Topological Scoring of Concept Maps for Cybersecurity Education

Pranita Deshpande
Department of Computer Science
University of New Orleans
pdeshpa1@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:
Pranita Deshpande and Irfan Ahmed. 2019. Topological Scoring of Concept Maps for Cybersecurity Education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education, Minneapolis, MN, USA, February 27-March 2, 2019 (SIGCSE '19),* ACM, New York, NY, 7 pages.
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 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.

Research has shown that concept mapping is beneficial for student learning, if it is used as an integral, on-going feature of the learning process, and not as an isolated activity at the beginning and/or end of a semester [13]. Concept maps are effective for students to clarify their knowledge structures [8]. The students who learn through concept maps have better learning outcomes over traditional approaches [22].

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. The topology and structural features of concept maps are considered promising for automating the assessment and grading of concept maps. However, they have never been explored for cybersecurity education. The concept maps for cybersecurity can be quite different from other areas of computer science including the frequency of keywords and phrases, interdisciplinary topics, and dynamic subject area [2, 3, 5–7, 9–11, 17, 19, 24–27].

In this paper, we present a dataset of 41 concept maps for two cybersecurity courses (developed with expert knowledge) to support research in this direction. The courses are digital forensics, and supervisory control and data acquisition (SCADA) system security. We utilize the Waterloo rubric [1] to establish the ground truth about the quality of the maps. The rubric evaluates five elements of a concept map i.e., breadth of net, interconnectedness, use of descriptive links, efficient links, layout and development over the time, and identifies the quality of a map as either Excellent, Good, Poor, or Fail.

We further utilize the ground-truth to evaluate the effectiveness of a recent state-of-the-art topological scoring method [12]. The method uses the structural features of a concept map (i.e., branch point count, average words per concept, concept count, linking phrase, orphan count, proposition count, Root child count, submap count) and provides a topological score. The evaluation results show that the topological scoring is promising. However, they are not equally effective as compared to the Rubric and require more research in this domain. The dataset is made publicly available at gitlab for other researchers to use [14]

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

*Ahmed completed this work while he was at the University of New Orleans

SIGCSE '19, February 27-March 2, 2019, Minneapolis, MN, USA.

ACM ISBN 978-1-4503-5890-3/19/02...$15.00
DOI: http://dx.doi.org/10.1145//3287324.3287495

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 presents 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

Topics	# of Concept Maps
Introduction to digital forensics	4
First response and evidence handling	2
Investigation steps	3
File systems	5
Memory Forensics	2
Tools for investigation	3
TOTAL	19

Table 1: Concept maps for digital forensics

Topics	# of Concept Maps
Introduction to SCADA Systems	4
PLC Programming	3
SCADA communication protocols	6
SCADA Vulnerabilities and Attack	5
SCADA security solutions	4
TOTAL	22

