Title	Automatic Cyberattack Emulation for Interactive Security Defense Training
Author(s)	Tang, Thanh Dat
Citation	
Issue Date	2017-09
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/14797
Rights	
Description	Supervisor:BEURAN, Razvan Florin, 情報科学研究科, 修士

Automatic Cyberattack Emulation for Interactive Security Defense Training

Tang Thanh Dat (1510210)

School of Information Science,
Japan Advanced Institute of Science and Technology

August 04, 2017

Keywords: Cybersecurity, Cybersecurity training and education, Cyber range, Interaction, Web-based learning.

The demand for improving the cybersecurity skills of system engineers is increasing as the number of cyberattacks is raising. There are many training programs and systems for creating training environments. However, in most cases, they only focus on setting up the machines, without a pedagogical point of view.

This thesis has three main contributions. Firstly, it introduces a system to automate learning content preparation and performing cyberattacks through the use of a training database of vulnerabilities. Secondly, it proposes the development of a training user interface inspired by pedagogy theories of distance learning. Last but not least, the implementation is validated in many aspects, from feature coverage to system performance. With the support of the theory, we have demonstrated that the user interface is easy to use and effective. The combination of a tool to setup cyber range from a previous work, an automatic cyberattack mechanism and an interactive web-based training interface creates a complete framework, so trainees can learn cybersecurity by themselves, independently from setting up training sessions manually, which always requires organizers and experts.

In this thesis, first of all, we define requirements for a modern e-learning system for cybersecurity training. We then describe how a defense training system is designed and implemented in this research. The output system is evaluated from two aspects: features and performance. To evaluate the system features, we compare it with other systems and the theory of authentic learning activity. System performance is also validated by user experience and running time - duration needed to create the training environment. The results demonstrate that the new system performs better than the original one in some aspects. Moreover, the pedagogic theories on interaction and authentic activity are proved to help improve the quality of cybersecurity training, so applying educational theories is a promising method to develop technical training programs.