

"USER PROFILING IN CYBERSECURITY EDUCATION AND TRAINING"

Research-in-Progress

Track N° 72

Karagiannis, Stylianos, Ionian University, Corfu, GR, skaragiannis@ionio.gr

Magkos, Emmanouil, Ionian University, Corfu, GR, emagos@ionio.gr

Abstract

This research aims to improve the cybersecurity learning process, by stressing the need for examining the particular characteristics and motivations of participants of cybersecurity education/training programs. We highlight the importance of user profiling in the cybersecurity educational process and particularly the necessity for well-structured user models to support the profiling process. Furthermore, we propose and implement a user profiling module for platforms which conduct adaptive educational programs in cybersecurity, considering the specific participants' skillset.

Keywords: Cybersecurity education, Cybersecurity training, User-profiling, Personalization, Adaptiveness, Intelligent tutoring systems

1 Introduction

Public and private sector maintain a high interest in *cybersecurity education and training* programs. The demand for cybersecurity professionals grows fast nowadays, a fact which establishes a need for encouraging students to engage in cybersecurity education (Mahdi, A. et al. 2016). *Profiling* the needs of users participating in cybersecurity learning programs is important for improving the current learning approaches and at the same time a necessity for conducting *personalized exercises* and amending the current educational approaches (Schiaffino and Amandi 2009, Kirlappos et al. 2014, Alvarez-Xochihua et al. 2010). Early educational methodologies in cybersecurity have paid little attention to user interests, instead mostly focused on learning goals when sequencing educational content (Karampiperis and Sampsonm 2005). It seems to be a need for exploring and for analyzing the main objectives of educational programs, focusing on *adaptiveness* and approaches like *intelligent tutoring* (Schiaffino and Amandi 2009, Dăboliș 2012, Liegle and Woo 2000, Sottolare 2015).

The broad variety of students' prior knowledge, capabilities and experience require adaptive and *personalized cybersecurity challenge exercises* in order to motivate the students and to enhance the effectiveness of cybersecurity education and training programs (Tsekeridou et al. 2008). Specifically, in academia, the broad variety of prior knowledge of students and the variety of experience sometimes create difficulties in running related education and training programs. As a result, a small size of *knowledge hyperspace* is achieved, with major difficulties in terms of adaption. Achieving high motivational rates in cybersecurity is unresolved, due to the high theoretical background and the advanced skills required for participating in cybersecurity education and training programs (Cheung et al. 2011, 2012). Specifically, conducting a program which appeals to the personalized characteristics, specific *skillset* and background knowledge of the participants is expected to improve the motivation rates of a learning program. In addition, user interests always constituted the most significant portion of the user profile in adaptive information retrieval and information filtering (Brusilovsky and Millán 2007, Poo et al. 2003). The creation of *user models* has been seen as necessary for conducting adaptive and personalized educational programs (Kelly and Tangney 2002). Collecting data about the skills and background knowledge is essential for the user profiling process (Golemati et al. 2007).

On our approach, the main difference is that we generate and maintain the user models through the cybersecurity challenges and exercises enriching the user model with information regarding the total progress while maintaining interaction with the platform. This way the platform or module will propose different challenges according to the participants' progress and acquired skillset. During the learning process, these data will evaluate the skillset and the development of each participant. Considering this, the module will present dynamic content, different exercises and security challenges, according to the participants' characteristics.

1.1 Our contribution

This research aims to improve the learning process in cybersecurity training programs. To this end, we first highlight the importance of user profiling in the educational process and particularly the necessity for maintaining well-structured user models to support the profiling process. Furthermore, we propose and implement a user profiling module for cybersecurity education and training platforms. Our envisaged platform will adjust to the specific characteristics of the participants while obtaining their high motivational rates. The module collects data about the skills and background knowledge as part of a user profiling process. The extracted data will be used for profiling the users which participate and allow the development of an adaptive recommending system which will better guide the students in the cybersecurity learning process, along with the recording of the improvement in other knowledge areas. The participants are called to give specific information and the platform will propose specific challenges which apply best. Finally, in this paper we examine the impact of cybersecurity education

and training programs in other knowledge areas along with the impact in developing specific skills and the possibilities for high interactivity rates among the participants.

1.2 Methodology

The collection of all data, necessary for the user profiling process was made using a platform created with *WordPress*, enhanced with the open source plugin *eforms*. The participants were called to fulfil personal details for creating a user profile such as background knowledge, skillset and motivations for participating in the process. The majority of the participants were affiliated with Ionian University, Corfu, Greece, but there were also students and graduates from other Greek universities.

