ACM Cybersecurity Curriculum Guidelines Mapping to CAE Knowledge Units

CAE Symposium 2019, Phoenix, AZ
November 21, 2019
Presenter: Cara Tang

Cara Tang, Portland Community College, OR
Cindy Tucker, Bluegrass Community & Tech. College, KY
Christian Servin, El Paso Community College, TX
Markus Geissler, Cosumnes River College, CA
Melissa Stange, Lord Fairfax Community College, VA

Outline

- ➔ ACM Cybersecurity Curricular Guidelines
  - ◆ CSEC2017
  - ◆ Cyber2yr2020
- ➔ Cyber2yr - CAE KU Mapping

ACM Cybersecurity Curricular Guidelines

ACM Curriculum Guidelines for Undergraduate 4-Year Programs

www.acm.org/education

- Computer Engineering – CE2016
- Computer Science – CS2013
- Information Systems – IS2010
- Information Technology – IT2017
- Software Engineering – SE2014
- **Cybersecurity – CSEC2017**

Under Development

- Data Science

CSEC2017

cybered.acm.org

Vision: *The CSEC2017 curricular volume will be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level.*

Organization

- Knowledge areas, knowledge units, topics
- Cross-cutting concepts - C, I, A, risk, ...
- Disciplinary lenses

CYBERSECURITY CURRICULA 2017

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity

A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education

Association for Computing Machinery

- Association for Computing Machinery (ACM)
- IEEE Computer Society (IEEE-CS)
- Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC)
- International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

Version 1.0 Report
31 December 2017

ACM Curriculum Guidelines for 2-Year Programs

ccecc.acm.org

- Information Technology - IT2yr2014
- Computer Science - CSTransfer2017

Under Development

- **Cybersecurity - Cyber2yr2020 - to be published Jan 2020**
- IT Transfer

acm CCECC Committee for Computing Education in Community Colleges

ACM CCECC Global Mission
Serve and support community and technical college educators in all aspects of computing education

Cyber2yr Task Group

Cara Tang* | Portland Community College, Portland, OR

Cindy Tucker* | Bluegrass Community and Technical College, Lexington, KY

Christian Servin* | El Paso Community College, El Paso, TX

Markus Geissler* | Cosumnes River College, Sacramento, CA

Melissa Stange* | Lord Fairfax Community College, Middletown, VA

Nancy Jones | Coastline Community College, Garden Grove, CA

James Kolasa | Bluegrass Community and Technical College, Lexington, KY

Amelia Phillips | Highline College, Des Moines, WA

Lambros Piskopos | Wilbur Wright College, Chicago, IL

Pam Schmelz | Ivy Tech Community College, Columbus, IN

* Steering Committee

Cyber2yr Advisors

Antonio Bologna | Rapid 7

Elizabeth Hawthorne | Union County College

Phil Helsel | Microsoft

Sidd Kaza | Towson University

Sepehr (Sepi) Hejazi Moghadam | Google

Bill Newhouse | NICE (National Initiative for Cybersecurity Education)

