様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ５ 月 １９ 日現在

機関番号：１３３０２
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００４７８

研究課題名（和文）CyTrONE: Cyber Range Framework for Effective Cybersecurity Training

研究課題名（英文）CyTrONE: Cyber Range Framework for Effective Cybersecurity Training

研究代表者
ＢＥＵＲＡＮ　Ｒａｚｖａｎ（BEURAN, Razvan）

北陸先端科学技術大学院大学・先端科学技術研究科・特任准教授

研究者番号：４０７７１７８８

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：CyTrONE というサイバーセキュリティ演習フレームワークを実装し、実践的な演習を簡単に実施できるようにした。このフレームワークは演習機能全体を制御し、それから追加モジュールで演習管理システムのサイバーセキュリティ演習対応、演習環境（サイバーレンジ）の作成、演習シナリオの進行を管理する。
また、学生を対象とした演習質問（5つのカテゴリで合計38問）と専門家を対象とした演習シナリオ（情報セキュリティテストと評価技術を参考した2つのレベルで合計20問）の2セットのCyTrONE 用の演習コンテンツを作成した。CyTrONE のソースコードと演習コンテンツはウェブで公開された。

研究成果の学術的意義や社会的意義
CyTrONE フレームワークは、効果的なサイバーセキュリティ演習の重要な2つの問題を解決した：（1）演習コンテンツを簡単に変更および追加する機能　（2）演習環境を自動的に作成および管理する機能。この2つの機能は、演習コンテンツ用の専用テキスト形式の利用と、トレーニング環境用のサイバーレンジ生成システムを導入することで実現した。
演習フレームワークのソースコードと演習コンテンツが両方とも公開されたため、実質的に誰でも、いつでも、どこでもセキュリティ演習を実施でき、社会全体に貢献することができた。

研究成果の概要（英文）：We implemented a cybersecurity training framework named CyTrONE that makes it possible to easily conduct realistic hands-on training activities. The framework controls the overall training functionality, and uses additional modules for cybersecurity training support in the Moodle Learning Management System, to create training environments (cyber ranges) on demand, as well as manage training scenario progression.
We also created two sets of training content for CyTrONE: (i) Training questions aimed at students and other young learners with a total of 38 questions in five content categories; (ii) Training scenario inspired by information security testing and assessment techniques that is aimed at young professionals, with a total of 20 questions split into two levels.
The CyTrONE source code was released on GitHub (https://github.com/crond-jaist) and the training content was made public on our web site (https://www.jaist.ac.jp/misc/crond/achievements-en.html), our contribution to society.

研究分野：networking

キーワード：cybersecurity training　integrated framework

１．研究開始当初の背景

Frequently occurring cybersecurity incidents, such as the security breach that took place at the Japan Pension Service in June 2015, lead to the establishment of several cybersecurity education and training programs in Japan that use training environments named cyber ranges for practical hands-on activities (see Figure 1).

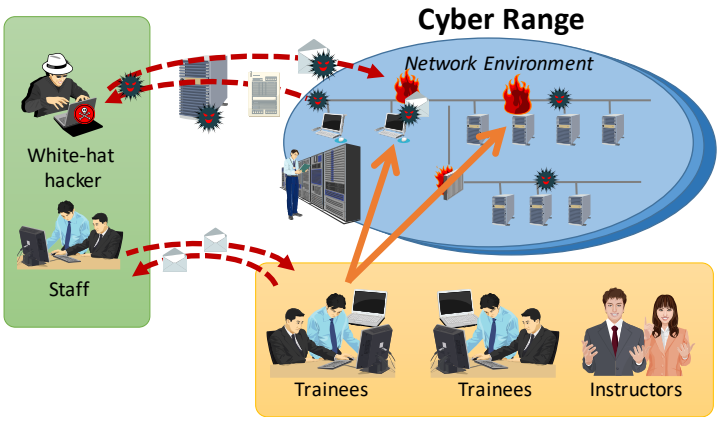

Figure 1: Hands-on cybersecurity training using cyber range.