1.3 Outline

The rest of the paper is organized as follows. In Section 2 we discuss related work about user profiling and cybersecurity education. In Section 3 we highlight the importance of user profiling in cybersecurity education and training. In Section 4 we present a baseline implementation of a user profiling module for cybersecurity education and training platforms. In Section 5 we outline the steps towards and our thoughts about the future research.

2 Related Work

For applying an effective learning methodology, we have to consider well the required details before and after cybersecurity challenge exercises.

2.1 Required skillset and possible drawbacks in conducting cybersecurity curriculum

Criteria that affect the cybersecurity curriculum and particularly the impact of users' technical skills and knowledge during cybersecurity competitions have been discussed in the related literature (Weiss et al. 2015, Haney and Lutters 2017). However, the wide variety of the required skills, the different trainees' characteristics and the different motivation criteria have not been adequately extracted using well-structured user models. As a result, it seems that most cybersecurity education and training programs would probably not succeed in extracting explicit information about the progress of the participants and would eventually fail to collect detailed information about the development of technical and non-technical skills (Halevi 2016).

2.2 Scoreboards for extracting results

Conducting successful cybersecurity education and training programs seems to require the collection and analysis of results during and after the process. A well-known approach for presenting results from cybersecurity challenges are scoreboards (Davis et al. 2014, Mansurov 2016, Werther et al. 2011). However, the technical skillset and personalized information about each participant are not often available on these scoreboards. In this work, we propose a basic infrastructure for acquiring this kind of information and creating dynamic, robust and more detailed scoreboards.

Participants' characteristics, motivations and best practices in cybersecurity education and training processes have also been highlighted in the context of intelligent tutoring systems (Xochihua et al. 2010, Haney and Lutters 2017). However, the actual motivation criteria of the participants, specifically in participating in cybersecurity education and training programs, have not been adequately examined. Not meeting the participants' needs will eventually lead to a lack of incentives for keeping the participants interested and focused on the learning process (Vandewaetere, et al. 2012). Designing a well-structured intelligent tutoring system which will consider the participants' needs will help users

to successfully complete the learning process and organizers to extract knowledge related to their motivation criteria.

2.3 Users' motivation criteria and characteristics on creating cybersecurity curriculum

The importance of user profiling in the cybersecurity learning process has been stressed out in the literature (Alvarez-Xochihua et al. 2010). By highlighting the users' interests and the main motivational criteria, some studies also categorized the interests in short-term and long-term (Schiaffino and Amandi 2009). They mostly focus on the criteria which affect the users' motivation and the personal interests of the participants. In this paper, we will examine and implement the user profiling process as part of a cybersecurity curriculum process.

3 User profiling in cybersecurity education and training

A profile is a depiction of somebody, containing the foremost imperative or interesting facts of her/his personality and behavior. User profiling is important for creating adaptive systems, intelligent tutoring systems, recommender systems, intelligent e-commerce approaches and knowledge management systems (Schiaffino and Amandi 2009).

3.1 User models and user profiling methods

A user model is a structured representation of the user, containing direct and indirect information about the user's characteristics, requirements, knowledge and other personal preferences (Wang et al. 2006, Gauch et al. 2007). Creation and management of user models specifically in academia face a lot of challenges, as different levels of expertise and background knowledge of the participants might apply. Some of the challenges include the difficulty to extract reliable data and to create appropriate user models which reflect the actual user profiles.

Another important aspect of developing user profiling methods is the ability to maintain high levels of user management since it is important to clarify the different scales in skills, prior knowledge and to extract patterns related to the participants' behaviour during the cybersecurity challenges.

3.2 Cybersecurity education and training programs

Cybersecurity education and training programs usually include *Capture the Flag* (CTF) competitions and conferences with workshops and labs along with a high variety of sandboxed security challenges (Nakaya et al. 2016, Taylor et al. 2017, Leune and Petrilli 2017). During the competitions, it is very important to hold information about the participants' skillset, background knowledge and motivations for participating in such activities (Cheung et al. 2011).

Maintaining user models, before, during and after cybersecurity education and training programs is very important since it might enhance the ability to extract results of the learning process and to improve the information extracted from scoreboards. Correlated information extracted from the participants might also help to create user groups, according to specific characteristics such as the acquired skillset and the motivation for participating in cybersecurity education and training programs. For example, it is important to create teams which will include participants with a variety of skills and test the results in comparison to teams with narrow and specific skills.

