Carnegie Mellon University

Risk Management and Information Assurance Decision Support

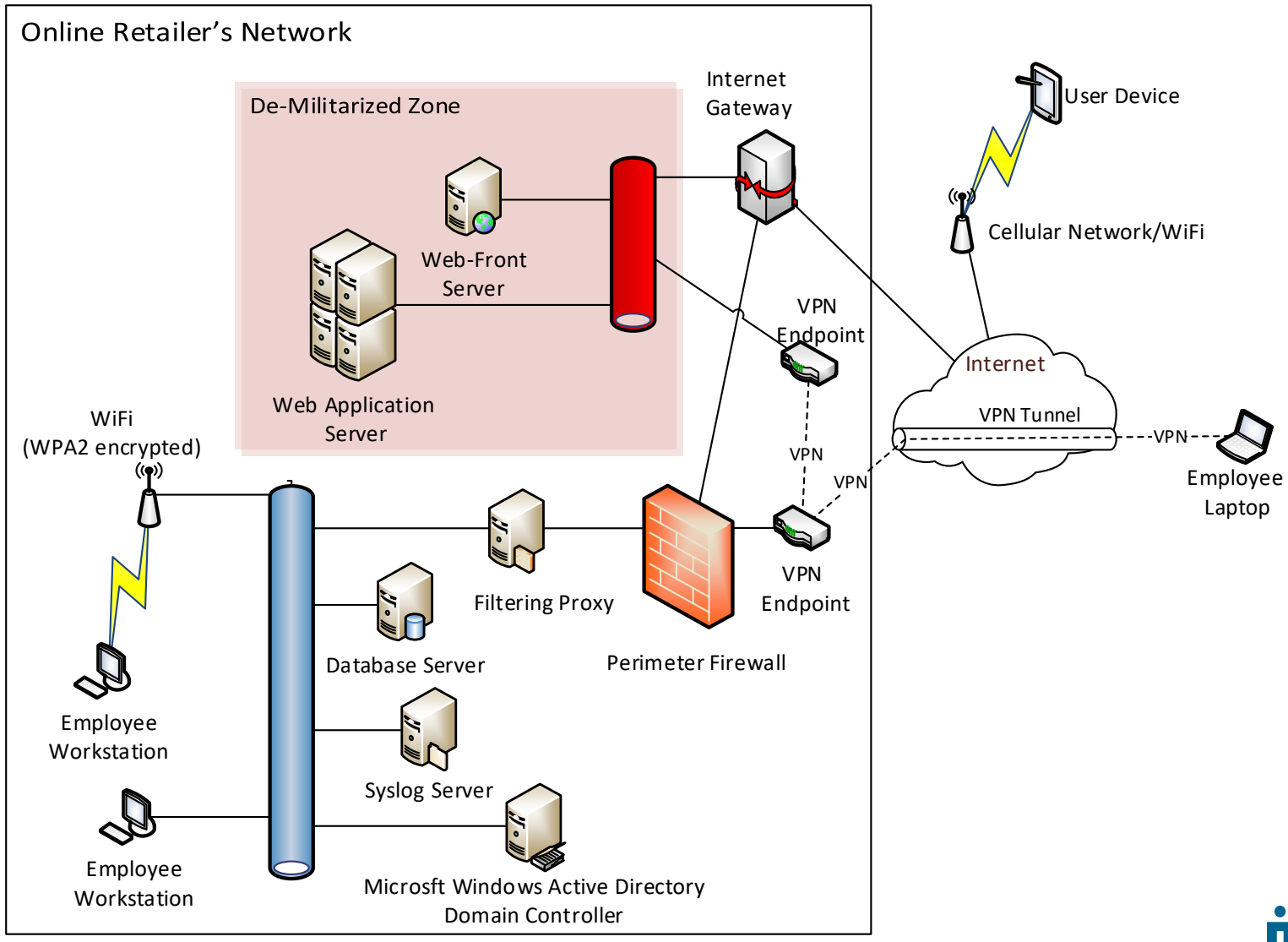
Travis D. Breaux
Joint work with Hanan Hibshi
May 8, 2019

institute for SOFTWARE RESEARCH

The Risk Assessment Challenge

- Organizations, like the DoD, rely on security experts
- Security requirements are composed in scenarios
- Experts reason over different permutations and scenarios
- Experts are scarce
  - in 2016, 100,000 information security analysts in the U.S.
  - by 2026, 56% growth in demand for security professionals
- Experts are diverse
  - With stove piped knowledge (databases, networks, mobile)