For example, CYDER is a program coordinated by the National Institute of Information and Communications Technology that provides training for IT personnel of government organizations and companies. Hardening Project is a security contest organized by the Web Application Security Forum in which teams of security experts and IT professionals compete with each other in terms of the security improvements they can implement for a realistic e-commerce company network. enPiT-Security (SecCap) is an education program targeting students that is supported by the Ministry of Education, Culture, Sports, Science and Technology, and organized by a consortium of five institutions, including our university, Japan Advanced Institute of Science and Technology (JAIST).

The Cyber Range Organization and Design (CROND) chair was created at JAIST in April 2015 with the purpose of supporting cybersecurity education and training through designing and implementing architectures for cyber ranges and create the associated curricula and education materials. We did a deep analysis of current cybersecurity education and training programs and established a set of requirements for creating an effective cybersecurity training framework. According to our analysis, the key features for an effective training system are:

(1) Ability to easily modify and add training content
(2) Ability to automatically create and manage the training environment

In this project we proceeded to develop a cybersecurity training system that meets the above requirements, as it will be described next.

２．研究の目的

The main objective of this project is to implement the cybersecurity training framework named CyTrONE (Cybersecurity Training and Operation Network Environment). An overview of the framework concept is shown in Figure 2. Specifically, based on training organizer input, CyTrONE will generate the training content for a particular training session, and upload it to an e-Learning system (also known as Learning Management System, LMS). Simultaneously, CyTrONE will create the cyber range training environment corresponding to that training content. This automatic generation is made possible through the use of an easily updatable training database, which contains all the necessary information, such as the training description, the cyber range representation, and all the relevant resources, so as to generate both the content shown to trainees, and the associated training environment. By using CyTrONE, it is possible for practically anyone to conduct security training anytime and anywhere, given that a server infrastructure is available for the cyber range creation.

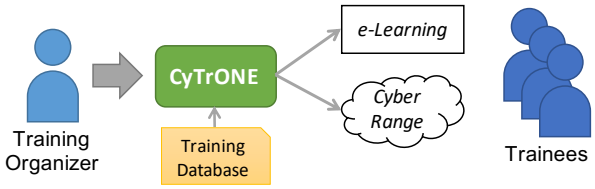

Figure 2: Use of the CyTrONE framework for cybersecurity personnel training.

The concrete goals of this research project are as follows:

(1) Develop a fully configurable cybersecurity training framework, so that based on organizer input and a training database, CyTrONE will automatically produce the training content and training environment necessary for that training.
(2) Create the associated training database that includes training material targeting various audiences, such as technical college students and company employees, by leveraging information regarding well-known security issues and industry best practices.
(3) Collaborate with current cybersecurity education training programs organizers in order to integrate CyTrONE into their workflow, and thus contribute to the society at large.
(4) Make public the security training framework and the associated database by releasing them as an open source project, so that they can be freely used by other organizations.

３．研究の方法

We divided the CyTrONE project into four work packages, for a total duration of three years. Work package WP1 refers to the design and implementation of the training framework itself and is spread over the entire project period. WP2 relates to the development of the training database and is to be carried out mainly over the first two years. WP3 contains activities related to user trials, as well as the integration with existing training programs, such as CYDER and Hardening, mainly during the third year of the project. Finally, WP4 focuses on project promotion and initiation of collaborations based on the developed framework.

WP1: Training Framework Development

The CyTrONE framework has been conceived using a modular architecture paradigm. This makes it possible to design and develop its components in an independent and flexible manner. Communication between modules uses the standard HTTP protocol and JSON format, to simplify the debugging and testing processes, thus leading to a good feasibility of the architecture.

In the first part, we focused on the integration with the CyRIS cyber range instantiation system and implemented basic prototypes of the User Interface and the additional modules Training Description Generation and Content Description Processing. In parallel we proceeded with the integration with the Moodle LMS by actually implementing the necessary content upload support in the Training Description Generation module. Finally, we documented the framework functionality and supported the user trials that are part of WP3.

WP2: Training Database Development

This work package refers to the design of the training database and the implementation of the training content for CyTrONE. For the database representation we used the YAML text-based format which provides a representation that is easy to understand by humans and also machine readable. One database file in this format represents the information about training that will be displayed to trainees, another one will describe the associated cyber range that needs to be created to conduct that training, and a top file will indicate to CyTrONE what content files are to be used for each training.

