Received October 18, 2019, accepted October 29, 2019, date of publication November 11, 2019, date of current version December 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2952585

Crowdsourcing Approach for Developing Hands-On Experiments in Cybersecurity Education

LE WANG[1,2], ZHIHONG TIAN[1], ZHAOQUAN GU[1], AND HUI LU[1]
[1]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China
[2]Computer School, National University of Defense Technology, Changsha 410073, China

Corresponding author: Zhihong Tian (tianzhihong@gzhu.edu.cn)

This work was supported in part by the Guangdong Postgraduate Education Innovation Project under Grant 2019JGXM82, in part by the National Key Research and Development Plan under Grant 2018YFB0803504, in part by the National Natural Science Foundation of China under Grant 61572153, Grant 61702220, Grant 61871140, Grant 61702223, Grant 61572492, and Grant U1636215, in part by the Guangdong Province Key Research and Development Plan under Grant 2019B010137004, and in part by the Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2019).

ABSTRACT The operational skills are essential for the cybersecurity practitioners and the hands-on experiments can be utilized to train their practical skills. As malicious attacks are continually changing and new vulnerability appears quickly with the increasing number of new software, it has been a challenging problem to develop hands-on experiments rapidly and continuously which are consistent with realistic threat scenarios. Normally, skilled engineers are familiar with threat scenarios and the attack/defense skills, but they have no motivation to develop hands-on experiments for education. In contrast, the faculties are good at teaching and training but they have no resource or experience to deploy lots of hands-on experiments by themselves. In this paper, we propose a framework called RC^{2}F by adopting the crowdsourcing approach, which acts as a platform for the engineers and the faculties as well as channels between them for resource exchanging. In the framework, we also introduce two incentive models to motivate the participants, where the constructor-oriented Forward Incentive Model (FIM for short) encourages the engineers by the incentive mechanism and the demand-oriented Backward Incentive Model (BIM for short) balances the educational resources for the faculties. We also provide a comprehensive case based on the practical data to analyze the proposed framework. And the results validate that the proposed framework as well as the FIM and BIM models can address the challenge in developing hands-on experiments.

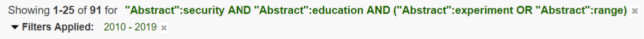
INDEX TERMS Cybersecurity, crowdsourcing, hands-on experiment, education, incentive model.

I. INTRODUCTION

The operational skills play an important role for the cybersecurity practitioners due to the intrinsic characteristics of the cybersecurity discipline. Many colleges and universities have developed cyber platforms or cyber ranges to provide hands-on experiments for the students or practitioners [1]. As stated in [2], the authors found that the available resources for instruction (i.e. hands-on experiments) would make great impact on the curriculum, which are highly related to the knowledge and skills that the students may gain. Hence, developing hands-on experiments with high quality would achieve good teaching effect, and many studies try to design these experiments from realistic scenarios that are shown to be more popular with the faculties and students [3].

However, with the increasing demand for cybersecurity practitioners, the existing platforms cannot meet the urgent demands by providing a large number of hands-on experiments or covering as many subjects as possible. For example, the Arizona State University (Temple) developed only 20 experiments from 2011 to 2014 [4]. As the cybersecurity technologies change dynamically; many advanced attack or defense methods have been proposed in the past five years, but no experiment could be utilized to replay the new security events or predict security subjects that may occur in the future. Therefore, it has been an important and challenging task to develop a large number of realistic experiments that can reflect the latest security subjects and technologies continuously.

The associate editor coordinating the review of this manuscript and approving it for publication was Zheli Liu.


Showing **1-25** of **91** for "Abstract":security AND "Abstract":education AND ("Abstract":experiment OR "Abstract":range) ×

▾ **Filters Applied:** 2010 - 2019 ×

FIGURE 1. Number of papers in the IEEE database from 2010 to 2019 focusing on security education and taking advantage of cyber range or hands-on experiment. The figure also shows the condition of query.

In our work, we aim at developing hands-on experiments in the cyber range for cybersecurity education. A plenty of studies focus on the cybersecurity education by providing hands-on experiments in the cyber ranges. In the recent 10 years, about 100 papers have been published in the IEEE database as shown in Figure 1. Notice that, a few papers are not related to the cybersecurity education, but they are misrecognized due to the IEEE search engine (for example, the work in [5] is irrelevant). However, there are still a lot of related works, not to mention the published results in other databases.