3.3 The importance of teamwork

In cybersecurity, another important aspect is to create appropriate teams, which will be able to act immediately during cybersecurity incidents. During education and training programs, it is possible to create teams and to be able to evaluate the effectiveness of each team. This process will be enhanced

by appending data from the created user models, along with explicit information about each participant and team. An important aspect of this approach is to create the infrastructure and give the ability for communication and knowledge sharing between the participants and the teams.

4 Implementation and Results

Our module uses submit forms for collecting user profile data. For creating the questionnaires, we focused on the high utilization and the user interface. For example, we wanted the participants to feel like they create a new user account and not only fill a research questionnaire form. We tried to have an instant user feedback about our approach and to give them the opportunity to help in the development of the *cybersecurity education and training platform*.

The collection of questions included information such as the participants' university, background knowledge and various other questions related to the skillset of Information Technology (IT) and cybersecurity. Special focus was given on the users' motivations in participating in cybersecurity education and training programs. On the first page of the quiz, we tried to collect data, about which cybersecurity topics the participants are most interested in. Cybersecurity knowledge areas have also been mentioned in other studies. However, we tried to focus on the main areas and topics of cybersecurity (Burley et al. 2017, Namin et al. 2016, Parekh et al. 2017, Rashid, Danezis and Joosen 2017, Yasinsac 2002). An important aspect of information is to create the user models containing information about the skills that the participants feel comfortable with. It is important to correlate this information with specific topics that the participants feel confident and to gather information about their total experience in computer systems. Finally, along with the topics from IT, we also presented topics from mathematics and physics, which directly relate to cybersecurity topics.

4.1 Personalized questions and dynamic content

The questionnaires were designed to be interactive and personalized, in order to avoid unnecessary and unrelated questions. It is important to maintain the uniqueness of answers on the multiple choice questions in order to offer an interactive and personalized experience. The outcome might be a high-level of interactive experience which attracts the participants' interest.

The screenshot displays a user profile creation interface. On the left, a section titled "You estimate your skills and feel confident" shows three horizontal sliders for "Programming", "Mathematics", and "Networks". The "Networks" slider is set to 0. A green arrow points from the "Networks" slider to a questionnaire form. The form has a teal header with tabs: "Create User", "Knowledge Areas", "Skills", and "Feedback". The "Knowledge Areas" tab is active, showing three sections: "Which Programming languages are you familiar with?", "Mathematical Background", and "Network Skills". Each section has a list of checkboxes. The "Network Skills" section is crossed out with a large 'X', indicating it is hidden or dynamic content. The form also includes "PREVIOUS", "SUBMIT", and "NEXT" buttons at the bottom.

Section	Options
Which Programming languages are you familiar with?	<input type="checkbox"/> C, <input type="checkbox"/> C++, <input type="checkbox"/> Java, <input type="checkbox"/> PHP, <input type="checkbox"/> JavaScript, <input type="checkbox"/> Assembly, <input type="checkbox"/> C#, <input type="checkbox"/> Python, <input type="checkbox"/> Ruby, <input type="checkbox"/> .Net
Mathematical Background	<input type="checkbox"/> Computation, <input type="checkbox"/> Information theory and signal processing, <input type="checkbox"/> Probability and statistics, <input type="checkbox"/> Logic, <input type="checkbox"/> Number Theory
Network Skills	<input type="checkbox"/> TCP/IP Model, <input type="checkbox"/> Network's Hardware, <input type="checkbox"/> IP Networking and Subnet Masking, <input type="checkbox"/> DNS and DHCP, <input type="checkbox"/> Firewall, <input type="checkbox"/> WLAN, <input type="checkbox"/> Optical Infrastructure, <input type="checkbox"/> TCP / UDP Ports, <input type="checkbox"/> Sockets

Figure 1. Providing hidden or dynamic content according to previous choices

We might achieve this goal if we integrate a module to the platform which will create unique questions and answers. In this study, the only personalized feature we added, was to present different

multiple-choice questions according to the previous answers during the submission (Fig. 1). In Fig. 1 the third question is not appearing on participants with no network skills. Moreover, we maintain the option for the possibility to have scoring or/and numeric attributes to each multiple choice option.

4.2 Collected Answers and Discussion

The answers to the questions include nominal, ordinal and interval values. Specifically, in our approach, we can set the data types we want, after the gathering of information.

The total number of the participants (32) were mostly affiliated with the Ionian University (Fig. 2).

