

University of Houston  Clear Lake

**Introductory Cybersecurity Course for Traditional CS  
Undergraduate Students**  
**-Design, Evaluation, and Lessons Learned-**

2019 UHCL CyberEd Workshop

Wei Wei, Ph.D.

April 5th, 2019

# Background

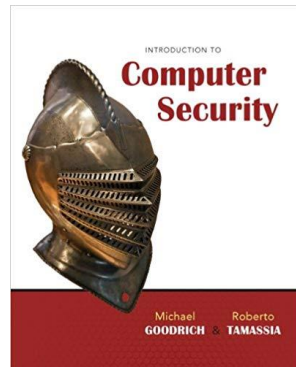
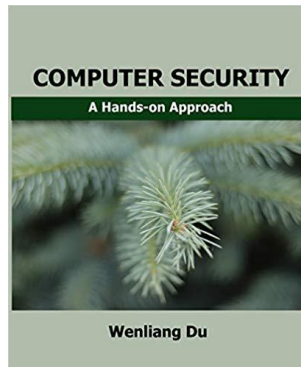
- UHCL CyberCorps project (NSF grant 1723596) proposed to implement three new courses in order to meet the CAE-CDE 4Y designation requirements.
- CSCI 4391 Cyber Attacks and Defense is the first of the three, which acts as a comprehensive introductory course to cybersecurity.
  - Three credit hours upper level course
  - Lecture and lab
  - Open to all computing students (CS, CIS, ITEC, CENG)

# Course Design

- General principles:
  - Provides comprehensive coverage of identified KUs that are not covered (enough) elsewhere.
  - Content from those KUs must be organized in a meaningful structure.
  - Topics (sub-topics) are compiled in a modular format to enable “plugability”.
  - Embed hands-on labs.

# Learning Materials

- Recommended textbooks:
  - Computer Security: A Hands-on Approach by Wenliang Du
  - Introduction to Computer Security by Michael Goodrich, Roberto Tamassia
- Other resources:
  - Lecture notes
  - Online learning resources including:
    - SEED website
    - Technical tutorials
    - Federal agency websites
    - Professional development websites
    - Cybersecurity related professional organizations
    - Cybersecurity workforce building websites
    - ...



# Student Demographics

	Frequency ( <i>n</i> )	Percentage (%)
--	------------------------	----------------

## 1. Gender

Male	9	81.8
Female	2	18.2

## 2. Race/Ethnicity

Caucasian	5	50.0
Hispanic or Latino	3	30.0
Indian	1	10.0
Two or More Races	1	10.0

	Frequency ( <i>n</i> )	Percentage (%)
--	------------------------	----------------

## 1. Grade Level

Junior	2	18.2
Senior	9	81.8

## 2. College Major

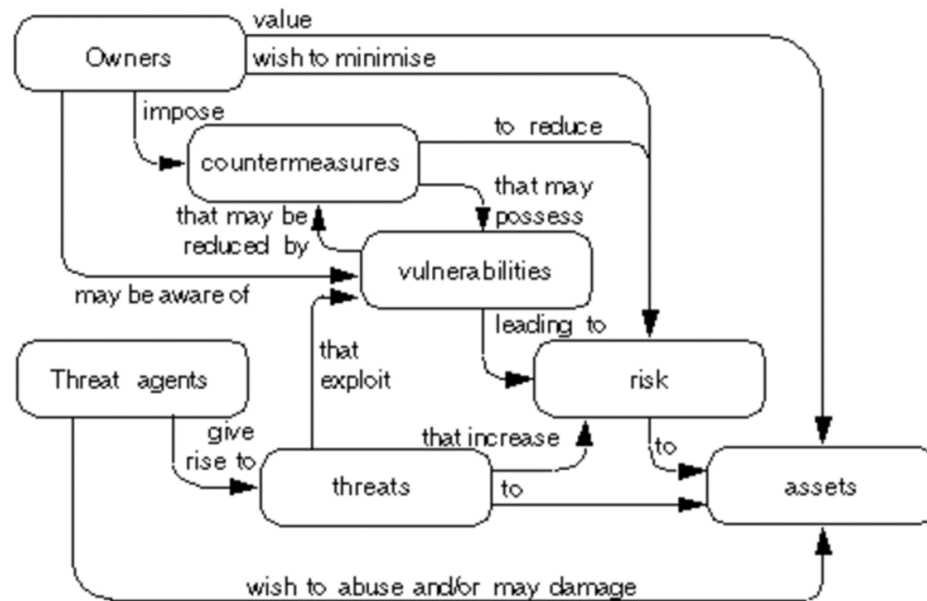
Computer Engineering	1	9.1
Computer Information Systems	2	18.2
Computer Science	7	63.6
Information Technology	1	9.1

