Understanding Cybersecurity Decision Making through Knowledge Elicitation Techniques

Kristina Davtyan and David Schuster
San José State University, Department of Psychology

SJSU SAN JOSÉ STATE UNIVERSITY

VECTR Lab

Introduction

Abstract

- Recent high-profile security breaches at Equifax and Sony have highlighted the importance of the role of cybersecurity in today's digital forward world.
- As human factors psychology researchers, we recognize the opportunity to contribute to the workforce development by conducting research to better understand the factors that predict the success of expert cybersecurity professionals' decision making.
- We describe an ongoing knowledge elicitation study to understand how mental models and situation awareness predict decision making.

Background

- Research shows data breaches will exceed $150 million by 2020, and the global cyber security professionals shortage is expected to rise to 1.8 million by 2022 (Moard, 2015; ICS, 2017).
- Computer Network Defense (CND) is the process of analyzing and responding to threats.
- Successful CND relies on critical decisions made by individuals.
- Situation Awareness (SA) is goal-relevant knowledge held during task performance
- Mental models are internal representations of the task environment.
- Together SA and mental models are cognitive constructs that determine successful decision making.
- Cognitive Task Analysis (CTA) is a method of understanding individual and group SA and mental models.
- Our NSF-funded study seeks to understand subject matter experts' (SME's) decision making by way of elucidating their particular knowledge structure about the cyber security domain.

Cognitive Task Analysis

Concept Maps

- A vast body of literature has identified concept maps as a reliable cognitive task analysis tool (Crandall, Klein, & Hoffman, 2006).
- Concept maps are a graphical representation of knowledge that identifies important concepts and their relationships.
- Two concepts and a linking phrase form a complete sentence.
- The process of a concept map begins with a focus question that can be tailored to apply to particular job role.
- The probe question facilitates the creation of a list of most relevant concepts.
- Concepts are ordered in a hierarchical fashion, descending from more general to more more specific/particular at the bottom.

Card Sorting

- We are using free card sorting in order to understand how SME's classify their knowledge about creating secure network systems.
- Participants are given a deck of cards and asked to sort them into piles. Participants label the piles.
- A parking lot of concepts relating to cybersecurity was adopted from the National Initiative for Cybersecurity (NICE) framework

Procedures

- Our research participant population are cybersecurity professionals from enterprise technology companies in the San Francisco Bay Area whose primary job role is to protect and defend networks.
- The NICE network identifies protect and defend workforce category as follows: "[specialists who] identify, analyze, and mitigate threats to internal information technology (IT) systems and/or networks". (Newhouse, Keith, Scribner, & Witte, 2017, p.11).
- SME's participate in a 1.5 hour long in-person or remote data collection session, completing concept map and card sorting activities.
- We use free concept mapping software Cmaps and a web based card sorting program developed in the lab.

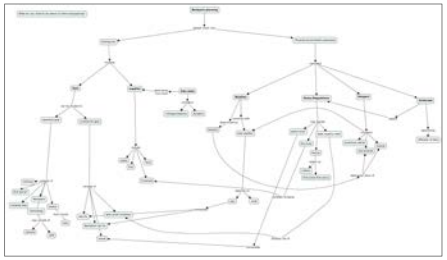

Fig 1. Practice concept map student research assistants created during concept map training

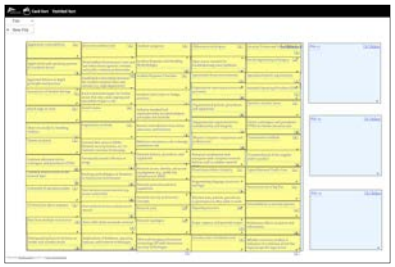

Fig 2. A screenshot of our open cart sort program with an unsorted parking lot of terms

Research Goals

Discussion

- We are utilizing concept maps to capture SME's knowledge about their domain, specifically their mental representation of interconnected concepts that enable them to make decisions in their network defender roles.
- We expect that concept maps of experts and novices will differ in terms of number of nodes and links between them.
- We are specifically interested in the common representation of knowledge that expert cybersecurity specialists hold.
- Open card sort will allow us to discover patterns in the way SME's classify important concepts and be used to validate the NICE Framework.
- By leveraging our research, we can improve training and increase access to cybersecurity careers.

Acknowledgments

- This material is based upon work supported by the National Science Foundation under Grant No. (1553018). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

- Center for Cyber Safety and Education and (ISC)².(2017). 2017 Global Information Security Workforce Study. Frost & Sullivan.
- Crandall, B., Klein, G., & Hoffman, R.R. (2006). "Working Minds: A Practitioner's Guide to Cognitive Task Analysis". Cambridge, MA: MIT Press.
- Moar, J. (2015). The Future of Cybercrime & Security: Financial and Corporate Threats 2017-2022. Basingstoke, U.K.: Juniper.
- Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework(Report No. 800-181). doi:10.6028/NIST.SP.800-181.