Topological Scoring of Concept Maps for Cybersecurity Education

Pranita Deshpande
Department of Computer Science
University of New Orleans
pdespha1@my.uno.edu

Irfan Ahmed
Department of Computer Science
Virginia Commonwealth University
iahmed3@vcu.edu

ABSTRACT
Concept maps are a well-known pedagogical tool for organizing and representing knowledge and developing a deep understanding of concepts. Unfortunately, the grading of concept maps tends to be manual and tedious thereby, posing serious limitation for an instructor to use them in class efficiently. To automate the assessment and grading, the topology and structural features of concept maps are utilized. However, they have never been explored for cybersecurity education. This paper evaluates the effectiveness of topological scoring of the concept maps for two cybersecurity courses: digital forensics, and SCADA system security. We create a dataset of 41 high-quality concept maps developed with expert knowledge. We utilize Waterloo rubric to manually validate the quality of the concept maps based on their contents and further compare the rubric outcome (obtained via manual analysis) with the automated topological scoring of the maps. The evaluation results show that the topological scoring is promising. However, it is not equally effective and warrants for advanced techniques to better utilize the topology of the maps. The dataset is made publicly available for further research on this topic.

ACM Reference format:
DOI: http://dx.doi.org/10.1145/3287324.3287495

1 INTRODUCTION
Concept maps are a visual tool for organizing and representing knowledge. They include concepts, represented as text boxes, and relationships between pairs of concepts indicated by a connecting link. The most abstract concepts are placed at the top of the diagram, while progressively more specific ones are placed underneath them. This simple design allows seamless and effective linking and exploration of concept at different levels of detail.

We develop the first dataset of concept maps for cybersecurity courses and make it publicly available for research and education.

Contributions. We summarize the contribution of the paper as follows:

• Concept Map Dataset We develop the first dataset of concept maps for cybersecurity courses and make it publicly available for research and education.

• Establish the Ground Truth We assess and record the quality of the maps (ground-truth) in the datasets using the Waterloo Rubric.

• Identify an Open Research Problem We point out (via experimental analysis) that topological scoring requires attention from education research community to develop effective...
solutions for automated assessment and grading of concept maps. Our dataset is useful for the research in this direction.

Roadmap. The rest of the paper is organized as follows: Section 2 presents the related work. Section 3 discusses the datasets including steps to create concept maps and guidelines from our experience, followed by concept map examples in section 4. Sections 5 and 6 present the evaluation methods and results. Section 7 concludes the paper.

2 RELATED WORK

Concept mapping has received relatively little attention in cybersecurity education as compared to other pedagogical techniques such as peer instruction [4, 15, 20, 21].

Dexter [16] uses concept maps to detail required concepts for cybersecurity management, delving into sub-topics such as malicious behavior (deployment of code and usage of vulnerability scanners) on an organization’s network targeting their information assets and perimeter defenses such as firewalls, routers, and IDS systems. The author also uses the concept maps to highlight policies and technologies that are key to an organizations cybersecurity management.

Tanner and Dampier [28] highlight the potential use of concept maps in digital forensic investigations, detailing in concept maps the six phases of the digital investigative process (identification, collection, preservation, examination, analysis, and presentation) as well as important procedures and concepts within each phase such as chain of custody or software used in particular phases. The authors note that the maps could be tailored on a per-investigation process to display contexts of specific evidence such as a suspect property and case timeline, and how each piece of evidence was examined. Tanner and Dampier further detail how case-specific concept maps may be shared by the law enforcement community as well as how a concept map could be shown in court in order to detail a complex investigative process.

Hay et al. [18] describe the pedagogical use of concept mapping in a general higher educational context, and summarize prior use of concept maps in both the teaching and learning processes. The authors focus on the usage of concept mapping to measure students prior knowledge, as well as allowing for the instructor to teach new material in the context of students prior understanding. They suggest that concept mapping be performed both by students and instructors, and identify several core practice of responsible university teaching that could be accomplished through concept mapping such as measuring the prior knowledge of students, presenting in a deliberate manner in the context of a known student knowledge base, and measuring change among the student population so that learning (where it occurs) is identified and the causes of non-learning are addressed.

