Cybersecurity Curricular Guidelines

Matt Bishop, University of California Davis, co-chair
Diana Burley The George Washington University, co-chair
Scott Buck, Intel Corp.
Joseph J. Ekstrom, Brigham Young University
Lynn Futcher, Nelson Mandela Metropolitan University
David Gibson, United States Air Force Academy
Elizabeth K. Hawthorne, Union County College
Siddharth Kaza, Towson University
Yair Levy, Nova Southeastern University
Herbert Mattord, Kennesaw State University
Allen Parrish, United States Naval Academy

Background

- What should a "cybersecurity professional" know and what skills should they have?
- Disagreement due to nature of cybersecurity
  - Used in many different roles
  - Encompasses many disciplines
- Indeed, many different definitions of cybersecurity

Joint Task Force

- Assembled by ACM, IEEE_Computer Society, AIG Special Interest Group on Security, IFIP WG 11.8
- Goal: to develop cybersecurity curricular guidelines for undergraduate programs that emphasize different areas of specialization
  - Not curriculum development!
  - Institutions can use it as a basis for developing curricula, certification requirements, though

What Is Cybersecurity?

"A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries."

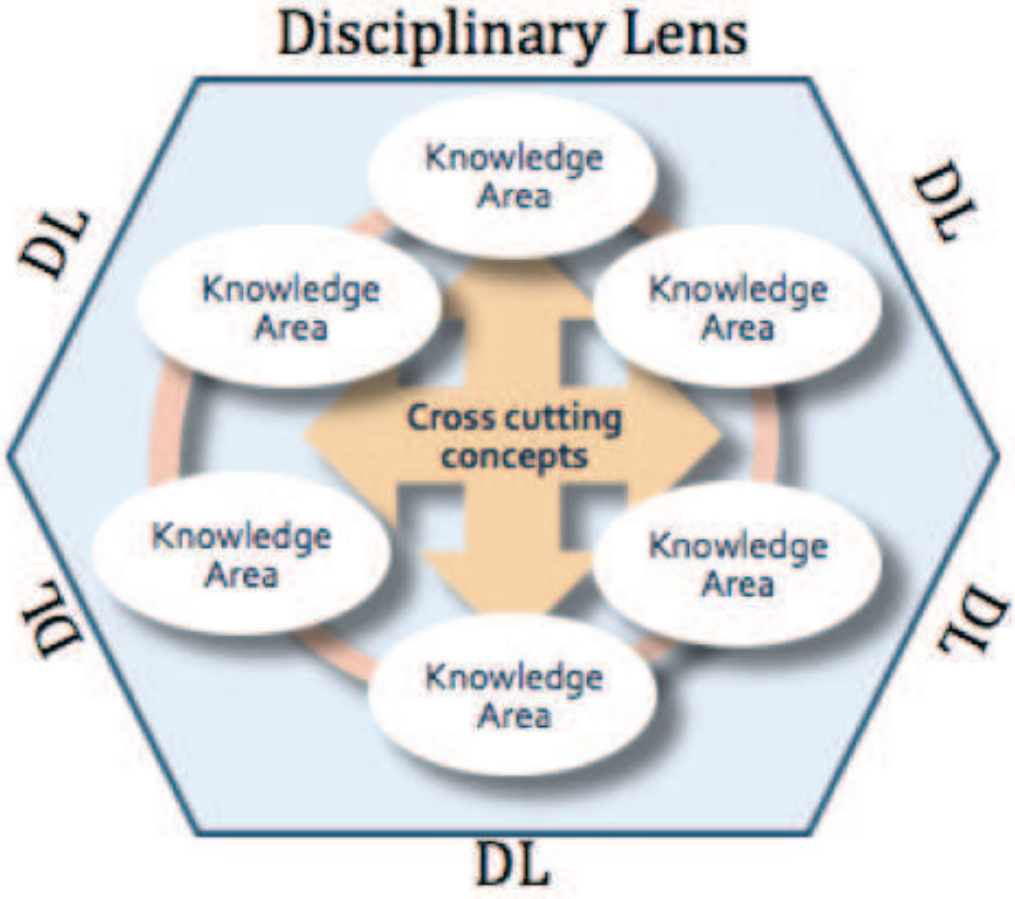
— CSEC 2017 report, p. 10

Bases for Guidelines

Cybersecurity education programs should:

