SEED Labs 2.0:
A Hands-on Approach in Cybersecurity Education

Wenliang (Kevin) Du, Ph.D.

Laura J. and L. Douglas Meredith Professor
Dept. of Electrical Eng. & Computer Science
Syracuse University
Email: wedu@syr.edu

Outline

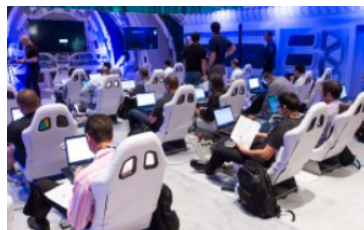Hands-on Learning

SEED Labs

(20 years of work)

Related SEED Projects

2

Hands-on Learning

Real-world
problem solving

Cyber Range

KALI
BY OFFENSIVE SECURITY

Labs in classroom

Kali Linux and SEED Labs

Objectives of SEED Project

Cost

- Free

- No need for dedicated hardware

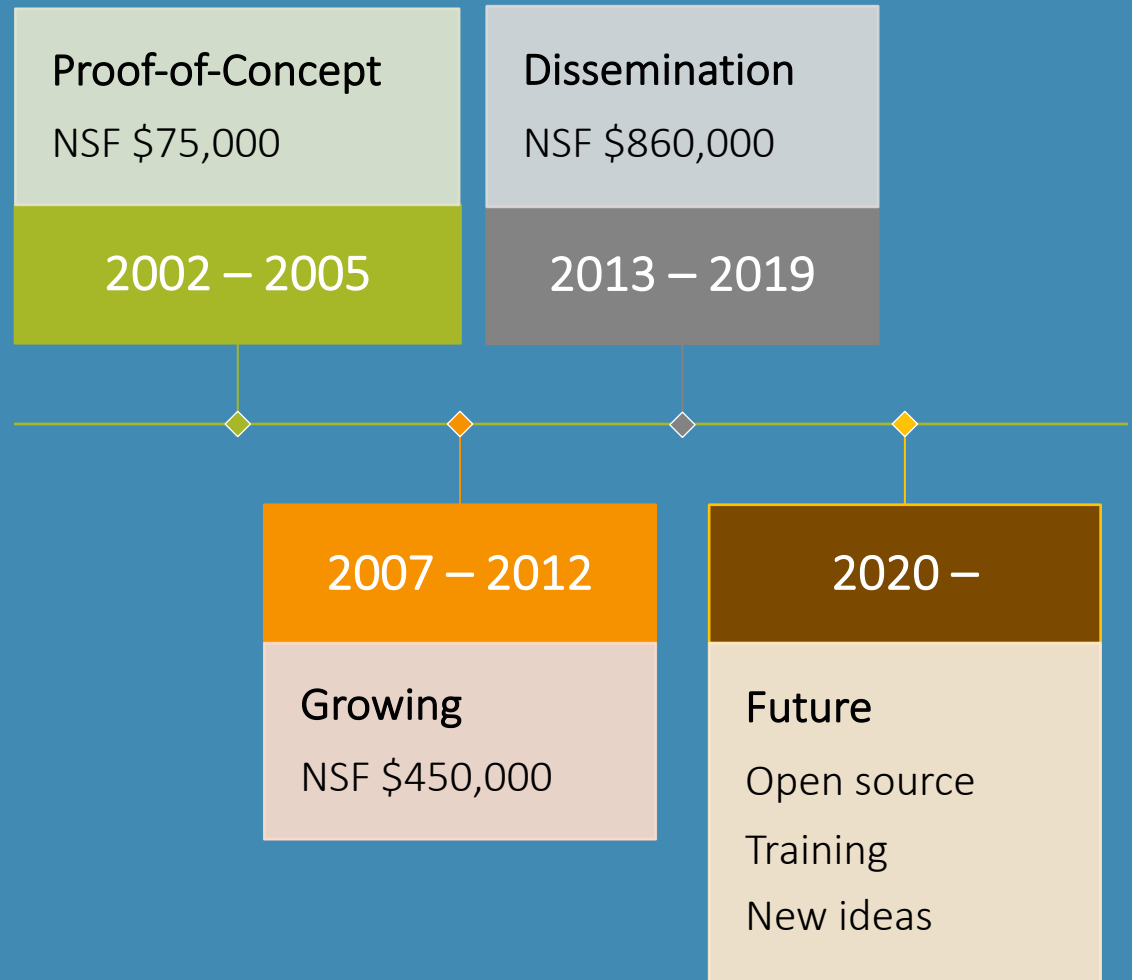## Quality

- Engaging activities

- Focus on education

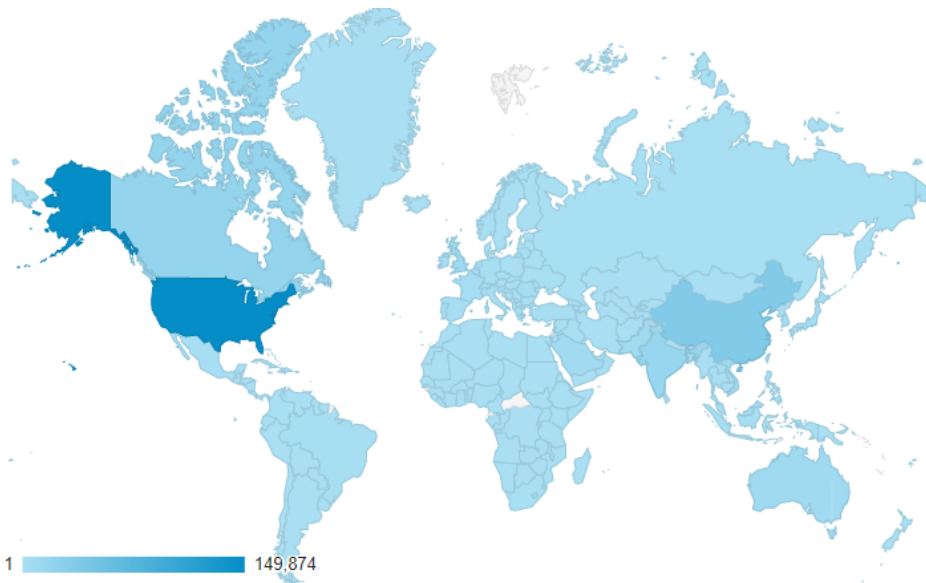## Coverage

- Fundamental principles

- Classic & current attacks

Efficiency

- Focused

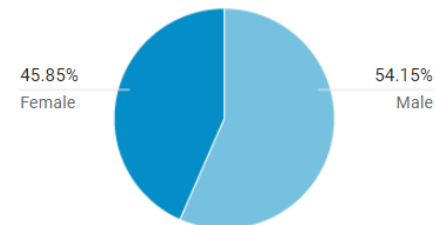- Minimize non-essential activities

5

Project Phases

Proof-of-Concept

NSF $75,000

2002 – 2005

Dissemination

NSF $860,000

2013 – 2019

2007 – 2012

Growing

NSF $450,000

2020 –

Future

Open source

Training

New ideas

6

Adoption (2018.4 – 2021.3)

