Poster: A Model to Evaluate Cybersecurity Talents

Fangjiao Zhang[1,2], Xiang Cui[3,1], Di Wu[1,2], Qixu Liu[1,2]
1 (Institute of Information Engineering, Chinese Academy of Sciences)
2 (School of Cyber Security, University of Chinese Academy of Sciences)
3 (Cyberspace Institute of Advanced Technology, Guangzhou University)
zhangfangjao@iie.ac.cn

***Abstract*—In recent years, cybersecurity situation is becoming increasingly severe. Malicious attacks pose a great threat to the Internet and even the country. Therefore, the cybersecurity talents is badly needed. On one hand, the quantity of related talents is insufficient; on the other hand, the means or tools to evaluate them are limited. So far, there haven't been a perfect system to objectively assess talents for companies or others. Employers often judge employees by their performances in cybersecurity competitions, represented by CTF (Capture the Flag). However, it's not enough. Because of inherent disadvantages, competitions cannot build practical scenarios accurately and the performances in competitions can not reflect one's true proficiency and skills. In this paper, we propose a system model to evaluate cybersecurity talents comprehensively and accurately. It will become a vital tool for ones that badly need cybersecurity talents.**

Keywords—cybersecurity; talents; evaluate

I. INTRODUCTION

Recently, major cybersecurity incidents are continuing without end, especially the WannaCry ransomware, one of the few security incidents globally these years, broke out in May 2017. Cyber attacks are getting cheaper and cheaper, and easily cause mass panic. Cybersecurity talents cultivation has aroused public attention and become an important research topic in the cyber security field. In spite of the efforts to cultivate the talents, there is a serious shortage of cybersecurity talents, not only in China but also in the worldwide. According to the estimate of open data, the gap in China is nearly one million and is increasing annually. Meanwhile, the number would rise to a whopping 1.8million by 2022, an increase of 20% from 2015, reported by International Information System Security Certification Consortium (ISC)^2[1].

In addition to national campaigns to promote cybersecurity awareness, security competitions have become the main means of discovering, cultivating and selecting cybersecurity talents. In all kinds of competitions, Capture the flag (CTF) is the most typical and popular competition. Competitions provide an experimental environment for hand-on exercises by which participants can digest and understand the theories learned in the classroom better. As recorded in CTFtime, there are 129 CTF events which serve 9808 teams [2]. At first, CTF is mainly Jeopardy-style, a form similar to the examination. For this type, participants just need to focus on solving several specific challenges independently. Over time, another type emerge: attack-defense mode (Attack With Defense, AWD). Participants in this mode attack and defend in cyberspace, exploiting opponents' service vulnerabilities and repairing their own ones to score points in cyberspace. Even so, there are some disadvantages in existing competitions [3]. Most competitions, something like examination-oriented methods, are far away from the real world and focus more on skills to solve problems. Moreover, they emphasize attack skills and are hard to improve defensive abilities. The latter is more urgent needed for companies. There are apparent deficiencies for companies using competitions to evaluate cybersecurity talents they needed.

Due to this issue, we presented a system model to evaluate cybersecurity talents to make up the deficiencies of competitions. The system can implement the process of automatic questions building and automatic system grading. The questions built are based on employees' prior knowledge and skills they input. Then the system will judge employees' performances from how they answer the questions generated before. Using it as a reference, the employer can select the right candidates they want. Combined with actual offensive and defensive scenarios, the system gives the fine-grained and comprehensive evaluation for cybersecurity talents.

II. DESIGN

The architecture of the model presented is shown as Figure 1. As we can see, the system mainly consists of two modules: automatic question & answer system and talents evaluation. We will introduce how the two modules work together in the following.

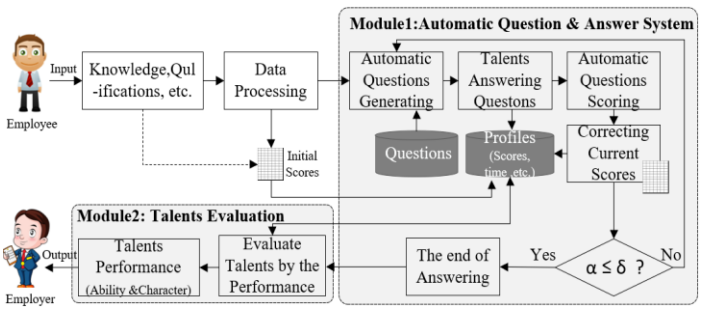

Fig. 1. The architecture of the system model.

Before evaluating cybersecurity talents, the employee need to type in his past experiences, including subjects learned, competitions involved, awards received and certificates

acquired. Based on the employee's knowledge and skills, the system justifies what abilities the employee should be equipped with [4]. All abilities considered, initial technical scores, constantly revised later, are given by the system. It should be noted that abilities will be processed and represented by a certain data format, which is essential to some further data processing.

