EDU: A Capture-the-Flag Service for Computer Security Courses

NSF Award #: 1623400 PI: Wu-chang Feng (wuchang@pdx.edu)

Goals

- Create effective games for use in security courses
- Make games freely available and easy to use for instructors

Portland State
Computer Science

Approach

- Adapt Capture-the-Flag (CTF) security challenge paradigm
- Scaffold levels and align with established curricula
- Apply metamorphism to levels to deter cheating
- Deliver across multiple formats to ease adoption.

Impact:

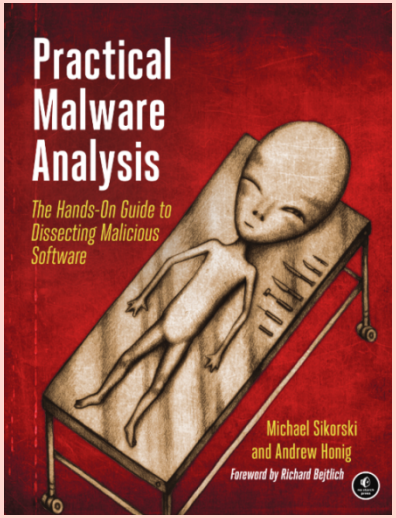
- Effective and popular with students (4.7/5.0)
- Hosted offering used at Lewis & Clark College and Evergreen State College
- Spin-off CTF in development based on "Computer Systems Programming", Bryant & O'Hallaron, 3rd ed.

Initial CTF game: Malware Reverse-Engineering

Aligned with "Practical Malware Analysis", Sikorski & Honig

27 levels covering chapters on:

- Static Analysis
- Dynamic Analysis
- Disassemblers
- Debuggers
- Malware Behavior
- Data Encoding
- Anti-Disassembly
- Anti-Debugging
- Packers and Unpacking



Availability

Hosted service (https://malware.oregonctf.org),
Source-code, virtual machine and container distributions.