PRELIMINARY EXPERIMENTS ON RELATIVE COMPREHENSIBILITY OF TABULAR & GRAPHICAL RISK MODELS

Katsiaryna Labunets

University of Trento, Italy (katsiaryna.labunets@unitn.it)

Joint work with

Yan Li[1], Fabio Massacci[2], Federica Paci[3], Martina Ragosta[4], Bjørnar Solhaug[1], Ketil Stølen[1], Alessandra Tedeschi[2]

[1]SINTEF, [2]University of Trento, [3]University of Southampton, [4]DeepBlue

Motivation - 1

- Risk recommendations should be “consumed” mostly by not-experts in security
- Security Risk Assessment in ATM
  - SESAR SecRAM method
    - Tabular-based
    - **Non-experts** in security **can apply it**
  - Future methods
    - new graphical models to support risk assessment

Motivation - 2

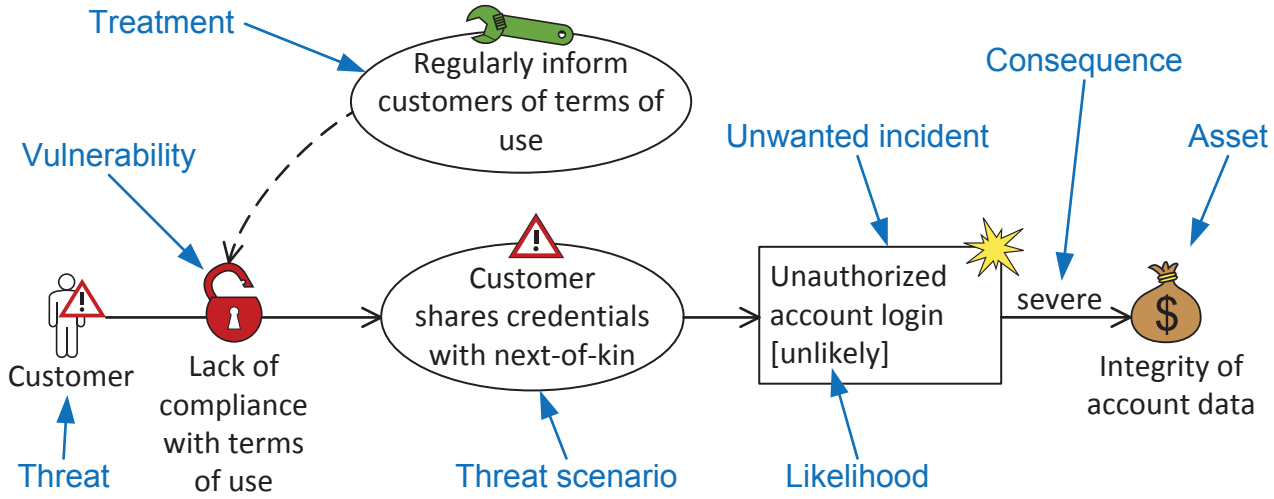
- What if the security representation is not easy to understand?
  - Stakeholder does not understand you
  - The security recommendations are not implemented

Research Method

- Goal
  - Tabular vs. graphical risk models: which is easier to understand?
- Treatments
  - Graphical risk model (CORAS)
  - Tabular risk model (NIST)
- Context

  Security risk assessment for the Online Banking scenario
  - Participants
    - 35 MSc students – University of Trento, Italy
    - 11 MSc students – University of Oslo, Norway
  - 8 comprehensibility question

