Investigating Threshold Concept and Troublesome Knowledge in Cyber Security

Ievgeniia Kuzminykh
Department of Informatics
King's College London
London, UK
ievgeniia.kuzminykh@kcl.ac.uk

Bogdan Ghita
School of Engineering, Computing and Mathematics
University of Plymouth
Plymouth, UK
bogdan.ghita@plymouth.ac.uk

Hannan Xiao
Department of Informatics
King's College London
London, UK
hannan.xiao@kcl.ac.uk

Maryna Yevdokymenko
Department of Infocommunication Engineering
Kharkov National University of Radio Electronics
Kharkov, Ukraine

Oleksandra Yeremenko
Department of Infocommunication Engineering
Kharkov National University of Radio Electronics
Kharkov, Ukraine

***Abstract*—One of the main challenges encountered in the learning process is determining the content and concepts that present challenges for students, defined by the literature as troublesome knowledge. This paper focuses on exploring the potential threshold concept in the context of cyber security programmes delivered in higher education institutions. The analysis is done using a combination of academic view, collected through CoRe matrix questionnaires, and student perspective, gathered through surveys during the learning process of several cryptography courses. Following the aggregation of the two data sources, the study identifies eight troublesome knowledge areas within the observed courses, of which two satisfied the requirements for being a threshold concept.**

Keywords—troublesome knowledge, threshold concept, cyber security, CoRe, active learning

I. INTRODUCTION

Cybersecurity is a dynamic, evolving subject in higher education institutions. Over the recent years, there has been an overwhelming demand for cybersecurity specialists both in the commercial sector and within educational institutions. This demand was reflected in the educational offer, as most universities now run a computer science programme related to cybersecurity, all striving to deliver highly trained graduates, in line with the current market needs and employer requirements. Despite these efforts, the market continues to be a demand one, having a limited number of experts for the ever-increasing cyber security sector. The 2019/2020 Official Annual Cybersecurity Jobs Report conducted by Cybersecurity Ventures [1] showed that the number of open cybersecurity positions increased by 350% between 2013 to 2021, more specifically from one million positions in 2013 to 3.5 million vacancies in 2021. However, fewer than one in four persons applying for these positions are even qualified; this demonstrates the big skill gap between the university graduates and industry demands that dictates the requirements in higher education [2]. Therefore, it is very important to give the high quality and state-of-the-art education in field of cybersecurity.

In the context of education, the task of the teacher is to provide an effective teaching process and a comfortable learning environment for the students [3-7]. Similarly, the student should demonstrate diligence and an ability to assimilate and integrate the taught content. As part of the body of knowledge, some course topics can be more challenging for the students, which can lead to gaps in knowledge and a subsequent decline in the quality of the graduates as specialists. To improve the quality of education, the teacher should equally facilitate the student's understanding of both straightforward and complex sections of the course. This study investigates the process of assimilating troublesome knowledge in cyber security programmes to understand how students experience the process of learning these concepts and to develop more effective ways to support their journey through education.

We focus on troublesome knowledge as it has been highlighted as a potential candidate for threshold concepts in cyber security education. As good teachers we need to know how to distinguish troublesome knowledge and threshold concept. Knowledge that is troublesome (difficult for understanding) does not need to be threshold [8]. Meyer and Land [9,10] describe the threshold concept as "a transformed way of understanding, interpreting, or viewing something without which the learner cannot progress". Totally, Meyer and Land proposed five key features that define a particular knowledge to be a threshold concept:

- Transformative: the knowledge that significant shift appears in the student's perception of the subject.
- Troublesome: difficult to understand and potentially can be troublesome for students who engaged with these concepts.
- Irreversible: the knowledge is difficult to unlearn, and after transformation it is hard to see the world in the same way as before.
- Integrative: can influence and tie with existing knowledge and be integrated to as a new part of student's cognitive view.
- Bounded: the subject can have the limits of a conceptual area.

Many research studies have attempted to identify the thresholds in computing: the authors of [11] identified over 50 references to threshold concepts in computing, while the analysis in [12] synthesised over 30 concepts proposed in the literature, such as abstraction, inheritance, polymorphism, and design patterns. In spite of the large number of studies about threshold concepts focusing on Computer science

978-1-6654-2814-9/21/$31.00 ©2021 IEEE

programmes, none of them appears to focus on computer security, information security, or other adjacent areas.

