東海大学紀要情報理工学部
Vol.20 , 2020, pp. 11–18
DOI: 10.18995/24352152.20.11

Introduce the CyExec System for Cybersecurity Training Platform and Cybersecurity Research Trends Related to Data Analysis

by

Sanggyu Shin †1

Abstract

Recently, the threats of cyberattacks, mainly targeted attacks, are increasing rapidly, and many cybersecurity incidents are frequently occurring. On the other hand, capable personnel is much lacking, becoming an urgent issue that strengthens the systematic human resource development cultivating cybersecurity activities capabilities. Only a few universities and companies in Japan are conducting education using an effective training system on the market because of expensive and difficult to use that adopted and operation the training system like Cyber Range in higher education institutions and SMEs. In this paper, I introduce CyExec, an effective cybersecurity training platform that can be exercised at a lower cost and based on the open environment. Also, I introduce the cybersecurity research trends related to data analysis.

Keywords: CyExec, cybersecurity, training platform

1 Introduction

This paper introduces CyExec, a training platform for cybersecurity education based on a virtual environment [1]. Additionally, recapitulate the cybersecurity education curriculum and research trends related to data analysis.

It is the world problem that the growing workforce shortage of qualified cybersecurity professionals and practitioners. On the CSO website, both government and non-government sources project nearly 1.8 million cybersecurity-related positions going unfilled by 2022 [2]. The workforce demand is acute, immediate, and growing worldwide [3].

Cyberattacks are bringing profound social influences, causing vast cybersecurity incidents and even affecting business continuity. In Japan, $530 million of cryptocurrencies stolen occurred in January 2018, and cyberattacks targeted the organizations associated with the Pyeongchang Winter Olympics in February 2018 [4]. Kevin Morooney – former Vice Provost for Information Technology at Pennsylvania State University – told The New York Times that Penn State faced an average of 20 million attacks per day, an amount “typical for a research university [5].”

A recent study conducted by consulting firm Frost & Sullivan projects that there will be 1.8 million unfilled cybersecurity jobs by 2020 in America and that this talent shortage exists on a global scale, with nearly 70 percent of professionals globally saying there are too few cybersecurity workers on staff. With demand for cybersecurity talent far outpacing supply, companies often pay top dollar for cybersecurity expertise [6]. On cybersecurity strategy of the Government of Japan cited human resource development as a serious issue. The Japanese government also estimated the insufficiency of human resources of cybersecurity to grow at 190,000 by 2020. Additionally, the lack of technical knowledge and skill is worried even in personnel engaged in cybersecurity operations [7][8].

In an effort to develop a security workforce, some higher education institutions provide practical exercise-style education. For example, Cyber Range provides exercise environments that are similarly real-world for assuming an actual security incident [9][10]. Participants of the Cyber Range exercises learn practical defense technology against

†1 Tokai University, Kanagawa, Japan

an assumed cyberattack on the virtual environment network. Participants also learn the systematic correspondence method depending on the organization's roles by using possible realistic scenarios such as real malware infection. Therefore, high training effects can be expected [9].

However, universities have not enough exercise infrastructure to bring up a cybersecurity workforce because of the high cost of introducing the practical exercises system and the lack of personnel to maintain the practice environment. Therefore, it is strongly required in the universities that a cybersecurity exercise platform can promote joint development and typical use. These requirements are the reason why we developed a cybersecurity exercises platform, "Cybersecurity Exercises" (from now on referred to as CyExec), using a virtual computer environment of VirtualBox and Docker [11][12].

In this paper, I introduce the constitution of the cybersecurity exercises platform CyExec and the training contents we implemented on it. In Chapter 2, I introduce cybersecurity in higher education, including the topics that the international standard of cybersecurity education and information security education in Japan. Introduces an overview of the CyExec that cybersecurity exercise system in Chapter 3. Chapter 4 introduces the cybersecurity trends recently, and Chapter 5 introduces cybersecurity and data analytics.