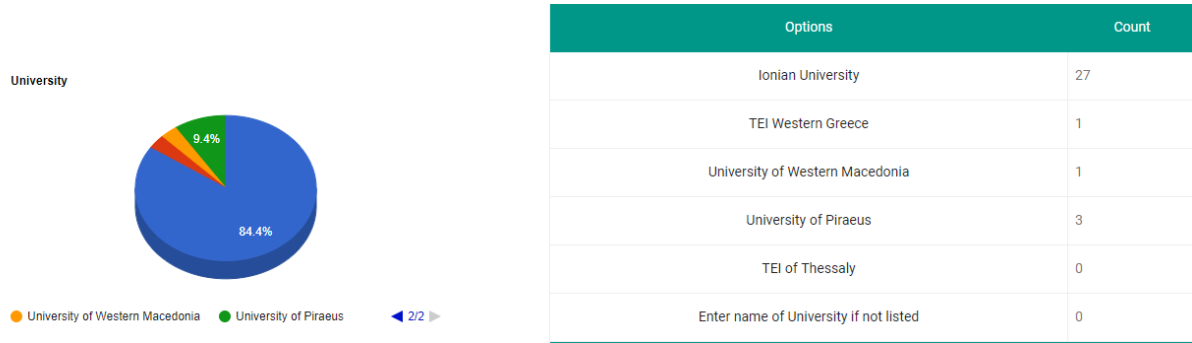


Figure 2. The total number of the participants

From the answers to Question 2 (Fig. 3), it seems that the participants recognize the importance of adaptiveness and that of personalized content since the majority feel more confident on developing skills when the learning experience is personalized.

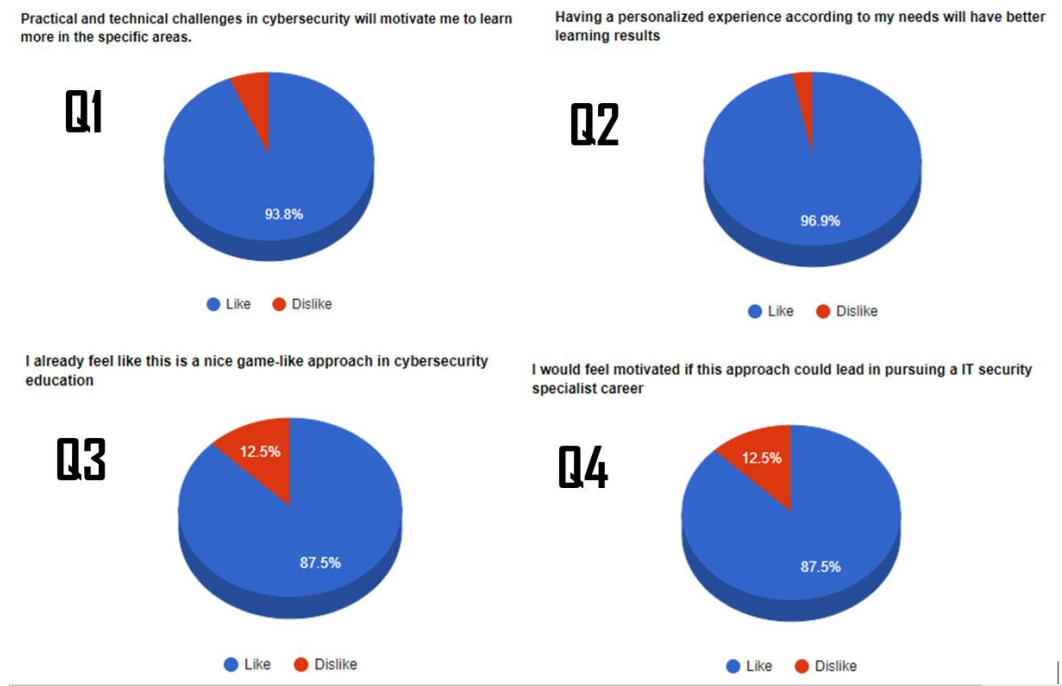


Figure 3. Feedback from the participants for our approach on answering specific questions before submitting the form

Moreover, we can assume that the participants are mostly interested in real-life challenges examples on cybersecurity topics. Specifically, in Question 1 (Fig. 3), we had the feedback “Some examples of

everyday life problems and a platform which will give me theoretical basic knowledges through tests and exercises". In Question 3, we had a positive attitude on gamification elements, although we did not present any specific details. However, we also had some negative feedbacks on gamification elements, such as the following: "There is a difference between a game and a good understanding concept. I prefer an environment which will make me understand simple things even if i don't know anything of cyber security but not via a game because the meaning can be different from person to person.". It seems that more experienced participants (4 to 6 years experience) leave more strict feedback and we observe that more experienced participants pursue specific skills and knowledge. However, in academia, it is important to keep both of the aspects and develop a platform that will help develop a broad aspect of skills and knowledge.