Table 2: Concept maps for SCADA system security

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

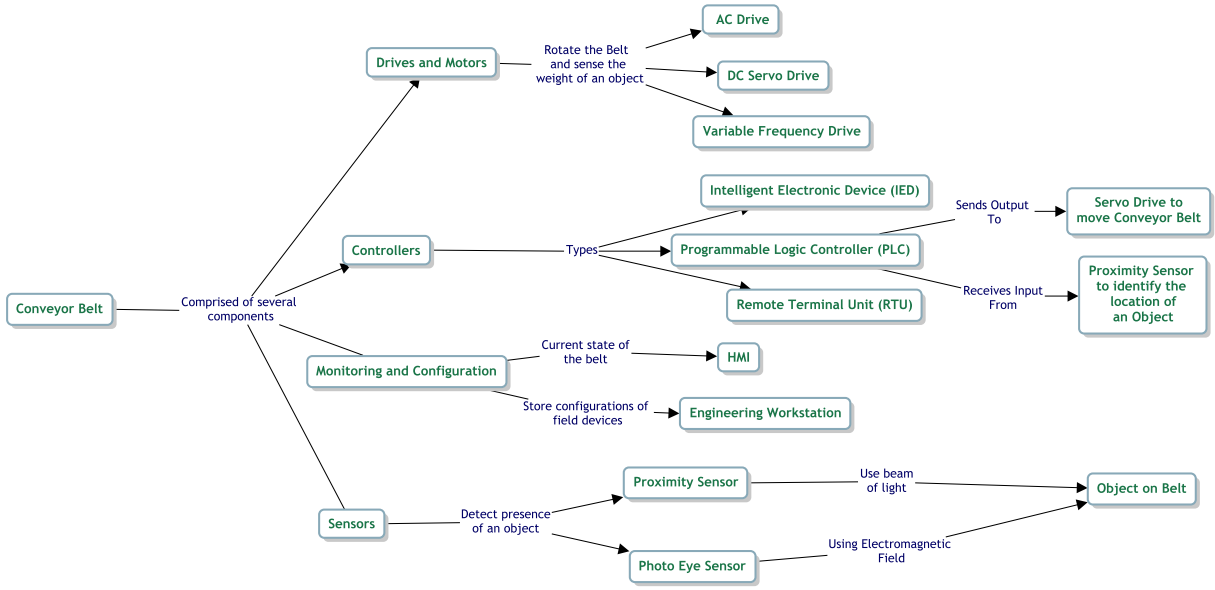

Figure 1: Working of ICS with Conveyor as an example

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 therm 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.

