vWaterLabs: Developing Hands-On Laboratories for Water-focused Industrial Control Systems Cybersecurity Education

Stu Steiner, Matthew J. Kirkland, Daniel Conte de Leon

Center for Network Computing and Cybersecurity
Department of Computer Science
Eastern Washington University

Center for Secure and Dependable Systems
Department of Computer Science
University of Idaho

CCSC Southwest 2021

Overview

1. Background and Problem
2. Approach and Objectives
3. Proposed Solution: vWaterLabs
4. Conclusions
5. References

Background

1. Background and Problem
2. Approach and Objectives
3. Proposed Solution: vWaterLabs
4. Conclusions
5. References

Teaching Cybersecurity

Teaching cybersecurity is different than teaching traditional CS courses (CS1, CS2, etc.).

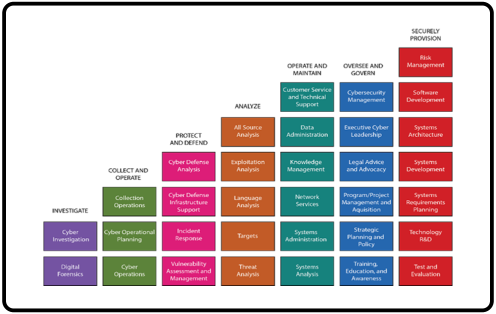
Cybersecurity Categories

- Offensive
- Defensive
- Policy/Operations

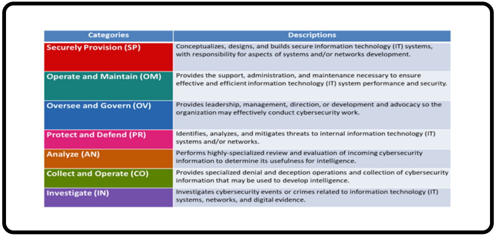
National Centers of Academic Excellence in Cybersecurity Knowledge Units (KUs) which are mapped to the NICE Framework

- Required 3 foundational KUs
- Required 5 technical KUs
- Required 14 of 58 KUs

Teaching Cybersecurity



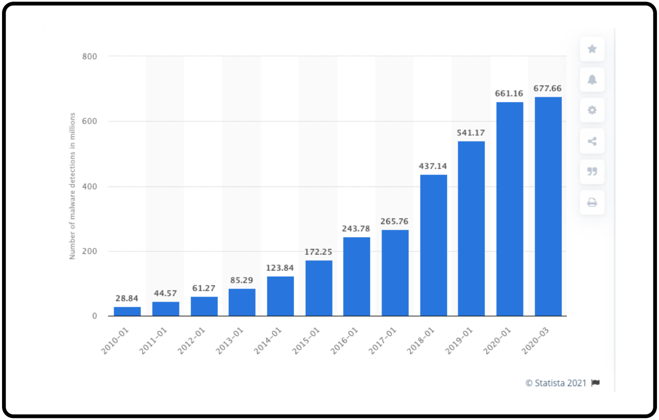
INVESTIGATE	COLLECT AND OPERATE	PROTECT AND DEFEND	ANALYZE	OPERATE AND MAINTAIN	OVERSEE AND GOVERN	SECURELY PROVISION
						Risk Management
				Customer Service and Technical Support	Cybersecurity Management	Software Development
			All Source Analysis	Data Administration	Executive Cyber Leadership	Systems Architecture
		Cyber Defense Analysis	Exploitation Analysis	Knowledge Management	Legal Advice and Advocacy	Systems Development
	Collection Operations	Cyber Defense Infrastructure Support	Language Analysis	Network Services	Program/Project Management and Aquisition	Systems Requirements Planning
Cyber Investigation	Cyber Operational Planning	Incident Response	Targets	Systems Administration	Strategic Planning and Policy	Technology R&D
Digital Forensics	Cyber Operations	Vulnerability Assessment and Management	Threat Analysis	Systems Analysis	Training, Education, and Awareness	Test and Evaluation



Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Increased Cyber Attacks

For the last 10 years, there has been a steady increase in cyber attacks, especially for attacks that are malware related [1].



Increased Cyber Attacks

Included in the increased cyber attacks are attacks on Industrial Control Systems (ICS).