Summarizing, the majority (23) of the participants seem to be interested in actively participating in the development process and of collaborating in building labs related to cybersecurity topics. We see some of the feedback on this specific question in Fig. 4:



Figure 4. Feedback from the participants for our approach on answering specific questions before submitting the form about the active participation

Some of the final feedback answers are: "Please contact me for further information as I'm interested in dealing with this kind of topics.". "I m interesting of that", "Of course i will provide any necessary help to a good action of learning cyber security staff.". "Cool", "I won't be able to participate at the development during summer." Since we are conducting the research mostly on the Ionian University, we expected this positive outcome of having high interest in actively participating. On our approach, we tried to set the appropriate research questions without excluding the possibility for conducting exploratory cases and conclusions. Finally, during the research, we tried to have an interactive way of communicating with the participants, integrating a live chat system and ticket response system. In the questionnaires, we also focused on receiving feedback about our approach. Moreover, we have committed to maintain communication with most of the users and to create a communication infrastructure for the future. The participants responded positively in having future communication with us (Fig. 3).

4.3 User Interface

In our study, we highlight how the user interface and the total user experience affects the learning process. A clean and user-friendly environment assures the high rates of user interactivity and helps to extract appropriate information from the data (Question 3, in Fig. 3). It is also important to maintain a high percentage of utilization during the data collection, in order to gather more information from the participants.

4.4 Skillset Evaluation

An important aspect is to examine the collected information about the participants' opinion about their skills. Therefore, the questions have to be as simple as they can for obtaining the required information

related to the participants' skills and have a summary of their confidence on various topics (Ford et al. 2017). In our approach, we maintain the option to create dynamic multiple choice quizzes, which will appeal to the specific answers and create an exam-style evaluation for scoring the skillset. For example, if a participant feels comfortable with a score of the value 9 in programming, a high-level challenge will be placed. If the participant answers wrong, the level drops down a little and set a new challenge at a lower level. At the end of the quizzes, the levels of the particular skills are changed and the participants have to take again the exam phase to approach a higher level of skillset. The scoreboard will be used for the development of the intelligent tutoring system, but in a future work, more advanced techniques have to be used for extracting and analyzing related data. The reliability of the scoreboard of the skillset will be also examined and improved.

5 Conclusions and Future Work

In this study, we highlight the impact of cybersecurity education and training programs in other knowledge areas and scientific fields (Rowe et al. 2011). The basic weaknesses of the participants have to be considered as well in order to offer the best possible tutoring experience.

The positive outcome from a well-structured tutoring system is the achievement of uniform and progressive development of the participants and the extraction of conclusions about the acquired skills during the programs. Moreover, we proposed and implemented a user profiling module for enhancing cybersecurity education and training programs.

Our current approach, although interactive, does not achieve high rates of personalization. Even if all the above-proposed methods and techniques are used, information about the behaviour of the participant during the program is not collected.

In a future work, extra questionnaires and quizzes will be presented for evaluating the skills and extract scoreboards. The participants will be called to solve specific challenges, quizzes and also be able to explore personalized news' feeds. In a future work, various Wordpress plugins will be used for enhancing the social network elements and for creating personalized challenges regarding the learning and training process such as *buddypress* and *learnpress*.






For enriching the collection of information from the participants, external sources might be used, such as information from social network websites. However, it is important to mention the issues in privacy and to ensure that the gathered information complies with the appropriate laws, related to personal information.

Quizzes is an easy way to gather scores and to examine the skills of the participants. However, it is not as reliable as other complicated approaches. For automating the process, we need to ensure that every participant will have to give a unique answer. In future research, we will enhance the platform, ensuring that the answers will be dynamically generated to prohibit cheating and the possibility for automatic challenge generation (Burket et al. 2015, Schreuders et al. 2017, Irvine et al. 2017).