Casey O’Brien | National CyberWatch Center

Allen Parrish | Mississippi State University

John Sands | Moraine Valley Community College, CSSIA

Brian Ventura | SANS Instructor

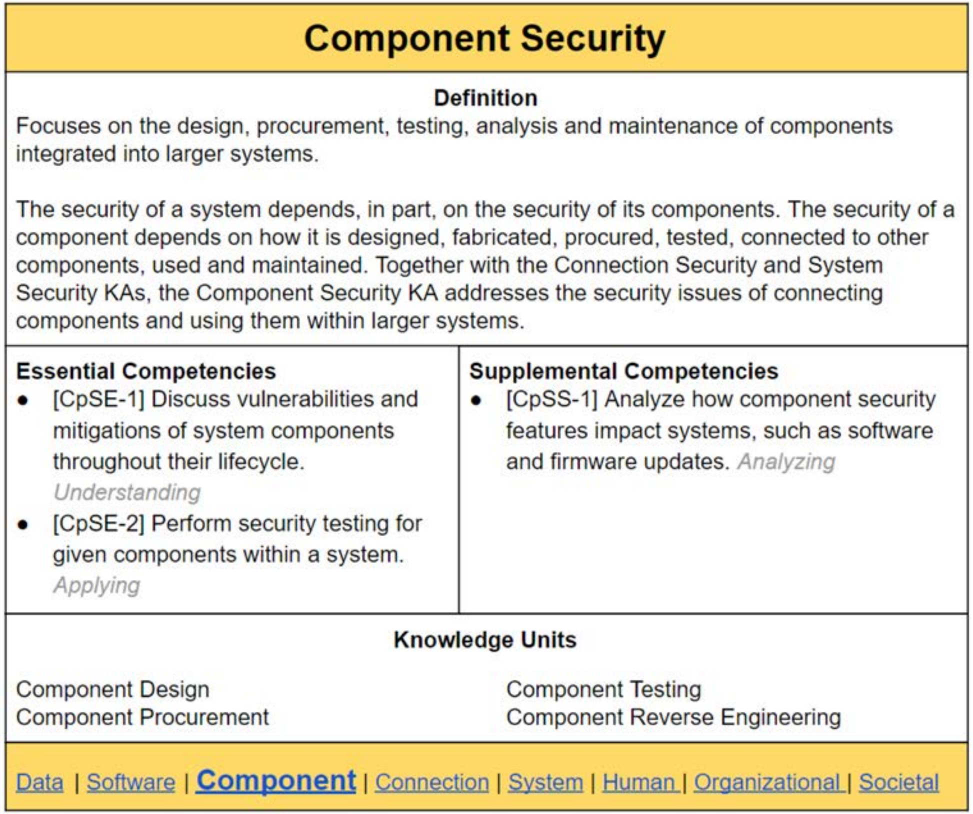
Cyber2yr Project

- Curriculum guidelines for associate degree programs (2 years)
- Main influences:
  - ACM CSEC2017
  - **CAE knowledge units (KUs) - 2019 Foundational + Technical Core**
  - NICE Cybersecurity Workforce Framework
- Competencies (high-level) and learning outcomes (more detailed) instead of topics
- Focus on **student achievement**
- Use Bloom’s Revised Taxonomy

Cyber2yr Curricular Framework Structure

- Cross-Cutting Competencies
- **Data** Security Competencies - Essential and Supplemental
    - Knowledge Units
    - Learning Outcomes - Essential and Supplemental
- **Software** Security
- **Component** Security
- **Connection** Security
- **System** Security
- **Human** Security
- **Organizational** Security
- **Societal** Security

Sample Knowledge Area



Component Security

Definition

Focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems.

The security of a system depends, in part, on the security of its components. The security of a component depends on how it is designed, fabricated, procured, tested, connected to other components, used and maintained. Together with the Connection Security and System Security KAs, the Component Security KA addresses the security issues of connecting components and using them within larger systems.

Essential Competencies

- [CpSE-1] Discuss vulnerabilities and mitigations of system components throughout their lifecycle. *Understanding*
- [CpSE-2] Perform security testing for given components within a system. *Applying*

Supplemental Competencies

- [CpSS-1] Analyze how component security features impact systems, such as software and firmware updates. *Analyzing*

Knowledge Units

Component Design
Component Procurement

Component Testing
Component Reverse Engineering

Data | Software | **Component** | Connection | System | Human | Organizational | Societal

Cyber2yr - CAE KU Mapping

Mapped to CAE KUs

Foundational Core

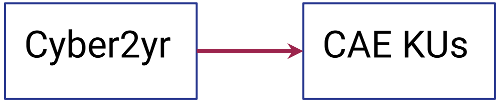
- CSF - Cybersecurity Foundations
- CSP - Cybersecurity Principles
- ISC - IT Systems Components

Technical Core

- BCY - Basic Cryptography
- BNW - Basic Networking
- BSP - Basic Scripting and Programming
- NDF - Network Defense
- OSC - Operating Systems

100% of CAE KU Outcomes and Topics map to Cyber2yr competencies and/or learning outcomes

Mapping - Cross-Cutting Concepts



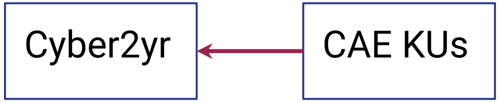
Cyber2yr Cross-Cutting Competency:

- [CC-1] Outline via appropriate methods, and using industry standard terminology, cybersecurity-related issues within an organization as they pertain to Confidentiality, Integrity, and Availability.

CAE KU: **Cybersecurity Foundations** (CSF)

- **Outcome 1**: Describe the fundamental concepts of the cybersecurity discipline and use to provide system security.
- **Outcome 5**: Properly use the vocabulary associated with cybersecurity.
- **Topic 10**: Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy.

Mapping - Network Defense (NDF)



CAE KU: Network Defense (NDF)

- Topic 1c: Outline concepts of network defense, such as … (c) Network Hardening

Cyber2yr:

- **Connection Security**
  - **Competency**: [CnSS-3] Implement appropriate defenses throughout an enterprise to harden the network against attackers.
  - **Learning Outcome**: Implement configuration settings on devices throughout an enterprise to harden the network against attackers.
- **Organizational Security Learning Outcome**: Implement hardening techniques to protect the operating system.

Cyber2yr2020

acm CCECC
Committee for Computing
Education in Community Colleges

Final version to be published January 2020

IronDog Draft available now at ccecc.acm.org

Cyber2yr - CAE mapping to be published January 2020

Draft available now by emailing cara.tang@pcc.edu

ccecc.acm.org