Risk Modeling: Tables vs. Diagrams

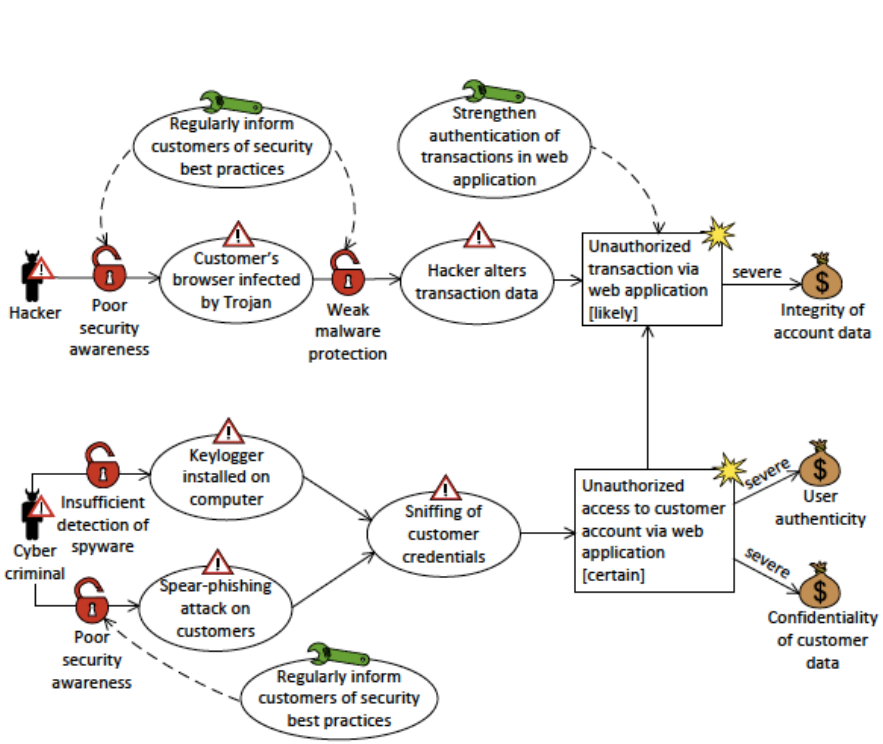


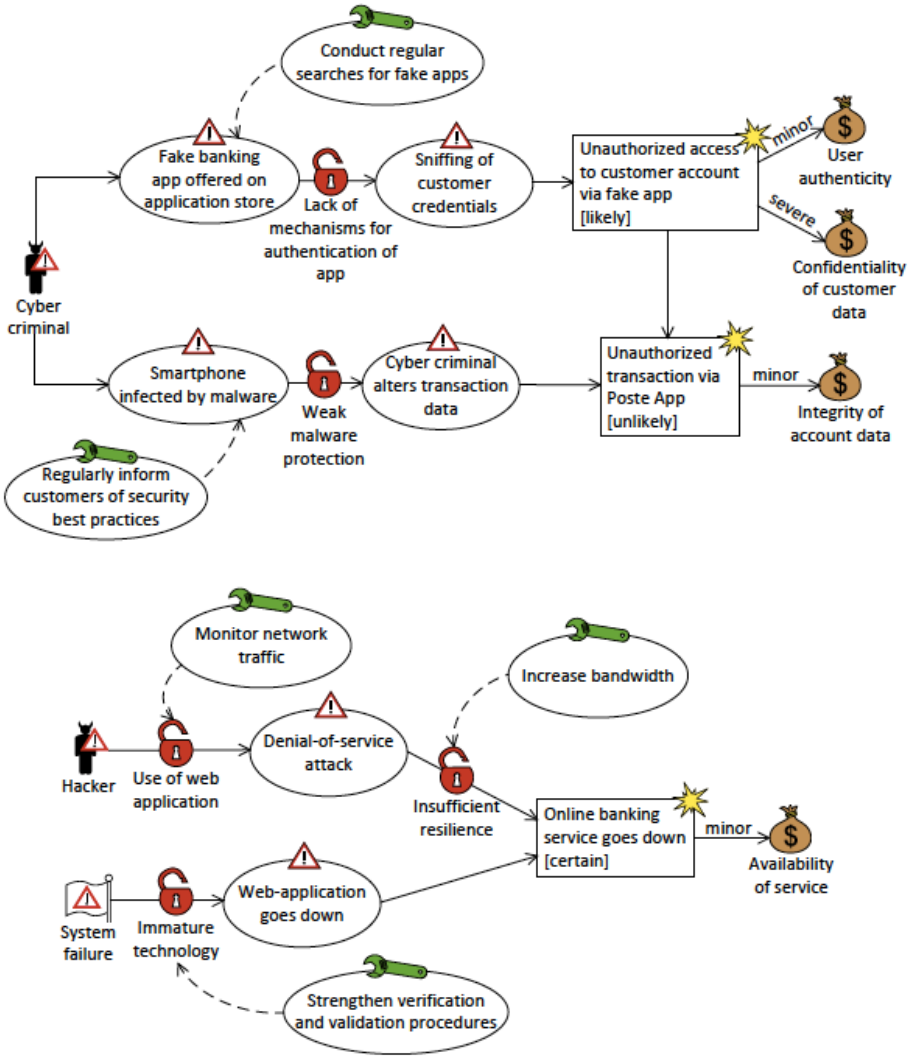
CORAS diagram

Threat event	Threat source	Vulnerability	Impact	Overall likelihood	Level of impact	Asset	Security control
Customer shares credentials with next-of-kin	Customer	Lack of compliance with terms of use	Unauthorized account login	Unlikely	Severe	Integrity of account data	Regularly inform customers of terms of use

NIST table row entry

Used Risk Models: CORAS





EMFASE

UNIVERSITY OF TRENTO

Used Risk Models: NIST

Threat Event	Threat Source	Vulnerabilities	Impact	Asset	Overall Likelihood	Level of Impact	Security Controls
Customers' browser infected by Trojan and this leads to Hackers alters transaction data.	Hacker	1. Poor security awareness 2. Weak malware protection	Unauthorized transaction via web application.	Integrity of account data	Likely	Severe	1. Regularly inform customers about security best practices to increase their security awareness and improve malware protection. 2. Strengthen authentication of transaction in web application to prevent unauthorized transaction vis web application.
Keylogger installed on computer and this leads to sniffing customer credentials. Which leads to unauthorized access to customer account via web application.	Cyber criminal	Insufficient detection of spyware	Unauthorized transaction via web application.	Integrity of account data	Likely	Severe	
Spear-phishing attack on customers leads to sniffing customer credentials. Which leads to unauthorized access to customer account via web application.	Cyber criminal	Poor security awareness	Unauthorized transaction via web application.	Integrity of account data	Likely	Severe	1. Regularly inform customers about security best practices to increase their security awareness. 2. Strengthen authentication of transaction in web application to prevent unauthorized transaction vis web application.
Keylogger installed on customer's computer and this leads to sniffing customer credentials.	Cyber criminal	Insufficient detection of spyware	Unauthorized access to customer account via web application.	User authenticity	Certain	Severe	
Spear-phishing attack on customers leads to sniffing customer credentials.	Cyber criminal	Poor security awareness	Unauthorized access to customer account via web application.	User authenticity	Certain	Severe	Regularly inform customers about security best practices to increase their security awareness.