In 2020 the ICS vulnerabilities added to the National Vulnerability Database were roughly 10% more than 2019. [2]

The top three sectors were:

- Energy 236 vulnerabilities reported
- Critical manufacturing 191 vulnerabilities reported
- Water and wastewater 171 vulnerabilities reported

Open Cybersecurity Positions

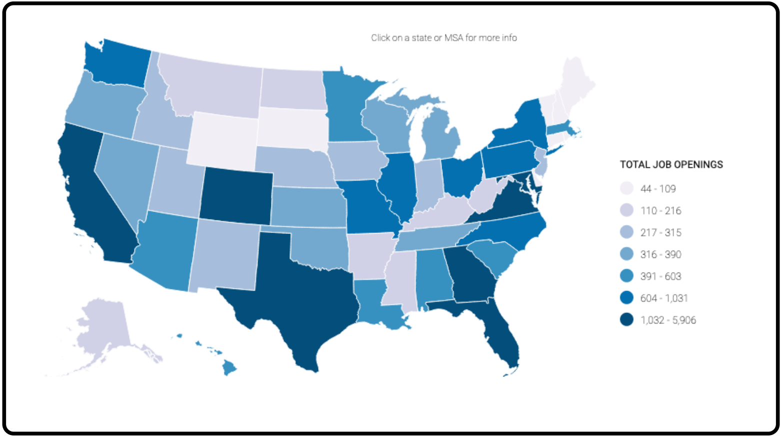
As the number of cyber attacks grows so does the number of open cybersecurity positions.

As stated by the website cyberseek.org [3]

- Cybersecurity talent gaps exist across the country.
- Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region.

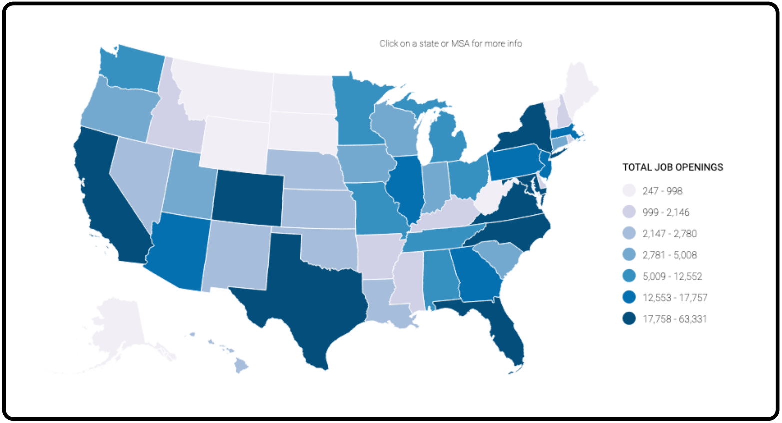
Open Cybersecurity Positions

Open Public Positions by State [3]



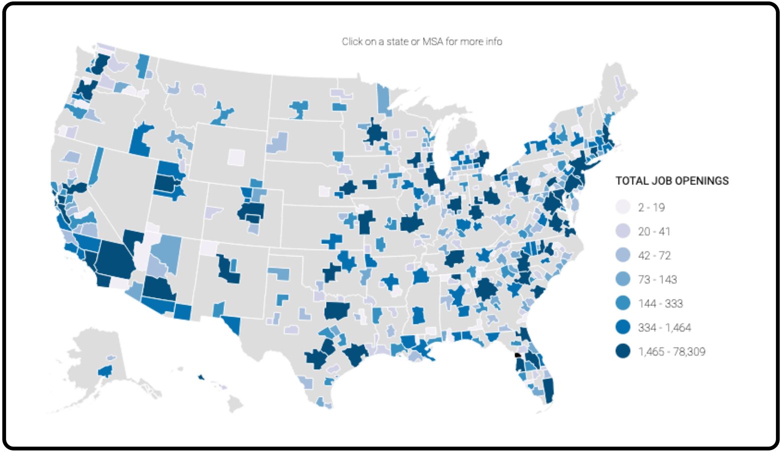
Open Cybersecurity Positions

Open Private Positions by State [3]



Open Cybersecurity Positions

All Open Positions by Metro Area [3]



Increased ICS Positions

Besides a familiarity with cybersecurity, ICS cybersecurity requires specialized training that most higher educational institutions currently don't teach.

The following ICS position specifications were obtained from many different job sites (e.g. Monster, Indeed, etc.)

Required ICS skills set include knowledge of:

- Information Technology (IT)/Operational Technology (OT)
- Supervisor Control and Data Acquisition (SCADA)
- Programmable Logic Controllers (PLC)

ICS Education

Properly securing industrial control systems, especially critical infrastructure systems, requires special skill set.

- Due to the inherent nature of critical infrastructure systems, these systems can't be used for training.
- Instead of testing running systems a promising solution is the use of testbeds.

ICS Education

Physical testbeds have both advantages and disadvantages.