Security in a Composable System



Example Scenario

You are a **website administrator** responsible for securing a web app against cyberattacks. Currently, you are evaluating the following settings:

The web app performs **$WebAuth**.

- Basic authentication
- Form-based authentication using encrypted credentials stored in a database

The web app will **$StoredUserData** in a database for display to other users.

- store user-supplied content from GET requests
- require CSRF tokens, escape and validate user-supplied content from POST requests before storing

The **Cross-Site Request Forgery** attack is a serious security concern.

Please answer the following questions with regards to mitigating this threat.

Process Overview

Step 1: IT analyst chooses scenario scope and components / requirements

Step 2: Analyst identifies levels for components

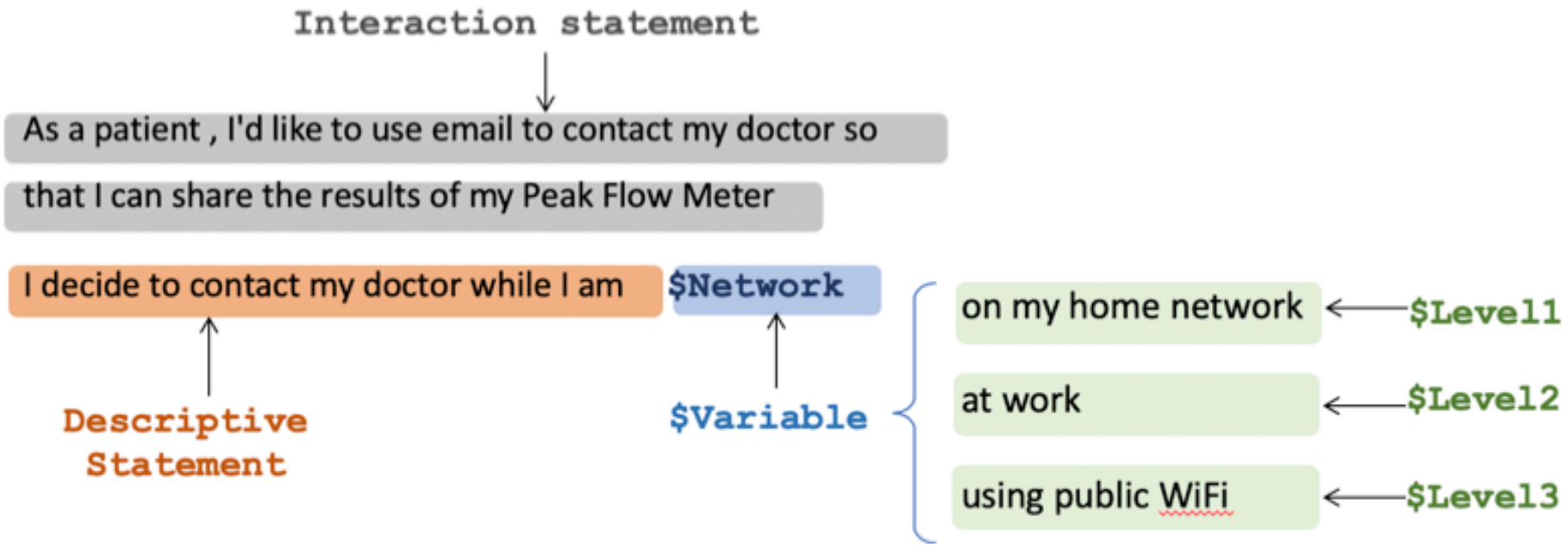
Step 3: Analyst publishes scenarios, which are pooled for assessment

