An Experimental Comparison of Two Risk-Based Security Methods (ESEM 2013)

Katsiaryna Labunets, Fabio Massacci, Federica Paci, and Le Minh Sang Tran
University of Trento, Italy

email: <name.surname@unitn.it>

EOSESE, Lille, France
June 30th, 2014

UNIVERSITY OF TRENTO - Italy

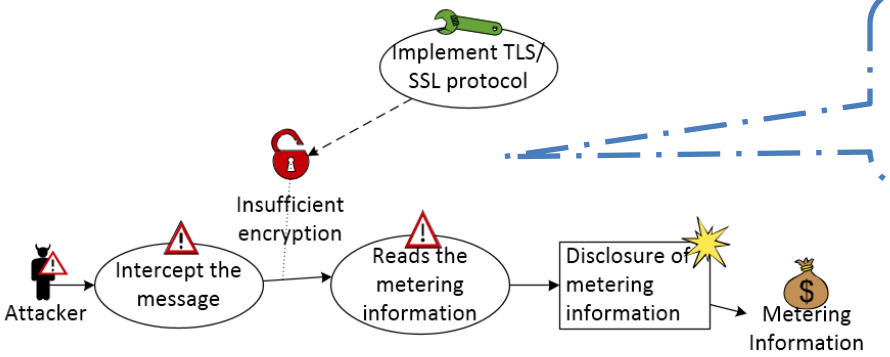
Motivation and Background

- Several methodologies and standards to identify threats and possible security requirements are available
  - Risk-based e.g SREP, SecRAM, ISO 27005, NIST SP 800-30
  - Goal-based e.g SABSA
  - Problem-based e.g SECURITY ARGUMENTATION
- What standard to use?
- What methodology to follow?

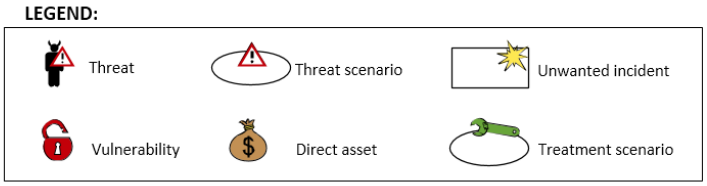
Research Goal (1)

- Limited empirical evidence on how security engineering methods work in practice
  - Opdahl [Opdahl 2009] misuse cases, attack trees
  - Massacci et al. [NordSec2012] risk-based vs goal-based vs problem-based

Research Goal (2)



CORAS = Graphical Method,
Threats & Countermeasures in 1 diagram
Whole book describes methodology