Advantages

- Enables educational and training activities.
- Allows for experimentation that is not feasible on real infrastructure
- High fidelity representation of real systems.

Disadvantages

- Properly building a fully functional testbed is expensive
- Properly building a fully functional testbed requires a large space that often isn't available.
- Scheduling student access to the testbed can be problematic.

Approach and Objectives

1. Background and Problem
2. Approach and Objectives
3. Proposed Solution: vWaterLabs
4. Conclusions
5. References

Approach and Objectives

Questions:
1) How does an institution build a fully functional testbed?
2) How do students properly access the testbed?
3) What labs are needed for ICS security education?

Hypotheses
1) Would creating a virtual testbed solve any disadvantages?
2) Would targeted labs, for the virtual testbed, help institutions train their students for ICS cybersecurity?

Approach and Objectives

- **Objective 1**: Identify testbed characteristics.
- **Objective 2**: Build a virtual ICS testbed.
- **Objective 3**: Create ICS cybersecurity labs for the virtual testbed.
- **Objective 4**: Evaluate the ICS cybersecurity labs.
- **Objective 5**: Make the virtual testbed and labs available to all.

Proposed Solution: vWaterLabs

1. Background and Problem
2. Approach and Objectives
3. Proposed Solution: vWaterLabs
4. Conclusions
5. References

vWaterLabs: Features

vWaterLabs is a fully functional virtual testbed and set of labs for ICS cybersecurity.

vWaterLabs features include:

- Virtual testbed built based on research of prior testbeds.
- Virtual labs for PLC, SCADA, HMI understanding.
- Virtual labs for MODBUS, and DNP3 protocol.
- Virtual labs for ICS cybersecurity.

vWaterLabs: Features

Two versions of vWaterLabs

Version 1

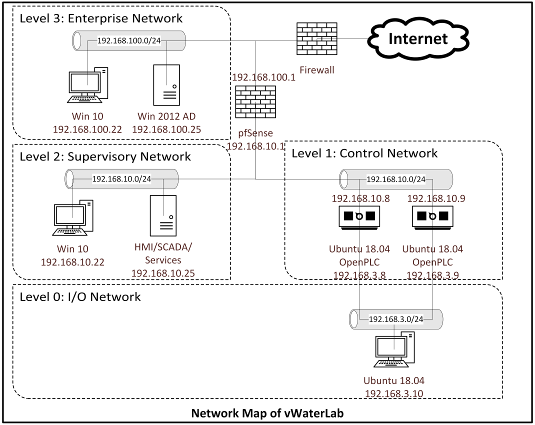
- Two longer tutorials
- Testbed virtual machines not available
- No new labs available

Version 2

- Smaller labs
- Available testbed virtual machines
- Short YouTube videos
- More challenge/understanding checks

vWaterLabs: Features

vWaterLabs Network Map



Network Map of vWaterLab

vWaterLabs: Features

vWaterLabs lab demonstration with specifications.

GitHub site:
https://github.com/ICSSecurityLabs/ICSSecurityLabs

YouTube video: https://youtu.be/cXLpIkujKyU

vWaterLabs evaluations

- Version 1 of Labs offered one time
- Version 1 offering did not evaluate the labs
- Version 2 offered in April 2021 in a network security course
- Version 2 will evaluate the labs

Conclusions

1. Background and Problem
2. Approach and Objectives
3. Proposed Solution: vWaterLabs
4. Conclusions
5. References

Conclusions

vWaterLabs is a viable solution for teaching ICS cybersecurity

- Current labs explain PLC programming, HMI, MODBUS and ICS firewalls.
- New labs are being developed.
- Old labs are updated after being taught and assessed.
- Small physical testbed being developed.

Conclusion

vWaterLabs testbed and labs developed under consortium of EWU and University of Idaho

- Consortium is named ICS Security
- Open source and available from https://github.com/ICSSecurityLabs/ICSSecurityLabs

Thank You and Questions

Questions?

References

1. Background and Problem
2. Approach and Objectives
3. Proposed Solution: vWaterLabs
4. Conclusions
5. References

References I

- H. Ward, “Cumulative Detections of Newly-Developed Malware Applications Worldwide,” 2021. [Online]. Available: https://www.statista.com/statistics/680953/global-malware-volume/
- E. Kovacs, “Over 70% of ICS Vulnerabilities Disclosed in First Half of 2020 Remotely Exploitable,” 2020. [Online]. Available: https://tinyurl.com/8wchsfr3
- C. Seek, “Cybersecurity Supply/Demand Heat Map,” 2021. [Online]. Available: https://www.cyberseek.org/heatmap.html