University of Houston Clear Lake

Revamping a Traditional Computer Science Undergraduate Program toward CAE-CDE 4Y Designation

-A Case Study at the University of Houston-Clear Lake-

2019 UHCL CyberEd Workshop

Wei Wei, Ph.D.

April 5th, 2019

Agenda

- Introduction & Background
- Project Motivation
- Project Design
  - General design approach
  - Specific design process
  - Design artifacts
- Project Implementation

Project Overview

- This project is supported by NSF CyberCorps Grant 1723596.

- Project overall goal:
  - present a ***feasible*** modernization approach for a ***traditional*** computer science degree program to undergo rigorous ***self-study***, ***gap analysis***, and curricular development, in order to integrate ***cybersecurity knowledge and skills*** into the four-year program, while maintaining its current ABET and regional accreditations.

Computer Science (CS) at UHCL

- UHCL was established in 1974 to meet the local education needs in the Clear Lake area.

- The College of Science and Engineering (CSE) houses the Department of Computing Sciences (DCS), which includes:
  - Computer Science (CS)
    - Largest program within CSE with total enrollment of 466
    - ABET accredited
  - Computer Information Systems (CIS)
    - ABET accredited
  - Information Technology (ITEC)

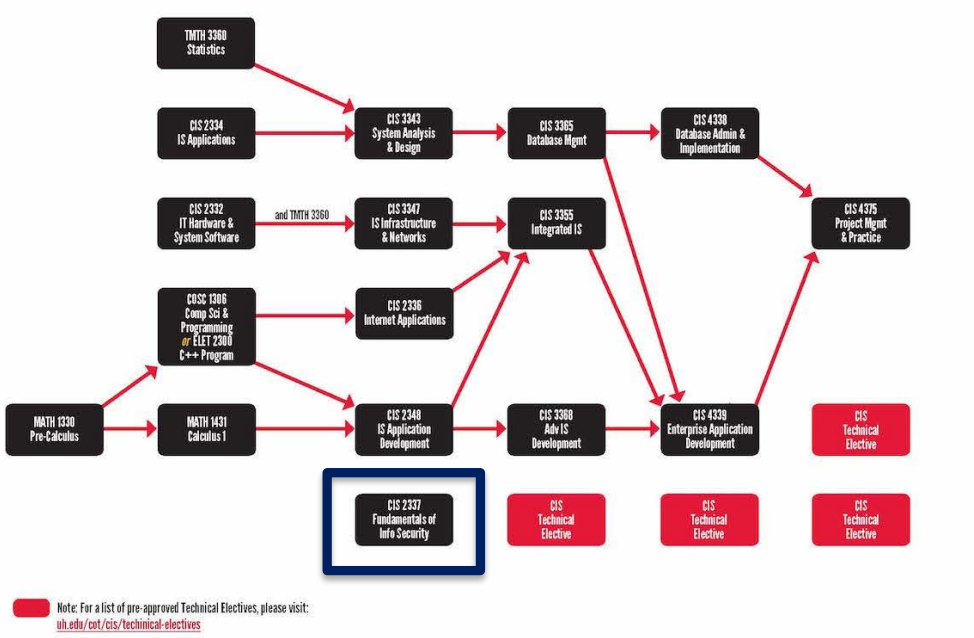
Project Motivation-I

- The global "Cybersecurity Hiring Crisis"
  - High demand and low supply of cybersecurity professionals
  - Desperate needs of cyber-operators
  - To bridge the gap:
    - Training
    - Higher education
      - The Center of Academic Excellence in Cyber Defense Education (CAE-CDE)

Project Motivation-II

- Texas has one of the widest cybersecurity talent gaps.
- The Greater Houston area has many high profile targets and needs more education programs.