Gender   100% of total sessions

45.85% Female   54.15% Male

Age   100% of total sessions

27.50%	33.50%	15.50%	12.50%	5.50%	5.50%
18-24	25-34	35-44	45-54	55-64	65+

1   149,874

More than 1000 institutes

7

Users in France

8
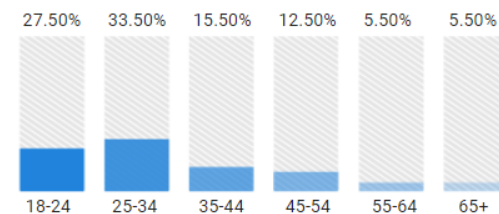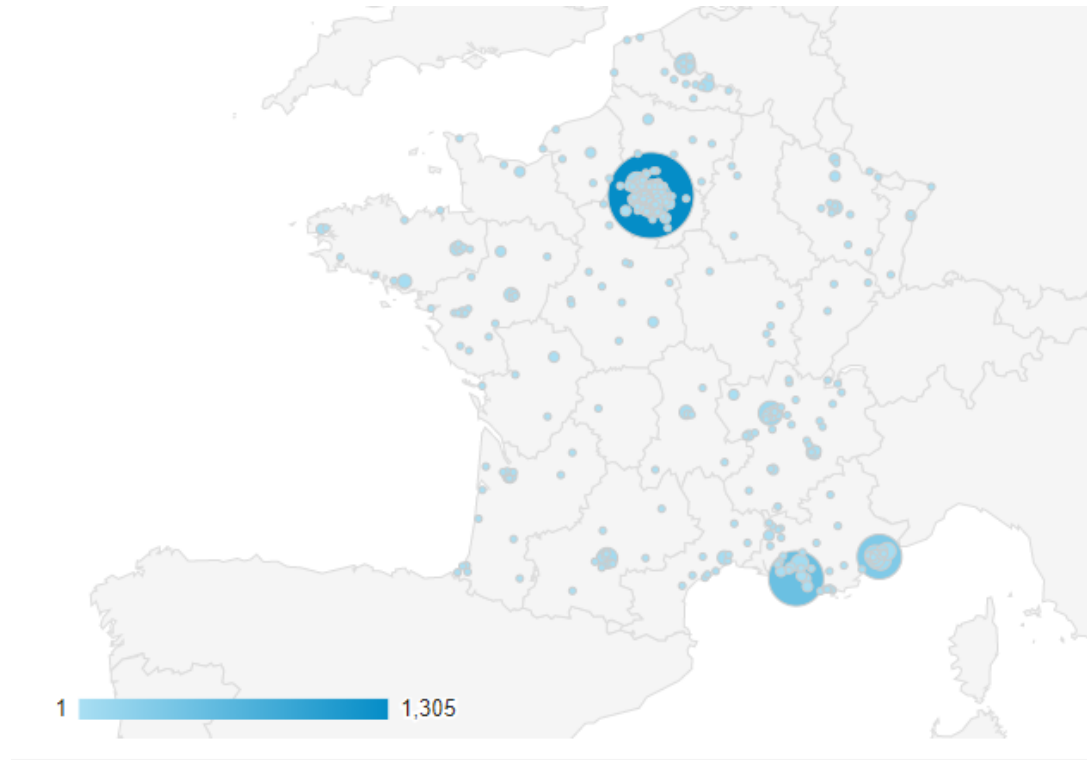
Adoption

- ❑ Universities/colleges
- ❑ High schools
- ❑ State-wide adoption: Virginia Cyber Range
- ❑ Company's internal training, interviews
- ❑ Military and law enforcement

Army (West Point), Air Force, Navy,
Coast Guard Academy, FBI
Cyber Protection Battalion

9

Lab Environment

SEED Labs

Android | Linux (Ubuntu)

VirtualBox

Host OS
(Windows, Linux, Mac)

SEED Labs 2.0

Ubuntu 20.04
(64-bit)