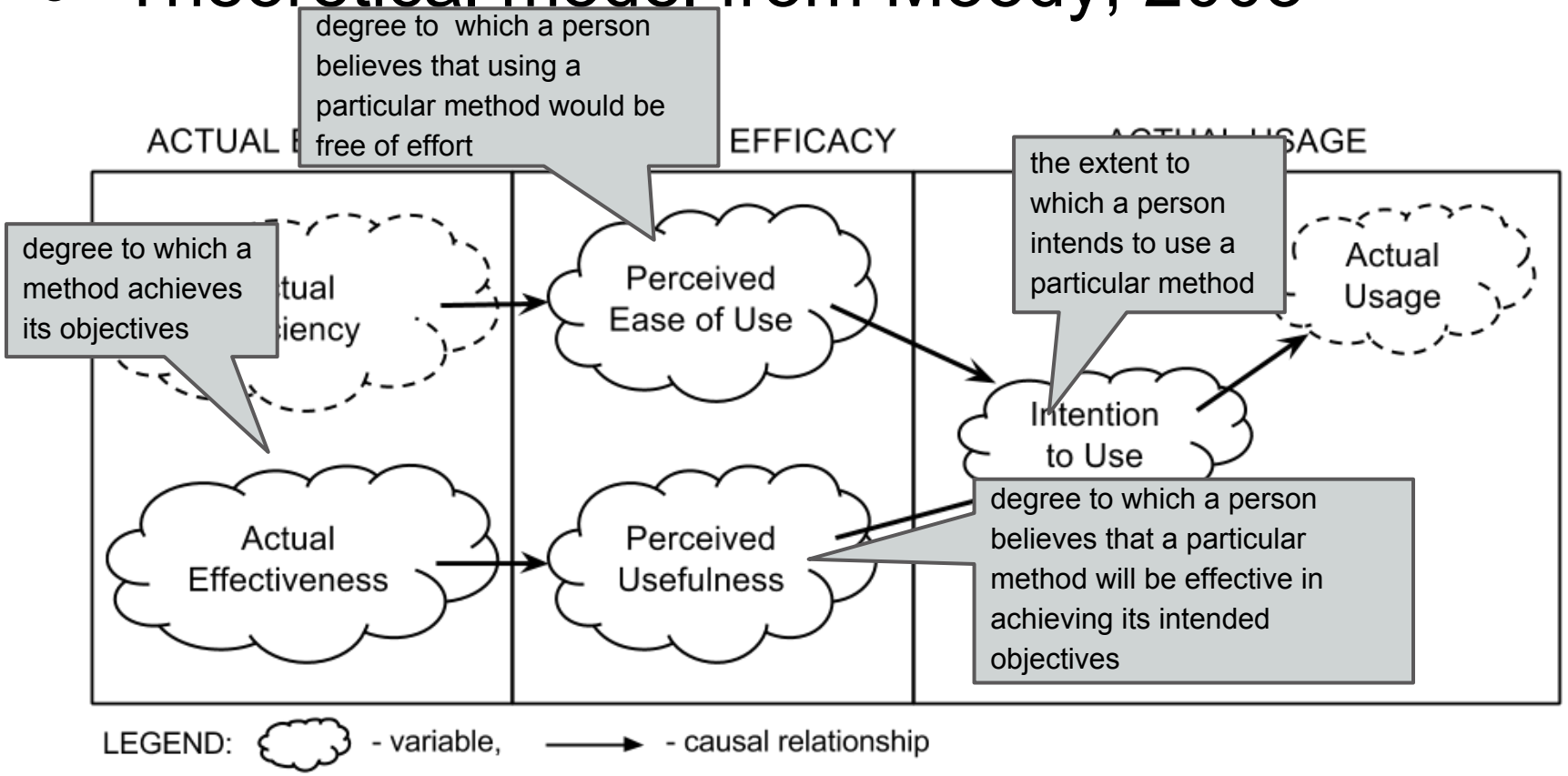


SREP = Textual Method,
Threats & Security Requirements in 2 Tables
Research papers describe the approach

Name of Misuse Case: Spoof of information		
ID 1		
Summary: the attacker gains access to the message exchange between the SM and SNN and disclose the secret exchange of information		
Probability: Frequent		
Preconditions: 1) The attacker have access to the communication channel between SM and SNN		
User Interactions	Misuser interactions	System Interaction
The SM sends the information about power consumption		
	The attacker reads the information	
		The SSN receives the information without knowing that someone have read the message
Postconditions: 1) The attacker knows personal information about the power consumption of the customer		