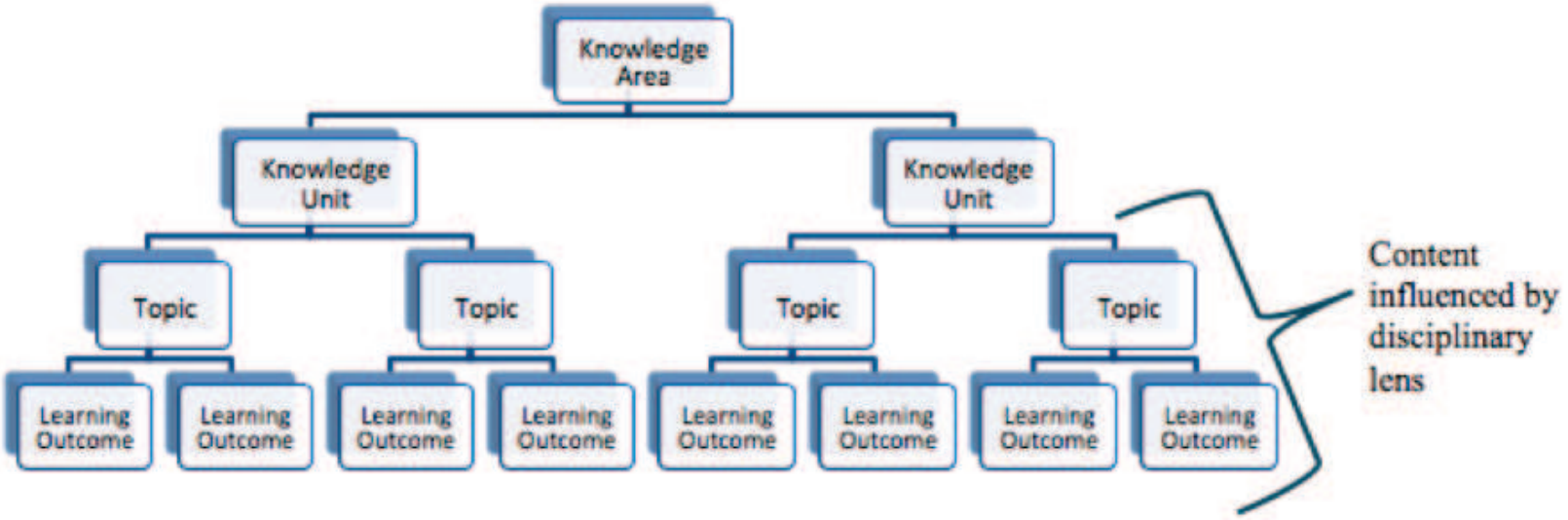
- Be based on core knowledge and skills;
- Have a computing-based foundation
- Teach concepts applicable to a broad range of cybersecurity expertise;
- Emphasize ethical obligations and responsibilities; and
- Be flexible so programs can tailor their curriculum to any specialized needs

The Model


Disciplinary Lens
DL
DL
DL
DL
DL
Knowledge Area
Knowledge Area
Knowledge Area
Knowledge Area
Knowledge Area
Knowledge Area
Cross cutting concepts

Knowledge Areas

- The subject matter of cybersecurity
- Each KA composed of Knowledge Units
  - These describe the set of topics and what students should know about them

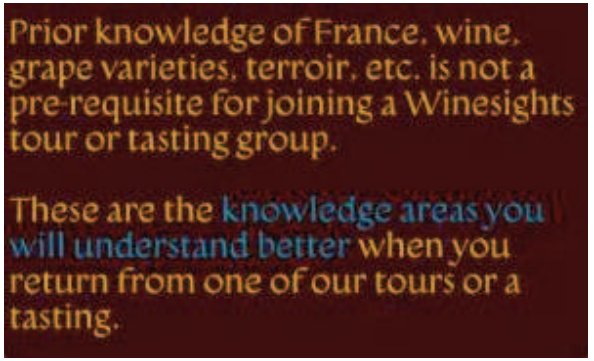


Knowledge Areas

- KAs meet 3 criteria:
  1. The area is important for multiple disciplines;
  2. The area provides a tool for understanding or exploring cybersecurity ideas; and
  3. The material in the area can be learned in varying levels of detail and understanding over time.