2 Cybersecurity in Higher Education

Some strategies exist for combating the cyberattacks faced by society. Some involve strategies that higher education IT professionals must employ themselves, while others include strategies that everyone in the higher education community, including end-users, must implement. Though the cybersecurity challenges facing higher education are significant and the cost of solving them is steep, the potential financial and reputational risks that come with insufficient defense are likely even higher [6].

Cybersecurity education is an issue not only in advanced countries but also in developing nations. The ability to prevent successful cyberattacks against a nation ' s critical infrastructure depends on the availability of a skilled cyber-literate workforce, and therefore, on an educational system that can build such capabilities [13].

2.1 Standard of Cybersecurity Education

Whether developing full new programs, defining new concentrations within existing programs, or augmenting existing course content, these institutions need curricular guidance based on a comprehensive view of the cybersecurity field, the base discipline's specific demands, and the relationship between the curriculum and cybersecurity workforce frameworks. In August 2015, the Association for Computing Machinery (ACM) Education Board recognized this urgent need [14]. It took measures to assemble a Joint Task Force on Cybersecurity Education (CSEC2017) with other professional and scientific computing societies to develop comprehensive curricular guidance in cybersecurity education [15]. Based on this mission, the CSEC2017 JTF established the following goals for the curricular volume:

- To describe a vision of proficiency in cybersecurity,
- To define a structure for the cybersecurity discipline by developing a thought model that defines the boundaries of the domain and outlines critical dimensions of the curricular design,
- To support the alignment of academic programs with industry needs in cybersecurity,
- To involve a broad global audience of stakeholders through continuous community engagement during the development process,
- To develop curricular guidance that is comprehensive enough to support a wide range of program types, and
- To develop curricular advice grounded in fundamental principles that provide stability yet is structured to provide flexibility to support evolving program needs.

2.2 Information security education in Japan

The environment surrounding ICT in Japan has been changing day by day, and information security threat has increased. It can be said that about 147 million viruses have been detected so far; nearly 18 million new malware were found in the second quarter of 2013. In order to improve this environment, the education for information security is started in

the kindergarten stage in japan [16].

The primary cybersecurity education and training programs available in Higher Education, which we believe are mostly unknown outside the country. Typical training systems include Secure Eggs, enPiT-Security (also known as SecCap), and CYDER [17].

Secure Eggs is an introductory hands-on cybersecurity course offered by Nomura Research Institute (NRI) Secure Technologies. The word Eggs in the program title, an acronym for "Essentials and Global Guidance for Security," emphasizes the program's focus on necessary cybersecurity skills [18].

A consortium of five Japanese universities started the enPiT-Security training program: JAIST, Tohoku University, Nara Institute of Science and Technology, Keio University, and Institute of Information Security. The SecCap program is a curriculum for university students to develop the necessary skills needed by IT security engineers through courses and hands-on activities regarding security-related aspects of operating systems, software, networks, and malware-related countermeasures technologies. The program participants were selected based on their cybersecurity knowledge and interests among the students at the end of their studies in the five participating universities [17][19].

CYDER (CYber Defense Exercise with Recurrence) is a training program initiated in September 2013 by the Ministry of Internal Affairs and Communications in Japan [6]. The program focuses on the improvement of competence in dealing with cyberattacks of the IT and cybersecurity-related personnel of central government offices, independent administrative agencies, and large companies. The practical cybersecurity training conducted in the CYDER program takes place over two days, based on a training scenario defined by several organizing parties. Throughout the program, there is a focus on the use of hands-on training so that the trainees become able to handle potential cybersecurity incidents in real life [20].

2.3 Cybersecurity training in higher education

In order to know the state of cybersecurity education, Y. Seto, et al. researched the contents/courses of cyber attacking and defense exercises in educational institutes such as universities or specialized institutions. The survey method was conducted by interviewing six organizations and others, including public information, questionnaire surveys by concerned parties, and participating in exercises [21][22]. Table 1 shows the target organizations and a brief of their training. Based on the survey, we divided the practices into the following two forms.

(1) Exercises by the learning applications
(2) Exercises by the Cyber Range We confirmed each type's main contents.