A. Automatic Question & Answer System

There are two databases here, one is for storing questions bank and the other is for storing all the relevant data of the employee. The questions in the bank are not limited to CTF but also problems people always encounter in practical work. And the employee's data includes personal knowledge, skills, scores, answer-question time, and so on. When the employee's input is finished, automatic question & answer system will generate questions automatically from questions bank in accordance with abilities the employee is equipped with. After answering, the system grade and reevaluate the employee based on his performance automatically. Then the system reproduces questions according to "current" abilities reevaluated. It can be treated as a learning examination questions system. Automatic question answering process would repeat until the employee's answers are stable. This is how the system can evaluate talents objectively and precisely.

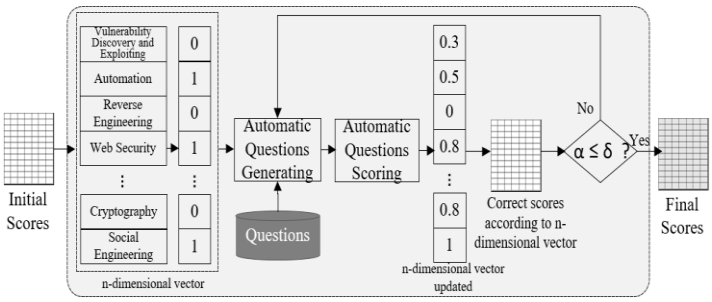

Fig. 2. Automatic question & answer system.

Figure 2 illustrates how the system reevaluate the employee continually, the key of the automatic question & answer system. The abilities of the employee the system judge automatically would be expressed as an *n*-dimensional vector. The variable *n* is the number of all the abilities cyber security involved. To evaluate the employee accurately, we hope that abilities are divided into more tiny sections. And if one has the ability of vulnerability discovery and exploiting, the corresponding parameter value is set to 1; if not, it is set to 0. All parameters of the vector are assigned by that logic. When the employees finish tying in prior experiences, the *n*-dimensional vector is automatically assigned. The system would generate customized questions from the bank for the employee by receiving the vector as input.

Based on the prior experiences, one could be evaluated more directly and precisely. When completing all the questions, the employee is assessed by their completion and graded automatically. Then the *n*-dimensional vector would be updated accordingly. As described in Figure 2, although one knows little about the vulnerability discovery and exploiting, he could answer the related questions. So, the corresponding parameter value increases to 0.3. Similarly, one claims to be familiar with automation, but he couldn't answer questions very well. The parameter value would decrease to 0.5. We call changes of the parameters the increment marked α. It might be positive or negative. The system would recalculate scores of the employee from increment variations. The process is continuing, as long as most increments are less than the threshold δ.

B. Talents Evaluation

The system would evaluate cybersecurity talents mainly in two aspects: ability and character. The final scores got in the question answering process above are used to measure the ability of the employee. But the scores are not just scores; they also contain a detailed scoring and proficiency levels in various skills of the employee. In character, we could collect certain data by some sensors to see whether the employee is impatient or not when encountering difficulties. The data includes heart rates, temperature and blood pressure, etc. The character is also an important reference for performance evaluation and future work. Ultimately, the employers select the right candidates combined with evaluations the system produces.

III. Conclusion and Future Work

Considering that there is not a perfect evaluation system for cybersecurity talents, we propose a system model in this paper. Through rounds of automatic questioning and answering, the system assesses the employee's ability precisely. Apart from that, the character of the employee is also evaluated together. Overall, the system would produce the fine-grained and comprehensive evaluation for cybersecurity talents. It is highly significant for companies or others who are in need for cybersecurity talents.

To increase the efficiency and accuracy of evaluating, we would enrich the questions bank and adopt neural networks in later research.

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful comments for improving this paper. This work is supported by the National Natural Science Foundation of China under grant (No. 61702508, No. 61602470), the Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences and Beijing Key Laboratory of Network security and Protection Technology.

References

[1] Cybersecurity Faces 1.8 Million Worker Shortfall By 2022. https://www.darkreading.com/careers-and-people/cybersecurity-faces-18-million-worker-shortfall-by-2022/d/d-id/1329084.

[2] CTFtime.org. https://ctftime.org/.

[3] Zhang X., Liu B., Gong X., Song Z. State-of-the-Art: Security Competition in Talent Education. International Conference on Information Security and Cryptology(Inscrypt) 2017. Lecture Notes in Computer Science, vol 10726.. 461-481.

[4] Celia Paulsen, Ernest L. McDuffie, William D. Newhouse, Patricia R. Toth. Nice: Creating a cybersecurity workforce and aware public. IEEE Security & Privacy 10 (2012) 76-79 .