Research Model

- Theoretical model from Moody, 2003



Research Questions

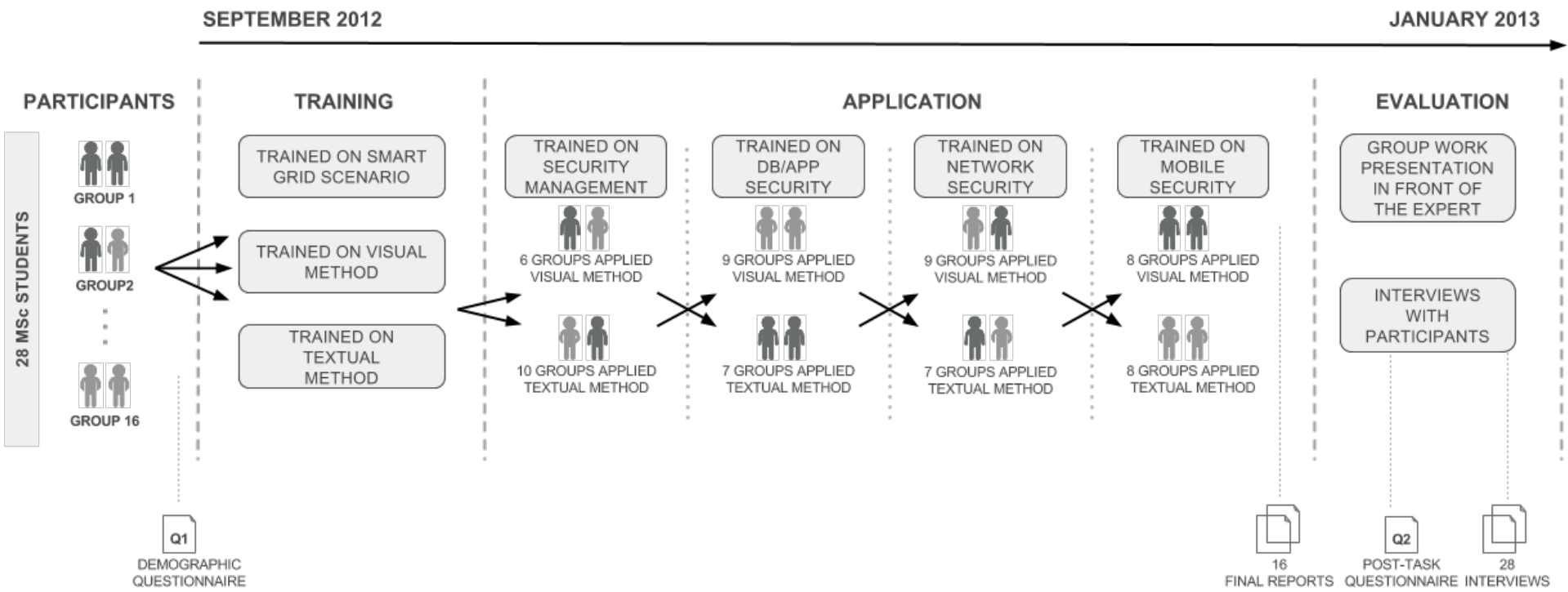
Is there a difference between visual and textual risk-based methods with respect to?

- *actual effectiveness (RQ1)*
- *overall preference (RQ3)*
- *perceived ease of use(RQ4)*
- *perceived usefulness (RQ5)*
- *intention to use (RQ6)*

Experiment Design

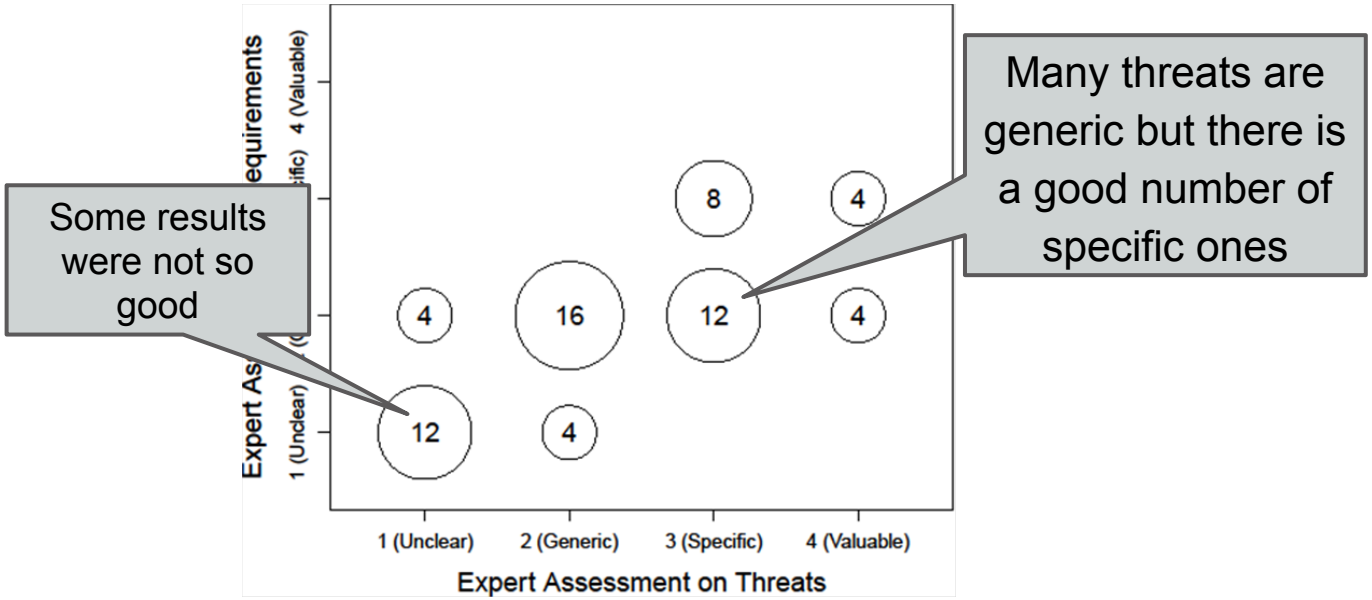
- **Variables and Metrics**
  - Actual Effectiveness
    - N° of “good quality” threats and security requirements
    - Quality Evaluated by a Security Expert
  - Perceived Ease of Use (PEOU), Perceived Usefulness (PU), Intention to Use (ITU)
    - Post-task questionnaire
- **Design**: Within-subject design/Randomized Group Assignment
  - 16 groups, 4 security analysis tasks from Smart Grid domain