Keylogger installed on customer's computer leads to sniffing customer credentials.	Cyber criminal	Insufficient detection of spyware	Unauthorized access to customer account via web application.	Confidentiality of customer data	Certain	Severe	
Spear-phishing attack on customers leads to sniffing customer credentials.	Cyber criminal	Poor security awareness	Unauthorized access to customer account via web application.	Confidentiality of customer data	Certain	Severe	Regularly inform customers about security best practices to increase their security awareness.
Fake banking app offered on application store and this leads to sniffing customer credentials.	Cyber criminal	Lack of mechanisms for authentication of app	Unauthorized access to customer account via fake app.	User authenticity	Likely	Minor	Conduct regular searches for fake apps.
Fake banking app offered on application store and this leads to sniffing customer credentials.	Cyber criminal	Lack of mechanisms for authentication of app	Unauthorized access to customer account via fake app.	Confidentiality of customer data	Likely	Severe	Conduct regular searches for fake apps.
Fake banking app offered on application store leads to sniffing customer credentials. Which leads to unauthorized access to customer account via fake app.	Cyber criminal	Lack of mechanisms for authentication of app	Unauthorized transaction via Poste App.	Integrity of account data	Unlikely	Minor	Conduct regular searches for fake apps.
Smartphone infected by malware and this leads to alteration of transaction data by Cyber criminal.	Cyber criminal	Weak malware protection	Unauthorized transaction via Poste App.	Integrity of account data	Unlikely	Minor	Regularly inform customers about security best practices to improve malware protection of their smartphones.
Denial-of-service attack.	Hacker	1. Use of web application 2. Insufficient resilience	Online banking service goes down.	Availability of service	Certain	Minor	1. Monitor network traffic to prevent use of web application by Hackers. 2. Increase bandwidth to improve resilience.
Web-application goes down	System failure	Immature technology	Online banking service goes down.	Availability of service	Certain	Minor	Strengthen verification and validation procedures to prevent use of immature technology.