For the actual training content, we focused on two paradigms. Young learners, such as students, need to be motivated to study about security and for them we have selected the challenge format of CTF (Capture The Flag) contests. On the other hand, for IT professionals we decided to follow industry best practices, such as those related to

security assessment. In both cases, then necessary resources needed to prepare the training environment (scripts, binary files, etc.) had to be implemented or created and included in the database.

WP3: User Trials and Integration

As part of WP3, we conducted user trials to validate the system in various training scenarios, from the point of view of training content and training environment. This included the user interfaces both for organizers, for which a web-based interface was created, and for trainees who access content via Moodle. We also investigated the way to integrate the framework with existing training projects, such as CYDER and Hardening Project, through our already established connections with those project organizers.

WP4: Project Promotion

For WP4, one important direction is preparing the open source release of the CyTrONE implementation and of the training content. In addition, we promoted our work to other potential collaborators, through participations and demonstrations at conferences and workshops, both nationally and abroad. Venues in Japan included the Interop Tokyo fair, and the CODE BLUE conference, and internationally USENIX conferences on security and security education topics.

４．研究成果

In what follows we shall present the research achievements of the project categorized based on the corresponding work packages.

WP1 Achievements

The training framework development was completed, and the final architecture is shown in Figure 3, which has the following components. CyTrONE is the overall management module, CyLMS is a module that adds cybersecurity training support to the Moodle LMS, and CyRIS is the cyber range instantiation module.

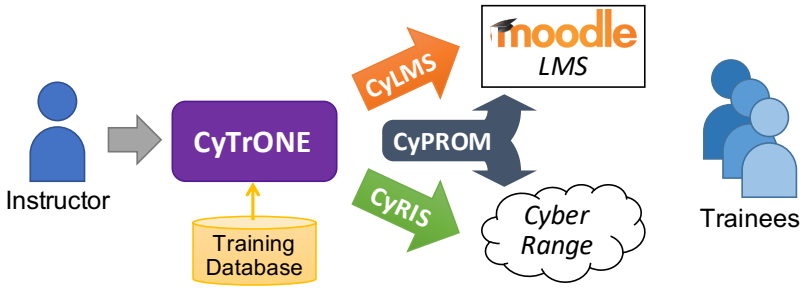

Figure 3: Overall architecture of the CyTrONE framework.

A fourth component exists that was not included in the initial plan, named CyPROM. The role of this module is to dynamically manage scenario progression, so that more realistic attack-defense scenarios can be created, for instance with attacks conducted automatically by the system while trainees defend their network.

WP2 Achievements

As mentioned already, the training database representation format was designed based on the YAML format in a modular form. The database also includes binary files, scripts, and other resources necessary to conduct each training.

So far, we have created two sets of training content for CyTrONE:

(1) Set of CTF-style training questions aimed at students and other young learners that currently contains a total of 38 questions in five content categories (binary analysis, cryptography, network, OS, and Web)
(2) Set of questions inspired by the NIST "Technical Guide to Information Security Testing and Assessment" that is aimed at young professionals; a total of 20 questions in two categories (levels) are included

WP3 Achievements

We have conducted several user trials for CyTrONE, both with students from our university and also with students and professors from Technical Colleges in Japan.

While CyTrONE was in the end not integrated with existing training programs, that finally decided to continue using their own tools, we did have fruitful discussions with commercial companies that expressed interest in using CyTrONE internally and possibly even implement their own systems based on CyTrONE.

Last but not least, starting from FY2018, CyTrONE has been used every year to conduct training sessions for the intensive course I465S "Literacy in Information Security Management" provided by our university.

WP4 Achievements

The project was promoted via demonstrations and exhibitions at various events in Japan, such as Interop Tokyo and CODE BLUE. We also published several papers and made presentations, as follows: **3** journal papers (Elsevier Computers & Security, Springer Education and Information Technologies), **4** refereed international conference papers (IEEE Workshop on Cyber Range Technologies and Applications CACOE 2019, IEEE International Conference on Engineering Education ICEED 2017, etc.), **1** invited lecture (Cyber Resilience Conference 2018) and **5** workshop presentations.

