SaTC: EDU: Transdisciplinary Cybersecurity Education for Law and Engineering Students

Chansu Yu (ENG); Sathish Kumar (ENG); Brian Ray (LAW); Debbie Jackson (EDU),
Cleveland State University, Cleveland, OH

Challenge:

* Cybersecurity cases are inherently multidisciplinary.

* An urgent need of cybersecurity professionals who knows both the technical and the legal and policy issues.
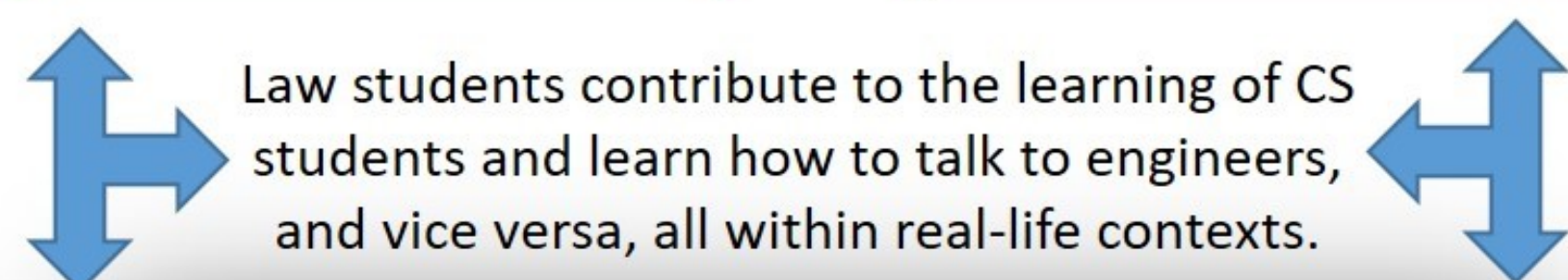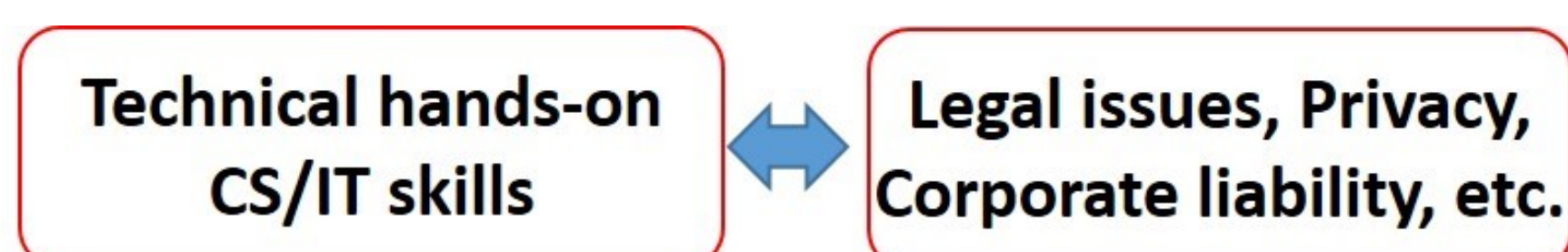
NIST's NICE Workforce Framework

