

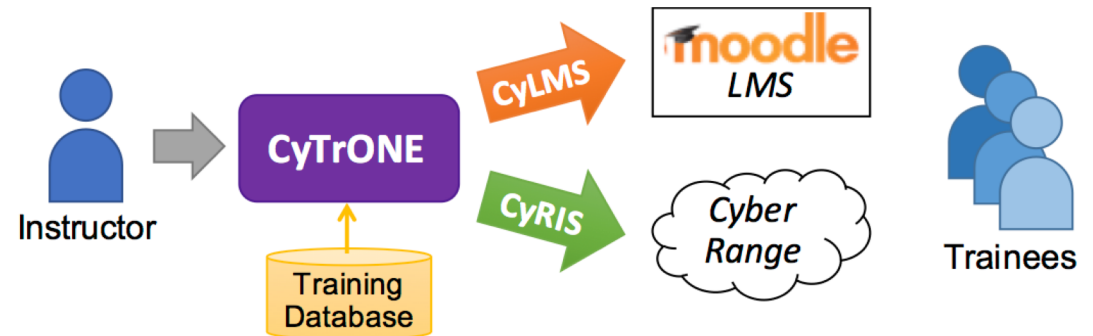
CyTrONE 用演習コンテンツ作ってみた

WIDE 研究会ライトニングトーク

awar@JAIST

2019/05/11

CyTrONE とは？



- サイバー演習環境を自動構築するフレームワーク
 - JAIST CROND が開発・公開 (GitHub)
 - <https://github.com/crond-jaist>
 - 演習環境 = 演習コンテンツ + 仮想マシン群 (サイバーレンジ)
 - CyTrONE は上記 2 要素をファイルとして読み込む
 - CyTrONE は CyLMS と CyRIS を呼び出して演習環境を構築
 - CyLMS: Moodle への問題セットをアップロード
 - CyRIS: 問題セットに対応する仮想マシン群を構成
 - 受講者は Moodle を見ながら必要に応じてサイバーレンジにアクセスして演習に取り組む

演習コンテンツ作ってみた

- JAIST 授業用 (2019 年 3 月 (済), 2020 年 3 月 (予定))
 - ウェブカメラ (に見立てたホスト) への侵入模擬
 - ポートスキャン, リモートログインクラック等
 - アライドテレシスアカデミー株式会社との共同研究成果を元に作成
 - 題材は IPA 情報処理安全確保支援士試験 (平成 29 年秋期)
 - 共同研究契約と授業で利用のため一般公開予定なし
- CyTrONE 用サンプルコンテンツ (GitHub にて近日公開予定)
 - CTF (Capture the Flag) スタイルの問題
 - pcap ファイル解析, ウェブ系 (XSS, ディレクトリトラバーサル) 等
 - Interop Tokyo 2018 出展内容を元に作成
 - 昨日の研究会第 1 日目のサイバーレンジワークショップで利用

時間配分を誤ったため、このページは
LTではお見せできませんでした。

苦勞とか（まとめにかえて）

- 問題セットとサイバーレンジの整合性の維持
 - 解答を誤って設定すると、受講者は正解にたどり着けない
 - 締切直前まで内容をいじっているとやらかしがち
- 難易度調整，ヒントの与え方
 - 受講者レベルが想定外に低かったり (JAIST 授業) 高かったり (WIDE WS) すると，正直どうしていいかわからなくなる
 - まだまだ試行錯誤中
- 作成者側が様々な分野を広く深く理解している必要がある
 - 大変です…
 - いろんな分野の理解が深まっていくのは楽しい
 - 今後も細く長く続けていきたい