In this study, we start by identifying the troublesome knowledge within the delivered content, then evaluate whether it also displays the rest of features that categorise the threshold. If the knowledge satisfies all features, it can be considered as a threshold. We focus on the troublesome knowledge characteristic as it is the defining one in terms of the learning process; determining what the students struggle with represents the starting point for improving their understanding and strengthening their abilities as graduates. While different educational systems will vary in their teaching techniques, their goal is the same – ensuring the students are equipped with the necessary knowledge. To demonstrate the similarity of the results regardless of the particular approach, this research will aggregate information from the cybersecurity academic community across universities in several European countries, including Sweden, Estonia, Ukraine, and the United Kingdom, with data gathered from both educators and students. The paper outlines the methodology used in the study and first results for the Cryptography subject in the cyber security curricula.

The structure of the paper is as follows: Section II describes the methodology used to collect data about troublesome knowledge and potential threshold concepts from the perspective of both educators and students. In Section III we present the results of a preliminary analysis of the data, including the identification of two threshold concepts in cyber securirty and the associated evidence. Section IV presents our conclusions and discuss future directions of this research area.

II. Methodology

The study consists of three key phases. The first phase focuses on identifying the potential threshold concepts using the perspective of the teachers. In the second phase, the troublesome knowledge is identified based on the views of the students. Finally, in the third phase we look at the candidates for threshold concept among the identified troublesome knowledge by analysing the remaining features of a threshold concept. The two sets of information obtained from teachers and students then can be joined, processed, and the results of the data analysis are summarised.

The information was collected using a combination of informal interviews, CoRe ("content representations") forms, questionnaires, and surveys. During the first phase, the teachers were asked to fill in a CoRe form. This allowed them to unpack the possible threshold concept in the course using their own perspective on the content knowledge. In the second phase, the students answered a questionnaire revolving around their understanding of the taught curricula. The questions aimed to identify what were difficult theoretical concepts that the students deemed to be challenging, how they got help and crossed the understanding threshold. During the third phase, the results from students were matched to key features of threshold concept.

A. Teacher Perspective: Informal Interviews and CoRe Form

The study started from the international project on capacity building in cyber security ENGENSEC (Educating the Next generation experts in Cyber Security: the new EU-recognized Master's program, http://engensec.eu/), which involved a consortium of 12 universities from four countries. The project consisted of the development and delivery of seven post-graduate level courses in cyber security as well as a virtual laboratory for practical exercises and hands-on skills training [13]. During the joint meetings, the project team discussed deliverables evaluation and students' feedback and noticed that some of the learning material triggered the students' interest while others created a significant number of complaints due to difficulties with understanding and assimilating the concepts. It was therefore decided to consolidate the efforts of different universities in identifying the threshold concept in cyber security subjects in a formal research study.

The teacher views on possible threshold concept in their disciplines were collected using a CoRe matrix, presented below in Table I. This tool is used in pedagogy to help educators to conceptualise their professional competence and develop of their own pedagogical content knowledge.

TABLE I. CoRe matrix sample

	Theme I	**Theme II**	**Theme III**
Title of theme/task/idea/lab (if applicable)			
What you intend the ***students*** to learn about this idea?			
Why is it important for students to know ***this***?			
Student's **confusion** around this idea			
Difficulties, or limitations, connected with teaching this idea.			
In your opinion, what **feelings**, **actions** caused a lack of understanding in acquisition of this knowledge			
What do you think **you or student** were lacking or might have been missing that caused it to be a problem?			

The CoRe matrix shows various aspects and connections between subject knowledge and pedagogical knowledge of the teacher. The matrix includes several themes, so-called "enduring" ideas, for a specific discipline in columns, and several pedagogical questions in rows, as shown in Table I. One of the objectives of this phase is to identify the fundamental themes that teachers consider decisive for students in developing their understanding of the subject [14].

B. Students Perspective: Questionnaires

Following from the interaction with the academic staff, we used a post-study questionnaire named "Reflect on your knowledge", embedded in the learning materials, to survey the level of student understanding and knowledge. In turn, this allowed us to identify the potential threshold concepts or at least troublesome for students. As part of the questionnaire, the students were asked to reflect on their understanding of the weekly material and identify topics that they deemed to be difficult for understanding. The following questions were used:

1. Rate how confident you feel in the achievement of the following outcomes and skills.

2. What have you taken from this week? What do you know about and what do you need to learn more about?

3. What topic was difficult, troublesome for your understanding in this week material?

4. What would you recommend to foster better understanding?

Identifying difficult topics in the subject will help to constructively align the module content and modify activities to facilitate the ability of the students to grasp the taught concepts.