* For example, Cyber Legal Advisor work role (OV-LGA-001) are required to have technical Knowledge of computer networking concepts and protocols, and network security methodologies (K0001).
* Securely Provision work category (SP) requires non-technical knowledge of laws, regulations, policies, and ethics (K0003).
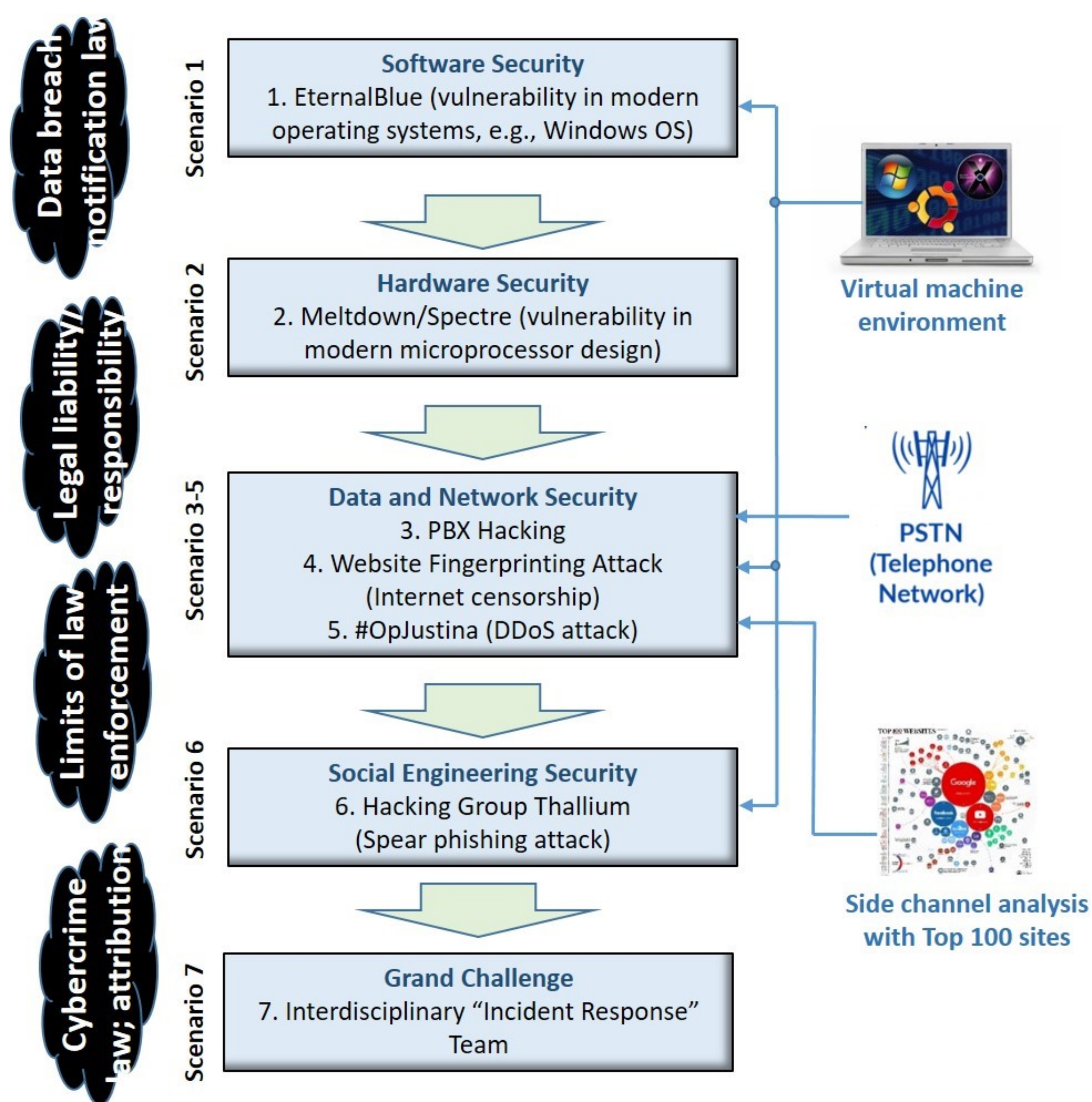
Solution:

Cybersecurity scenario-based curriculum

* Real-life scenarios;

* Hands-on lab experiment (VM platform from Ohio Cyber Range Institute);

* Interdisciplinary interactions

Technical hands-on CS/IT skills ↔ Legal issues, Privacy, Corporate liability, etc.

Law students contribute to the learning of CS students and learn how to talk to engineers, and vice versa, all within real-life contexts.

Eternal Blue Ransomware
#Op Justina (DDoS Attack)
Carna Botnet
Hacking Group Thallium
PBX Hacking
Website fingerprinting (Internet Censorship)
IoT Threats
Meltdown/Spectre

Scientific Impact:

* Designing and implementing a cybersecurity education framework that provides an unfragmented multifaceted view of security through real-life scenarios and interdisciplinary interactions.

* Aligning with NIST NICE Cybersecurity Workforce Framework

Data breach notification law
Legal liability, responsibility
Limits of law enforcement
Cybercrime law; attribution

Scenario 1 — Software Security
1. EternalBlue (vulnerability in modern operating systems, e.g., Windows OS)

Scenario 2 — Hardware Security
2. Meltdown/Spectre (vulnerability in modern microprocessor design)

Scenario 3-5 — Data and Network Security
3. PBX Hacking
4. Website Fingerprinting Attack (Internet censorship)
5. #OpJustina (DDoS attack)

Scenario 6 — Social Engineering Security
6. Hacking Group Thallium (Spear phishing attack)

Scenario 7 — Grand Challenge
7. Interdisciplinary "Incident Response" Team

Virtual machine environment

PSTN (Telephone Network)

Side channel analysis with Top 100 sites

Broader Impact:

* Open source textbook & lab manual of VM-based lab environments

• Interdisciplinary MS degree = Cybersecurity & Data Privacy Certificate (Law) + Cybersecurity Tech Certificate (Engineering)

* WiCyS 2022 (Women in Cybersecurity), March 17-19, Cleveland, OH

* Summer camp for HS students (along with CSforAll camps, supported by NSF)