Step 4: Experts rate scenarios for micro-payments

Step 5: System analyzes ratings and reports correlations among levels

Step 6: Analyst chooses levels to compose measurable security rating

Scenario Elicitation Language



Experiments to Evaluate Language

- Prototyped form-based tool to elicit scenarios
- Recruitment:
  - Students enrolled in a well-recognized Information Security Master's degree program in the US
  - Students include industry and/or government experience
- Compensated with $25 Amazon Gift Cards

Study Participant Tasks

1. Review training examples
2. Provide interaction statement
3. Provide up to 4 descriptive statements with variables and levels
4. Review final scenario
5. Rate experience with the tasks 1-4
   - Task difficulty (7-point scale)
   - Likelihood of using the tool (7-point scale)
6. Answer security knowledge questions
7. Answer demographic questions

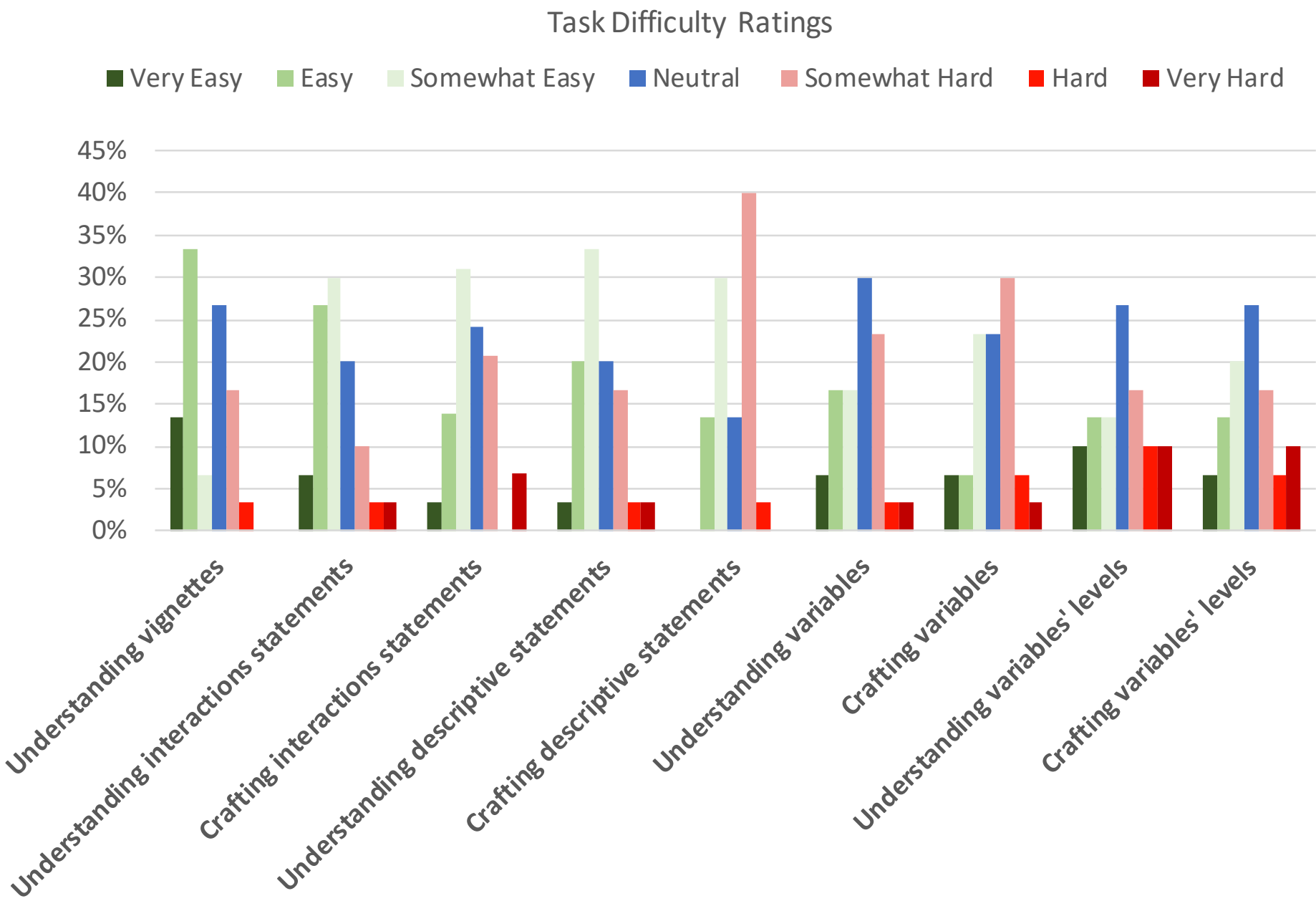
Analysis of Results

- Data is qualitative. We use grounded analysis open coding and coding theory to code the responses.
- Two raters
  - Cohen Kappa for inter-rater reliability
- Constructs:
  - Effectiveness: Task completion rates
  - Efficiency: Task completion time
  - Satisfaction: Task difficulty and likelihood-of-use