We investigated these works and found out that the research topics are limited to the following three aspects:

1) They show the importance of the hands-on experiments in cybersecurity education and provide some detailed methods;

2) They introduce solutions and technologies to develop the cyber range or the hands-on experiments;

3) They verify the effectiveness of the cyber ranges or the hands-on experiments.

In summary, extant studies only focus on the cyber range or the hands-on experiments themselves; no influential works have been proposed to solve the following problem: how to develop the hands-on experiments that can reflect the latest security subjects and technologies continuously in the cyber range? We face the following challenges in solving the problem. First, it is to analyze the situation of cybersecurity technology as well as cybersecurity education. And second, it goes to build a universally available collaboration framework for skilled engineers and faculties. The finals are designment of incentive mechanism for developers and users of hands-on experiments.

In this paper, we propose a crowdsourcing framework that addresses all the challenges. We summarize the contributions of our works as follows.

1) We formulate and summarize the characteristic of cybersecurity technologies, including confrontation, concomitance and rapid-changing, that would affect the cybersecurity education;
2) We propose and implement a crowdsourcing framework called RC^{2}F to develop the hands-on experiments rapidly and continuously in the cyber range;
3) We introduce a constructor-oriented forward incentive model called FIM to encourage the constructors (cybersecurity enterprises or skilled engineers who contribute the data or skills);
4) We introduce a demander-oriented backward incentive model called BIM to balance the educational resources for the demanders who use these experiments for education.

We also introduce a comprehensive case to demonstrate and validate the proposed framework and the models. The results also corroborate the feasibility of the framework.

The remainder of this paper is organized as follows. Section II discusses the characteristics of cybersecurity knowledge and technology, and the particularity of cybersecurity talents and education is also analyzed. In addition, we introduce the challenges of developing hands-on experiments for education. The crowdsourcing approach and the applications in education are introduced in Section III. Section IV describes the crowdsourcing framework as well as the proposed FIM and BIM models; the proposed framework can overcome the challenges for developing hands-on experiments rapidly and continuously. A comprehensive case is provided in details in Section V. Conclusions and future works are discussed in Section VI.

II. ART-OF-STATE IN CYBERSCURITY EDUCATION

Cybersecurity knowledge and technologies are main contents of cybersecurity education. To begin with, we introduce the characteristics of cybersecurity knowledge and technologies for a better understanding of cybersecurity education. Since the ultimate goal of the cybersecurity education is to enable the students (or practitioners) could master the cybersecurity skills and apply these technologies to deal with real threats and attacks in the cyberspace, the hands-on experiments that could reflect the practical cybersecurity scenario are the most important parts of training the practitioners. However, developing a plenty of hands-on experiments for cybersecurity education is very difficult and we also introduce the challenges in this section.

A. CHARACTERISTICS OF CYBERSECURITY KNOWLEDGE AND TECHNOLOGY

Cybersecurity is a typical interdisciplinary discipline. When we study the security issues, cybersecurity always shows the concomitance property (i.e. post-companion) [6]. For example, cloud security problems appeared only after cloud computing and cloud service are utilized, while IoT security issues should be considered when the Internet-of-Things are widely adopted in reality [7]–[9]. Regarding the cybersecurity education, it is quite difficult to predict and prepare necessary lectures or experiments in advance [10]. Once some concomitant security issue emerges, a large number of hands-on experiments need to be developed rapidly to meet the challenges of security threats and attacks [11].

Attack-defense confrontation is the concrete manifestation of cyberspace security. ‘A fall into a ditch makes you wiser’, this proverb describes the progressive patterns of technology in cybersecurity. In other words, defense technology, the dove of peace in the white box, is forced to evolve with various attack methods, the ghost in the black box. Therefore, considering the confrontation characteristics of cybersecurity, conducting the hands-on experiments for the practitioners is the best teaching and training approach.