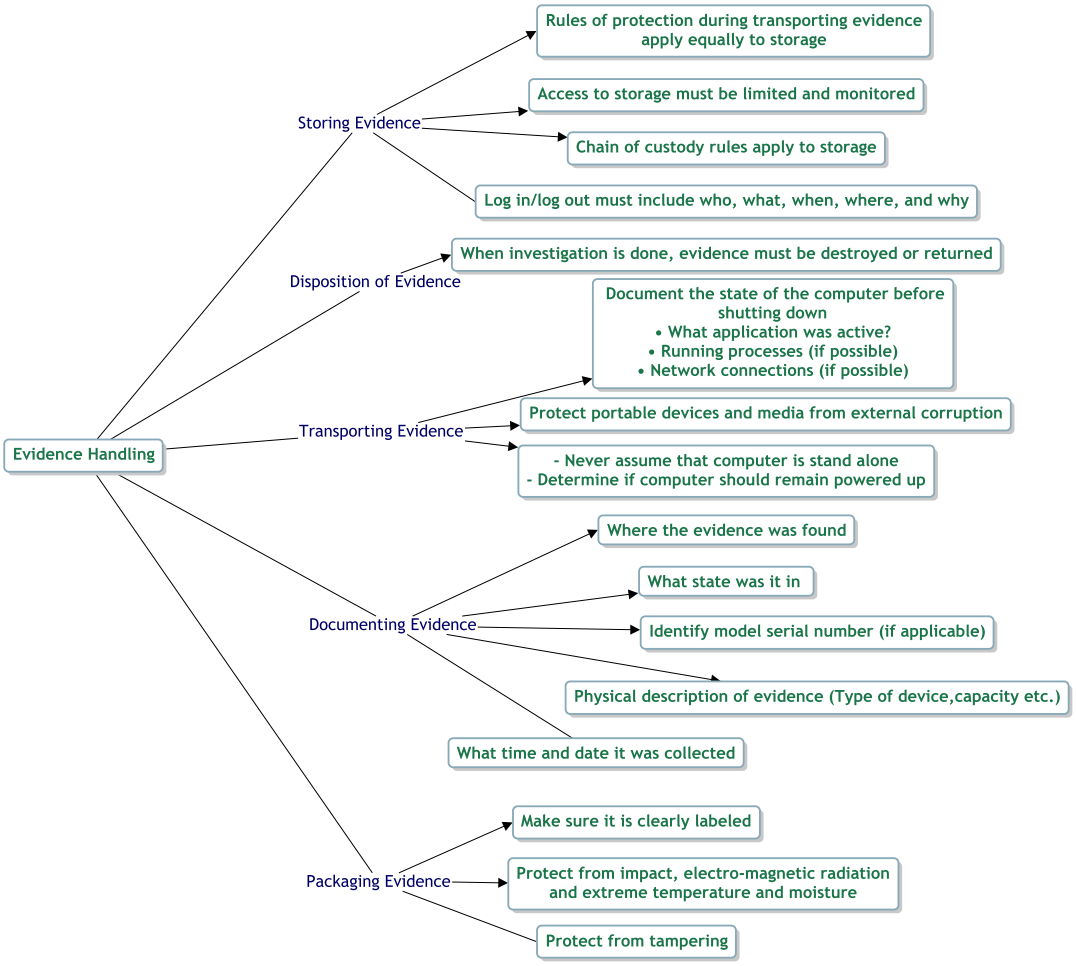

Figure 2: Different stages of handling of digital evidence

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.

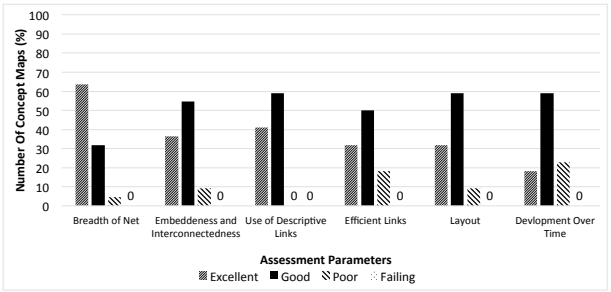

Figure 3: Rubric Assessment of SCADA system concept maps

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.

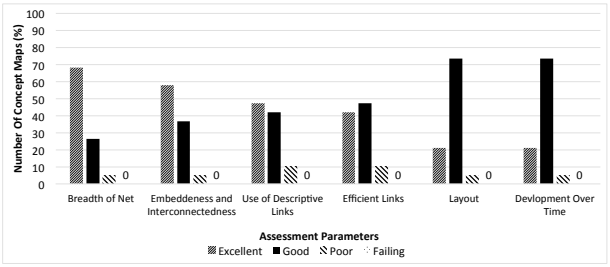

Figure 4: Rubric Assessment of Forensics concept maps

Accuracy Level	SCADA (%)	Forensics (%)
Accurate	13.64	0
Close to accurate	22.73	10.53
Close to inaccurate	27.27	31.58
Inaccurate	36.36	57.89

Table 3: Accuracy of the topological scoring when compared with the ground truth of Waterloo Rubric

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 where as 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 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 corresponds to close to inaccurate, and inaccurate respectively.

Table 3 summarize 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

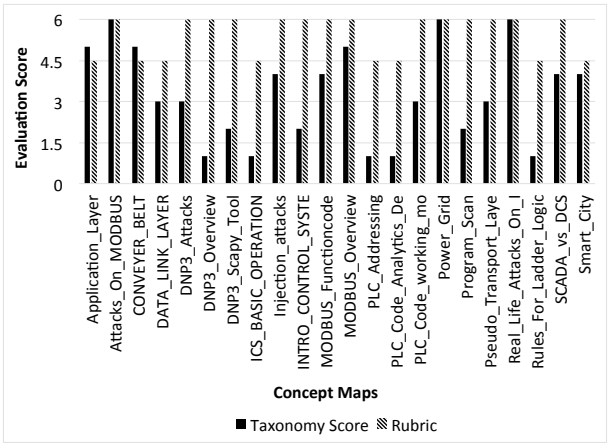

Figure 5: SCADA System Security - Comparison between the Waterloo Rubric and Topological Scoring