The Knowledge Areas

- Data Security
- Software Security
- System Security
- Human Security
- Organizational Security
- Societal Security



Overlap

Note a Knowledge Unit may be put into more than one KA

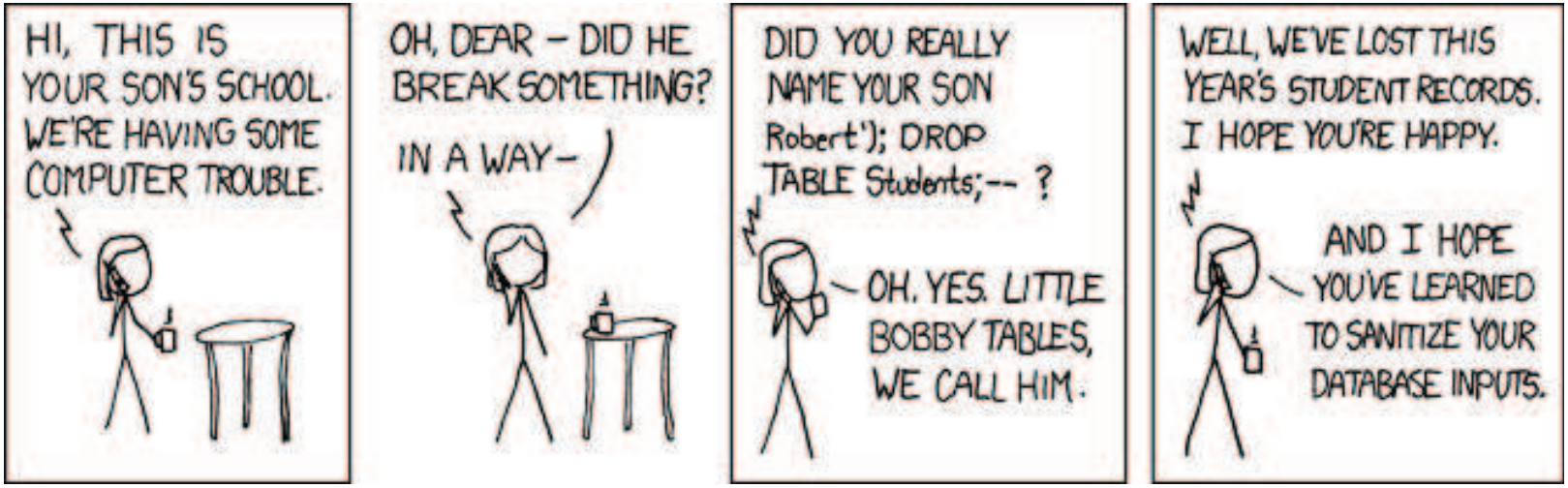
Example: design of a library that grabs and processes packets

- Software security KA: assurance question is how packets are protected and properly read
- System security KA: composition of components, as library interface ties network to system

Example: Software Security

CSEC2017 Knowledge Units:

- Fundamental design principles
- Practice
- Documentation



Example: Software Security

Original (in CSEC2017 Draft)

- KU: fundamental design principles
  - Separation (of domains)
  - Isolation
  - Encapsulation
  - Least Privilege
  - Simplicity (of design)
  - Minimization (of implementation)
  - Fail Safe Defaults Fail Secure
  - Modularity
  - Layering
  - Least Astonishment
  - Open Design
  - Usability
  - End-to-End Security
  - Defense in Depth

Working Group Modifications

- KU: fundamental design principles

  Simplicity principles:
  - Economy of mechanism
  - Minimize shared mechanisms
  - Least astonishment

  Restrictive principles:
  - Least privilege
  - Fail-safe defaults
  - Complete mediation
  - Separation
  - Minimize trust

  Methodology principles:
  - Open design
  - Layering
  - Abstraction
  - Complete linkage
  - Design for iteration

Example: Topic Validation

Mapped against a number of widely accepted lists of software problems

- Avoiding the Top 10 Software Security Design Flaws: IEEE Cyber Security
- OWASP Top 10 Most Critical Web Application Security Risks

Example: Data Security KA

Knowledge Units:

- Cryptography
- Digital Forensics
- Data Integrity and Authentication
- Access Control
- Secure Communication Protocols
- Cryptanalysis
- Privacy
- Information Storage Security