Security threats in cyberspace stem from not only the cyberterrorist and cyber-attacks, they also come from a large number of existing software vulnerabilities on the other hand. The forms and methods of cyber-attacks are changing constantly, and the number of software vulnerabilities is also increasing rapidly with the increasing number and complexity of software. For example, 6447 vulnerabilities were found in the complicated software in 2016, while 14714 and 16555 vulnerabilities were found in 2017 and 2018 respectively, with the growth rates of 128% and 12.5% (https://www.cvedetails.com). Hence, the cybersecurity practitioners must be prepared to thrive in a constantly evolving technological landscape (https://www.iste.org/). Therefore, it is necessary and important to design and develop a plenty of hands-on experiments rapidly in order to enable the practitioners can cope with the challenges of new cyber threats.

B. CHALLENGES OF DEVELOPING HANDS-ON EXPERIMENTS IN CYBER RANGE

Developing hands-on experiments that are consistent with realistic scenarios requires first-hand data on the security threats or the cyber-attacks. However, these data, including operation logs, tracking records, statistical results, and analysis [16], are mainly collected by the security enterprises or the government management agencies. In addition, in order to design and develop the hands-on experiments, it is necessary for the experienced engineers to reproduce the real attack routes and the defense methods. However, these people are mainly distributed in the security enterprises, and the enterprises or the engineers have no natural motivation to develop hands-on experiments for cybersecurity education. Therefore, it is the first challenge to motivate the experienced cybersecurity enterprises or skilled engineers to engage in developing the hands-on experiments.

The faculties are the direct participants in cybersecurity education and they can be considered as the demanders of the hands-on experiments. They are aware of what kinds of experiments are needed and what patterns of hands-on experiments are suitable from the cybersecurity education. As the direct beneficiaries, if there exists such appropriate hands-on experiments, they will not hesitate to adopt them for education. But when they are asked to summarize or refine their experimental requirements, especially the specific business background, operating style, operation steps or scenarios, they also show no initiative motivation for the additional work. Therefore, it is the second challenge to motivate the cybersecurity faculties to engage in the design of the hands-on experiments.

Concluding from the above analysis, the suitable constructors and the direct demanders in the cybersecurity education have no motivation to participate in developing a plenty of hands-on experiments. The reason behind the phenomenon might be the mismatch of the resources that are owned by both sides. The constructors from the enterprises could not understand the real needs of the cybersecurity education, and their data or skills cannot be exchanged for return. Correspondingly, the demanders from colleges and universities do not have real data and practical experience; their demands cannot be notified to the constructors directly. Therefore, a framework for exchanging the educational resources and the demands would be a bridge connecting both sides for addressing the above challenges.

III. CROWDSOURCING APPROACH AND ITS APPLICATIONS IN EDUCATION

Crowdsourcing is useful in gathering massive information by a large number of participants. The term Crowdsourcing basically means a bound of people combing together to solve a common problem in 2006 [12]; then it has been widely adopted in scientific research, software development, interactive question and answer, online education and other fields. The crowdsourcing approach can be regarded as making a cumulative contributions by combining the wisdom or efforts from a crowd of people.

Idea sharing is the first application mode of crowdsourcing in the field of education. Students can help each other with sharing ideas about their experiments or homework; faculties can share lesson strategies and teaching cases; and professors can offer personalized teaching guidance for students according to their feedback. This approach could help optimize the teaching style, courses and effects among student. (cited in Sep 27th, 2019, https://theknowledgereview.com/crowdsourcing-vital-factor-future-education/).

Cooperation is another important application mode of crowdsourcing in the field of education. A crowdsourcing based software program is established in [13] for medical students to memorize substantial amounts of information by generating concise, high-yield study materials. A game-based privacy learning system is designed and developed by leveraging the wisdom of a crowd of non-experts on Amazon Mechanic Turk in [14]. The empirical stud demonstrated that the crowd can provide high-quality ideas of designing and developing a practical, educational privacy learning game.

In addition, there is a combined application mode of crowdsourcing for education. For example, a crowdsourcing education program is designed in [15], which includes different components such as crowdteaching, crowdleraning, crowdtuition, crowdfunding, etc. The program can enhance each student's skills, optimize the lecturing process effectively by sharing and pooling the study materials, and also improve alumni financial situation by supporting tuition crowdfunding.

Different from the mentioned application modes above, our work mixes the cooperation modes of software development and teaching application. We propose a crowdsourcing approach to develop the hands-on experiments for cybersecurity education.