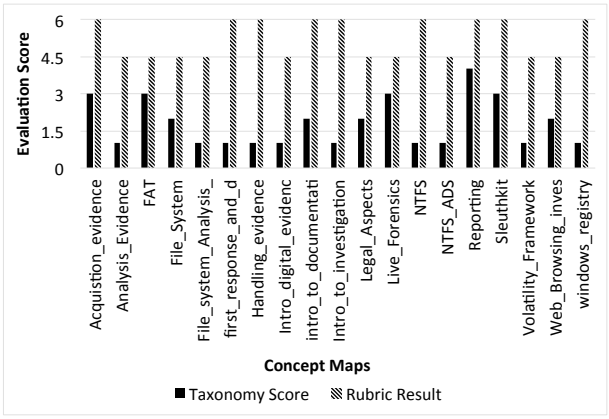

Figure 6: Digital Forensics - Comparison between the Waterloo Rubric and Topological Scoring

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

[1] 2016. Rubric for Assessing Concept Maps (Centre for Teaching Excellence, University of Waterloo). https://uwaterloo.ca/centre-for-teaching-excellence/sites/ca.centre-for-teaching-excellence/files/uploads/files/rubric_for_assessing_concept_maps.pdf. (2016).

[2] I. Ahmed, S. Obermeier, S. Sudhakaran, and V. Roussev. 2017. Programmable Logic Controller Forensics. *IEEE Security Privacy* 15, 6 (November 2017), 18–24. https://doi.org/10.1109/MSP.2017.4251102

[3] Irfan Ahmed, Golden G. Richard, Aleksandar Zoranic, and Vassil Roussev. 2015. Integrity Checking of Function Pointers in Kernel Pools via Virtual Machine Introspection. In *Information Security*, Yvo Desmedt (Ed.). Springer International Publishing, Cham, 3–19.

[4] Irfan Ahmed and Vassil Roussev. 2018. Peer Instruction Teaching Methodology for Cybersecurity Education. *IEEE Security Privacy* 16, 4 (July 2018).

[5] Irfan Ahmed, Vassil Roussev, and Aisha Ali Gombe. 2015. Robust Fingerprinting for Relocatable Code. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (CODASPY '15)*. ACM, New York, NY, USA, 219–229. https://doi.org/10.1145/2699026.2699104

[6] Irfan Ahmed, Vassil Roussev, William Johnson, Saranyan Senthivel, and Sneha Sudhakaran. 2016. A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy. In *Proceedings of the 2Nd Annual Industrial Control System Security Workshop (ICSS '16)*. ACM, New York, NY, USA, 1–9. https://doi.org/10.1145/3018981.3018984

[7] Irfan Ahmed, Aleksandar Zoranic, Salman Javaid, Golden Richard, and Vassil Roussev. 2013. Rule-Based Integrity Checking of Interrupt Descriptor Tables in Cloud Environments. In *Advances in Digital Forensics IX*, Gilbert Peterson and Sujeet Shenoi (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 305–328.

[8] Williams M. Akinsanya, C. 2004. *Concept mapping for meaningful learning*. Report. 41–46 pages.

[9] Sajal Bhatia, Sunny Behal, and Irfan Ahmed. 2018. *Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions*. Springer International Publishing, Cham, 55–97. https://doi.org/10.1007/978-3-319-97643-3_3

[10] Manish Bhatt and Irfan Ahmed. 2018. Leveraging relocations in ELF-binaries for Linux kernel version identification. *Digital Investigation* 26 (2018), S12 – S20. https://doi.org/10.1016/j.diin.2018.04.022

[11] Manish Bhatt, Irfan Ahmed, and Zhiqiang Lin. 2018. Using Virtual Machine Introspection for Operating Systems Security Education. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. ACM, 396–401.

[12] Alberto J Cañas, Larry Bunch, Joseph D Novak, and Priit Reiska. 2013. Cmapanalysis: An extensible concept map analysis tool. *Journal for Educators, Teachers and Trainers* (2013).

