Interactive Cyber Attack Emulation for Facilitating Security Training

Dat Tang, Cuong Pham, Ken-ichi Chinen, Razvan Beuran

Japan Advanced Institute of Science and Technology

(dat.ttt@jaist.ac.jp)

Motivation

- Cybersecurity training receives attention from organizations as it improves the readiness for protecting data, user privacy and maintaining organization operation
  - Preparing a cybersecurity training environment is time-consuming and tedious
  - To demonstrate an attack, white-hat hackers and experts are required to do it by themselves

Goals

- Focus on making an automatic and interactive cyber-attack emulation
  - Automatic: Create a cybersecurity incident for training purpose
  - Interactive: Based on users’ behavior, create an appropriate instantiation; get system state to inform users about their progress

Approach

CyTrONE Framework

- Cybersecurity Training and Operation Network Environment (CyTrONE) is a framework we developed for creating training environments automatically

Automatic Attack Preparation

- Method: Automate a security incident or vulnerability exploit following a timeline
  - Apply in incident response trainings and cyber attack demonstrations

Interactive

- Develop plugins on the Cyber Range Preparation block and a Learning Management System (LMS)
- Use Moodle – an Open-source platform
- Allow trainees to control and interact with real-time activities for cybersecurity training