For maintaining different cybersecurity challenges, sandbox approaches have to be designed as well. One of the best options is to create virtual labs which will represent a real environment (Luallen and Labruiere 2013, Karlov 2016, Son 2012, Irvine et al. 2017). Sandboxing is very popular for creating virtual environments. However, in our approach, the challenges have to be a bit different for every participant. In our future research, we will examine sandboxing approaches and the implementation of virtual labs with the option of readjusting the difficulty and the ability to adapt according to the participants. Moreover, it is important to have the ability to generate challenges and virtual labs for enhancing the adaptiveness and to create unique challenges according to the participant. The above methods will help us achieve our final goal, to achieve a higher level of adaptiveness and personalization.


6 Appendix

Data #1 #0000000048 On June 20, 2018 4:47 pm	
First Name	####
Last Name	####
Email	####
IP Address	94.67.206.241
Completion Time	18 minutes, 48 seconds
Administrator Remarks	Processing
User Account	Guest
Link	Submission link

Create User		Help us build the adaptive module
First Name <i>not required</i>		####
Last Name <i>not required</i>		####
Contact Email Address		####
University	<input checked="" type="radio"/> Ionian University <input type="radio"/> TEI Western Greece <input type="radio"/> University of Western Macedonia <input type="radio"/> University of Piraeus <input type="radio"/> TEI of Thessaly <input type="radio"/> Enter name of University if not listed	
Which year did you got into Undergraduate Studies?		2016
First time you got involved with Computer Systems (Personal Computer mostly)		2003

<p>Interested in Cybersecurity Topics?</p>	<div style="display: flex; flex-direction: column; gap: 5px;"> <div><input checked="" type="checkbox"/> Data Security</div> <div><input checked="" type="checkbox"/> Software Security</div> <div><input checked="" type="checkbox"/> Component Security</div> <div><input checked="" type="checkbox"/> Connection Security</div> <div><input checked="" type="checkbox"/> System Security</div> <div><input checked="" type="checkbox"/> Cyber warfare</div> <div><input checked="" type="checkbox"/> Reconnaissance</div> <div><input checked="" type="checkbox"/> Cryptography</div> <div><input checked="" type="checkbox"/> Web Exploitation</div> <div><input checked="" type="checkbox"/> Reverse Engineering</div> <div><input checked="" type="checkbox"/> Network security</div> <div><input checked="" type="checkbox"/> Data Security & Privacy</div> <div><input checked="" type="checkbox"/> Mobile Platform & Application Security</div> <div><input checked="" type="checkbox"/> IoT Security & Privacy</div> <div><input checked="" type="checkbox"/> Computer & Software Security</div> <div><input checked="" type="checkbox"/> Cloud Computing Security</div> <div><input checked="" type="checkbox"/> Human Behavior-Based Security</div> <div><input checked="" type="checkbox"/> Security Policy & Management</div> </div>
--	---

Knowledge Areas	Check the concepts and topics you feel confident!	
<p>Experience with Advanced I.T. Concepts <i>Experience with more advanced concepts such as Operating Systems, Hardware, Programming etc.</i></p>	<input type="radio"/> 0 to 2 Years <input checked="" type="radio"/> 2 to 4 Years <input type="radio"/> 4 to 6 Years <input type="radio"/> 6 Years or more...	
<p>Operating systems are you familiar with?</p>	<input type="checkbox"/> DOS <input checked="" type="checkbox"/> LINUX <input type="checkbox"/> UNIX <input checked="" type="checkbox"/> WINDOWS <input type="checkbox"/> OSX	
Programming	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	4/10
Mathematics	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	8/10
Networks	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	3/10
Physics	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	7/10
Operating Systems	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	2/10
Computer Architecture	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	4/10
Data Structures	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	6/10

