I-Wars – A Networked Cyber Operations Competition

John Franco (franco@ucmail.uc.edu) and
Hrishikesh Vinayak Bhide (bhidehk@mail.uc.edu) with much assistance from
Jonathon Meeks

Dept. Electrical Engineering and Computer Science
University of Cincinnati
Cincinnati, OH 45221-0030

February, 2020 – version 3.0

Purpose

I-Wars is a team competition that is intended to enhance the Cyber Operations (CO) community by reducing time and cost of apprenticeship training and by improving the motivation and quality of the CO workforce.

Critical to improving quality and reducing time and cost of apprenticeship training is ensuring a greater depth of knowledge and utility of CO skills in personnel entering the workforce. CO specialists 1) protect data, networks, and net-centric capabilities; and 2) neutralize the digital capabilities of adversaries including their ability to communicate, initiate attacks, and control infrastructure. Critical CO skills therefore include low-level programming, operating system weaknesses and vulnerabilities, network protocols, encryption, authentication, integrity protection, reverse engineering, and forensic analysis of traffic and data. The I-Wars competition can exercise some or all of those skills.

Motivation can be encouraged by continuity of CO education over the entire academic experience and its relevance to reality. The environment of the proposed competition mimics real life, thereby enhancing the relevance of the competition and increasing interest. Moreover, it is a simple matter to choose a particular level of experience for the competition. Thus, the competition may be executed at the 6 th grade level, where students have little experience and understanding of networks, operating systems, attack or defense, it may be executed at the high school level where crypto becomes a major component, it may be executed at the university level where students have some understanding of the above principles and implementations, and it can be used at the advanced level where participants can be expected to know how to reverse engineer binary code, low-level network protocols, assembly code and so on. If used frequently at many levels the expected impact of the proposed competition on the CO community will be greatly improved quality of CO specialists and a higher number of CO specialists who have enhanced motivation to succeed. Evaluation of the competition at several levels will provide an estimate of the numbers associated with this impact.

The competition is a game with rules defined in the competition manual (see folder `doc`). The game is played over a VPN or Cyber Range. VPN software is supplied and documented. Players get scored on assets they possess and the quantity and value of those assets change with the Economy and results of Wars. However, for the more advanced competitions, Players can used a variety of tools and ideas to steal wealth from other Players or deceive other Players into giving up wealth. Thus, Players not only need to play by the rules to gain wealth but they should also attack to gain wealth and know how to defend what they have from attack. In a well-played game the winners will be the ones who both attack and defend most successfully.

Software that supports every aspect of the competition is provided and is called the *Monitor*. Humans competing in a contest are called *Players*. The software they use to interface with the contest Monitor is called a *Client*. Clients may be developed by Players but a ready-made Client is supplied for less advanced competitions.

I-Wars Overview

Teams use ready-made or custom software systems called *Clients* to accumulate wealth in a variety of ways including trades, waging wars, exploiting Monitor vulnerabilities, and stealing wealth from other teams' Clients. Wealth is measured in a 'currency' called *Rupyulars*. Besides hard currency, teams may possess raw materials and/or finished products, all of which are referred to in the manual as assets. Each of the latter possessions has a value in Rupyulars which is determined by the Monitor. Values change during the competition roughly according to supply and demand. Each team is initially assigned a number of accounts: teams can name their accounts but the number is set by the Contest Administrator. The Contest Administrator also sets the amount of time the competition will be played and the start time and day. A scoreboard, updated by the Monitor and publicly accessible, shows teams ranked by the sum of wealth of their assigned accounts. When the competition ends, the winner is the team ranked the highest.

Wealth is distributed by the Monitor every hour to assigned accounts as raw resources (each having a unit value in Rupyulars) or Rupyulars themselves. There are six kinds of resources and three kinds of finished products that may be manufactured from the resources. The resources are: oil, steel, plastic, copper, glass, and rubber. The products are: weapons, computers, and vehicles. An account's wealth can be increased (or perhaps decreased) by

1. Constructing finished products from the raw resources,
2. Making deals with other systems to exchange resources, products, or Rupyulars,
3. Stealing items of wealth from other systems,
4. Making war with another system,
5. Trading on the Monitor's open market.

Each item, resource or product, has a per unit value in Rupyulars. That value changes by the minute and is governed by legitimate transactions between systems, and the overall amount of the given resource in the market. Resources may be exchanged for other resources or Rupyulars by agreement between two parties. In this case there is no obligation to fix any particular exchange value for any item, or even to accept an offer. Resources are used in certain fixed proportions to create units of finished products. Finished products will typically have more value than the raw materials used to construct them because they can be used to acquire additional wealth. Weapons can be used to wage war on other systems. Computers can be used to unlock secrets about particular systems such as the resources an adversary possesses. Vehicles are needed to deploy weapons. Raw resources cannot be recovered from a finished product.

Previous Versions: none distributed

Requirements:

Hardware:

64 bit processor, at least 2 cores, at least 1 GHz speed, Intel or AMD
512 GB SSD (optimal) but disk drive is OK, may also be run from flash drive
At least 4 GB ram, DDR3 or DDR4 preferred
Hi-res monitor, sound system preferred

Operating System:

macOS, Windows 10, any Linux version Ubuntu 18.04 LTS preferred, OpenBSD
note: macOS and OpenBSD have not been tested yet

Software:

OpenVPN: `https://openvpn.net/community-downloads/`
OpenSSL: `https://www.openssl.org/source/`
Java: `https://www.oracle.com/java/technologies/`
mutt: `http://www.mutt.org/`
tar: included with all OSes above
EasyRSA: `https://github.com/OpenVPN/easy-rsa`
lzo: `http://www.oberhumer.com/opensource/lzo/`
note: source versions of above are provided in `contrib.tar`