Elicitation by Critiquing: Applications to Computer Network Defense

Alexander Scott, Ian Cooke, Katarzyna Sliwinska, Novia Wong, & David Schuster
San Jose State University

VECTR Lab

SJSU SAN JOSÉ STATE UNIVERSITY

Abstract

- By understanding how network defenders conduct their work, human factors researchers can help optimize tools and training to strengthen the workforce.
- Cognitive Task Analysis (CTA) has been traditionally used for knowledge elicitation, but there are challenges for implementation in Computer Network Defence (CND.)
- We highlight these challenges and offer insight on how our discipline can overcome them.

Introduction

- Computer Network Defense (CND) is the process of protecting organizations and individuals against cyber threats by monitoring, identifying, analyzing, and defending network infrastructure from infiltration.
- As new defenses are built, adversaries develop new and unexpected ways of attacking to extract the sensitive data held by organizations and governments.
- While organizations are employing increasingly sophisticated automated tools designed to manage the flood of attacks, a human decision maker acts as a critical line of defense.
- We need to understand of human performance of cyber defenders.
- Cognitive task analysis (CTA) is well-positioned to provide insights into the cognitive strategies of experts that can be leveraged to inform the design of tools, training, selection, and evaluation procedures.
- We provide guidance for CTA practitioners conducting work in CND by:
  - Reviewing CTA techniques applied to similar domains to guide implementation in CND
  - Identifying primary challenges to the implementation of CTA techniques for CND
- We argue that Elicitation by Critiquing (EBC) shows promise in mitigating the challenges of applying CTA in CND.

Review of CTA Techniques

Examples of CTA in CND

- *Cognitive walkthrough.* Involves interviewing an Subject Matter Expert (SME) and walking through a typical taskflow. The time necessary for a single SME to walk through multiple scenarios and the need for high levels of practitioner domain knowledge is prohibitive for application in CND.
- *Concept mapping.* Concept mapping is a method designed to construct representations of the mental models of SMEs. A practical advantage of concept mapping is the ability for researchers to remotely administer the method.
- *Knowledge audit.* A knowledge audit (KA) is a semi-structured interview that involves collecting evocative descriptions of incidents while addressing predefined dimensions of expertise. The structured, simple, and short nature of a knowledge audit positions it as a useful technique for use in the CND domain.
- *Critical Decision Method.* The Critical Decision Method (CDM) is a semi-structured interview designed to provoke and describe the decision making of experts in a naturalistic setting. This method can require extensive domain knowledge, time, and access to sensitive information as scenarios can be derived from previous attacks.

Challenges in Application of CTA to CND

- *Rapid change.* The rapid pace of change in the CND domain may impact the efficacy of CTA in CND in that the way in which defenders interact with systems can fundamentally change from one version to the next.
- **Recommendation:** Consider automated methods of scoring knowledge elicitation activities.

- *Domain familiarity of the CTA practitioner.* To perform an effective CTA, practitioners need expertise and specific knowledge of the domain being investigated. The technical complexity of the CND domain presents an additional challenge for practitioners lacking a computer networking background.
- **Recommendation:** Utilize interdisciplinary research teams to decrease bootstrapping.

- *Expert time commitment*. Another challenge is the small workforce and high workload of CND experts, making an extended time commitment difficult. Traditional CTA methods require significantly long and repeated sessions and are difficult to apply to CND.
- **Recommendation:** Organize CTA research in an ongoing research initiative to make efficient use of time. E.g. using an KA to build the scenarios for a future CDM.

- *Access restrictions*. The secrecy of CND is a product of cybersecurity professionals' duty to protect sensitive customer data and the proprietary methods they use to stay ahead of adversaries.
- **Recommendation:** Emphasize the intention to extract expert knowledge as opposed to examine threat response.

- *CTA practitioner training.* Although CTA is demonstrably effective, the time needed to complete a full training for CTA makes it difficult to train new practitioners and also takes significant time and financial resources to implement.
- **Recommendation:** Apply an apprenticeship model of CTA data collection where junior members partner with senior members.

Elicitation by Critiquing and Applications in CND

Elicitation by Critiquing

- Elicitation by critiquing (EBC) is a method that can be employed under the constraints of CND, but has not, to our knowledge, been applied to CND to date.
- Out of the hundreds of available CTA methods, this method can address the majority of the challenges for CTA in CND.
- EBC begins by having a novice complete a task in the domain and capturing the domain task through film from the novice's point-of-view. The novice goes through the video and narrates decision making strategies and challenges. Domain experts individually critique the novice's decision making and cue recognition.

Application of EBC in CND

- *Rapid change.* EBC can also be used for validating and modifying scenarios, which makes it useful for rapidly changing domains. The CND scenarios for EBC can be evaluated by experts and modified as tools or procedures develop in CND.
- *Domain familiarity/training of the practitioner.* The reliance on pre-recorded scenarios developed prior to the CTA reduces the amount of training and domain knowledge required by the practitioner because the scenarios serve as the information the SME needs to critique.
- *Expert time commitment*. EBC is designed to overcome expert access constraints caused by the expensive and short-supplied nature of SME's. The method achieves this by reducing the need for continual and extensive expert input.
- *Access restrictions*. In order to mitigate security risks, EBC can be done remotely to limit access to secured facilities without losing data. Also, EBC scenarios are based on real CND, but are fictitious.

Discussion

Implications

- While much research effort has been put towards improving the capabilities of automated systems, research into optimizing the human element has the potential to be equally impactful.
- The features that make CND a critical domain for the optimization of cognitive work also contribute to the difficulty of CTA application.
- To address these challenges, methods used to investigate CND should have some or all the following characteristics: keep up with the state of the art, serve to quickly build practitioner domain expertise, reduce expert time commitment, not compromise the security of proprietary information, and utilize remote knowledge elicitation methods.
- EBC has promise for successful use in CND in accordance with our framework, despite not yet being implemented in CND before. An attempt to validate this method in CND should be conducted in future research.

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.