Comprehension Questions

We ask to identify a risk element of a specific type that is related to another element of a different type.

> *"Which **threats** can exploit the **vulnerability** 'Poor security awareness'? Please specify all threats:"*

One question per element type:

CORAS element types:

1. Threat
2. Vulnerability
3. Threat scenario
4. Unwanted incident
5. Likelihood
6. Consequence
7. Asset
8. Treatment

8 questions

Measurements

- **Precision** of the response to a question:
  - # of identified correct elements / # of all listed elements
- **Recall** of the response to a question:
  - # of identified correct elements / # of all expected correct elements
- **F-measure** is a weighted harmonic mean of precision and recall

$$F\text{-}measure = 2 \cdot \frac{precision \cdot recall}{precision + recall}$$

- **Subject's Comprehension**
  - Average F-measure of all questions about assigned risk model

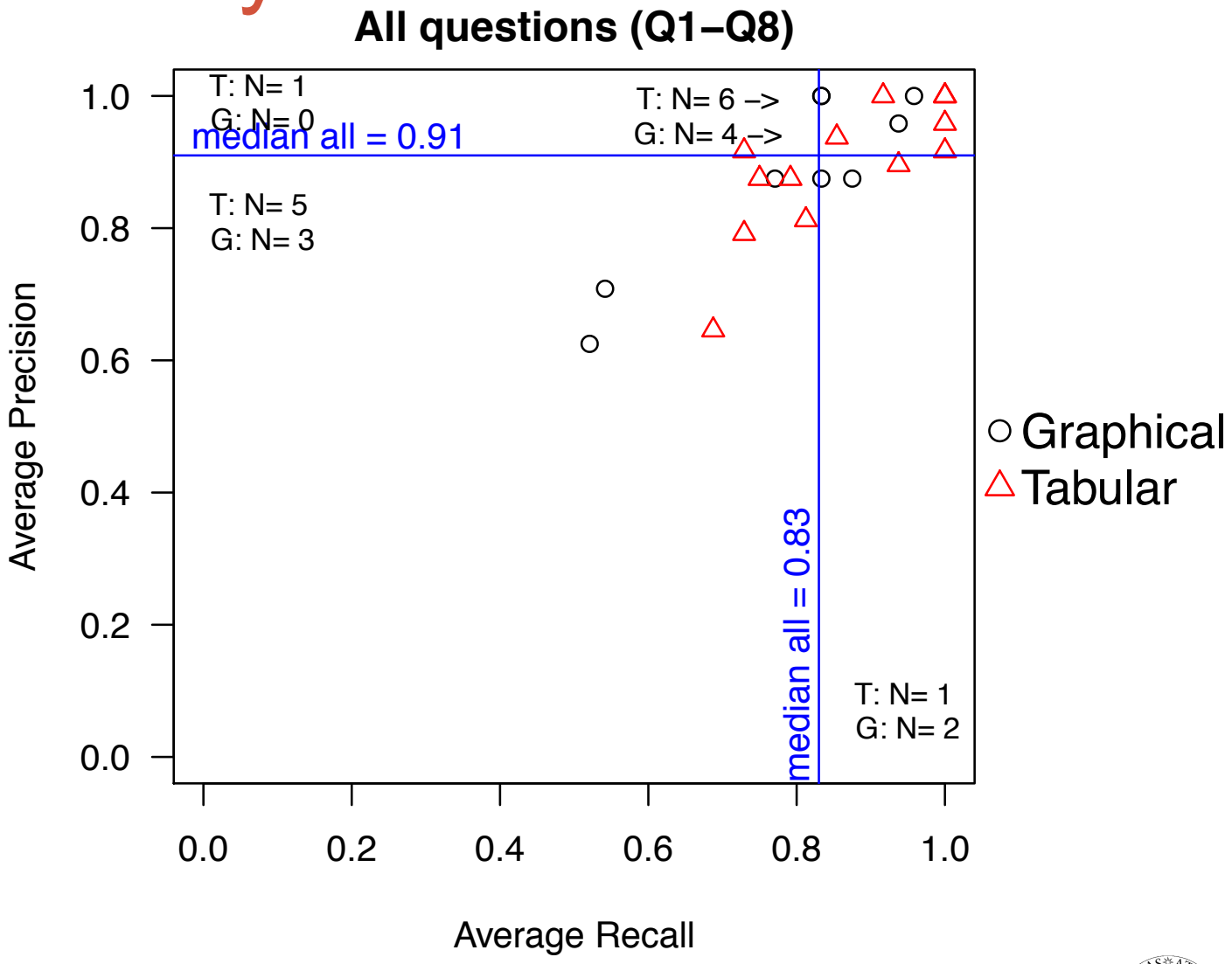
Experimental Protocol

- Training
  - Training on both risk modeling notations [8 min]
  - General introduction to the application scenario [2 min]
  - Demographics & Background questionnaire [5 min]
- Application
  - Comprehension questionnaire [20 min]
    - 8 questions
  - Post-task questionnaire [2 min]
    - To control possible effect of the experimental settings on the results
- Evaluation
  - 2 researchers independently checked the subjects' responses against the predefined set of correct answers

Data Collection

- Between subject design