# Course Coverage

Date	Module	Topics
Aug 28	Security Fundamentals	Security Concepts and Principles
Aug 30		
Sep 4		Security Management
Sep 6		
Sep 11		The Cybersecurity Industry and Careers
Sep 13		
Sep 18	Security Threats and Countermeasures	Security Threat & Cyber Crimes
Sep 20		Safeguard & Countermeasures
Sep 25		Safeguard the IT Infrastructure
Sep 27		
Oct 2		Introduction to Cryptography
Oct 4		
Oct 9	Network Security	Network Basics
Oct 11		Network Protocols
Oct 16		Network Administration Basics
Oct 18		
Oct 23		Network Security Basics
Oct 25		
Nov 1	Software Security	Software Vulnerabilities and Security
Nov 6		Low-level Attacks and Defense
Nov 8		
Nov 13		
Nov 15		Secure Programming
Nov 20		
Nov 27		Web-based System Attacks and Defense
Nov 29		
Dec 4	Cloud Security	Cloud Computing Fundamentals
Dec 6		Cloud Security

# Pedagogical Tools-I

- Lectures with visual aids: slides, videos
- Interactive session: group/class activities with focus



# Pedagogical Tools-I

- Tech demos: led by instructor and facilitated by TA
- Labs: in-class and take-home



# Hands-On

Lab Name	Learning Topics
Sending Encrypted Emails	Encryption, Public Key Infrastructure
<i>Secret-Key Encryption Lab*</i>	Encryption
<i>Buffer overflow*</i>	Software security
<i>SQL Injection*</i>	Database security
<i>Packet Sniffing and Spoofing*</i>	Network security
<i>Cross-Site Scripting* Attack</i>	Web security
<i>TCP/IP Attacks*</i>	Network Security
Wireshark Lab	Network Administration
Nmap Lab	Network Administration