Web Infrastructure		0/10
Which Programming languages are you familiar with?	<input checked="" type="checkbox"/> C <input checked="" type="checkbox"/> C++ <input type="checkbox"/> C# <input checked="" type="checkbox"/> Java <input checked="" type="checkbox"/> Python <input type="checkbox"/> PHP <input type="checkbox"/> Ruby <input type="checkbox"/> JavaScript <input type="checkbox"/> .Net <input type="checkbox"/> Assembly	
Mathematical Background	<input checked="" type="checkbox"/> Computation <input type="checkbox"/> Information theory and signal processing <input checked="" type="checkbox"/> Probability and statistics <input checked="" type="checkbox"/> Logic <input type="checkbox"/> Number Theory	
Network Skills	<input checked="" type="checkbox"/> TCP/IP Model <input checked="" type="checkbox"/> Network Hardware <input checked="" type="checkbox"/> IP Networking and Subnet Masking <input checked="" type="checkbox"/> DNS and DHCP <input type="checkbox"/> Firewalls <input type="checkbox"/> WLAN <input type="checkbox"/> Optical Infrastructure <input type="checkbox"/> TCP / UDP Ports <input type="checkbox"/> Sockets	
Physics	<input checked="" type="checkbox"/> Quantum Computation <input type="checkbox"/> Electromagnetism <input type="checkbox"/> Analog Electronics <input type="checkbox"/> Digital Electronics <input checked="" type="checkbox"/> Signal Processing	
Operating Systems	<input type="checkbox"/> Bash Programming <input type="checkbox"/> General history and boot processes <input type="checkbox"/> Process Management <input type="checkbox"/> Memory Management <input checked="" type="checkbox"/> File Systems <input checked="" type="checkbox"/> Networking <input type="checkbox"/> Command Line Interface (CLI)	

Computer Architecture	<input checked="" type="checkbox"/> Processors <input type="checkbox"/> Memory Management <input type="checkbox"/> Buses <input type="checkbox"/> I/O <input type="checkbox"/> Firewalls <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Optical Infrastructure <input type="checkbox"/> TCP / UDP Ports <input type="checkbox"/> Sockets <input checked="" type="checkbox"/> Hard Disk Management
Data Structures	<input checked="" type="checkbox"/> Arrays <input type="checkbox"/> Lists <input checked="" type="checkbox"/> Stack <input type="checkbox"/> Queues <input type="checkbox"/> Trees <input checked="" type="checkbox"/> Graphs

Feedback		Feedback
Practical and technical challenges in cybersecurity will motivate me to learn more in the specific areas.	<input checked="" type="checkbox"/> Like or Dislike <input checked="" type="checkbox"/>	The best way to learn something is to get your hands dirty. none has said i want more theory. Practice makes you evaluate yourself
Having a personalized experience according to my needs will have better learning results	<input checked="" type="checkbox"/> Like or Dislike <input checked="" type="checkbox"/>	
I already feel like this is a nice game-like approach in cybersecurity education	<input checked="" type="checkbox"/> Like or Dislike <input checked="" type="checkbox"/>	Well it is a really good approach in cyber security, because i haven't even submitted yet and i already found out more resources for what to start learning for this field.
I would feel motivated if this approach could lead in pursuing a IT security specialist career	<input checked="" type="checkbox"/> Like or Dislike <input checked="" type="checkbox"/>	That's the plan for now at least.
It would be nice if i had the opportunity to propose my own challenges	<input checked="" type="checkbox"/> Like or Dislike <input checked="" type="checkbox"/>	
Consider me as part of this lab. I want to actively participate at the development.	<input checked="" type="checkbox"/> Like or Dislike <input checked="" type="checkbox"/>	I might not have much experience but I really like a good puzzle or problem.

References

- Alvarez-Xochihua¹, O., Bettati¹, R., & Cifuentes, L. (2010). Mixed-initiative intelligent tutoring addressing case-based problem solving (Vol. 2). *Technical Report TAMU-CS-TR-2010-7*.
- Bashir, M., Lambert, A., Wee, J. M. C., & Guo, B. (2015). An examination of the vocational and psychological characteristics of cybersecurity competition participants. *Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*.
- Brusilovsky, P., & Millán, E. (2007). User models for adaptive hypermedia and adaptive educational systems. In *The adaptive web* (pp. 3-53). Springer, Berlin, Heidelberg.
- Burket, J., Chapman, P., Becker, T., Ganas, C., & Brumley, D. (2015). Automatic Problem Generation for Capture-the-Flag Competitions. *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.
- Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012, January). Effectiveness of cybersecurity competitions. In *Proceedings of the International Conference on Security and Management (SAM) (p. 1)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
- Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM) (p. 1)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
- Davis, A., Leek, T., Zhivich, M., Gwinnup, K., & Leonard, W. (2014, August). The Fun and Future of CTF. In *3GSE*.
- Ford, V., Siraj, A., Haynes, A., & Brown, E. (2017, March). Capture the Flag Unplugged: an Offline Cyber Competition. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education* (pp. 225-230). ACM.
- Gauch, S., Speretta, M., Chandramouli, A., & Micarelli, A. (2007). User profiles for personalized information access. In *The adaptive web* (pp. 54-89). Springer, Berlin, Heidelberg.
- Golemati, M., Katifori, A., Vassilakis, C., Lepouras, G., & Halatsis, C. (2007, April). Creating an ontology for the user profile: Method and applications. In *Proceedings of the first RCIS conference* (No. 2007, pp. 407-412).
- Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., ... & Chen, J. (2016, November). Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services* (pp. 318-324). ACM.
- Haney, J. M., & Lutters, W. G. Skills and Characteristics of Successful Cybersecurity Advocates. In *Proc. of the 13th Symposium on Usable Privacy and Security, ser. SOUPS* (Vol. 17).
- Irvine, C. E., Thompson, M. F., McCarrin, M., & Khosalim, J. (2017). Labtainers: a Docker-based framework for cybersecurity labs.
- Karampiperis, P., & Sampson, D. (2005). Adaptive learning resources sequencing in educational hypermedia systems. *Journal of Educational Technology & Society*, 8(4).
- Karlov, A. A. (2016). Virtualization in education: Information Security lab in your hands. *Physics of Particles and Nuclei Letters*, 13(5), 640-643.
- Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.
- Liegle, J. O., & Woo, H. G. (2000, November). Developing adaptive intelligent tutoring systems: a general framework and its implementations. In *Proceedings of the ISECON Conference, Philadelphia*.
- Luallen, M. E., & Labruyere, J. P. (2013, January). Developing a critical infrastructure and control systems cybersecurity curriculum. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 1782-1791). IEEE.