  - One subject received only one of two risk models
- 24 subjects were discarded
  - Due to incorrect time limit in SurveyGizmo
- In total we got data from 22 subjects
  - Tabular: 13 subjects
  - Graphical: 9 subjects

Preliminary Results



Distribution of mean precision and recall per subject by risk model type

Preliminary Results

- [Overall] Tabular = Graphical
  - 10% better mean recall using tabular risk model
    - => more complete responses

Mean	Tabular	Graphical
Precision	0.9	0.88
Recall	0.87	0.79
F-measure	0.89	0.83

- Need replications
  - At least 116 subjects in total for F-measure

Threats to validity

- Internal validity
  - Search in the risk model
    - Tabular: 62% of subjects used search (only 1 subject in Oslo)
    - Graphical: 22% of subjects used search
- External validity
  - Participants are students
    - We will replicate study with professionals
  - Only CORAS and NIST
    - Need to study other representations
- Conclusion validity
  - Statistical power
    - We plan to replicate the study

Summary

- Conclusions
  - Which representation is better?
    - Participants' level of comprehension is the same
  - Tables showed 10% better recall
    - More complete response → less chance to overlook things
- Future work
  - Replication with more subjects (professionals and students)
  - Different risk modeling notations
  - Task complexity factor
- Ads
  - Want to join the effort? → we are looking for replications
  - More Info? → http://securitylab.disi.unitn.it