We focused on troublesome knowledge as one of the threshold concept criteria. Further, based on the answers of students and teachers, the comparative analysis can determine whether certain troublesome knowledge is also a threshold concept or not. In this context, we determined whether the transferred knowledge can be classified as troublesome or threshold but also whether it satisfied other features and is therefore also transformative, integrative, or irreversible.

All collected answers were anonymised prior to processing; the resulting conclusions will be compared with the teacher insights and shared with the wider research community.

III. Results

A. Teachers Perspective

The teachers from different institutions (UK, Estonia, Ukraine) who taught cryptography identified several concepts that they perceived as fundamental and potentially able to trigger transformation in the student cognitive view. The most important aspect of cryptography is underlying math; applying the theory of prime numbers, primitive roots, and discrete logarithms to the cryptographic algorithms is of core importance. Based on the underlying mathematical concepts in cryptography, the teachers highlighted the following enduring themes:

- Symmetric block ciphers: Feistel cipher, DES cipher, AES cipher
- Asymmetric block ciphers: RSA, Diffie-Hellman key exchange, digital signatures
- Cryptographic hash functions
- Zero-knowledge protocols

The teachers also expected for the students who did not have strong background in number theory or for some reasons skipped this theme during undergraduate studies to encounter problems in understanding the modular arithmetic.

B. Students Perspective

The student views were derived from the level of confidence in the topic, in conjunction with the identified troublesome material, as per the answers to questions 1 and question 3 of questionnaire. As mentioned earlier, the content presented was also analysed to determine whether it includes some of the other features of threshold concept: transformative, irreversible and integrative. The bounded feature was not relevant in this context as is relates to disciplinary boundaries rather than student experience.

Participation in the "Reflect on your knowledge" activity varied from week to week, hence there was no fixed number of respondents. The answers were collected from two groups that sat the cryptography course as part of their master programme, one group including 44 students while the other had 75 students. The rate of confidence was calculated based on the percentage taken out of total number of respondents who participated in the survey.

The students highlighted the following eight topics that caused difficulties with understanding and hence can be categorised as troublesome concepts:

- Feistel cipher
- DES algorithm
- Modes of operations
- Number theory
- Extended Euclid Algorithm
- RSA algorithm
- Diffie-Hellman key exchange protocol
- Zero-knowledge protocol

The following subsections provide an overview and analysis of the specific subjects delivered in the module that students marked as difficult.

C. Feistel Cipher

Based on the questionnaire results, 43% of the respondents were not confident about the level of knowledge they achieved regarding composite Feistel cipher. The students reported that this concept was troublesome for them:

> *"I need to deep dive into the math around Feistel cipher. The proofs do make sense, but it is for me hard to explain mathematically."*
> *"I really don't get the Feistel Cipher yet, and will have to review and research more."*
> *"…solving tricky Feistel problems was challenging"*

The identified troublesome concepts were also investigated to determine whether they presented the integrative feature. The Feistel cipher theme gave students the idea to apply or review its application on their work environment.

> *"Feistel scheme is a base for many modern cryptographic solutions, at work I want to check what cryptographic libraries we use which could be inspired by Feistel."*

The analysis concluded that the Feistel cipher as an example of composite ciphers was deemed to be transformative knowledge since it "*helped understand how substitution ciphers and transposition ciphers can be attacked, and how composite ciphers give better security".*

The Feistel cipher theme can also be categorised as an irreversible concept because the students understood how it can provide better security and its learning included a significant element of practice and hand-on exercises.

D. DES, AES, and Modes of Operations

Cryptographic algorithms DES and AES, and modes of operations of block ciphers are compulsory components of symmetric block ciphers block of cryptography. Based on the responses, 18, 16 and 21 percent of students reported that they were not confident of them achieving the learning outcomes and skills in DES, AES, and modes of operations, respectively.