10

Lab Deployment
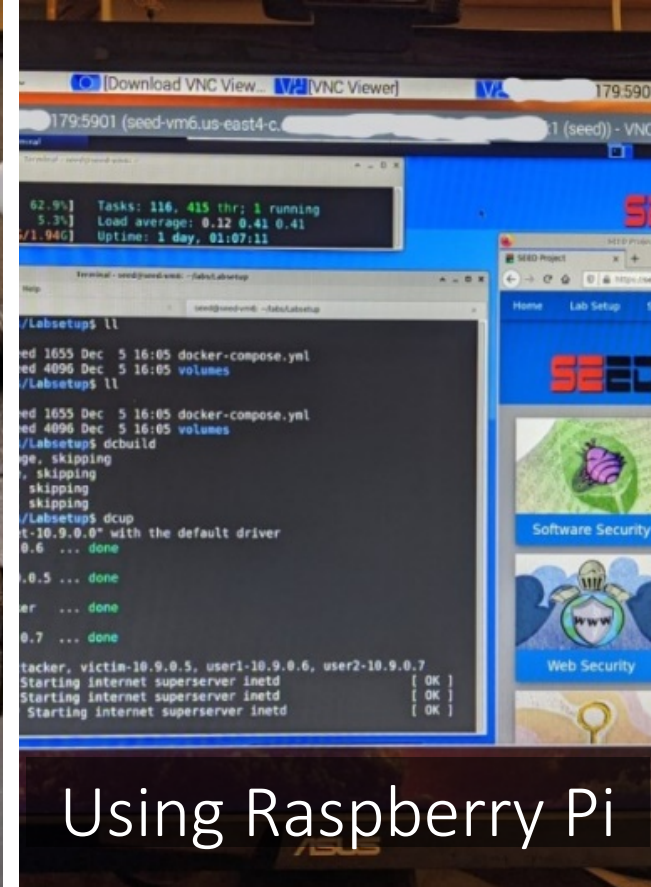

Personal Computer

Computer Lab

Cloud

- Amazon AWS
- Google Cloud
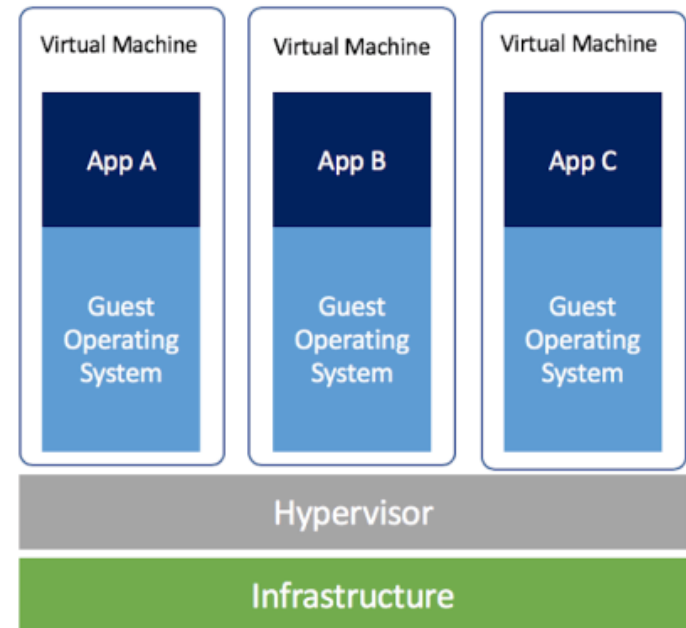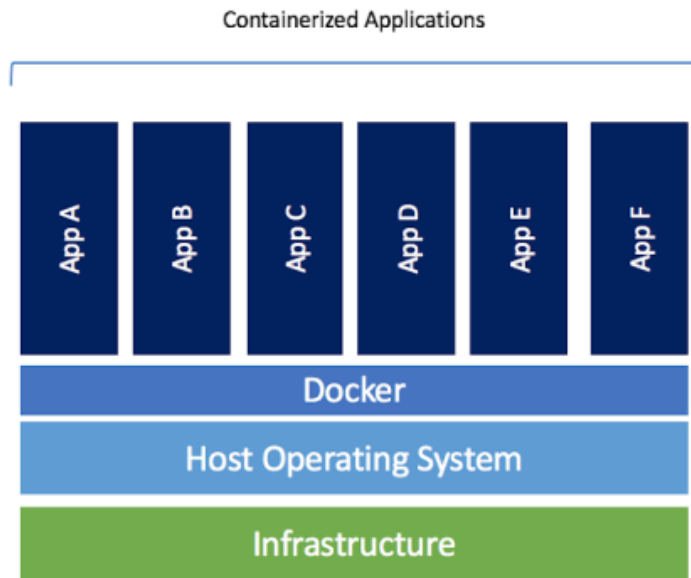- Microsoft Azure
- DigitalOcean
- Alibaba Cloud

Using tablet

Using smartphone

Using Raspberry Pi

Cloud Deployment (Using VNC)
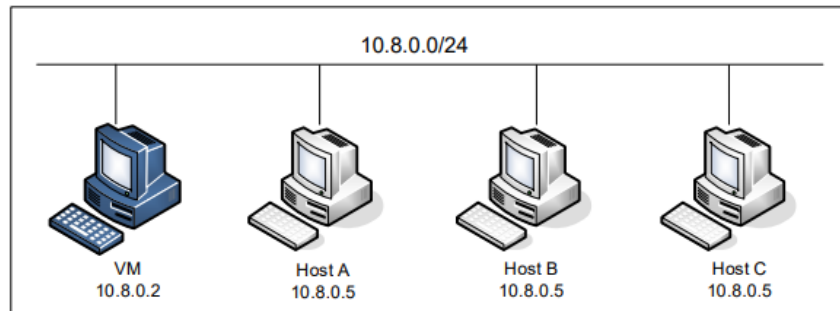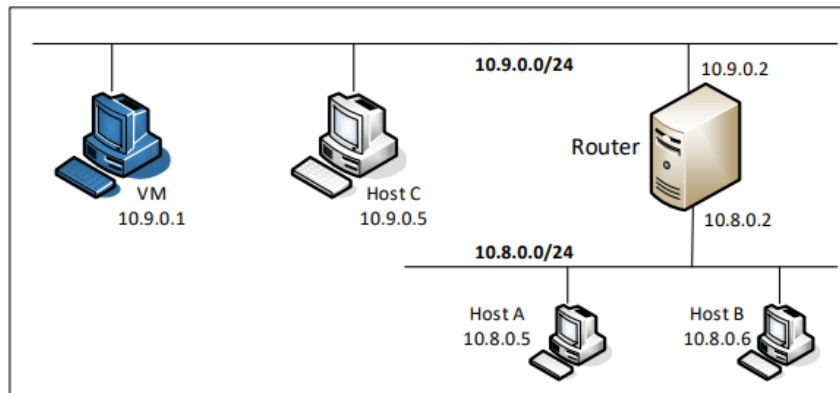
12