[13] A. Cañas. 2003. *A Summary of Literature Pertaining to the Use of Concept Mapping Techniques and Technologies for Education and Performance Support*. Report.

[14] Pranita Deshpande and Irfan Ahmed. 2018 (accessed July 23, 2018). *Concept Map Datasets for Cybersecurity Courses*. https://gitlab.com/iahmed4/concept-map-datasets-for-cybersecurity-courses

[15] Pranita Deshpande and Irfan Ahmed. 2019. Evaluation of Peer Instruction for Cybersecurity Education. In *Proceeding of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19)*.

[16] J. Dexter. 2002. *The Cyber Security Management System: A Conceptual Mapping*. Report. SANS Institute.

[17] Jonathan Grimm, Irfan Ahmed, Vassil Roussev, Manish Bhatt, and ManPyo Hong. 2018. Automatic Mitigation of Kernel Rootkits in Cloud Environments. In *Information Security Applications*, Brent ByungHoon Kang and Taesoo Kim (Eds.). Springer International Publishing, Cham, 137–149.

[18] David Hay, Ian Kinchin, and Simon Lygo-Baker. 2008. Making learning visible: the role of concept mapping in higher education. *Studies in Higher Education* 33, 3 (2008), 295–311. https://doi.org/10.1080/03075070802049251

[19] Salman Javaid, Aleksandar Zoranic, Irfan Ahmed, and Golden G Richard III. 2012. Atomizer: Fast, Scalable and Lightweight Heap Analyzer for Virtual Machines in a Cloud Environment. In *Proceedings of the 6th Layered Assurance Workshop (ACSAC'12)*.

[20] William Johnson, Irfan Ahmed, Vassil Roussev, and Cynthia B. Lee. 2017. Peer Instruction for Digital Forensics. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. USENIX Association, Vancouver, BC.

[21] William E. Johnson, Allison Luzader, Irfan Ahmed, Vassil Roussev, Golden G. Richard III, and Cynthia B. Lee. 2016. Development of Peer Instruction Questions for Cybersecurity Education. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. USENIX Association, Austin, TX. https://www.usenix.org/conference/ase16/workshop-program/presentation/johnson

[22] Paul Kim and Claudia Olaciregui. 2008. The effects of a concept map-based information display in an electronic portfolio system on information processing and retention in a fifth-grade science class covering the Earth's atmosphere. 39, 4 (2008), 700–714.

[23] Vassil Roussev. 2016. Digital forensic science: issues, methods, and challenges. *Synthesis Lectures on Information Security, Privacy, & Trust* 8, 5 (2016), 1–155.

[24] Vassil Roussev, Irfan Ahmed, and Thomas Sires. 2014. Image-based Kernel Fingerprinting. *Digit. Investig.* 11, S2 (Aug. 2014), S13–S21. https://doi.org/10.1016/j.diin.2014.05.013

[25] Vassil Roussev, Andres Barreto, and Irfan Ahmed. 2016. API-Based Forensic Acquisition of Cloud Drives. In *Advances in Digital Forensics XII*, Gilbert Peterson and Sujeet Shenoi (Eds.). Springer International Publishing, Cham, 213–235.

[26] Saranyan Senthivel, Irfan Ahmed, and Vassil Roussev. 2017. SCADA network forensics of the PCCC protocol. *Digital Investigation* 22 (2017), S57 – S65. https://doi.org/10.1016/j.diin.2017.06.012

[27] Saranyan Senthivel, Shrey Dhungana, Hyunguk Yoo, Irfan Ahmed, and Vassil Roussev. 2018. Denial of Engineering Operations Attacks in Industrial Control Systems. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18)*. ACM, New York, NY, USA, 319–329. https://doi.org/10.1145/3176258.3176319

[28] April Tanner and David Dampier. 2009. Concept Mapping for Digital Forensic Investigations. In *Advances in Digital Forensics V*, Gilbert Peterson and Sujeet Shenoi (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 291–300.