In addition, both the CyTrONE source code and the created training content were released publicly, as follows:

(1) The source code was released on the GitHub page of CROND:
https://github.com/crond-jaist
(2) The training content was released on the CROND web site:
https://www.jaist.ac.jp/misc/crond/achievements-en.html

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　1件／うちオープンアクセス　0件）

１．著者名 Z. Tan, R. Beuran, S. Hasegawa, W. Jiang, M. Zhao, Y. Tan	４．巻 －
２．論文標題 Adaptive security awareness training using linked open data datasets	５．発行年 2020年
３．雑誌名 Springer Education and Information Technologies	６．最初と最後の頁 －
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10639-020-10155-x	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 R. Beuran, D. Tang, Z. Tan, S. Hasegawa, Y. Tan, Y. Shinoda	４．巻 24-6
２．論文標題 Supporting Cybersecurity Education and Training via LMS Integration: CyLMS	５．発行年 2019年
３．雑誌名 Springer Education and Information Technologies	６．最初と最後の頁 3619, 3643
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10639-019-09942-y	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Beuran Razvan、Tang Dat、Pham Cuong、Chinen Ken-ichi、Tan Yasuo、Shinoda Yoichi	４．巻 78
２．論文標題 Integrated framework for hands-on cybersecurity training: CyTrONE	５．発行年 2018年
３．雑誌名 Elsevier Computers & Security	６．最初と最後の頁 43～59
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.cose.2018.06.001	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計10件（うち招待講演　1件／うち国際学会　8件）

１．発表者名 R. Beuran
２．発表標題 Realistic Cybersecurity Training via Scenario Progression Management
３．学会等名 IEEE European Symposium on Security and Privacy Workshops (EuroSPW 2019), Workshop on Cyber Range Applications and Technologies (CACOE'19)（国際学会）
４．発表年 2019年

１．発表者名
R. Beuran

２．発表標題
Towards an open exchange format for cybersecurity training content

３．学会等名
USENIX Security '19（国際学会）

４．発表年
2019年

１．発表者名
R. Beuran

２．発表標題
Creating a standard for cybersecurity training content exchange

３．学会等名
USENIX HotSec '19 Summit（国際学会）

４．発表年
2019年

１．発表者名
R. Beuran

２．発表標題
Cybersecurity Education and Training: Progress and Perspectives

３．学会等名
5th France-Japan Cybersecurity Workshop（国際学会）

４．発表年
2019年

１．発表者名
Chinen Ken-ichi

２．発表標題
クイズ型セキュリティ演習に お ける正解の多様化 --- CyTrONEにおける実例 ---

３．学会等名
電子情報通信学会

４．発表年
2019年

１．発表者名
Inoue Takuya

２．発表標題
サイバー演習の防御演習時におけるシナリオ進行の自動化システムの提案

３．学会等名
Internet Conference (IC 2018)（国際学会）

４．発表年
2018年

１．発表者名
Beuran Razvan

２．発表標題
Improving Cybersecurity Resilience via Education and Training

３．学会等名
Cyber Resilience Conference (CRC 2018)（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Kim Eunyoung

２．発表標題
On Designing a Cybersecurity Educational Program for Higher Education

３．学会等名
International Conference on Education Technology and Computers (ICETC 2018)（国際学会）

４．発表年
2018年

１．発表者名
Hasegawa Shinobu

２．発表標題
情報セキュリティアウェアネス向上のための意思決定トレーニング環境の提案

３．学会等名
教育システム情報学会

４．発表年
2018年

１．発表者名
Razvan Beuran

２．発表標題
Interactive Cybersecurity Defense Training Inspired by Web-based Learning Theory

３．学会等名
IEEE 9th International Conference on Engineering Education (ICEED 2017)（国際学会）

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
The source code of the CyTrONE framework and associated modules was released as open source and can be retrieved from GitHub:
https://github.com/crond-jaist
The training content we created for CyTrONE was made public and can be downloaded from our web site:
https://www.jaist.ac.jp/misc/crond/achievements-en.html

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	知念　賢一 (Chinen Ken-ichi) (20304157)	北陸先端科学技術大学院大学・先端科学技術研究科・特任准教授 (13302)	