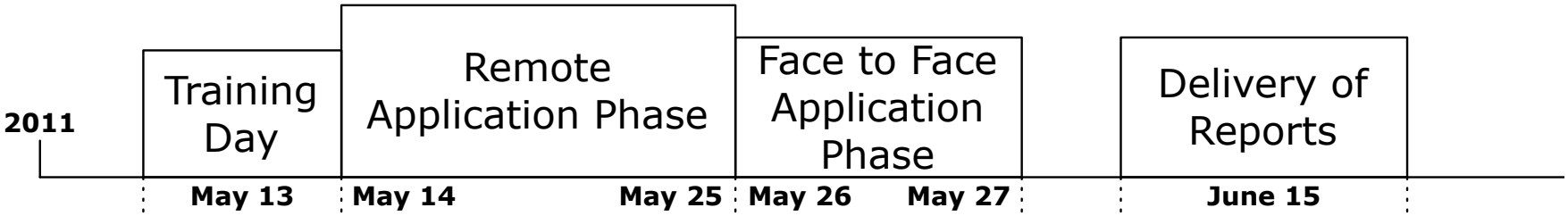
- CORAS: Risk Analysis method by SINTEF [72 citations]
- LINDDUN: Privacy requirements elicitation by KUL [11 citations]
- SECURE TROPOS: SRE method by UEL [78 citations]
- SECURITY ARGUMENTATION: SRE method by OU [132 citations]
- SI*: SRE method by UNITN [[139 citation]
- SREP: SRE method by UCLM [19 citations]

STUDIES DESIGN III: PROTOCOL

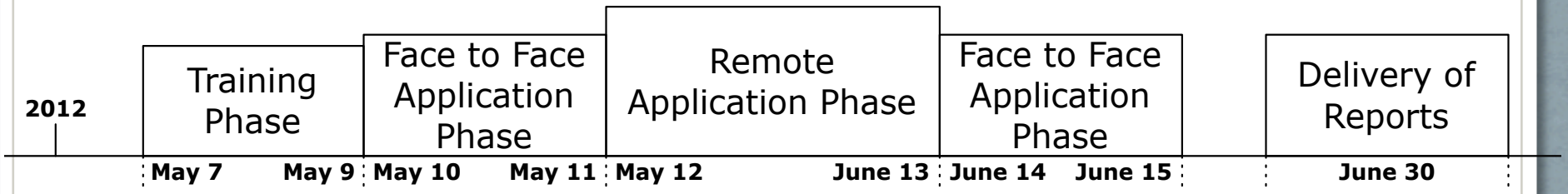
- **Training of Participants**
  - Designers and customers train participants on methods and case studies
- **Application of Methods**
  - Groups of participants apply methods to analyze the case study
- **Evaluation**
  - Participants evaluate the methods' effectiveness
  - Designers and customers evaluate correctness of application

STUDIES EXECUTION

eRISE 2011

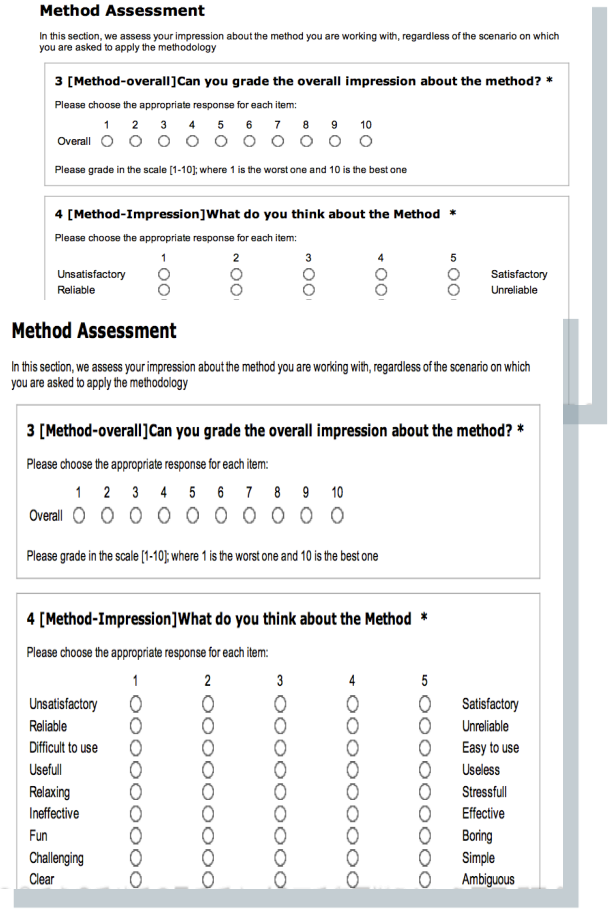


eRISE 2012



QUESTIONNAIRES: STATISTICAL ANALYSIS

- Collect Information about:
  - Participants' background
  - Methods' Effectiveness
  - Comparison with other methods
- Administered at different stages:
  - Beginning (Q1)
  - Post Training (Q2)
  - During Application (Q3)
  - Post Application (Q4)