> *"It was difficult for me as I needed some time to grasp the concept of DES and S boxes."*
> *"CFB and OFB (authors - modes of operations). Honestly, I had to refer to YouTube videos to obtain a better understanding of the material."*

The learned themes were successfully integrated to other subjects such as programming languages.

> *"I'm writing a tool in which I implement some of these algorithms manually to make sure I understand them"*

The questionnaire data does not provide any evidence of these concepts being irreversible or transformative.

E. Number Theory and Extended Euclid Algorithmrs

As expected by the teachers, some of the students reported challenges with the underlaying math:

> *"I found myself focused on the math rather than the material itself. It simply took a lot of time that would have been used for further reading/research."*

In contrast, another group of students, with a background in modular arithmetic from their prior studies, said that the low level of knowledge of some of their peers within the group had a negative impact on their ability to learn.

> *"I was really taken aback at the extent to which other students lacked the requisite mathematical abilities, slowing down the pace of the class."*

F. RSA algorithm and Diffie-Hellman key exchange protocol

The teachers indicated a strong likelihood that the students will encounter issues with understanding of theme of public key cryptography including asymmetric cryptographic algorithms RSA, Diffie-Hellman key exchange, digital signatures.

Surprisingly, the students reported high confidence in all these topics. However, in their questionnaires the students mentioned that RSA calculation was not easy to understand, and they were required more time and external resources.

> *"That public key algorithms seem conceptually simple but mathematically very challenging."*

> *"RSA has some modulus exponentiation calculus that can look a bit tricky but with a lot of practice it became obvious using the operations properties."*

The student answers also indicated that the concept is a transformative feature.

> *"I understood one more time why the key complexity and the cryptosystem design are the most important in the data transmission in term of keeping our data confidential."*

The learned themes were successfully integrated within the security principles body of knowledge and were expanded and applied to real life examples of use.

> *"I am going to ensure that authentication, encryption and digital signatures are applied where applicable to provide the confidentiality and data integrity."*

Once the underlying mathematical principles of public-key cryptography are understood, it is difficult to unlearn the fundamentals of asymmetric algorithms, therefore it can be classified as irreversible knowledge. It is also expected that many students will be using the received knowledge in their practice.

> *"I've used RSA for years in my work. It's been great to learn the underlying math and actually quite fun."*

However, based on the information from the questionnaires, we could not find the evidence of the Diffie-Hellman key exchange protocol topic being transformative or integrative knowledge.

G. Zero-knowledge Protocol

Only a small part of respondents (15%) was unsure in understanding the underlying zero-knowledge protocols.

Looking further, the zero-knowledge and Fiat Shamir protocols caused more difficulties in other authentication protocols.

> *"I found the mechanics of zero knowledge protocols a difficult concept to grasp at first and need time to understand things better"*

The zero-knowledge protocol concept also exhibited integrative feature for threshold concept, as many students got understanding of fundamentals of what they are using in practice in their organisations.

> *"I will read RFCs and check code of solutions with zero-knowledge protocol implemented. It will help in my work."*

Also, in the post course survey, many students noted that understanding the mechanisms of authentication protocols will be valuable for their future.

Table II provides a summary of the concepts identified by students to be troublesome and investigated by this study. The data collected from the questionnaires allowed a consistent analysis of the troublesome concepts in cyber security and led to the conclusion that, from the analysed set, two concepts satisfy the conditions to be categorised as threshold.

TABLE II. SUMMARY OF THEMES AND FEATURES FOR THRESHOLD CONCEPTS

Concept	Trouble-some	Transfor-mative	Irrever-sible	Inte-grative
Feistel cipher	v	v	v	v
DES	v			
Modes of operations	v			
Number theory	v			v
Extended Euclid Algorithm	v			v
RSA algorithm	v	v	v	v
Diffie-Hellman key exchange protocol	v		v	
Zero-knowledge protocol	v			v

IV. Conclusions

This paper investigates the threshold learning concept in the area of Cryptography, as delivered within a postgraduate cyber security programme. The study approach was to identify the troublesome concept using the CoRe matrix collected from teachers and, following the analysis of the matrix, a questionnaire shared with and completed by students. The obtained data was analysed for other factors that can categorise the threshold concept.