Institution	Type of Cyber Security Programs Offered	Affiliated Department	Location
Southern Methodist University	M.S., Certificate	IS/IT	Dallas
Texas A&M University	Minor, Certificate	CS	College Station
Texas A&M University-Corpus Christi	B.S.	IS/IT	Corpus Christi
University of Dallas	M.S., Certificate	IS/IT	Dallas
University of Houston	M.S.	IS/IT	Houston
University of Texas at Dallas	Minor, Track	IS/IT	Dallas
University of Texas at El Paso	B.S.	CS	El Paso
University of Texas at San Antonio	M.S., B.S.	IS/IT	San Antonio



CIS 2337 - Fundamentals of Information Security
Credit Hours: 3.0
Lecture Contact Hours: 3 *Lab Contact Hours:* 0
Information security, including technical security issues, people security issues, policy issues, privacy, and ethics.

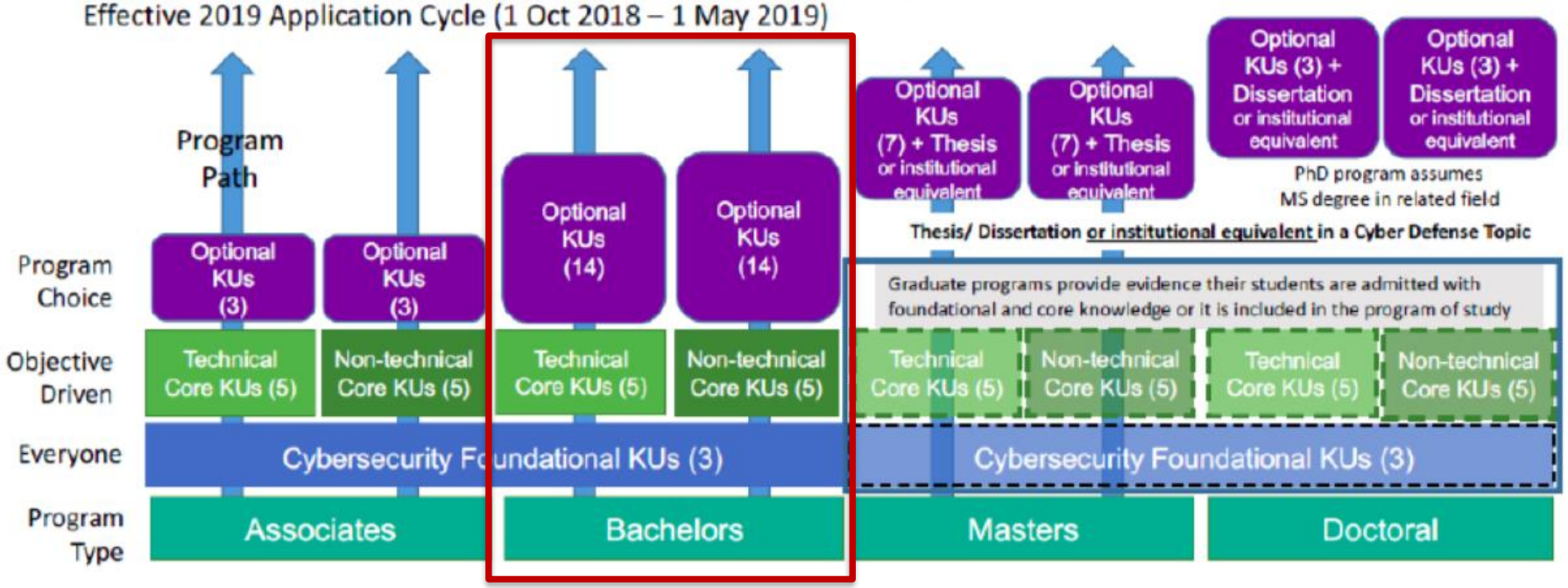
Other related electives:
CIS 3337 - Secure Application Design
CIS 3351 - Intrusion Detection and Incident Response
CIS 4357 - Digital Forensics
CIS 4367 - Advanced Digital Forensics