Experiment Execution



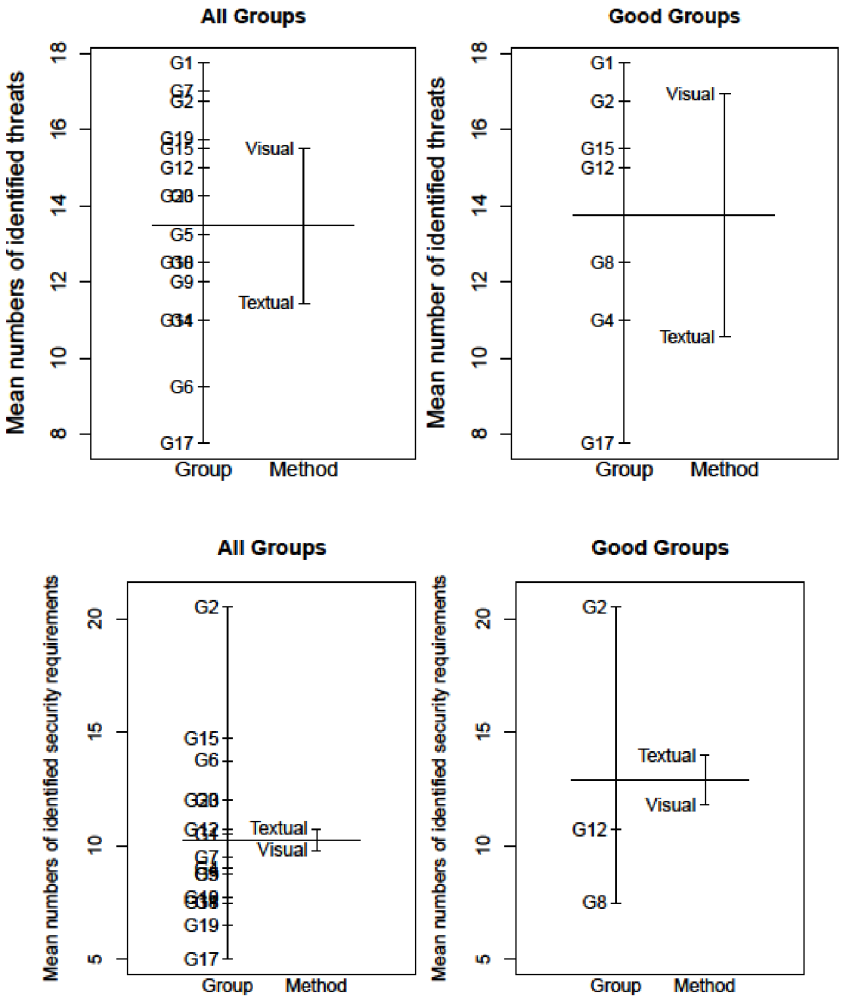
Reports Analysis

- Coding: N° of Threats and Security Requirements
- Expert Assessment of Results' Quality
  - Are identified threats meaningful?
  - Are identified security requirements appropriate?
- Statistical analysis: ANOVA with α = 0.05



