Reflecting on Visualization for Cyber Security

Carrie Gates • carrie.gates@ca.com
Sophie Engle • sjengle@cs.usfca.edu
INTRODUCTION
Introduction

• Short position paper
• Result of brainstorming session
  – Identify future research directions
  – Suggest approaches for future research
• Designed to encourage discussion
Brainstorming

• Why has visualization not been more successful in cyber security?
• How can visualization be used effectively for cyber security?
• How do you evaluate visualization for cyber security?
Motivation

• Success is important
  – Extensive resources required to develop, evaluate, and iterate visualizations

• Success is evasive
  – Avoid common pitfalls
  – Choose a suitable visualization goal

• Success is fuzzy
  – Accuracy and efficiency hard to evaluate
COMMON PITFALLS
What Should We Avoid?
XKCD: Convincing

I think we should give it another shot.

We should break up, and I can prove it.

Our relationship

Huh.

Maybe you're right.

I knew data would convince you.

No, I just think I can do better than someone who doesn't label her axes.

http://xkcd.com/833/
Using visualization for the wrong reasons.
Using visualization for the sake of visualization.
Visualization Goals

• Statistical Graphics
  – Accuracy, Informative

• Informative Art/Visualization Art
  – Aesthetics

• Infographics
  – Aesthetics, Informative

• Information Visualization
  – Accuracy, Informative, Aesthetics
Pretty Pictures ≠ InfoVis

• Avoid by specifying a question or goal first
• Do NOT get distracted by fancy encodings
• Do NOT get distracted by novel techniques
• Start with existing and well-tested techniques
• Try state-of-the-art or novel approaches when other techniques fail to perform well
Visualization is not a magic bullet.
Goldilocks Principle

http://w8r.com/the-colorful-story-book/the-three-bears
Goldilocks Principle

- Too Simple Problems
  - Do not need visualization

- Too Complex Problems
  - Rename "too undefined"
  - Part of the solution, but not THE solution

- Problem must be "just right"
  - Need good data and good problems

http://w8r.com/the-colorful-story-book/the-three-bears
USE CASES

What Could We Try?
Use Cases

- Visualization for a Specific Goal
- Visualization for Exploration
- Visualization as a Stepping Stone
- Visualization for Evaluation
- Visualization as Evidence
Visualization for a Specific Goal

• Must be accurate and informative
• Must support data analysis
  – Anomaly detection flags event as anomalous, but unknown whether is malicious
  – Use visualization to help resolve this grey area on case-by-case basis
• All other cases are subcases of this one
Visualization for Exploration

• Sometimes not having a well-formed question is the problem!
• Use visualization to explore data, provide context, and help form questions
• More difficult to evaluate, may lose usefulness after question is formed
Visualization as a Stepping Stone

• Use visualization as a stepping stone in analysis
  – Guide root cause analysis in a complex environment

• Neither the starting point or ending point
  – Does not provide the question
  – Does not provide the answer

• Provides context, more exploratory in nature
Visualization for Evaluation

• Aid evaluation of security mechanisms
  – Mechanisms must support complex policies
  – Multiple mechanisms protecting resources
  – Difficult to configure and maintain

• Does not replace mechanisms, only improves usage of those mechanisms
Visualization as Evidence

- Justification for response to cyber threat
  - A security analyst may need to justify changes to infrastructure to decision makers
- Illustrate evidence of an attack
  - Presenting forensic evidence to a jury
- More focused on story-telling than analysis
EVALUATION

How Do We Know What Works?
Evaluation

• Evaluation focused on visualization
  – Focus in visualization community (85%)
  – Focus on pushing boundaries of visualization

• Evaluation focused on data analysis process
  – Focus on application of visualization
  – Less research on this type of evaluation
  – Important for cyber security visualization
User Performance Evaluation

• Large study
  – Cannot require expert knowledge
  – Simple and measurable tasks
  – Possible for realistic cyber security tasks?

• Small study
  – Require domain experts
  – More complex but still measurable tasks
  – Applicability of results to other environments?
User Experience Evaluation

• Recruitment still an issue
  – Release visualization for anyone to use
  – Track adoption rate
  – Solicit feedback from users

• Usually requires expert users
  – Must use tool in environment for specific task
  – Usage often needs to be measured over time
Process Evaluation

• Focused less on techniques, more on tools
  – Techniques broadly applicable
  – Tools must be evaluated within context used

• Focus on understanding environment
  – Independent of any visualization tools

• Focus on visual data analysis process
  – Dependent of visualization tools in use
Environment Evaluation

• Perform evaluation as a precursor to building visualization tool
  – Help identify problem and visualization goal

• Evaluate how existing tools are used
  – Identify how to improve or supplement tools

• Data collected via field or lab observation, surveys, or interviews
Analysis Process Evaluation

• How well tool supports data exploration and knowledge discovery
• How well tool allows analyst to generate hypotheses and make decisions
• Often conducted via case studies
  – Target set of actual users
  – Realistic needs
  – Realistic evaluation
CONCLUSION

Reflecting on Visualization for Cyber Security
XKCD: The Important Field

http://xkcd.com/970/
Conclusion

• Short, position paper reflecting on cyber security visualization

• Brainstorming on what to avoid, what to try, and how to evaluate future research

• Highlights importance of the cyber security problem and visualization goal

• Designed to be part of a discussion
THE END

Questions, Comments, or Discussion?