Curriculum Design Considerations

- Resource constraints
- Program sustainability
- Changing environment
- Program quality
  - CAE-CDE designation requirements at Knowledge Units (KU) level
  - The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF)
  - Compliances with other guidelines/frameworks

Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) Designation Requirements,

Effective 2019 Application Cycle (1 Oct 2018 – 1 May 2019)



Knowledge Units (KUs):

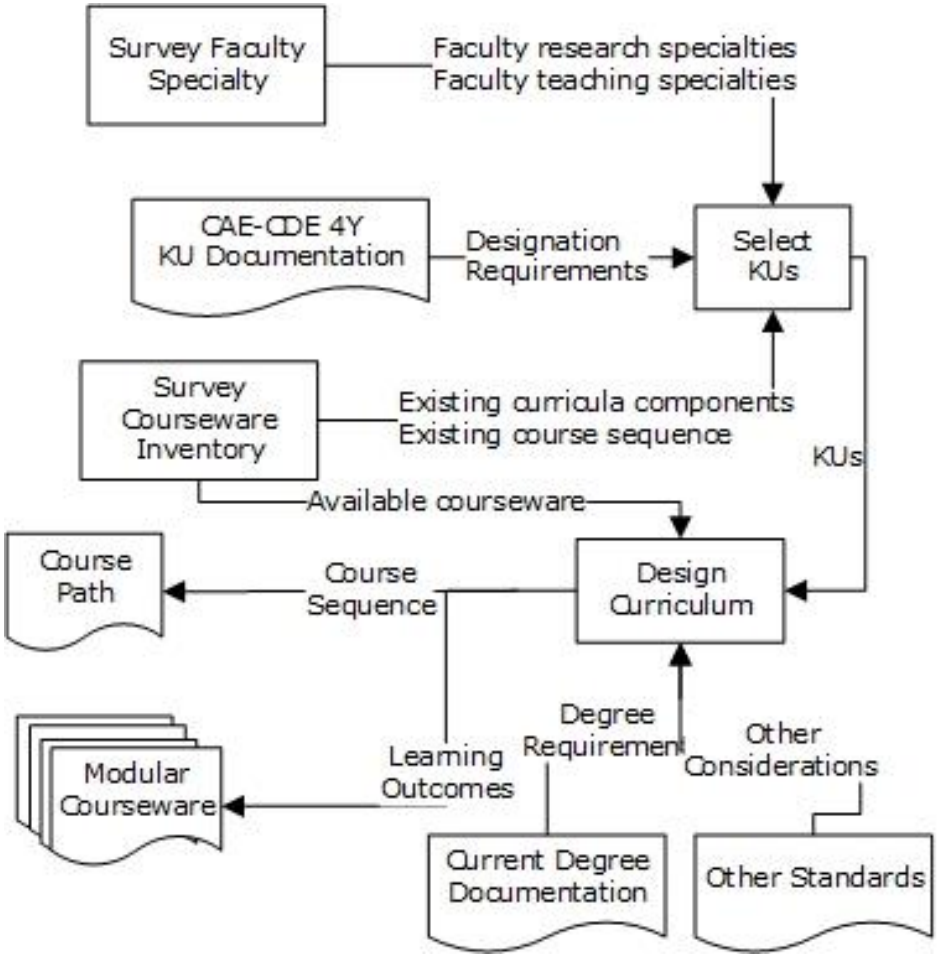
Foundational: Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components

Technical Core: Basic Scripting and Programming; Basic Networking; Network Defense; Basic Cryptography; Operating Systems Concepts

Nontechnical Core: Cyber Threats; Policy, Legal, Ethics, and Compliance; Security Program Management; Security Risk Analysis; Cybersecurity Planning and Management

Source: https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

Curriculum Design Process



To Fulfill the Designation Requirement

- Based on self study (gap analysis) results, we decided to cover the following 22 KUs:

3 Cybersecurity Foundational KUs:
• Cybersecurity Foundations (CSF) • Cybersecurity Principles (CSP) • IT Systems Components (ISC)
5 Technical Core KUs:
• Basic Cryptography (BCY) • Basic Networking (BNW) • Basic Scripting and Programming (BSP) • Operating Systems Concepts (OSC) • Network Defense (NDF)

14 Optional KUs:
• Databases (DAT) • Network Technology and Protocols (NTP) • Data Structures (DST) • Digital Forensics (DFS) • Policy, Legal, Ethics, and Compliance (PLE) • Linux System Administration (LSA) • Network Forensics (NWF) • Cyber Crime (CCR) • Cybersecurity Ethics (CSE) • Intrusion Detection/Prevention Systems (IDS) • Network Security Administration (NSF) • Secure Programming Practices (SPP) • Web Application Security (WAS) • Wireless Sensor Networks (WSN)

Implementation of the Selected KUs

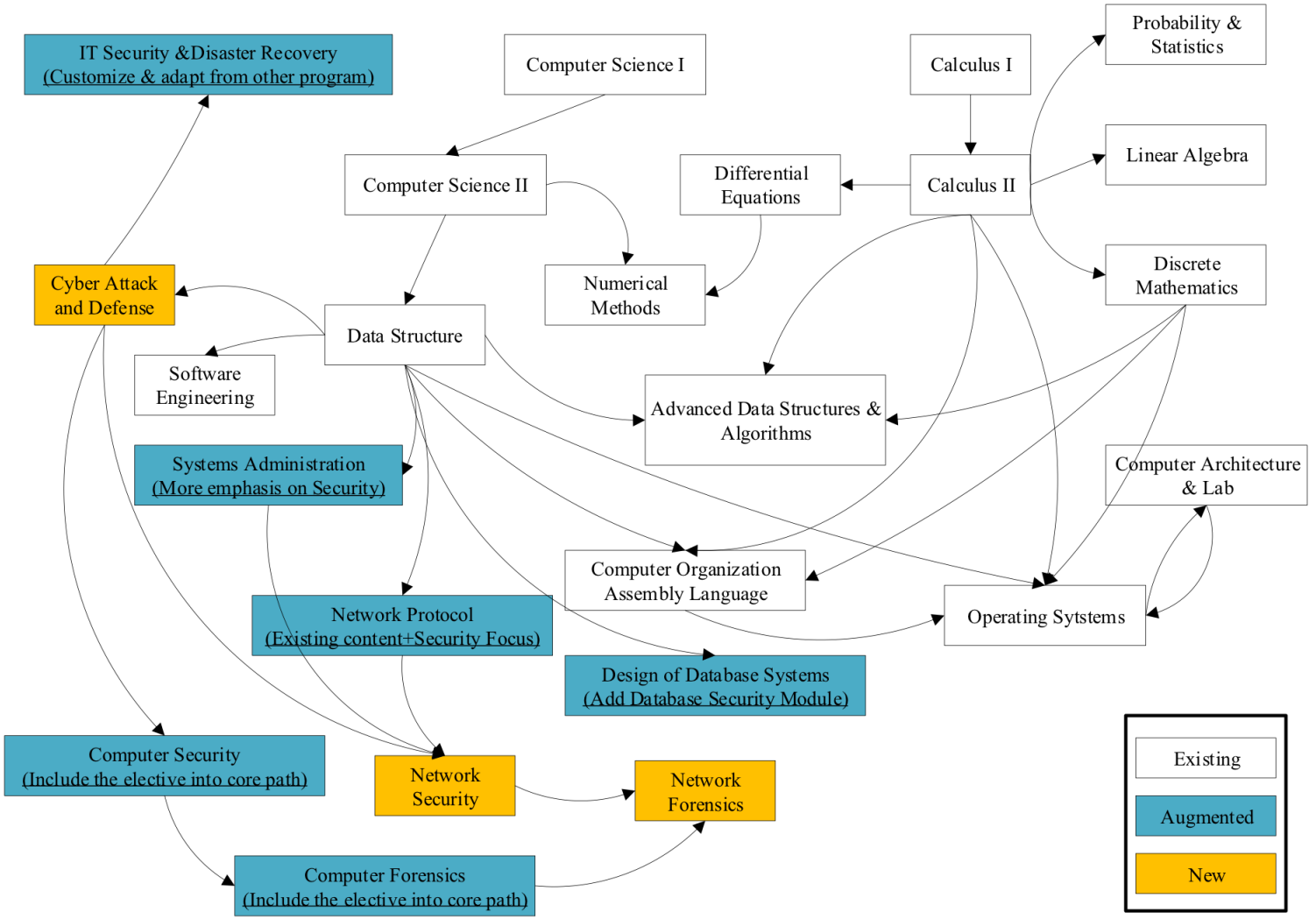
KUs	Source of Coverage
CSF	Cyber Attacks and Defense*
CSP	Cyber Attacks and Defense*
ISC	Multiple computing courses
BCY	Cyber Attacks and Defense*
BNW	Network Protocol
BSP	Multiple programming courses
OSC	Operating Systems
NDF	Network Security*
DAT	Design of Databases
NTP	Network Protocol
DST	Data Structures
DFS	Computer Forensics
PLE	Cyber Attacks and Defense*
LSA	Computer System Administration
NWF	Network Forensics*
CCR	Cyber Attacks and Defense*
CSE	Cyber Attacks and Defense*
IDS	Network Security*
NSF	Network Security*
SPP	Cyber Attacks and Defense*
WAS	Cyber Attacks and Defense*
WSN	Network Security*