According to a document from the Ministry of Economy, Trade and Industry of Japan, the security personnel needed in the future are as follow,

(1) advanced security technicians such as white hackers
(2) those who have acquired the security technologies necessary to create secure information systems
(3) those who manage the security of the company in cooperation with in-house security technicians.

3 CyExec - Cybersecurity Exercises Platform

The goal of CyExec is to provide an exercise system that learns the necessary technology of cyberattacks and defense intended for introduction in higher education institutions and small and medium enterprises [21]. The features of CyExec as follow.

3.1 Low cost, highly portable exercise environment

Most of the costs of building and maintaining the exercise system are equipment and the cost of licensing software. The system requires specialized skills to renew the exercise, and the price, such as labor cost, is substantial.

In order to reduce these costs, CyExec was built an exercise environment using virtualization technology to quickly implement the developed exercise program in an existing computer environment (client PC, server, etc.). Using VirtualBox, we implemented the exercise program operating environment in a virtual environment.

Table 1 Contents of the exercise and training to raise the security personnel resources

Name	Overview
Tokyo Institute of Technology	The university offered a specialized study program of Five courses from 2016 as their cybersecurity. External lecturers from cooperating companies assign exercise subjects. Training focuses on how to use tools and OWASP applications etc.
Institute of Information Security	IIS introduced a large-scale exercise system, operated in cooperation with companies. The learners can be mastering a wide range of practical security skills through exercises, from technical subjects to social science subjects, towards multi-talent security human resources.
enPiT	Covering a wide range of practical security skills, from technical entity to social science subject, toward the training of human security resources sought by industry. Learning security practical skills in various forms such as learning using learning applications, joint exercises, group exercises.
Tokyo Denki University	International Cyber Security Special Course "CySec" started in 2015. The graduate students and people aim to become senior security engineers or CISO engineers. Practice exercises on security technology, attack countermeasure, and network design.
The university of AIZU	Developed and implemented practical cyber defense exercises from 2016 for administrative agencies, local governments, independent executive agencies, and essential social infrastructure operators in the country as stipulated in the Cyber Security Basic Law. Practical exercises by constructing a virtual exercise environment at NICT "StarBED."
NICT (National Institute of Information and Communications Technology)	Developed and implemented practical cyber defence exercises from 2016 for administrative agencies, local governments, independent administrative agencies, and important social infrastructure operators in the country as stipulated in the Cyber Security Basic Law. Practical exercises by constructing a virtual exercise environment at NICT "StarBED."

3.2 Exercise environment to secure joint development and use

The development of the training program curriculum requires a high level of expertise and time, and advances in the security technology field rapidly change. For these reasons, it is challenging to complete the exercise program development at a single higher education institution. Therefore, it needs to develop practice programs that several higher education institutions and private companies need to work together.

The CyEcex realizes joint development and exercise programs in multiple organizations by introducing the ecosystem concept. The ecosystem is not a single organization, but a word that indicates that the whole related organization develops through associated organizations ' collaboration. CyExec enriches the exercise program of CyExec not only by a single organization but also by joint development and use of related organizations.

For the training system, to realize joint development and utilization by multiple higher education institutions, it is necessary to develop and utilize exercise programs among different institutions quickly. To achieve this request, we implemented container technology using Docker.

The CyExec implemented Docker on the virtual environment configured with VirtualBox and install a container on Docker. By implementing vulnerability assessments and various exercise programs on attacks and defenses and running them on a Docker container, we could easily construct a practice environment for each purpose. The CyEcex can also be used jointly by creating an image file of a container that runs the developed exercise program and publishing it in related organizations. Table 2 shows the comparison of CyExec and other exercise systems.