IV. RPOPOSED CROWDSOURCING FAMEWORK AND MODELS

In this section, we present the crowdsourcing approach for developing the hands-on experiments. We introduce

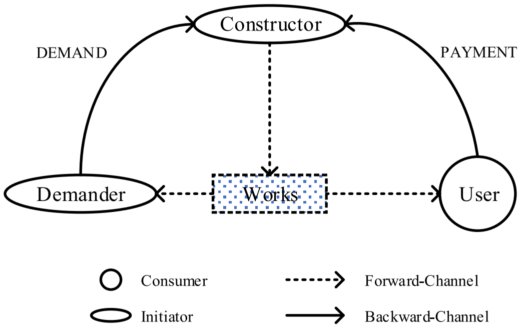


FIGURE 2. Composition and Cooperation Diagram of RC^{2}F, the crowdsourcing framework. Figure shows the three entities which participate in crowdsourcing activities, and two channels which exchange resources among entities through Works as an intermediary.

the implementable crowdsourcing framework called RC^{2}F for developing the experiments rapidly and continuously. In addition, we present two models where FIM (a constructor-oriented Forward Incentive Model) motivates the constructors and BIM (a demand-oriented Backward Incentive Model) motivates the demanders respectively.

A. THE IMPLEMENTABLE CROWDSOURCING FRAMEWORK

The object of crowdsourcing is to generate some product through cooperation. In cybersecurity education, the product refers to the hands-on experiments. We propose and implement a crowdsourcing framework called RC^{2}F that consists of three entities. The first entity is Constructor, which is not only the owner of the resources, but also the constructor of the experiments. Generally, the constructors can be the cybersecurity enterprise or the skilled engineer in cybersecurity education (without otherwise specified, we use constructor in the following parts). The second entity is Demander, which is not only the user that could be the direct beneficiary of the crowdsourcing products, but also the demand designer. Generally, the demanders could refer to the faculties in cybersecurity education. The third entity is User, which has no other interactive activities in the crowdsourcing process apart from paying for the use of generated product (i.e. the hands-on experiments). The users could refer to student or lecturer who learn knowledge and acquire cybersecurity experience through the education framework.

Constructor and Demander are two initial entities, that is to say, crowdsourcing is initiated by one of them. After that, crowdsourcing activities would run iteratively (or once). The User as consumer entity could not initiate crowdsourcing, but it is essential for the sustainability (iteration) of crowdsourcing activities (like wheel).

RC^{2}F defines two channels at the same time, which exchange resources among the entities. As shown in Figure 2, the Forward-Channel converts the resources owned by the Constructor into Works (the generated products such as the hands-on experiments) and passes them furtherly to Demander and User. The Backward-Channel delivers the DEMAND owned by the Demander and PAYMENT of User to Constructor as returns.

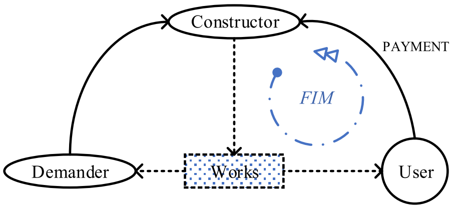


FIGURE 3. The location and start-stop entity of FIM model in RC^{2}F.

Equilibrium can be found by analyzing the model from one of three entities perspective. For the User entity, the forward channel provides Works as service, and the backward channel sends PAYMENT as a reward. Thus the User entity is balanced. For the Constructor entity, the forward channel transmits Works as service to User (as well as Demander, though it is a little different with the former scenario) and the entity receives PAYMENT from User by the backward channel. Besides, the forward channel transmits Works from Constructor to Demander in order to meet the latter's DEMAND, which is proposed by Demander and delivered to Constructor through the backward channel. Therefore, the Constructor entity is also balanced. For the Demander entity, the DEMAND is designed and proposed through the backward channel and Works is provided by the forward channel in order to meet its need (it can be regarded as a reward). It is also a kind of qualitative balance for Demander.

Equilibrium means fairness. It implies that participating entities would receive the corresponding returns while contributing to the crowdsourcing framework. When the framework needs to measure the contributions, quantification models are needed to calculate the amount of contribution and benefit. It should be noted that only the contribution of the initial entity is worth quantifying. Once the crowdsourcing process starts, the behavior of the consumer entity cannot be predicted and controlled. Other entities' contributions and returns in the framework will gradually be balanced.