Method Assessment

In this section, we assess your impression about the method you are working with, regardless of the scenario on which you are asked to apply the methodology

3 [Method-overall]Can you grade the overall impression about the method? *

Please choose the appropriate response for each item:

	1	2	3	4	5	6	7	8	9	10
Overall	○	○	○	○	○	○	○	○	○	○

Please grade in the scale [1-10]; where 1 is the worst one and 10 is the best one

4 [Method-Impression]What do you think about the Method *

Please choose the appropriate response for each item:

	1	2	3	4	5	
Unsatisfactory	○	○	○	○	○	Satisfactory
Reliable	○	○	○	○	○	Unreliable
Difficult to use	○	○	○	○	○	Easy to use
Usefull	○	○	○	○	○	Useless
Relaxing	○	○	○	○	○	Stressfull
Ineffective	○	○	○	○	○	Effective
Fun	○	○	○	○	○	Boring
Challenging	○	○	○	○	○	Simple
Clear	○	○	○	○	○	Ambiguous

Method Assessment

In this section, we assess your impression about the method you are working with, regardless of the scenario on which you are asked to apply the methodology

3 [Method-overall]Can you grade the overall impression about the method? *

Please choose the appropriate response for each item:

	1	2	3	4	5	6	7	8	9	10
Overall	○	○	○	○	○	○	○	○	○	○

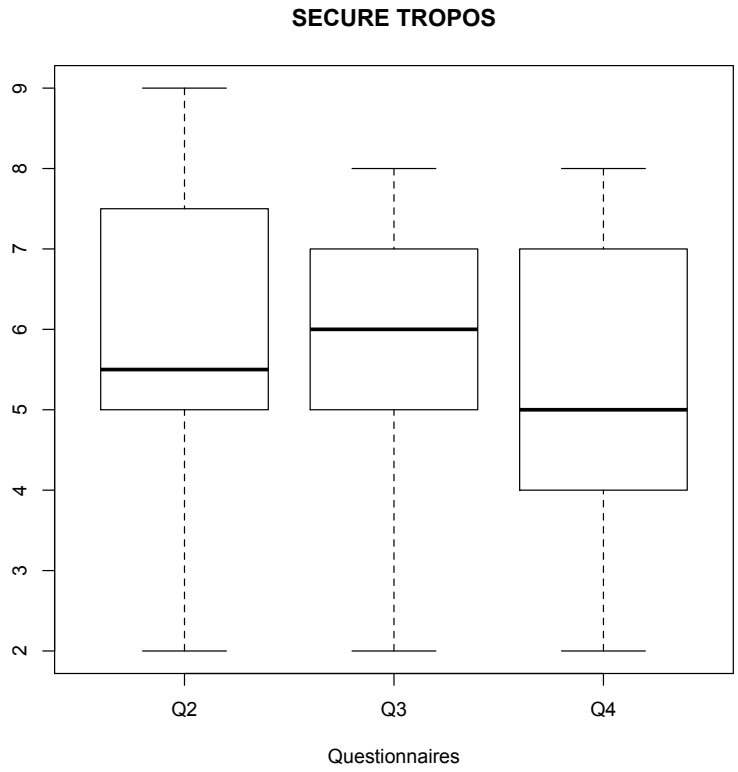
Please grade in the scale [1-10]; where 1 is the worst one and 10 is the best one