Figure 1 shows the architecture of the CyExec exercise system. The exercise system's architecture is to install Docker on the guest OS running on VirtualBox on the host OS and implement the process on which the attack and defense exercise program runs on the container on Docker. The portability that can operate in the existing computer environment of VirtualBox and the Docker container's high ex-

Table 2 The comparison of CyExec and other exercise systems

	Exercise system example (Developer)		
	Proposed exercise system CyExec	WebGoat (OWASP), AppGoat (IPA)	CYBERIUM (Fujitsu), TAME Range (DNP)
Cost	· Program, text development free	· Text development cost	· Expensive system introduction operation cost
Exercise form	· Individual learning / Large-scale exercise · Operation of other exercise systems is also possible	· Individual learning/Small exercise	· Large scale exercise
Exercise content	· Can learn from the fundamentals of vulnerability detection to an organizational response method · Customizable according to study purpose	· Fixed exercise content · Update depends on the developer · Practice exercises concerning commentary/usage guides	· Personnel with expertise is required for operation · Update by development/provider (paid)
Feature	· High portability/extensibility with the ecosystem as a development concept · Improvement of the appropriate curriculum by cooperative development	· It can be carried out on student PCs and can be used on their own · Easy to introduce practical environment · Supplementary text required	· Exercise imitating the real environment · Practical exercises using actual malware

tensibility enable joint development and use of our exercise program.

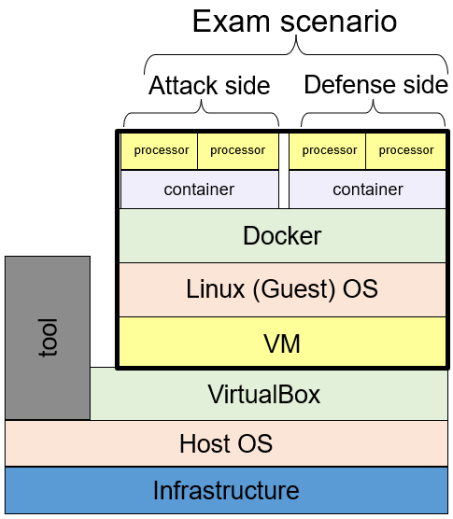

Figure 1 The architecture of the CyExec exercise system

3.3 Exercise example

Figure 2 shows the system configuration of the applied exercise. We implemented Docker on a virtual environment configured with VirtualBox and installed a container on Docker. Implementing various exercise programs related to attack and defense, such as virtual digital signage and trap server used by attackers, and running them on containers, it is possible to construct an exercise environment for each purpose easily. We built a physical environment that imitated digital signage using Raspberry Pi. By connecting via CyExec, it is possible to perform safe exercises in an isolated environment from the outside while using the actual machine. By preparing IoT devices as a rial physical environment, the learner could imagine the attack's actual situation. Therefore, we expect to enable easy-to-understand exercises with high educational effects. If a lecturer cannot prepare the physical environment, practices in virtual environments only are also possible.

4 Cybersecurity Trends

By the COVID-19, nearly 70 organizations surveyed by Skybox said over a third of their workforce would remain remote for at least the next 18 months [24].

Bitdefender researchers agree and say securing

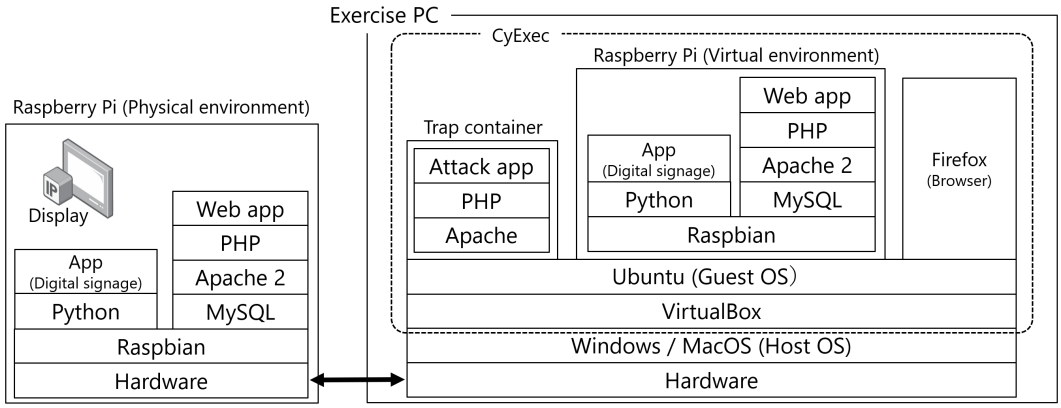

Figure 2 System configuration of the applied exercise

remote workers will become a primary focus for organizations. Cybersecurity is an essential issue since remote workers will continue to present a unique set of hackers' opportunities. Independent cybersecurity and data privacy consultancy Bridewell Consulting issued six predictions that will impact cybersecurity in 2021 [25].