Using Containers in SEED Labs 2.0

13

Using Containers

Network
Topology I

Network
Topology II

14

A Complex Example

Close to 40 Labs
https://seedsecuritylabs.org

Software Security — 9

Network Security — 14

Web Security — 4

System Security — 2

Cryptography — 8

Mobile Security — 2
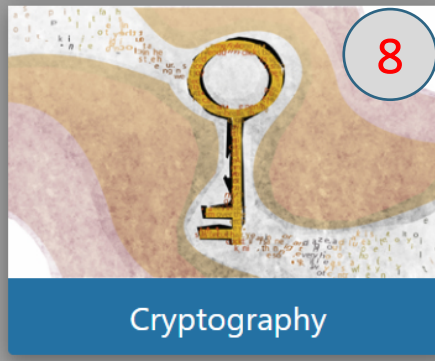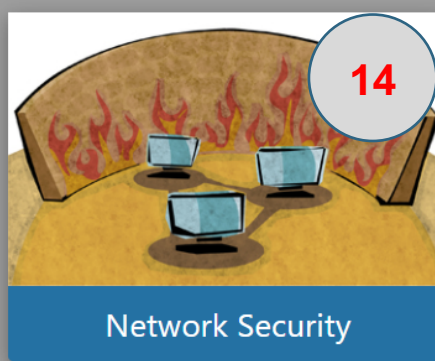
16
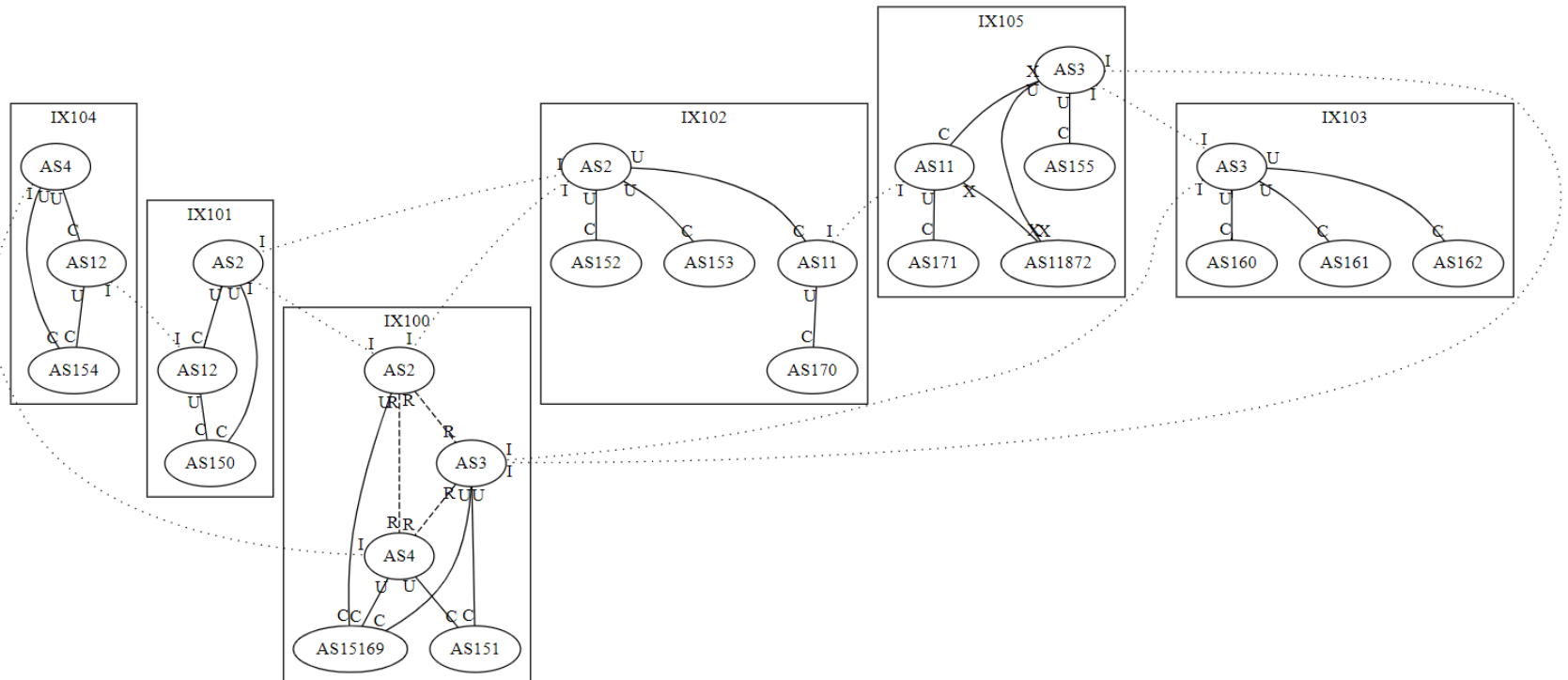
Three Types of Labs