Module 1. Security Fundamentals
• Submodule 1: Security Concepts and Principles • Submodule 2: Security Management • Submodule 3: The Cybersecurity Profession and Careers
Module 2. Security Threats and Countermeasures
• Submodule 1: Security Threats • Submodule 2: Cyber Crimes • Submodule 3: Countermeasures • Submodule 4: Safeguard the IT Infrastructure • Submodule 5: Introduction to Cryptography
Module 3. Network Security
• Submodule 1: Networking basics • Submodule 2: Network Protocols • Submodule 3: Network Administration Basics • Submodule 4: Network Security Basics
Module 4. Software Security
• Submodule 1: Software Vulnerabilities and Security • Submodule 2: Low-level Attacks and Defense • Submodule 3: Secure Programming • Submodule 4: Web-based System Security
Module 5. Cloud Security
• Submodule 1: Cloud Computing Fundamentals • Submodule 2: Cloud Security Basics

Cybersecurity in UHCL Computing

Course Number	Course Title	Offering/Notes
CSCI/CINF 4323	Computer Security	Offered annually
CSCI 5235	Network Security	Offered annually
CSCI 4391-1*	Cyber Attacks and Defense	Initially offered in Fall 2018
CSCI 4391-2*	Network Defense	Initially offered in Spring 2019
CSCI 4391-3*	Network Forensics	To be offered in Fall 2019
ITEC 2381	Forensic Fundamentals	Offered annually
ITEC 3388	Cybersecurity I	Offered annually
ITEC 4383	Cybersecurity II	Offered annually
ITEC 4366	Computer Security and Disaster Recovery	Offered annually
ITEC 4381	Computer Forensics	Offered annually
ITEC 4382	Registry & Internet Forensics	Offered as needed

Integration into Existing CS Curriculum



So Far…

- New course development:
  - Cyber Attacks and Defense: offered in Fall 2018
  - Network Defense: offered in Spring 2019
  - Network Forensics: plan to offer in Fall 2019
- Continuous assessment

Lessons Learned

- The learning curve could be steep.
- It is not always easy to overcome resource constraints.
- Administrative support and faculty buy-in are essential.