Also, with the digital revolution around all businesses, small or large corporations, organizations, and even governments rely on computerized systems to manage their day-to-day activities, thus making cybersecurity a primary goal to safeguard data from various online attacks or any unauthorized access. Continuous change in technologies also implies a parallel shift in cybersecurity trends as news of data breach, ransomware, and hacks become the norm. N. Duggal and other workers who the cybersecurity field upped the issue of cybersecurity trends for 2021 [26].

5 Cybersecurity and data analytics

In general, cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. As a definition, cybersecurity analytics has its industry definition as "analyzing data to detect anomalies, unusual user behavior, and other threats". It aggregates data from across the entire enterprise ecosystem and turns that data into actionable insights — so that the IT team can promptly act on minimizing those risks. Advanced features like artificial intelligence (AI) and machine learning (ML) further help by automating the detection and remediation process." Cybersecurity analytics combines big data capabilities with threat intelligence to help detect, analyze and alleviate insider threats, as well as targeted attacks from bad external actors and persistent cyber threats [27].

The need for automated, scalable, machine-speed vulnerability detection and patching is large and growing fast as more and more systems—from household appliances to major military platforms—get connected to and become dependent upon the internet. To help overcome these challenges, DARPA launched the Cyber Grand Challenge, a competition to create automatic defensive systems capable of reasoning about flaws, formulating patches and deploying them on a network in real time [28].

There are two main ways to find software vulnerabilities using artificial intelligence technology. First, it is a method to extract patterns from vulnerability data and then find parts with code flows similar to this pattern in the program under analysis. The second method is to construct a framework that behaves like a single organism that explores, tracks, and validates the program's central part. The former is a data-driven technique, and the latter is an algorithm-driven technique. It is fast and effective in the former case, but only similarity patterns can be found, and its coverage is limited. In the latter case, it is a method of delegating all processes from vulnerability discovery to verification in the machine, which requires more consideration than data-driven techniques and is challenging to

implement. Some teams opened to the public their paper when they participated in the CGC [29][30].

S. Chr presented MAYHEM, a new system for automatically finding exploitable bugs in binary (i.e., executable) programs. Every bug reported by MAYHEM is accompanied by a working shell-spawning exploit. The working exploits ensure soundness and that each bug report is security-critical and actionable. MAYHEM works on raw binary code without debugging information [29].

Y. Shoshitaishvili discussed their cyber reasoning system, Mechanical Phish, which they have open-sourced; the lessons they learned in participating in this ground-breaking competition; and their system's performance as a tool in assisting humans during the DEF CON Capture-the-Flag competition, which followed the DARPA Cyber Grand Challenge [30].

6 Conclusion

Cyber-attacks such as targeted attacks are increasing, and it is becoming a problem of digital society. Human resource development, which has attack and defense technology, is an important theme. Therefore, the environment improvement to security human resource development has not progressed due to the exercise system's building cost and the shortage of personnel who maintain and manage the exercise environment. Therefore, this paper introduced CyExec that developed for the cybersecurity exercise system, an ecosystem consisting of virtual computer environments using VirtualBox and Docker. Additionally, through this paper, I introduced cybersecurity trends and cybersecurity and data analytics recently.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number JP 19K03006 and supported by Transcosmos fundation.

REFERENCES

[1] S. Shin, Y. Seto, CyExec – Training Platform for Cybersecurity Education Based on a Virtual Environment, IJLTLE. Vol. 3, No. 1, pp.1-20 (2020).

[2] CSO Online: https://www.csoonline.com/article/2953258/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[3] The 2015 (ISC)2 Global Information Security Workforce Study: https://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf

[4] Information and Security White Paper 2019 (in Japanese), white paper, Information-technology Promotion Agency, Japan (IPA) (2019).