Example: Cryptography (KU) Topics

Cryptography		
	Basic concepts	**Description:** • Encryption/decryption, sender authentication, data integrity, non-repudiation • Attack classification (ciphertext-only, known plaintext, chosen plaintext, chosen ciphertext) • Secret key (symmetric), cryptography and public-key (asymmetric) cryptography • Information-theoretic security (one-time pad, Shannon Theorem) • Computational security

	Advanced Concepts	**Description:**
		• Advanced protocols
		  ○ zero-knowledge proofs, and protocols
		  ○ secret sharing
		  ○ commitment
		  ○ oblivious transfer
		  ○ secure multi-party computation
		• Advanced recent developments: fully homomorphic encryption, obfuscation, quantum cryptography

Cross-Cutting Concepts

- Framework for making connections among KAs, unifying underlying ideas
- Fundamental to students' abilities to understand core ideas through any disciplinary lens
- They span most, if not all, of the KAs

The Concepts

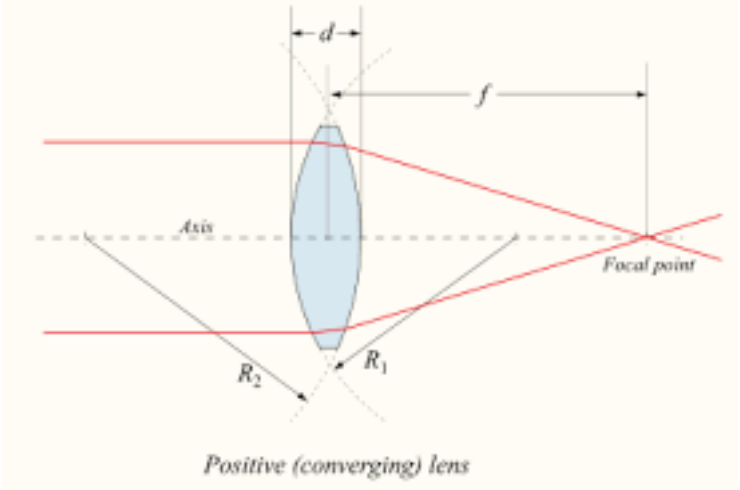
- Confidentiality: property defined by rules controlling spread of information
- Why?
  - Key component of data security, systems security, organizational security
  - Also component of human security in guise of privacy
  - And societal security from the combination of all these

The Concepts

- Integrity
  - Key component: assurance
- Availability
  - Accessibility not enough; must meet any stated QoS
- Risk
  - Function of probability of threat being realized and damage incurred should this happen
- Adversarial Thinking
  - Requires understanding what threats will compromise entity, how to make them happen

Disciplinary Lens

- KAs are common to all cybersecurity
- Depth, approach that folks are expected to know varies depending on how they will use that knowledge
- We use ACM disciplines



The Disciplines

- Computer Science
- Computer Engineering
- Information Systems
- Information Technology
- Software Engineering
- Mixed Disciplinary

Guidelines and Professional Practice

- Linked through seven application areas
- Workforce frameworks can codify their bodies of knowledge by going from the application areas back to the model
  - Then extract both core knowledge, cross-cutting concepts they find appropriate
  - View them through the appropriate disciplinary lens
- These areas allow the definition of competency levels for each area

Application Areas

- Public policy
- Procurement
- Management
- IT security operations
- Software development
- Enterprise architecture
- Research

Conclusion

- CSEC2017 is a *basis* for curricula, and is ***not*** itself a curriculum
- CSEC2017 still under development
  - 15 community engagement efforts so far
  - 6 working groups composed of experts *not* on the task force
  - Global surveys of cybersecurity experts and educators
  - Web site for submitting comments is

    http://www.csec2017.org

Acknowledgements

Based upon work funded by the following:

- National Science Foundation Grant No. DGE-1623104
- National Security Agency's CNAP Curriculum Development Effort (RFI-2017-00022)
- ACM Education Board
- Intel Corporation

We thank them for their support

And we thank all those who have been involved, and will be involved, in the KA working groups

Web Site

https://www.csec2017.org/

- Current version is Draft 0.75, released ***yesterday!!!!!***
- Comment period open until July 3
  - Then we revise it …

A Contrarian View

The future, according to some scientists, will be exactly like the past, only far more expensive

– John Sladek