B. THE CONSTRUCTOR-ORIENTED FORWARD INCENTIVE MODEL

FIM (the constructor-oriented Forward Incentive Model) qualitatively describes the incentive characteristic of RC^{2}F for Constructor in a mathematical way. Furthermore, after instantiation for specific application, FIM model can also be used to design incentive mechanism for Constructor.

In the operating scene, there are three parameters in FIM which are positively correlated with the incentive of Constructor:

$$FIM \propto Count_U \cdot Mark \cdot Money \tag{1}$$

$Count_U$ refers to the number of works produced by Constructor and ordered by User. *Mark* represents the evaluation of Works ordered by User. When it comes to a specific work (i.e. experiment), it is a specific number indicating the satisfaction of users ordering this work; otherwise, it is a statistical value indicating the evaluation to all of works developed by one Constructor.Money is the fee or reward that User pays

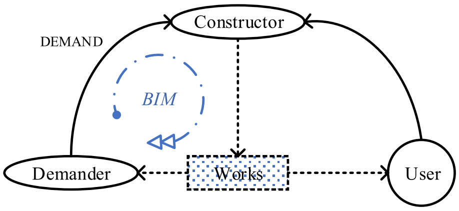


FIGURE 4. The location and start-stop entity of BIM model in RC^{2}F.

Constructor for the use of his works. In practice, it may be money, points or virtual money.

As implemented in the RC^{2}F framework, the $Count_U$ parameter in FIM is included in the Forward-Channel, while the *Mark* and *Money* parameters are included in the PAYMENT load of the Backward-Channel.

C. THE DEMANDER-ORIENTED BACKWRAD INCENTIVE MODEL

Similar to the FIM model, BIM (the demander-oriented Backward Incentive Model) qualitatively describes the incentive characteristic of Demander. Same as FIM, BIM also can be used to design incentive mechanism for Demander.

In the operating scene, there are three parameters in BIM. Two of them, $Count_D$ and $Demand_{DC}$, are positively correlated with BIM (i.e. incentive to Demander). And the other parameter *Demand* is negatively correlated with it (i.e. negative incentive effect against Demander) as the following formulation:

$$BIM \propto Count_D \cdot \left(Demand_{DC} \big/ Demand\right) \tag{2}$$

Demand refers to the number of requirements put forward by Demander. $Demand_{DC}$ represents the count of requirements fulfilled by Constructor. The combination of the two parameters evaluates the requirements from the perspective of quality and realizability. $Count_D$ is the number of works ordered by Demander. In practice, the size of $Count_D$ implies Demander's recognition of Constructor's works. For example, in the context of cybersecurity education, the larger $Count_D$ is, the more consistent Constructor's works are with the hands-on experimental requirement.

As implemented in the RC^{2}F framework, the $Count_D$ parameter can be found in the Forward-Channel, while the $Demand_{DC}$ and *Demand* parameters are included in the DEMAND of the Backward-Channel.

V. A CASE STUDY AT CIAT

The RC^{2}F framework and the two incentive models have been validated through educational practice in CIAT (Cyberspace Institute of Advanced Technology) of Guangzhou University).

In September 2018, Guangzhou University set up an experimental class (called F-Class) on cyberspace security at CIAT (http://wyy.gzhu.edu.cn/index.htm). F-Class brings together a large number of excellent researchers and carries out a lot of pedagogy research in cybersecurity education. "Characteristics of cybersecurity knowledge and technology" and "Challenges of developing hands-on experiments in cyber range" described in Section II were explored in the course of the study. According to these conclusions, F-Class deployed a large-scale internal cyber range for training students' operational ability. Crowdsourcing approach was employed to develop hands-on experiments in the cyber range according to the requirements of the curriculum. The RC^{2}F framework was designed in the progress, as well as the FIM and BIM models were instantiated.

TABLE 1. SSA hans-on experements requirement.