3 DEVELOPING A CONCEPT MAP DATASET

Overview. Concept map is a graphical tool to represent concepts and the relationships among them on a particular topic. The mapping organizes the concepts in a hierarchy, with the most general ones at the top of the map and the most specific concepts at the bottom. The concepts are connected through arrows (or links) and propositions—a word or phrase describing the link. Concept mapping is a cognitively intensive task that examines the level of a student’s understanding of concepts. It is particularly useful for in-class activities and homework assignments, and offers opportunities to improve the effectiveness of the instruction.

Concept mapping can be used to measure the level of a student’s understanding of cybersecurity concepts throughout the course, via Concept map-based exercises. In particular, a poorly constructed (by a student) map that has missing links and gaps in logic, or incorrect information can allow the instructor to quickly correct misconceptions developed by a student.

Conversely, instructors can use a correct map in class as the basis for in-class discussion. The map requires students to actively build their understanding of foundational concepts, and allow them to reason about the bigger picture and the connections among concepts.

Steps to Create a Concept Map. We use the following systematic approach to develop a concept map.

1. Select a target concept.
2. Identify keywords that represent some aspect of the concept.
3. Recognize any relationships among the keywords in appropriate words and phrases and then,
4. Draw the concept map; circle the keywords and connect them with the relationship words/phrases.

Guidelines of Do’s and Don’ts. From our experience of developing and improving concept maps including several revisions, and reviews and comments from other participants, we develop a guideline list of Do’s and Don’ts while developing a concept map.

- A connection between two nodes should be unidirectional.
- A connecting phrase should describe the relationship between two nodes clearly. Otherwise, avoid such connections and elaborate them with additional keyword(s) between them.
- A connecting loop across one or multiple nodes tend to create confusion and should be avoided.

Dataset Details. We develop the concept maps for two cybersecurity courses: digital forensics, and SCADA system security.

Digital forensics is defined as the application of scientific tools and methods to identify, collect, and analyze digital artifacts in support of legal proceedings [23]. We have developed 19 concept maps for digital forensics investigation course. The course provides an introduction to digital forensics, and then covers the first response and evidence handling, file systems, memory forensics, and tools for investigation. The maps are divided into six different course modules. The distribution of the concept maps with respect to their topics are presented in Table 1 and described as follows.

- Introduction to digital forensics covers the concept maps on digital evidence including the location, type and documentation of evidence, types of digital forensics investigation, and legal aspects.
- First response and evidence handling covers the concept maps on how a digital forensics investigator should respond to a case before starting the investigation, what are
the necessary steps and procedures which should be taken care of and how the evidence should be handled.

- **Investigation steps** focus on the steps/tasks that should be performed during a forensic investigation including the acquisition and analysis of the evidence, and the reporting that describes the entire investigation procedure and give a conclusion to a case.
- **File systems** covers the concept maps on file system investigation including an overview of different file systems, file allocation table, new technology file system, and investigating tips and techniques on file system.
- **Memory Forensics** covers the concept maps on memory analysis and live forensics including an explanation of volatility data and how important the data is for investigation.
- **Tools for investigation** covers the concept maps on the usage of different tools and techniques for file system investigation including sleuth kit, and windows registry and web browser investigation.

**SCADA systems** control major portions of the U.S. critical infrastructure — power grid, pipe-lines, water management, etc. — and protecting their integrity and availability is of primary importance to national security. We have developed 22 concept maps for the SCADA security course work. The course is designed for computer science students who have no understanding of control system and cover topics from introductory to advance level. The maps are divided for five different course modules, starting from an introduction to SCADA systems and then, covers PLC programming, communication protocols, and cyberattacks and security solution. The distribution of concept maps with respect to their topics are presented in Table 2 and described as follows:

- **Introduction to SCADA Systems** covers the basic concepts of a SCADA system, and its components, provides a brief understanding of some physical processes.
- **Programming of the Programmable Logic Controllers (PLC)** mainly covers Ladder Logic programming including rules to write a program and addressing formats of PLC.
- **SCADA communication protocols** covers two protocols, Modbus and DNP3 along with the header and message formats.
- **SCADA Vulnerabilities and Attack** covers real-world attacks and vulnerabilities including the attack taxonomies on MODBUS and DNP3 protocols.
- **SCADA security solutions** covers security solution for SCADA systems such as PLC code detection.