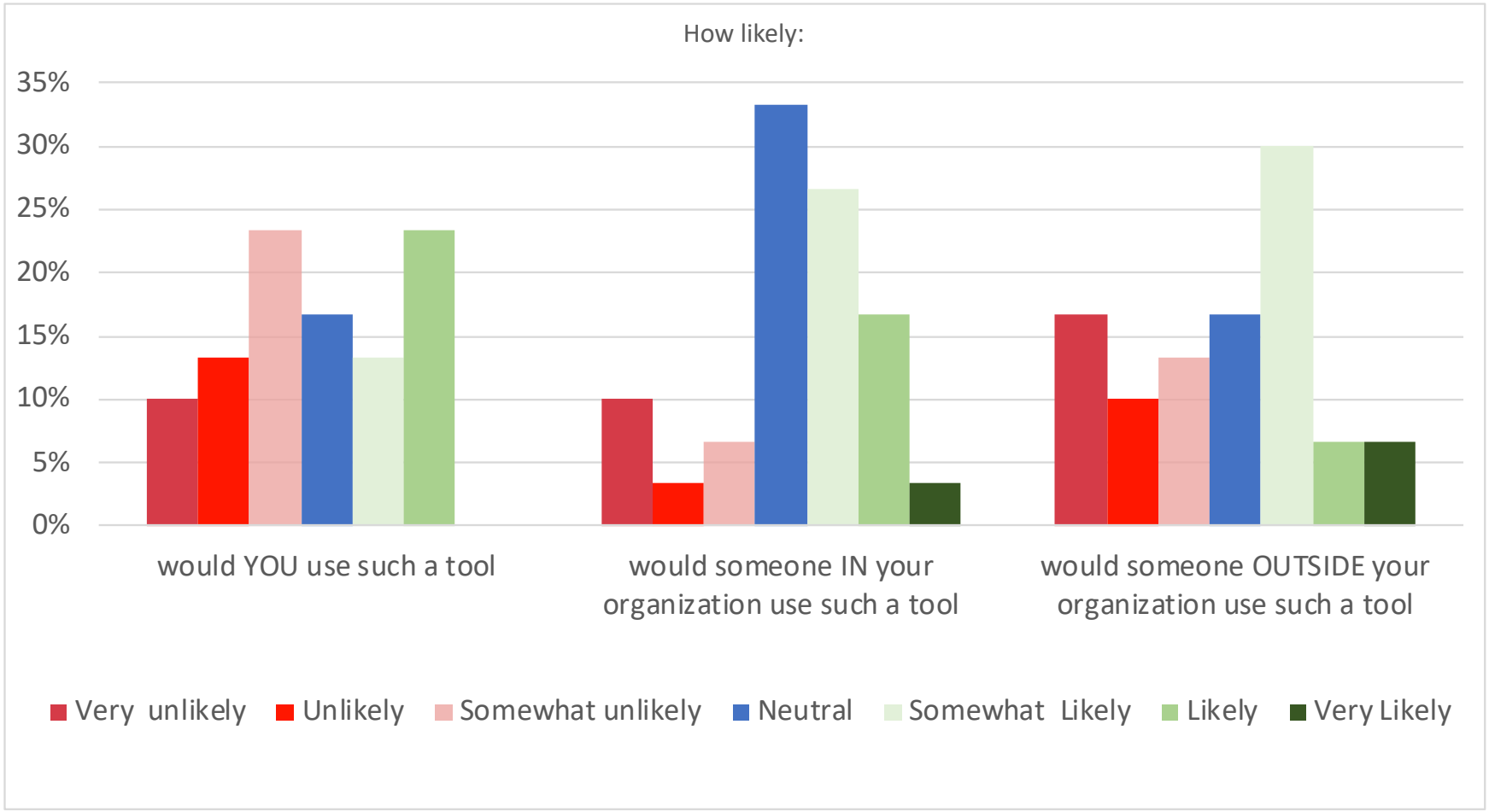
Task Completion

Coded Task	Full Accuracy	Partial Accuracy	Failure
Interaction Statement	complete	incomplete	Not provided, NA
Descriptive Statement	correct	partial	incorrect
Variable	correct	partial, level	incorrect

- **Full completion: 57% (17 Participants)**
  - Full accuracy of: interaction statement AND at least One descriptive statement with variables and levels
- **Partial Completion: 43% (13 Participants)**
  - Partial accuracy of: interaction statement AND at least One descriptive statement with variables and levels
- **Failure 0%**


Task Difficulty Ratings
Very Easy
Easy
Somewhat Easy
Neutral
Somewhat Hard
Hard
Very Hard
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
Understanding vignettes
Understanding interactions statements
Crafting interactions statements
Understanding descriptive statements
Crafting descriptive statements
Understanding variables
Crafting variables
Understanding variables' levels
Crafting variables' levels

Participant Satisfaction: Likelihood-of-Use



Structured Scenario Elicitation Benefits

- Systematized and scalable collection of scenarios
  - The method can be tailored based on organizational needs
  - Breakdown of scenarios into elements offers increased scalability over unstructured narrative elicitation
- Homogenous stakeholder scenarios
  - Common scenario structure enables scaling analysis
- Diverse viewpoints on requirements expression
  - Analysts express requirements differently, with potential ambiguities and inconsistencies
  - Collected data can be used to predict scenario improvements at time of writing