Req No.	Subject	Time (H)	Requirement of Content
No.1	Static Analysis Tool	6	The Use and Practice of IDA pro
No.2	Dynamic Analysis Tool	6	The Use and Practice of Olly Dbg
No.3	Binary Edit Tool	4	The Use and Practice of VmWare, PE editor, Hexadecimal Editor, etc.
No.4	Debug Tool	6	The Use and Practice of WinDbg
No.5	Penetration Testing Tool	6	The Use and Practice of metasploit
No.6	Environmental Deployment I	4	The Use and Practice of docker
No.7	Environmental Deployment II	4	The Use and Practice of LLVM Compiler
No.8	Programming Exercises	6	Shellcode Programing
No.9	Reverse Analysis I	10	Stack and Heap Overflow
No.10	Reverse Analysis II	10	Binary Vulnerability (CVE) Reproduction
No.11	Web Security Analysis	10	Penetration Testing and CVE Reproduction
No.12	Auto Vulnerability Analysis	10	The Use and Practice of libFuzzer

A. REQUIREMENT OF CURRICULUM

There were seventeen courses in F-Class curriculum. All of them need hands-on experiments for practicing the students' operational ability. We take the course "Software Security and Analysis" (abbreviated as "SSA") as an example to illustrate its experimental requirements.

SSA hands-on experiments included tool exercises, reverse analysis, penetration testing and automated vulnerability mining. The total experiment lasted more than 80 hours. Considering the other 16 courses, it is impossible to rapidly develop and deploy such a large number of experiments that were consistent with real scenarios by the instructors of CIAT. Crowdsourcing is the preferring approach. A specific experiment corresponds to a crowdsourcing project. The process of developing the experiment is consistent with the order in Table 1: they are ordered from tools' practice to application, and from manual to automatic analysis. The publishing order of the crowdsourcing projects was also the developing process of the experiments.

B. ENTITIES IN CROWDSOURCING

There were three entities. Instructors who taught SSA course acted as Demanders and Users at the same time.

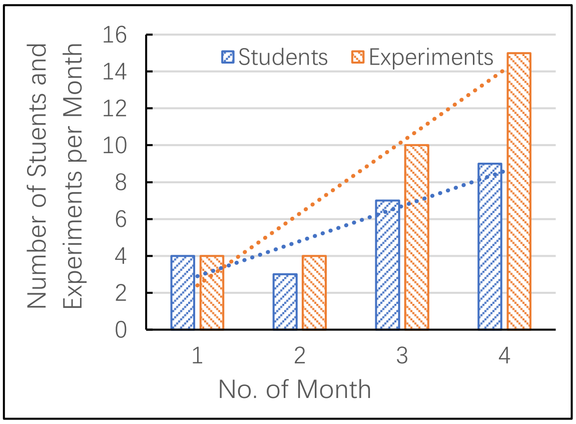


FIGURE 5. The numbers of students, who took part in crowdsourcing homework, and experiments, which were developed by students per month in four.

Instructor was Demander when each crowdsourcing project was released, and he was User when the experiment was accepted and deployed in the cyber range. Senior students were Constructor, who bid for projects and submitted experimental works.

The crowdsourcing was an optional item for the homework of comprehensive practical course, which lasted four months. Students applying for this course could choose the crowdsourcing item in multiple post-selection items. The credit was determined by the quality of the experiment works that the student submitted.

As shown in Figure 5, the number of student participating in crowdsourcing homework shows saddle-like change. It implies that some students quit crowdsourcing, and then more students joined in afterwards. With the number of students rising wavily, the number of accepted experiments increased steadily. Eventually, the number of experiments per month reached twice of the number of students. It could verify that the RC^{2}F framework and the two models are effective.

C. INSTANTIATION OF TWO INCENTIVE MODEL

Limited by the conditions and scale of verification practice, the instantiation of the two models was simplified. We keep the main bodies and key parameters for further analysis.

1) FIM INSTANTIATION AND ANALYSIS

Three main parameters of the FIM model, i.e. $Count_U$, *Mark* and *Money*, were all instantiated in verification practice. There was no more parameter appended. $Count_U$ was instantiated as the number of experimental works which were accepted by instructor and could be deployed in cyber range. Instructor scored the accepted experimental works; the score was taken as the instantiation of *Mark* which ranged in [0,2]. The total score of each student taking part in crowdsourcing must range in [3], [5]. If the score exceeds 5, a certain amount of money would be paid to the student, which was the instantiation of *Money*.

A total of 21 students participated in the crowdsourcing. As shown in Table 2,7 students quitted with no submission, and one student scored only 1.5 points with one experiment work. This implies that a third of the crowdsourcing participants did not contribute.

TABLE 2. Instantiation of fim in F-class.