### 4 EXAMPLES OF CONCEPT MAPS

This section presents two examples of the concept maps from digital forensics and SCADA system.

#### 4.1 SCADA System: Working of a Conveyor Belt

The main components of a typical conveyor belt are drives, actuators, controllers, monitors and sensors. Programmable logic controller (PLC) receives an input signal from proximity sensor that shows that an object is placed on the belt. The PLC runs its control logic and sends an output signal to Servo drive to move the conveyor belt to make some space for the next object. The whole conveyor belt physical process can be remotely monitored by using human-machine-interface (HMI) and the data received by the HMI is also stored in historian. There are two types of sensors proximity sensor and photo eye sensor, which detects the presence of the object using beam of light and electromagnetic field respectively.

Figure 1 shows the concept map on the working and components of a conveyor belt. The map consists of four levels of hierarchy, and mostly uses succinct phrases to link two nodes. Nodes are also using short descriptive phrases or long words. To develop this map, we use our systematic approach as follows:

- The target concept addresses a typical working model of conveyor belt including its components.
- We select the keywords including components, sensors and actuators used and how it was used.
- To connect the nodes that can make sufficient understanding of their relationships, we mostly use phrases, instead of words.

#### 4.2 Digital Forensics: Handling Digital Evidence

When a forensic investigator collects an evidence from a crime scene, it is required that the evidence is handled properly, which typically involves five stages i.e., storage of evidence, disposition, transporting, documentation, and packing of evidence. **Storing of evidence** imposes rules and regulation such as access to storage must be limited and monitored, chain of custody should be maintained, login and log out details of who, what, when, where and why. **Transporting the evidence** includes protecting portable devices and media from external corruption, determining if a suspect computer should remain powered up, what applications and other processes were active. **Documenting the evidence** records where the evidence was found, what state it was in, model number, serial numbers, and time and date of evidence collection. After the investigation is done evidence must be destroyed or returned.

Figure 2 shows the concept map explaining the stages of evidence handling. The map consists of three levels of hierarchy. The nodes
and connecting links are self explanatory phrases. To develop this map, we use our systematic approach as follows:

- The targeted concept is the concept of handling of digital evidence.
- Key nodes indicated the actions and duties to be performed in each individual stage.
- Connecting nodes indicate the different stages in digital evidence handling.

5 CONCEPT MAP ASSESSMENT METHODS

We utilize two different assessment methods for concept maps: the Waterloo Rubric [1], and Topological Scoring [12]. The rubric via manual analysis established the ground truth for the concept maps in the datasets. The scoring is an automated method to assess the quality of the maps.

5.1 Waterloo Rubric (manual analysis)

The Waterloo Rubrics is developed by the University of Waterloo for the assessment of the concept maps [1]. The rubric identifies the quality of the maps at four levels i.e. Excellent, Good, Poor, and Fail based-on the following six elements i.e., breadth of net, interconnectedness, use of descriptive links, efficient links, layout, and development time.

Breadth of net evaluates the significance of target concepts and their description in multiple levels. For excellent, a map includes important concepts and describe them in multiple levels. However, for fail, a map misses many important concepts.

Interconnectedness evaluates the number of concepts interlinked with other concepts. For excellent, all concepts are interlinked, and for fail, few concepts are interlinked.

Use of descriptive links evaluates the quality of description as accurately defined to vague and incorrectly defined. The first is ranked as excellent while the later is fail.

Efficient links evaluates the uniqueness of the information of the links and the quality of description of the relationships among the nodes. For excellent, each link type is distinct and clearly describes the relationship, while for fail, most links are vaguely described, and not distinct from each other.

Layout evaluates the physical layout of a concept map including its size to be fit in one page, and hierarchical structure. For excellent, maps fit in one page and have clear multiple hierarchy, while for fail, map consists of multiple pages and has no hierarchical organization.

Development over time evaluates whether a concept map is built incrementally as them progress and new concepts are learned. For excellent, final map shows considerable cognitive progression from base map and a significantly greater depth of understanding of the domain, while for fail final map shows no significant cognitive profession from the base map and no increase in the understanding of the domain.