Attack Labs

Exploration Labs

Design and Implementation Labs

17

Classical Attacks

Buffer-Overflow Attack

Return-to-libc Attack

Format-String Attack

Race Condition Attack

SQL Injection Attack

Cross-Site Request Forgery

Samy Worm (XSS)

ClickJacking Attack

Android Rooting Attack

Android Repackaging Attack

Packet sniffing and spoofing

ARP Cache Poisoning Attack

IP/ICMP Attacks

TCP Attacks

Mitnick Attack (TCP attack)

Kaminsky Attack (DNS attack)

BGP Attacks

Hash Length Extension Attack

Attacks on Encryption

18

Recent Attacks

Dirty COW Attack
Meltdown Attack
Spectre Attack
Shellshock Attack

Heartbleed Attack
MD5 Collision Attack
Attacks on IoT

Exploration Labs

Objective: Explore how security mechanisms work

Existing

- Set-UID program Lab
- Firewall Exploration Lab
- Secret-Key Encryption Lab
- Public-Key Encryption Lab
- PKI Lab, TLS Programming Lab
- Shellcode Lab

New

- DNS-in-a-Box Lab
- BGP Labs

Under Development

- Container & Docker
- Bitcoin & Blockchain

20

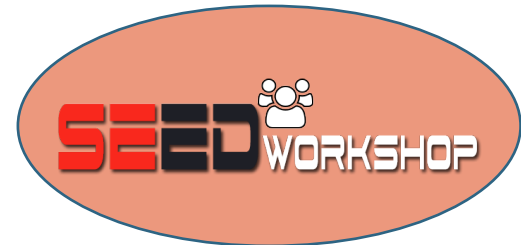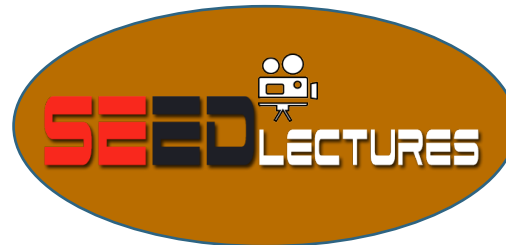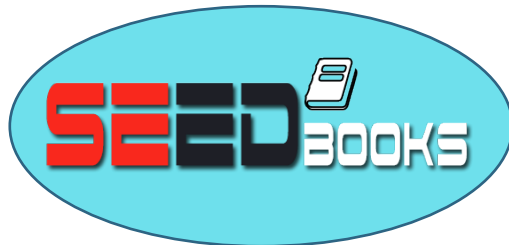# Design and Implementation Labs

- VPN Lab
- Firewall Lab

Open Source

GitHub: https://github.com/seed-labs

Instructor Manual:

Send me email (wedu@syr.edu)

Related Projects

23

Textbook

- Adopted by 192 institutes worldwide

- Self-published in 2019
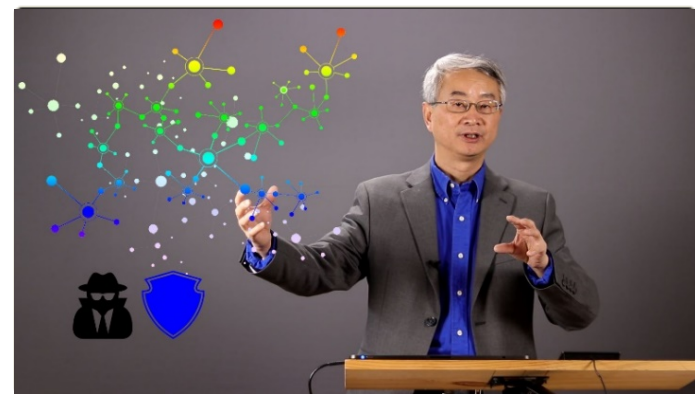
https://www.handsonsecurity.net/