No. Student	$Count_U$	*Mark*	*Money*
No.1	2	3.5	0
No.2	*1*	*1.5*	*0*
No.3	2	3	0
No.4	**4**	**6.5**	**150**
No.5	2	3.5	0
No.6	3	4.5	0
No.7	3	5	0
No.8	2	3	0
No.9	**3**	**5.5**	**50**
No.11	2	3.5	0
No.12	2	3	0
No.13	2	3	0
No.15	3	4	0
No.19	2	3	0

TABLE 3. Instantiation of bim in F-class.

Req No.	*Demand*	$Demand_{DC}$	Req No.	*Demand*	$Demand_{DC}$
No.1	2	**3**	No.7	**2**	1
No.2	2	**4**	No.8	3	**5**
No.3	2	**4**	No.9	**4**	2
No.4	**2**	1	No.10	**4**	3
No.5	2	2	No.11	4	**5**
No.6	2	2	No.12	**3**	1

2) BIM INSTANTIATION AND ANALYSIS

With the simplified verification scenario in F-Class, the instructor acts as Demander and User at the same time. Hence $Count_D$ was the same as $Count_C$ in FIM. $Demand_{DC}$ and *Demand* were instantiated with their original meanings.

The course homework does not set limit on the number of submissions that each project could receive. As shown in Table 3, $Demand_{DC} > Demand$ in some rows, such as projects No.1-3. In addition, because of the mismatch between project requirements and students' abilities, some projects' submissions were far less than the requirements, such as project No.12. The feasibility of the BIM model was verified by practice in F-Class, it also showed that external constraints were needed to ensure the effectiveness of the model. For example, the order of works accepted for each project (e.g. first come first served) should be declared in advance to avoid the result $Demand_{DC} > Demand$.

VI. CONCLUSION AND FUTURE WORK

In this paper, we summarized the characteristics of cybersecurity knowledge and technology, which included confrontation, concomitance and rapid-changing. Developing hands-on experiments rapidly and continuously was essential for training students' capability. It is indispensable to establish an implementable mechanism for resource exchange among security enterprises and educational institutions. We proposed the crowdsourcing framework RC^{2}F to provide resources exchanging channels among the participants and introduced two incentive models for demander (come from cybersecurity education institute) and constructor (come from cybersecurity enterprises or skilled engineers) respectively. RC^{2}F and the incentive models (FIM and BIM) were verified by F-Class's educational activities in CIAT of Guangzhou University. RC^{2}F was able to transmit requirements from Demander to Constructor and return rewards from User to Constructor. Besides, the FIM model could convert User's satisfaction to incentive towards Constructor, while the BIM model could describe the relationship between crowdsourcing works and requirements to encourage Demander release the preferable crowdsourcing needs.

While the RC^{2}F framework as well as FIM and BIM are proposed for cybersecurity education, they could also be adopted in other crowdsourcing scenarios.

Concerning the framework and the proposed methods in this paper, the following aspects can be further studied. First, we could explore what kind of external conditions and constraints should be refined. Second, conducting a large-scale verification practice could be useful in optimizing the structure and improving the feasibility. Finally, more crowdsourcing scenarios could be used to explore the advantages and disadvantages of the proposed framework.

REFERENCES

[1] Z. Tian, Y. Cui, L. An, S. Su, X. Yin, L. Yin, and X. Cui, "A real-time correlation of host-level events in cyber range service for smart campus," *IEEE Access*, vol. 6, pp. 35355–35364, 2018, doi: 10.1109/ACCESS.2018.2846590.

[2] M. Dark, "Advancing cybersecurity education," *IEEE Secur. Privacy*, vol. 12, no. 6, pp. 79–83, Nov. 2014, doi: 10.1109/MSP.2014.108.

[3] T. Zseby, F. I. Vázquez, A. King, and K. C. Claffy, "Teaching network security with IP darkspace data," *IEEE Trans. Edu.*, vol. 59, no. 1, pp. 1–7, Feb. 2016, doi: 10.1109/TE.2015.2417512.

[4] L. Xu, D. Huang, and W.-T. Tsai, "Cloud-based virtual laboratory for network security education," *IEEE Trans. Edu.*, vol. 57, no. 3, pp. 145–150, Aug. 2014, doi: 10.1109/TE.2013.2282285.