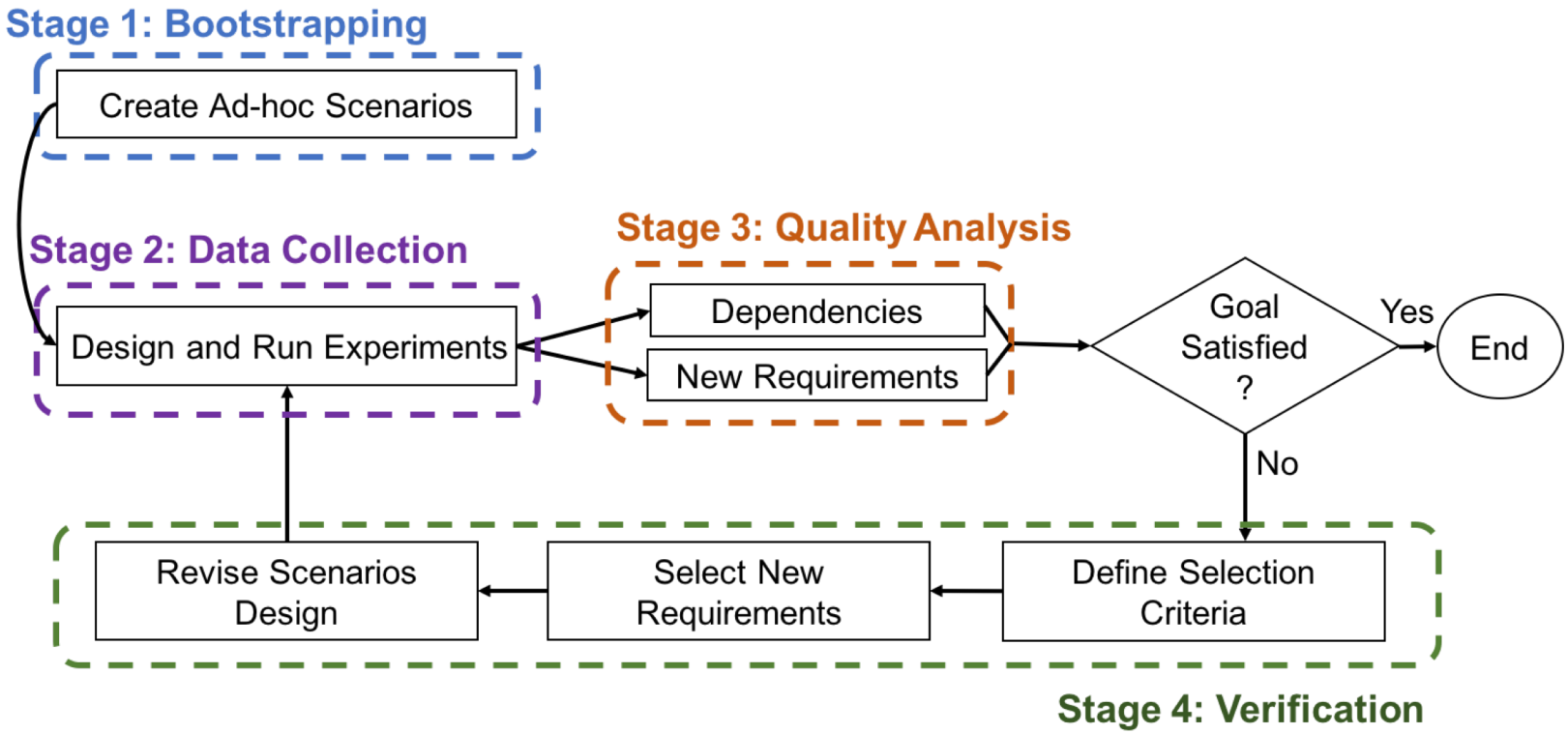
Questions

This research is funded in part by ONR Award #N00244-17-S-FO03 and Award #HQ00341810014

BACKUP SLIDES

The Multifactor Quality Measurement

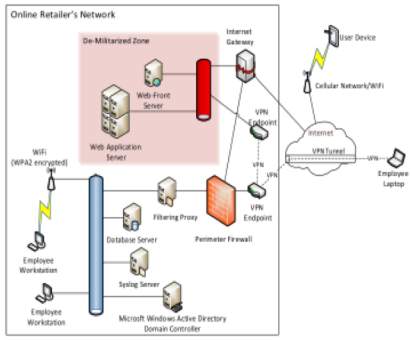
- For qualities like security where the phenomena exist in the stakeholders' interpretation of the domain



Technical Vision

Enterprise

Enterprise's Network



Security Experts

Step 1: IT user chooses security components/requirements to be evaluated

Step 2: IT user chooses levels (options) for the requirements being evaluated

Step 3: IT user finalize security vignettes and send out invitations to security experts

Security Evaluation Application

Step 4: security experts receive invitations to evaluate the vignettes

Step 5: security experts provide ratings and suggestions for mitigations

Step 6: system processes and analyze experts' data

Step 7: IT user reviews analysis results of experts opinion

Demographics

- 30 participants
  - Male: 70%
  - Female: 27%
- Years of computer security experience
  - Less than 1 year : 20%
  - 1- 2 years: 43%
  - 3 - 4 years: 23%
  - 5 – 7 years: 13%
- Age range:
  - 18 – 24: 60%
  - 25- 34: 40%
- Security Knowledge test scores
  - Above 60%: 31%
  - Between 40% and 60%: 41%
  - Below 40%: 5%