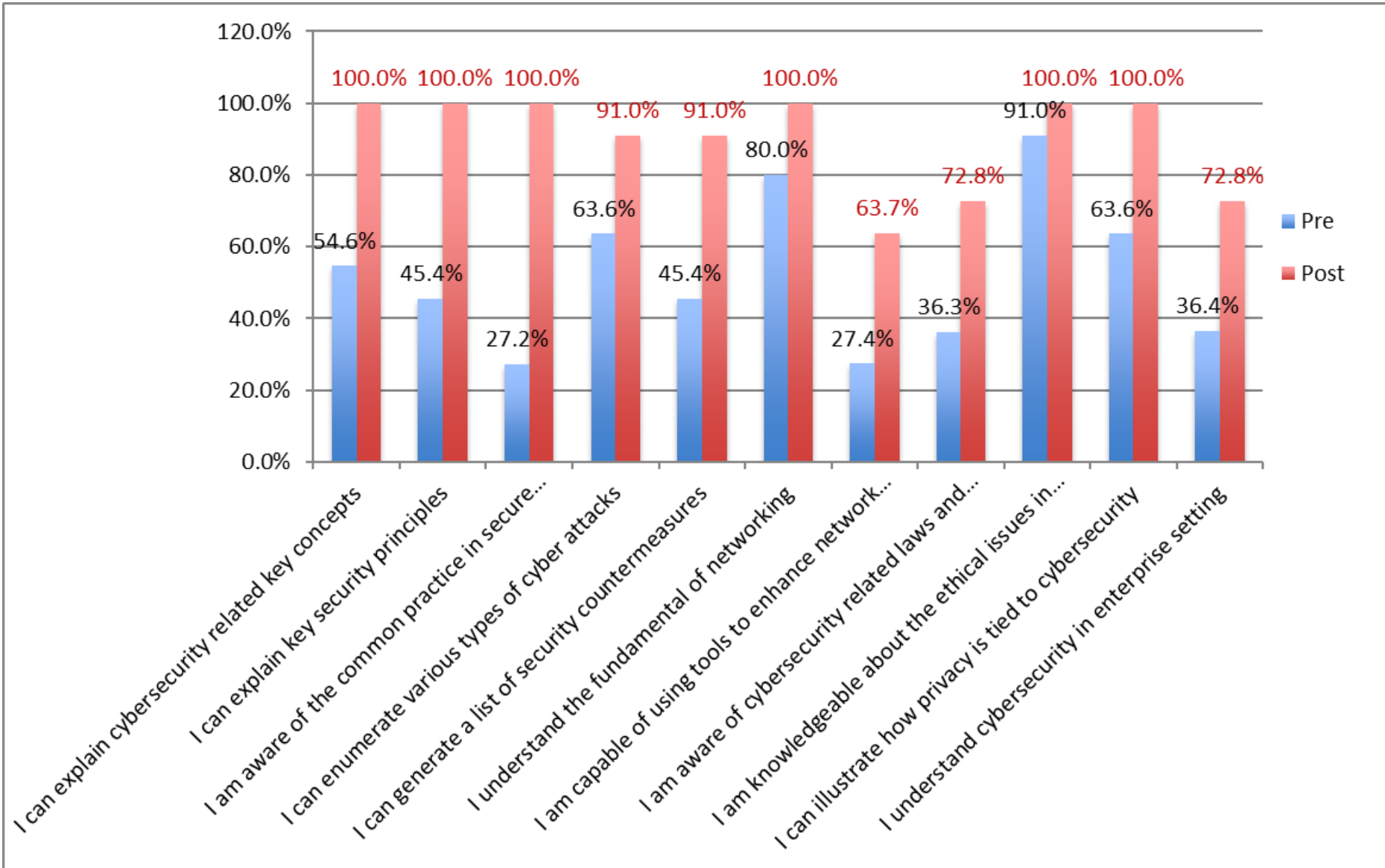
# Pre- & Post- Test on Knowledge

- **Assessment design:**
  - Students were administered a 20-item multiple choice assessment created by an expert in cybersecurity and computer science. Students were required to take a pre-test at the very beginning of the semester and a post-test at the end of the semester.
- **Assessment results:**

Cyber Attacks and Defense	N	M	SD	<i>t</i> -value	df	<i>p</i> -value
1. Pre-Scores	9	68.5	11.1	-1.417	8	.194
2. Post-Scores	9	75.0	14.1			

# Pre- & Post- Survey on Perception

- Assessment design:
  - At the beginning and again at the end of the semester students were asked to take a survey to determine whether participating in the cyber defense track would increase their cybersecurity awareness and change their perception of cybersecurity
- Notable findings:
  - At the end of the semester, 100% of the students felt they could
    - explain cybersecurity related key concepts and principles.
    - were aware of the common practice in secure programming.
    - understood the fundamentals of networking
    - were knowledgeable about the ethical issues in cybersecurity.
    - could illustrate how privacy is tied to cybersecurity
  - 91.0% of the students felt they had the ability to generate a list security counter-measures in comparison to 45.4% at the start of the semester



# Focus Group Student Comments-I

- *“In other classes, we just touched on the names of SQL injection and the risk factors. In this class, we got a greater understanding of what it actually was.”*
- *“This class provided us with the ‘know how’ of cybersecurity not just the concepts of cybersecurity. Other classes tell you what to do, but not cover the real ‘how to’ and this class did just that.”*
- *“My increased knowledge on the level of escalating and evolving threats and vulnerabilities to computers and networks helped me understand that the job market will always be there - job security.”*

# Focus Group Student Comments-II

- *“I joined the Air National Guard and picked a job in cybersecurity. This class helped me make that choice.”*
- *“We would but a lot of us are seniors and don’t have the time. If I had taken the course earlier in the program, I probably would have gone that route.”*
- *“Although we are not tested on the labs, that’s the part you want to learn because by ‘doing’ it you will not forget it – it will stink in your mind.”*
- *“I think the labs themselves are very good. I think some of us needed more of a foundation. I felt some of the people in class had more of a foundation with Linux than I did so I was struggling to get caught up with that plus learning new things in the lab.”*

# Lessons Learned

- Students' technical background vary, which could be a challenge.
- There is tradeoff between breadth and depth.
- Students do enjoy getting their hands dirty, doesn't mean the experience is frustration-free.
- The SEED project offers a viable solution, especially when resources are limited.