Videos

SEED LECTURES

Computer Security: A Hands-on Approach

Wenliang Du

4.7 ★★★★⯪ (320)

12 total hours • 84 lectures • All Levels

$15.99 ~~$49.99~~
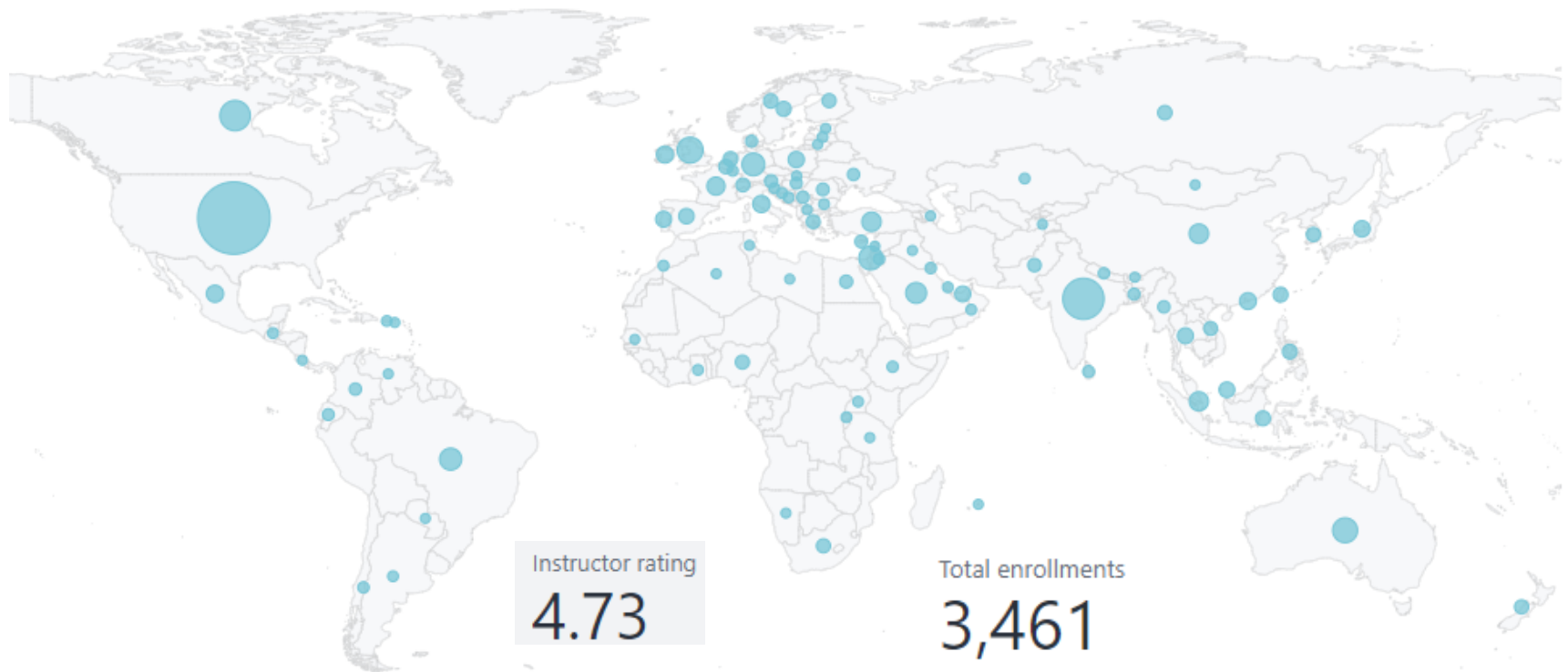
Internet Security: A Hands-on Approach

Wenliang Du

4.7 ★★★★⯪ (285)

