A Gap Analysis of Visual and Functional Requirements in Cybersecurity Monitoring Tools

Christian Luidold

christian.luidold@univie.ac.at

Research Group Multimedia Information Systems,
University of Vienna

Thomas Schaberreiter

thomas.schaberreiter@univie.ac.at

Research Group Multimedia Information Systems,
University of Vienna

SECURWARE 2020 Valencia, Spain

Presenter: Christian Luidold

About the Author

Christian Luidold is currently pursuing a Master Degree at the Faculty of Computer Science at the University of Vienna. Working in the ODYSSEUS project, he is developing a data processing strategy for multiple stakeholder groups encompassing heterogeneous data sources including social media analysis.

Acknowledgment

This work was partially funded by the Austrian FFG research program KIRAS in course of the project ODYSSEUS ("Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten") under Grant No. 873539.

Motivation

Main Idea: Facilitate research regarding visual and functional prototyping
Goal: Identification of Gaps between State-of-the-Art Research and funded Projects, categorized in:

- Applicability to CI research
- Related Project Goals: Evaluation of Projects regarding Requirements Analysis
- Related State-of-the-Art Goals: Providing a Trend Analysis regarding Visual and related Functional Concepts
- Comparison between CI projects and State-of-the-Art

Overview

- Introduction
- Projects Analyzed
- VizSec Analysis
- Identified Concepts
- Conclusion
- Ideas on the Horizon

Introduction

Projects focusing on Critical Infrastructures (CI) and Critical Infrastructure Protection (CIP) encompassing a diverse set of interdependent processes and stakeholder groups demand for extensive preparation during the early project phases in order to correctly assess opportunities, probabilities and limitations. For this purpose we provide an evaluation of two funded projects and state-of-the-art research regarding design decisions and outputs. Finally, we compare those views in the context of four identified concepts in regard to effective early project design.

Projects Analyzed

A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis (CS-AWARE) [1]

- Focus on cybersecurity for SMEs, local public administration and individuals
- Included stakeholders: management, operations, general public, etc.
- Closed project

Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten (ODYSSEUS) [3]

- Focus on critical infrastructure protection and dependent stakeholders
- Included stakeholders: supply infrastructures, ICT, transport networks, etc.
- Ongoing project

VizSec Analysis 2017-2019: Dimensions Evaluated

- Main Focus of Contribution by Liu et al. [4]
  - Empirical Methodology
  - Systems & Frameworks
  - Applications
- Visualization Techniques by Keim [2]
  - E.g. 2D/3D, Geometrically Transformed, etc.
  - Extended by geographical Maps and Textual Representations
- User Involvement by Staheli et al. [5]
  - No Users
  - Lay Users
  - Novices
  - Experts
- Interactivity & Mapping by Keim [2] and Wagner et al. [6]
  - I.e. Degree of Interaction & Static vs. Dynamic Mapping
  - Extended by Collaboration and Customization

Included Content

- Prototypes, Models, Approaches, etc.
- User Studies, User Stories / User Interviews

VizSec Results

- Main Focus of Contribution
  - Majority focusing on presenting applications or to a lesser extend empirical methodologies
  - Systems and framework barely included
- Visualization Techniques
  - Focus on simple 2D charts
  - Raw data included in less than 50% despite demand from domain experts
- User Involvement
  - Domain experts involved in about 50% of contributions
  - Mostly focused on evaluating finished prototypes
- Interactivity & Mapping
  - High interactivity is essential especially regarding sorting & filtering
  - Dynamic mapping for facilitating real-time analysis is rarely used

Included Content

- Nearly all contributions provide prototypes to support their research
- Requirements analyses regarding domain experts needs rarely included

Identified Concepts

During the analyzed project phases and according to the design decisions made by state-of-the-art research 4 main concepts were identified to be of increased relevance:

- Collaboration
  - Information sharing between CI stakeholders and government authorities during incidents to enhance mitigation and response actions
- Enhanced Situational Awareness
  - Incorporation of external data (i.a. social media or distinct information sharing communities)
- Multi-Stakeholder Involvement
  - Inclusion of different stakeholders to support incident handling & data sharing across departments and increase coordination with external organizations and authorities
- Multi-Stakeholder Visualization
  - Accommodation of different user groups by representing data to suit their specific requirements

Identified Concepts: Collaboration

State-of-the-Art Analysis

- Focus on analysing Data
  - Provide custom Visualizations
- Lack functionality of Information Sharing
  - Import/Export of Results
  - Notifications, etc.