- Mahdi, A. O., Alhabbash, M. I., & Naser, S. S. A. (2016). An intelligent tutoring system for teaching advanced topics in information security.
- Mansurov, A. (2016). A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia. *Modern Applied Science*, 10(11), 159.
- Nakaya, M., Akagi, S., & Tominaga, H. (2016). Implementation and Trial Practices for Hacking Competition CTF as Introductory Educational Experience for Information Literacy and Security Learning. *Proceedings of ICIA*, 5, 57-62.
- Namin, A. S., Aguirre-Muñoz, Z., & Jones, K. S. (2016). Teaching cybersecurity through competition. *In Annual International Conference On Computer Science Education: Innovation & Technology*.
- Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2017)
- Poo, D., Chng, B., & Goh, J. M. (2003, January). A hybrid approach for user profiling. In System Sciences, 2003. *Proceedings of the 36th Annual Hawaii International Conference on* (pp. 9-pp). *IEEE*.
- Rashid, A., Danezis, G., & Joosen, W. (2017). Establishing a Guide to the Cyber Security Body of Knowledge.
- Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. *In Proceedings of the 2011 conference on Information technology education* (pp. 113-122). *ACM*.
- Schiaffino, S., & Amandi, A. (2009). Intelligent user profiling. *In Artificial Intelligence An International Perspective* (pp. 193-216). *Springer, Berlin, Heidelberg*.
- Schreuders, Z. C., Shaw, T., Ravichandran, G., Keighley, J., & Ordean, M. (2017, August). Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events. *In USENIX. USENIX Association*.
- Son, J., Irrechukwu, C., & Fitzgibbons, P. (2012). Virtual Lab for Online Cyber Security Education. *Communications of the IIMA*, 12(4), 5.
- Teaching cybersecurity analysis skills in the cloud. *In Proceedings of the 46th ACM Technical Symposium on Computer Science Education* (pp. 332-337). *ACM*.
- Tsekeridou, S., Tiropanis, T., Christou, I., & Vakilzadeh, H. (2008). Toward virtual campuses: collaborative virtual labs & personalized learning services in a real-life context.
- Vandewaetere, M., Vandercruysse, S., & Clarebout, G. (2012). Learners' perceptions and illusions of adaptivity in computer-based learning environments. *Educational Technology Research and Development*, 60(2), 307-324.
- Wang, J., Li, Z., Yao, J., Sun, Z., Li, M., & Ma, W. Y. (2006, January). Adaptive user profile model and collaborative filtering for personalized news. *In Asia-Pacific Web Conference* (pp. 474-485). *Springer, Berlin, Heidelberg*.
- Werther, J., Zhivich, M., Leek, T., & Zeldovich, N. (2011, August). Experiences in Cyber Security Education: The MIT Lincoln Laboratory Capture-the-Flag Exercise. *In CSET*.
- Weiss, R. S., Boesen, S., Sullivan, J. F., Locasto, M. E., Mache, J., & Nilsen, E. (2015, February).
- Yasinsac, A. (2002). Information security curricula in computer science departments: Theory and practice. *The George Washington University Journal of Information Security*, 1(2), 1-9.