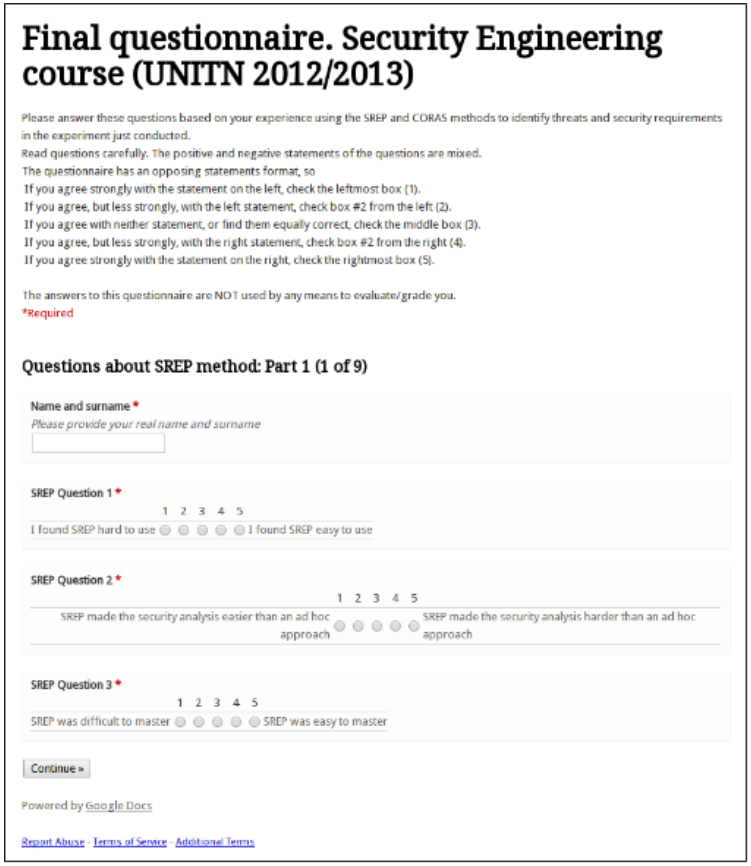
Actual Effectiveness (RQ1)

- Threats
  - Visual Method is better than Textual
  - Both for Good and All Groups
  - Statistically significant for both groups
- Security Requirements
  - Textual slightly better than Visual
  - Only tiny difference between Good and All groups
  - But Not statistically significant



Questionnaire Analysis

- 22 questions in opposite statement format
  - 12 questions on PEOU, PU, ITU
  - 5 questions on specific method' aspects
  - 4 questions on tasks' difficulty
- Statistical test: Wilcoxon rank-sum test with $\alpha = 0.05$



Final questionnaire. Security Engineering course (UNITN 2012/2013)

Please answer these questions based on your experience using the SREP and CORAS methods to identify threats and security requirements in the experiment just conducted.
Read questions carefully. The positive and negative statements of the questions are mixed.
The questionnaire has an opposing statements format, so
If you agree strongly with the statement on the left, check the leftmost box (1).
If you agree, but less strongly, with the left statement, check box #2 from the left (2).
If you agree with neither statement, or find them equally correct, check the middle box (3).
If you agree, but less strongly, with the right statement, check box #2 from the right (4).
If you agree strongly with the statement on the right, check the rightmost box (5).

The answers to this questionnaire are NOT used by any means to evaluate/grade you.
*Required

Questions about SREP method: Part 1 (1 of 9)

Name and surname *
Please provide your real name and surname

SREP Question 1 *
1 2 3 4 5
I found SREP hard to use ○ ○ ○ ○ ○ I found SREP easy to use

SREP Question 2 *
1 2 3 4 5
SREP made the security analysis easier than an ad hoc approach ○ ○ ○ ○ ○ SREP made the security analysis harder than an ad hoc approach

SREP Question 3 *
1 2 3 4 5
SREP was difficult to master ○ ○ ○ ○ ○ SREP was easy to master

Continue »