5.2 Topological Scoring (automated analysis)

Topological scoring [12] utilizes structural features of a concept map to compute a score between zero and six, where higher score indicates higher quality of the map. A brief description of the features are as follows:

Average Words per Concept is the total count of words, as separated by whitespace, in all concepts divided by the number of concept in a map. Concise concepts are important to the taxonomy score.

Branch Point Count is the total number of concepts and linking phrases that have at least one incoming connection and more than one outgoing connection.

Concept Count is the number of concept in a map.

Linking Phrase Count is the number of linking phrases in a map.

Orphan Count is the number of concepts in the map that have no connections.
**Proposition Count** is the number of propositions (i.e. concept-linking phrase-concept) in a map.

**Root Child Count** is the number of concepts in a map that has an incoming connection from a root concept. A root concept is defined as one that has outgoing connections but no incoming connections.

**Sub Map Count** is the number of root concepts found in a map.

**Taxonomy Score** is the topological taxonomy score computed for a map.

### 6 ASSESSMENT RESULTS

We obtain the results of the Waterloo rubric and topological scoring on the concept maps of both courses and then, compare them to measure the effectiveness of the automated scoring method.

#### 6.1 Waterloo Rubric

Figure 3 shows the assessment results on the concept maps of SCADA system security for each element of rubric. The results show that most of the maps are graded either excellent or good. For instance, using *breadth of net*, 14 maps are graded to excellent where as 7 maps are good. Similarly, using *interconnectedness*, 8 maps are excellent, where as 12 maps are good.

Figure 4 shows the assessment results on the concept maps of digital forensics. The results validate the high quality of concept maps using each element separately. For instance, *breadth of net* identifies 13 and 5 maps as excellent and good; *interconnectedness* identifies 11 and 7 maps as excellent and good respectively.
6.2 Topological Scoring and Comparison with the Rubric (Ground Truth)

Analysis of Topological Scores. Figure 5 and 6 show the topological scores and the comparison with the Rubric results on the concept map of both SCADA system and digital forensics respectively. Recall that higher score refers to higher quality of a concept map. The results show that most of the maps have moderate scores. In particular, out of 22 maps of SCADA system, 8 maps score a rank of 2 or below whereas 14 maps score 3 and above including 6 maps have the rank of five or higher. Furthermore, out of 19 maps of forensics, 9 maps score the rank of 2 and higher whereas 10 maps have the score of five or higher. Additionally, out of 19 maps of forensics, 9 maps score the rank of 2 and higher whereas 10 maps have the score of 1. Highest rank of a concept map is 4 for the topic of “report writing of investigation”.

Comparison between Topological Scores and Waterloo Rubric. The Rubric grading is the ground truth. It assesses the quality of a concept map based-on content manually. To compare the ground truth with the automated topological scores, we normalized the rubric scale between zero and six where the distance between two consecutive levels (such as Excellent and Good) is 1.5.

Figures 5 and 6 shows the comparison between the ground truth rubric and topological score. We quantify the effectiveness of the scoring as accurate, close to accurate, close to inaccurate, and inaccurate. If the result of ground truth and scoring is same, it is accurate. If the score deviates one level from the ground truth, it is close to accurate. Two and three level deviations correspond to close to inaccurate, and inaccurate respectively.

Table 3 summarizes the results for the concept maps of both courses. It shows that the scoring achieves some level of accuracy. However, it is not significant and requires further research on this topic.

7 CONCLUSION

The paper presented a dataset of 41 concept maps for two cybersecurity courses useful for improving students’ learning experience in class. We evaluated the quality of the maps using two well-known techniques. One was the Waterloo Rubric (manual assessment) based-on the six elements of quality (such as breadth of net, interconnectedness, and use of descriptive links) to classify a map into excellent, good, poor, and fail. The other was topological scoring (automated assessment) based-on the structural features of a map to compute the rank between zero and six.

The evaluation results showed that the rubric identified most of the maps as Excellent or Good and provided the ground-truth about the quality of the maps. However, when we compared the topological scoring with the ground-truth, the scoring did not achieve significant accuracy thereby, pointing out an open research problem for automated assessment and grading of concept maps.

8 ACKNOWLEDGEMENT

This work was in part supported by the NSF grants # 1500101 and 1623276.
REFERENCES