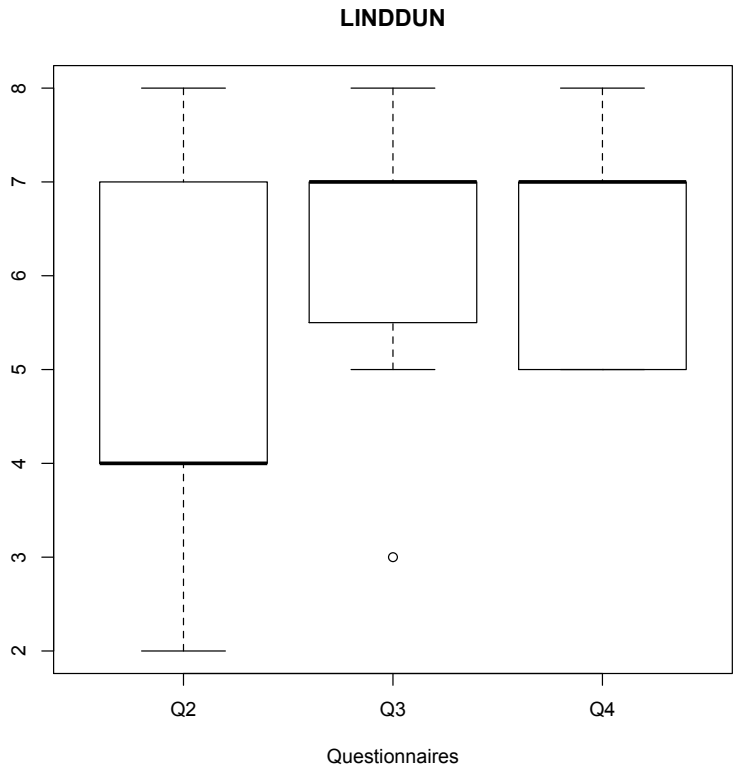
4 [Method-Impression]What do you think about the Method *

Please choose the appropriate response for each item:

	1	2	3	4	5	
Unsatisfactory	○	○	○	○	○	Satisfactory
Reliable	○	○	○	○	○	Unreliable
Difficult to use	○	○	○	○	○	Easy to use
Usefull	○	○	○	○	○	Useless
Relaxing	○	○	○	○	○	Stressfull
Ineffective	○	○	○	○	○	Effective
Fun	○	○	○	○	○	Boring
Challenging	○	○	○	○	○	Simple
Clear	○	○	○	○	○	Ambiguous

QUESTIONNAIRES: RESULTS





FOCUS GROUPS TRANSCRIPTS: CODING

- Focus groups aimed at collecting information about
  - Opinions of participants on methods' application
- Analyzed using coding
  - content analysis technique used in grounded theory
- Three main categories identified
  - Mindmapping
  - Identification of Security Requirements
  - Knowledge

Timespan	Content
0:00.0 - 1:48.0	How is the process suggested by the method? MP: the process starts by focusing on the data flow and that is important. but the process only focuss data flow, we need to also consider the business process. about the data flow not in statical way but i dynamic way. So its an evolution of data flow over time. and this is not well stated and not quite part process.
1:48.1 - 3:37.0	ZP: I think the use of the diagrams is very useful to provide an overview of the method. next line is not clear. [noisy, not clear]. ZP: architecture of the method is very wrong, a lot of things needs to be done in 6 steps. and sometim very easy to map what we designed using the data flow and what the method actually asks. its not ver concept wise and so it is hard to apply the method.
3:37.3 - 4:48.0	ZiP: I'd like to add something. About the threat tree pattern, it is useful because it makes you think ab threats. but it could have an impact on other things. So it would be good to think also about the other rather than only the threat pattern. Federica: So you mean to say you could have done more, but somehow it doesn't allow. ZiP: yes. ma would be good if we could think of other things (impact) during the threat pattern.

FOCUS GROUPS TRANSCRIPTS: RESULTS

Mindmapping

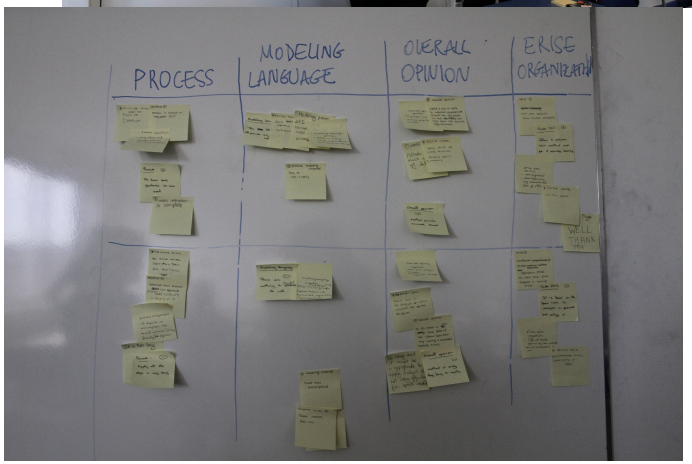
- *CORAS helps to organize the ideas in the mind, by using the diagrams.* Professional
- SECURE TROPOS … *is a good way to mindmap the use case,* Professional