[5] R. Sacatelli, T. Schofield, K. Todoroff, A. Carandang, A. Eng, I. Lowry, H. Mather, A. Ramos, S. Swart, M. Dottori, N. Strandskov, J. Kohut, O. Schofield, and S. Glenn, "Ocean predictive skill assessments in the South Atlantic: Crowd-sourcing of student-based discovery," in *Proc. OCEANS*, St. John's, NL, Canada, Sep. 2014, pp. 1–7, doi: 10.1109/OCEANS.2014.7003134.

[6] Q. Tan, Y. Gao, J. Shi, X. Wang, B. Fang, and Z. Tian, "Toward a comprehensive insight into the eclipse attacks of tor hidden services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1584–1593, Apr. 2019.

[7] Z. Tian, W. Shi, Y. Wang, C. Zhu, X. Du, S. Su, Y. Sun, and N. Guizani, "Real-time lateral movement detection based on evidence reasoning network for edge computing environment," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4285–4294, Jul. 2019.

[8] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Inf. Sci.*, vol. 491, pp. 151–165, Jul. 2019, doi: 10.1016/j.ins.2019.04.011.

[9] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun. Mag.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.

[10] Z. Tian, S. Su, W. Shi, X. Du, M. Guizani, and X. Yu, "A data-driven method for future Internet route decision modeling," *Future Gener. Comput. Syst.*, vol. 95, pp. 212–220, Jun. 2018.

[11] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1223–1229, Mar. 2009.

[12] J. Howe, "The rise of crowdsourcing," *Wired*, vol. 14, no. 6, pp. 1–4, Jun. 2006.

[13] H. C. Bow, J. R. Dattilo, A. M. Jonas, and C. U. Lehmann, "A crowdsourcing model for creating preclinical medical education study tools," *Acad. Med.*, vol. 88, no. 6, pp. 766–770, 2013.

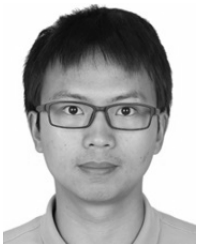
[14] W. Wang, Y. Tao, K. Wang, D. Jedruszczak, and B. Knutson, "Leveraging crowd for game-based learning: A case study of privacy education game design and evaluation by crowdsourcing," 2016, *arXiv:1603.02766*. [Online]. Available: https://arxiv.org/abs/1603.02766

[15] R. Llorente and M. Morant, "Crowdsourcing in higher education," in *Advances in Crowdsourcing* F. Garrigos-Simon, I. Gil-Pechuán, and S. Estelles-Miguel, Eds. Cham, Switzerland: Springer, 2015, pp. 87–95.

[16] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Comput. Commun.*, vol. 30, nos. 11–12, pp. 2314–2341, Sep. 2007.

LE WANG received the Ph.D. degree in computer science from the National University of Defense Technology (NUDT). He is currently an Associate Professor with the Cyberspace Institute of Advanced Technology, Guangzhou University, and a Postdoctoral Student with the Computer School, NUDT. His current research interests include network and big data security. He is a member of the China Computer Federation.

ZHIHONG TIAN received the Ph.D. degree. He was a Standing Director of the CyberSecurity Association of China. From 2003 to 2016, he was with the Harbin Institute of Technology. He is currently a Professor, the Ph.D. Supervisor, and the Dean of the Cyberspace Institute of Advanced Technology, Guangzhou University. His current research interests include computer networks and network security. He was a member of the China Computer Federation.



ZHAOQUAN GU received the bachelor's and Ph.D. degrees in computer science from Tsinghua University, in 2011, and 2015, respectively. He is currently a Professor with the Cyberspace Institute of Advanced Technology (CIAT), Guangzhou University, China. His research interests include wireless networks, distributed computing, and big data analysis.

HUI LU received the B.E. degree in electronic science and technology and the M.S. degree in optical engineering from Southwest Jiaotong University, Chengdu, China, and the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2003, 2006, and 2010, respectively. He was a Research Associate with the Institute of Microelectronics, Chinese Academy of Sciences, China, from 2010 to 2017. He joined Guangzhou University, Guangzhou, China, in 2017, where he is currently an Associate Professor with the Cyberspace Institute of Advanced Technology. His research interests include cyberspace security and intelligent attack-defense.