Based on the analysis, it can be concluded that the following concepts represent troublesome knowledge in cryptography: Feistel cipher, S-boxes in DES algorithm, modes of operation of block ciphers, RSA algorithm, and Zero-knowledge protocol. This matches the concepts identified as enduring themes in the CoRe form by teachers. Therefore, we can conclude that the CoRe form with existing questions can help not only to conceptualise the professional competence of the educators but also to identify the troublesome themes in the subject.

After reviewing the troublesome concepts, further analysis determined that only two of them can be categorised as threshold concepts: Feistel cipher and RSA algorithm. However, our results were limited by the comments obtained during questionnaires, which are more prescriptive versus interviews or essays.

As part of our future work, we plan to investigate in more detailed the identified candidates for threshold concepts in order to establish how they can migrate from troublesome to threshold. In addition, we are also planning to work on other disciplines in cyber security programme to determine any similarities or differences in the underlying areas driving the understanding of these concepts.

References

[1] Herjavec Group. (2020). *2019/2020 Cybersecurity Jobs Report.* Accessed on: Sep. 1, 2020. [Online]. Available: https://www.herjavecgroup.com/wp- content/uploads/2019/10/HG-CV-2019-Cybersecurity-Jobs-Report.pdf

[2] "Cyber security skills in the UK labour market 2020", March 12, 2020. Accessed on: Sep. 1, 2020. [Online]. Available: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020

[3] O. Yeremenko, M. Yevdokymenko, I. Kuzminykh, A. Kruhlova. "Cybersecurity Virtual Laboratory for Distance Learning", *ACM womENcourage* 2020, 24-27 September 2020, online conference.

[4] I. Kuzminykh, M. Yevdokymenko, O. Yeremenko, O. Lemeshko. "Increasing Teacher Competence in Cybersecurity using the EU Security Frameworks", unpublished.

[5] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, I. Kuzminykh, "Features of creating the virtual cybersecurity lab for distance learning", in *New Collegium*, 3, 41-45.

[6] O. Lemeshko, T. Strelkova, O. Yeremenko, M. Yevdokymenko, I. Kuzminykh, "Experience of adaptation and organization of Distance Learning in Ukrainian Universities", in *Revealing Inequities in Online Education During Global Crises,* L. Kyei-Blankson, J. Blankson, E. Ntuli, Eds. IGI Global, 2021.

[7] I. Kuzminykh, B. Ghita, H. Xiao, "The Relationship Between Student Engagement and Academic Performance in Online Education", presented at *4th Int Conf on E-Society, E-Edu and E-Technology (ICSET'20)*. ACM, Taiwan, China, August 21-23, 2021.

[8] S. Hill, "The difference between troublesome knowledge and threshold concepts", *Studies in Higher Education*, vol. 45, no. 3, pp. 665-676, 2020, doi: 10.1080/03075079.2019.1619679.

[9] J.H.F Meyer, R. Land, "Threshold concepts and troublesome knowledge (1) – linkages to ways of thinking and practising", in *Improving student learning – ten years on*, C. Rust, Ed. Oxford: OCSLD, pp. 412–24, 2003.

[10] J.H.F. Meyer and R. Land. *Overcoming barriers to student understanding: Threshold concepts and troublesome knowledge,* New York, NY: Routledge, 2006.

[11] M. T. Flanagan. *Threshold Concepts: Undergraduate Teaching, Postgraduate Training, Professional Development and School Education*. Accessed on: Sep. 1, 2020. [Online]. Available: https://www.ee.ucl.ac.uk/~mflanaga/thresholds.html

[12] K. Sanders and R. McCartney. "Threshold concepts in computing: past, present, and future", in *Proc. 16th Koli Calling Int. Conf. on Comp. Edu. Research*, ACM, 2016, pp. 91–100, doi:https://doi.org/10.1145/2999541.2999546

[13] A. Carlsson, I. Kuzminykh, R. Gustavsson R. "Virtual Security Labs Supporting Distance Education in ReSeLa Framewor", in Chall. Digital Transform. in Edu. (ICL 2018), M. Auer, T. Tsiatsos, Eds. Adv. in Intel. Sys. and Com., vol 917, pp. 577-587, Springer, Cham. doi: 10.1007/978-3-030-11935-5_55

[14] C. Eames, J. Williams, A. Hume, J. Lockley. (2011). "*CoRe: A way to build pedagogical content knowledge for beginning teachers*", Wellington: Teaching and Learning Research Initiative, 2011.