Project Experience

- Communication needs to be established in a timely manner
  - Facilitates Mitigation Actions & Proactive Measures

Current State

- Collaboration is rarely accommodated for

Gap

- Information Sharing between CI Stakeholders and Government

Recommendation

- Enable Collaboration functionalities by Design

Identified Concepts: Enhanced Situational Awareness

State-of-the-Art Analysis

- Situational Awareness only included, if it affects underlying data directly
- Small number of CIP research includes Twitter Analysis

Project Experience

- Information from external sources needs to be incorporated
  - E.g. Incidents Reports from organizations, governments, social media etc.
  - Facilitate Proactive Measures

Current State

- Mostly no Situational Awareness or limited to organizational bounds

Gap

- Usage of external information sources

Recommendation

- Include analysis of data outside the organizational scope

Identified Concepts: Multi-Stakeholder Involvement

State-of-the-Art Analysis

- Generally at most Single Stakeholder Group
- Typically during the evaluation phase

Project Experience

- Include all relevant Stakeholder Groups
  - Identify Stakeholders during Design Phase, i.e., through Workshops or User Interviews
  - Validate project state and outcomes during each project phase

Current State

- Either none or Single Stakeholder Group involved

Gap

- Recognition of dependent perspectives from different Stakeholder Groups

Recommendation

- Identify Stakeholders early and include them into the project phases

Identified Concepts: Multi-Stakeholder Visualization

State-of-the-Art Analysis

- Generally focus on single Use Case
- Encourage the idea of Collaboration
  - Rarely included in evaluation phases

Project Experience

- Multiple Views to accommodate different Stakeholder Groups
  - E.g. operators, analysts, first responders, etc.
  - Characteristics of views identified

Current State

- Mostly accommodated for just a single Stakeholder Group

Gap

- Support for multiple Stakeholder Groups

Recommendation

- Conduct workshops and evaluate prototypes with different Stakeholder Groups

Conclusions Drawn

The two main points taken from the evaluation of concepts are:

- Visualization has demonstrated its value, but it needs to be combined with other areas such as Collaboration, Situational Awareness and Multi-Stakeholder Involvement
- Only when we combine these approaches, they can all deliver their full effectiveness and efficiency
- Discussions:
  - Visualizations are highly valuable, proven
  - Problem: Full potential is sometimes wasted, because we don't combine it with other features

These findings confirm many of the lessons learned in requirement engineering software projects

Major Takeaways

Two core points learned from the evaluation of concepts are:

1. User Workshops and User Interviews are indispensable in early stages of every project, as CS-AWARE and ODYSSEUS have shown
2. Collaboration and Coordination, including domain interdependent stakeholders, are key success factors

Ideas on the Horizon

The four identified concepts will be used in combination for:

- Prototype development in national projects such as ODYSSEUS
- Only when we combine these approaches, they can all deliver their full effectiveness and efficiency
- As basis for further theoretical research
- In future European Union projects
- To support the requirements analysis phase
- Combinations such as visualization, rich pictures, in soft systems, will be further explored from a collaboration & coordination perspective

References

[1] *A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis CS-AWARE Project H2020 CORDIS European Commission*. [retrieved: September, 2020]. 2020. URL: https://cordis.europa.eu/project/id/740723.

[2] Daniel A Keim. "Information visualization and visual data mining". In: *IEEE transactions on Visualization and Computer Graphics* 8.1 (2002), pp. 1–8.

[3] *KIRAS - Sicherheitsforschung*. retrieved: August, 2020]. 2020. URL: https://www.kiras.at/en/financed-proposals/detail/d/odysseus-simulation-und-analyse-kritischer-netzwerk-infrastrukturen-in-staedten.

[4] Shixia Liu et al. "A survey on information visualization: recent advances and challenges". In: *The Visual Computer* 30.12 (2014), pp. 1373–1393. ISSN: 1432-2315. DOI: 10.1007/s00371-013-0892-3. URL: https://doi.org/10.1007/s00371-013-0892-3.

[5] Diane Staheli et al. "Visualization Evaluation for Cyber Security: Trends and Future Directions". In: *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*. VizSec '14. Paris, France: ACM, 2014, pp. 49–56. ISBN: 978-1-4503-2826-5. DOI: 10.1145/2671491.2671492. URL: http://doi.acm.org/10.1145/2671491.2671492.

[6] Markus Wagner et al. "A Survey of Visualization Systems for Malware Analysis". In: *EuroVis*. 2015.

Thank you for your attention!

A Gap Analysis of Visual and Functional Requirements in Cybersecurity Monitoring Tools

Contact email: christian.luidold@univie.ac.at

This work was partially funded by the Austrian FFG research program KIRAS in course of the project ODYSSEUS ("Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten") under Grant No. 873539.