Identification of SR

- *CORAS, it doesn't tell me this is a risk, I decide this is a risk*, Student
- *SECURE TROPOS.. is not a method to find security recommendations,* Professional
- *SREP helps to find out specific security requirement*, Professional
- LINDDUN *steps help to ensure safety of a company data*, Professional

POST-IT NOTES: AFFINITY ANALYSIS

- Participants divided in two groups
- Each participant filled in a post-it note with a **positive** and **negative** aspect of
  - Method
  - Modeling language
  - Process
  - Tool
- Participants group post-it notes
- Participants prioritize post-it notes



POST-IT NOTES: RESULTS

Positive Aspects

- CORAS: Detailed process
- LINDDUN: Focused on privacy, Data Flow Diagrams
- SECURE TROPOS: Support for Mindmapping
- SECURITY ARGUMENTATION: Argumentation Analysis
- SI*: Help Brainstorming
- SREP: Familiar vocabulary

Negative Aspects

- CORAS: Definition of likelihood and consequence scales
- LINDDUN: Threat Prioritization
- SECURE TROPOS: sProcess not well defined
- SECURITY ARGUMENTATION: Tool's Bugs
- SI*: Risk Analysis
- SREP: Long Process

REPORTS: EVALUATION

- **Designers** evaluate ….

  the correctness of method application and of the results

- **Customers** evaluate ….

  if the security requirements are specific for the case study

REPORTS: RESULTS (1)

1-5	6-10	11-15

Groups	Method	Designer	Customer
Group 1	CORAS	10	15
Group 2	CORAS	14	9
Group 3	CORAS	7	9
Group 4	SEC. TROPOS	9	7
Group 5	SEC. TROPOS	12	5
Group 6	SEC. TROPOS	15	13
Group 7	SEC.ARG	14	9
Group 8	SEC. ARG	10	10
Group 9	SEC. ARG	12	9

REPORTS: RESULTS (2)

1-5	6-10	11-15

Groups	Method	Designer	Customer
Group 10	SREP	10	13
Group 11	SREP	13	8
Group 12	SREP	11	14
Group 13	LINDDUN	12	14
Group 14	LINDDUN	6	12
Group 15	LINDDUN	14	8
Group 16	SI*	8	N/A
Group 17	SI*	6	N/A
Group 18	SI*	5	N/A

MAIN FINDINGS: PARTICIPANTS' OPINIONS

- CORAS, SECURE TROPOS, SECURITY ARGUMENTATION AND SI*
  - Support brainstorming
  - Do not help to identify security requirements
  - Analysts have to use their knowledge in security to identify security requirements
- SREP and LINDDUN
  - Guide the analyst through the identification of security/privacy requirements

WHY

- Detailed Process
  - CORAS, SREP, LINDDUN
- Patterns that guide the identification of security requirements
  - LINDDUN, SREP
- Graphical Models
  - CORAS, LINDDUN, SI*, SECURE TROPOS

WHY NOT

- No detailed process to identify security requirements
  - SI*, SECURE TROPOS
- Lack of patterns/guidelines to identify requirements
  - CORAS, SI*, SECURE TROPOS, SECURITY ARGUMENTATION
- Tool with lot of bugs
  - CORAS, SI*, SECURE TROPOS, SECURITY ARGUMENTATION

SREP and LINDDUN have no tool but perform well

THREATS TO VALIDITY

- **Internal Validity**
  - Participants' knowledge of other methods
  - Training Time too short
- **External Validity**
  - Generalization of our results
- **Conclusion Validity**
  - Statistical significance
  - Correctness of requirements identified

CONCLUSIONS

- eRISE
  - 2 qualitative studies over 2 years , 6 designers, 91 participants, 7 observers, 2 customers
  - Evaluation based on an application scenario is a lot easier !!!
- CORAS, SECURITY ARGUMENTATION, SECURE TROPOS and SI*
  - Support Brainstorming
  - Expertise in security is required
- SREP and LINDDUN
  - Guide to the identification of security/privacy requirements
- Next year eRISE 2013 (Do you want to join?)