[5] Penn State ' s College of Engineering Hit by Cyberattack: https://bits.blogs.nytimes.com/2015/05/15/penn-states-college-of-engineering-hit-by-cyberattack/?_r=0

[6] S. Campbell, Cybersecurity in Higher Education: Problems and Solutions: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

[7] National Center of Incident and Strategy for Cybersecurity, Japan, Cybersecurity Strategy (2018): https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf

[8] Ministry of Economy, Trade and Industry, Japan, Survey on latest trends and future estimates of IT personnel (in Japanese) (2016): https://www.meti.go.jp/committee/kenkyukai/shoujo/daiyoji_sangyo_skill/pdf/001_s02_00.pdf

[9] M. Edure, Practical Exercises for Cyber Attacks, Information processing, Vol. 55, No. 7, pp. 666-672 (2014).

[10] N. Ryotaro, H. Kumi and S. Yoichi, Development of Container-based virtual exercise system CyExec related to cyber-attack and defense, The 80th National Convention of IPSJ (2018).

[11] S. Toyoda, R. Nakata, K. Hasegawa, S. Shin, Y. Seto, Proposal of Cyber attack and defense Exercise system CyExec composed of ecosystem, Computer Security Symposium, Nagano (2018).

[12] Y. Kasai, Y. Seto, et al., Development of practice contents for cyber security exercise system CyExec, Symposium on Cryptography and Information Security, (2019)

[13] Frankie E. Catota, M. Granger Morgan1 and Douglas C. Sicker, Cybersecurity education in a developing nation: the Ecuadorian environment, J. of Cybersecurity, Vol. 5, Issue. 1 (2019).

[14] ACM Computing Disciplines Overview: https://www.acm.org/education/curricula-recommendations

[15] Cybersecurity Curricular Guidelines — CSEC 2017: https://cybered.hosting.acm.org/wp/
[16] Information security education for students in Japan: https://www.nier.go.jp/English/educationjapan/pdf/201403ISE.pdf
[17] R. Beuran, K. Chinen, Y. Tan, Y. Shinoda, Towards Effective Cybersecurity Education and Training, Research Report - School of Information Science (2016).
[18] Nomura Research Institute (NRI) Secure Technologies: http://www.nrisecure.com/.
[19] enPiT University Consortium. enPiT-Security (SecCap) Training Program: https://www.seccap.jp/
[20] Ministry of Internal Affairs and Communications, Japan. Cyber Defense Exercise with Recurrence (CYDER) Training Program (press release): http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130925 02.html
[21] Ministry of Education, Culture, Sports, Science and Technology, Japan, Annual report 2016, enPiT (2017): http://www.enpit.jp/img_new/publications/enPiT_annualreport_uni_2017.pdf
[22] Cyber Defense Exercise with Recurrence: https://cyder.nict.go.jp/.
[23] T. Shinichi, et al., Proposal of Cyberattack and defense Exercise system CyExec composed of the ecosystem, CSS2018 (2018).
[24] Threatpost, 2021 Cybersecurity Trends: Bigger Budgets, Endpoint Emphasis and Cloud: https://threatpost.com/2021-cybersecurity-trends/162629/
[25] M Jones, Six cybersecurity trends heading our way in 2021: https://techhq.com/2020/12/six-cybersecurity-trends-heading-our-way-in-2021/
[26] N. Duggal, Top 10 Cyber Security Trends For 2021: https://www.simplilearn.com/top-cybersecurity-trends-article
[27] L, Sarker, et al., Cybersecurity data science: an overview from machine learning perspective, J. of Big Data, Vol. 7, No. 41 (2020).
[28] Cyber Grand Challenge (CGC): https://www.darpa.mil/program/cyber-grand-challenge
[29] S. Cha, T. Avgerinos, A. Rebert and D. Brumley, Unleashing MAYHEM on Binary Code, 2012 IEEE Symposium on Security and Privacy (2012).
[30] Y. Shoshitaishvili, Mechanical Phish: Resilient Autonomous Hacking, IEEE Security & Privacy, Vol. 16, Issue. 2 (2018).