19.5 total hours • 112 lectures • All Levels

$15.99 ~~$69.99~~

https://www.handsonsecurity.net/video.html

25

Course Enrollment

Instructor rating
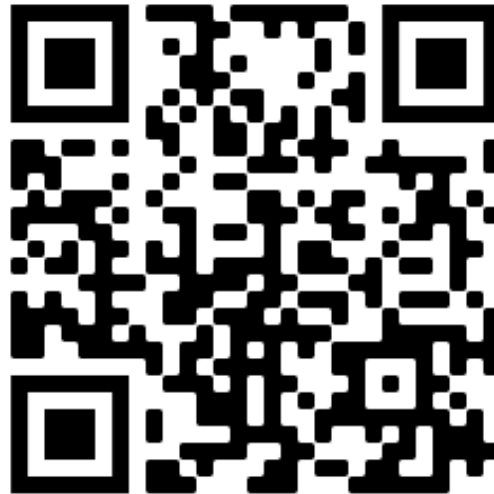4.73

Total enrollments
3,461

Workshops

2015: 60 faculties
2016: 70 faculties
2017: 70 faculties
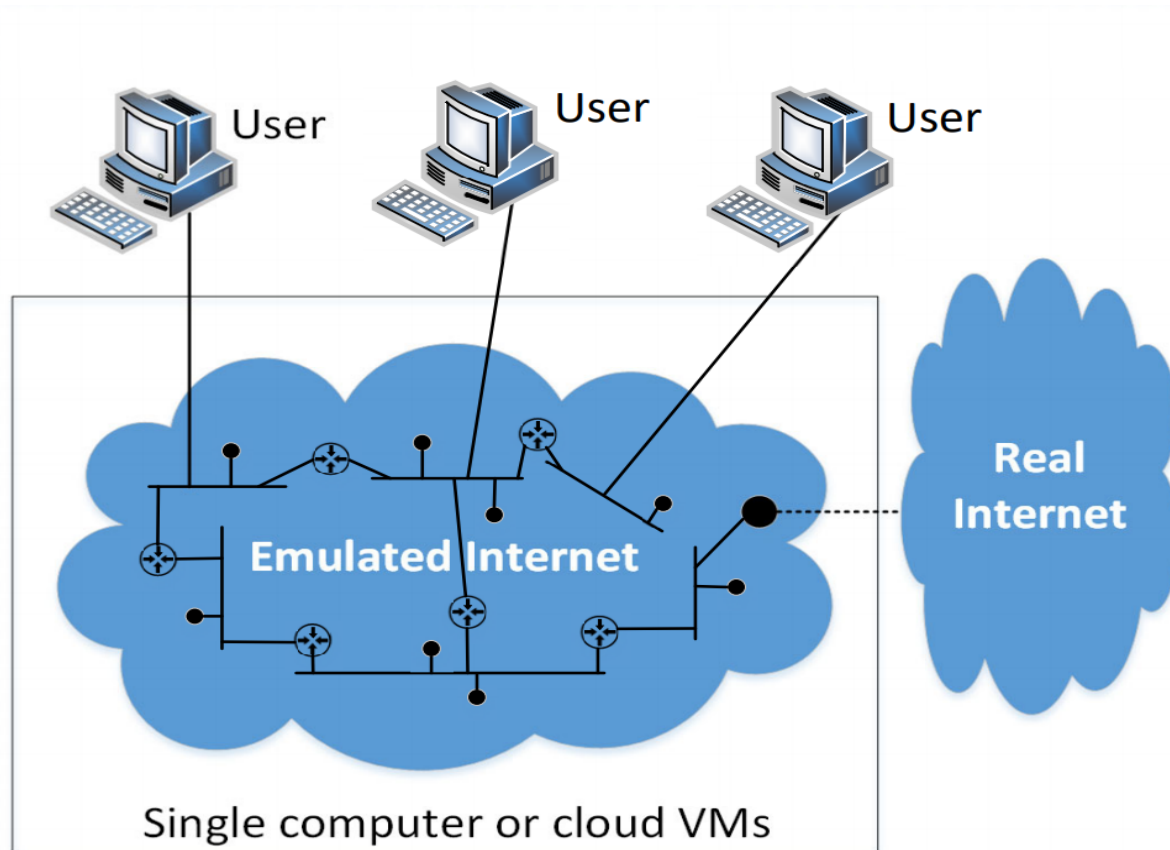2018: 80 faculties
2019: 90 faculties
2020: 120 faculties

2021 Workshops

June – August

- **Free**, Online (Zoom)
- **Instructors only**
- 10 weeks: 3 hours/week
- Cover 2-3 labs each week

https://seedsecuritylabs.org/workshops/

User

User

User

Emulated Internet

Real Internet

Single computer or cloud VMs

BGP Attack Lab
Botnet Lab
Darknet Lab
Morris Worm Lab
SDN Security Lab
etc.

Current Work: Internet Emulator

Thank You !

Questions ?

30