Powered by Google Docs

Report Abuse - Terms of Service - Additional Terms

Participants perception

- Perceived Easy of Use (RQ4)
  - Preference is higher for visual method
  - Not statistically significant for all participants
  - 10% statistical significance for good participants
- Perceived Usefulness (RQ5)
  - Higher preference for visual method
  - Not statistically significant for all participants
  - 10% statistical significance for good participants
- Intention to Use (RQ6)
  - Higher for visual method with statistical significance only for good participants

Interviews Analysis

- **Qualitative analysis**
  1. Identify recurrent statements
  2. Identify main emerging categories for each group of statements
  3. Count the frequency of statements

Speaker 1:	Thank you for coming. Today, just a short interview, we would like to ask you about you about your opinion between the two methods, CORAS and SREP. No pressures on this. No way to affect your grade. Firstly, I would like to ask about how organization in your groups. You work together, you work on both SREP and CORAS, or you divide the work? For example, you work only in SREP and your partner work only in CORAS or vice versa.
Speaker 2:	We both work together on the SREP and also on CORAS. We have [inaudible 00:49]. First, we try to read the case studies and we're trying to [inaudible 00:57] or break out for the CORAS, we trying to identify the assets and treats and all the steps. In both of them, we didn't already buy it, both study and on the second part, and on the second [inaudible 00:01:21]. The first part is there are assets and we try to reuse some of the assets on the second daily [learning 01:38] and we try to add some points on that, but other than that case we ...
Speaker 1:	Okay. So ...
Speaker 2:	We both, yeah.
Speaker 1:	All of you, what do you work more on that? CORAS or SREP? Which one will you work more on that? For you only.
Speaker 2:	For me, I was working in CORAS ...
Speaker 1:	More? Okay.
Speaker 2:	... more. Yeah, more on the drawing on creating the [inaudible 00:02:17]

Why Methods ARE Effective: Visual

- ➔ Visual summary for security analysis

  "Diagrams are useful. You have an overview of the possible threat scenarios and you can find links among the scenarios"

- ➔ Helps in identifying threats

  "Yes, it helped to identify which are the threats. In CORAS method everything is visualized. The diagrams helped brainstorming on threats"

Why Methods ARE Effective: Textual

- ➔ Clear Process

  "Well defined steps. Clear process to follow"

- ➔ Helps in identifying security requirements

  "The order of steps helped to identify security mitigations"

  "Steps by steps helped to discover more"

Why Methods ARE NOT Effective: Visual

- ➔ Scalability of Visual Notation

  "The diagrams are not scalable when there are too many links"

- ➔ Primitive Tool

  "The tool takes too much to arrange things"

  "When the diagrams are too large, the tool occupies too much memory"

Why Methods ARE NOT Effective: Textual

➔ Tabular Summary of Results

"It is not easy to represent what you think because there are a lot of tables. If you are a project manager and you want to show the results of the security analysis to your boss it is difficult because you use tables"

Threats to validity

- Conclusion Validity
  - Statistical Power -> ANOVA power = 0.89, Wilcoxon power = 0.86
- Internal Validity
  - Bias in data analysis -> 3 different researchers, expert assessment
- Construct Validity
  - Research instruments -> post-task questionnaire and interview guide reviewed by 3 different researchers
- External Validity
  - Realism of application scenarios and tasks

More Experiments

- CORAS (visual) vs SecRAM (textual) - Fall 2013
  - 29 MSc students, individual work, 2 security tasks from Smart Grid
  - Results:
    - Actual Effectiveness: CORAS ~ SecRAM
    - PEOU, PU, ITU: CORAS > SecRAM
  - Paper is accepted at EmpiRE 2014
- CORAS (visual) vs SecRAM (textual) - May 2014
  - 55 professionals in IT Audit of IS, group work, application scenario from Home Banking domain
  - Data Analysis in process

Conclusions and Future Work

- Controlled experiment with 28 Msc students to compare visual vs textual risk-based methods
- Main findings
  - Visual method more effective in identifying threats
    - Why: diagrams help brainstorming
  - Textual method more effective in identifying security requirements
    - Why: clear and systematic process
  - Visual method perception higher than the textual one
- Future work
  - Guidelines that provide decision support for selection
  - Causal explanations of why choosing a risk assessment method in given circumstances will be the best decision