

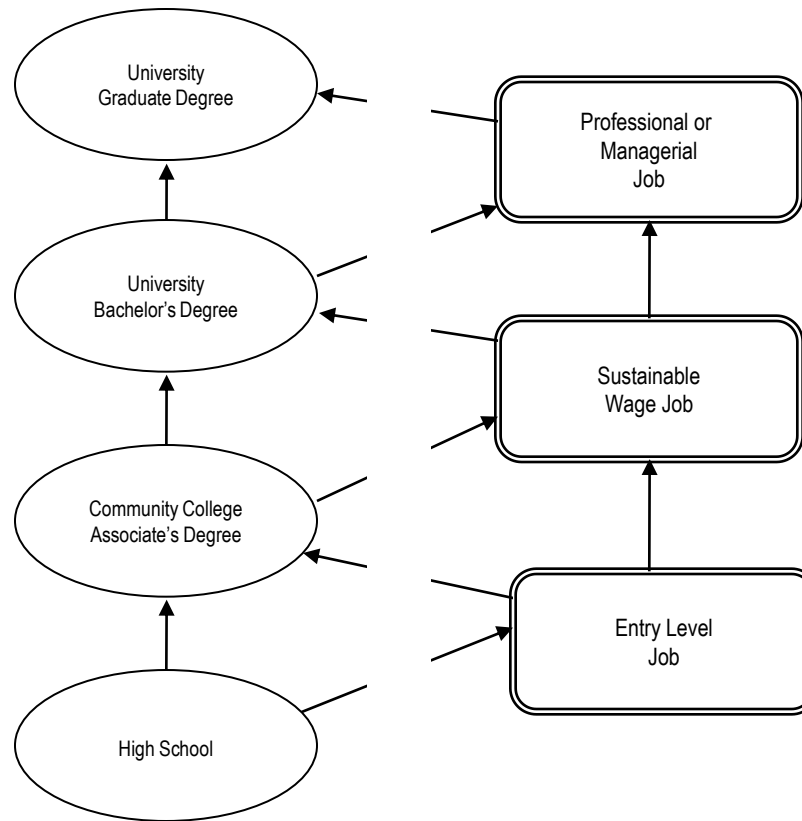


Boston Area Advanced Technological Education Connections (BATEC)





Our current education model:





BATEC Mission

BATEC is developing and supporting a coordinated, self-sustaining, regional it education and workforce system – one that will attract a diverse student population to it careers, promote lifelong learning of technical skills and support the it workforce needs of our region.

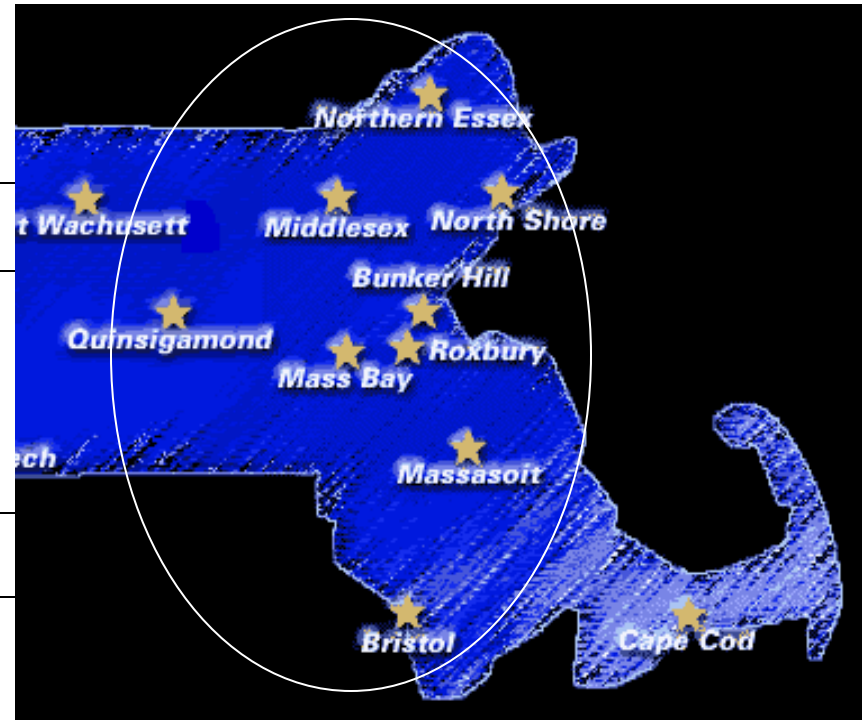


BATEC Service Area

Community Colleges

- Roxbury CC
- Bunker Hill CC
- Middlesex CC

- Quinsigamond CC
- Bristol CC
- Northern Essex CC





BATEC Vision

■ **Curriculum Development**

- Regionally Connected
- Advanced in Content and Pedagogy
- Industry-Linked

■ **Professional Development**

- High Quality
- Combination of Technology and Pedagogy
- Multiple Formats



BATEC Vision (cont.)

■ **Student Success**

- Informed decisions
- Holistic – Technical, Employability Skills, Leadership
- Connected to Industry

■ **Education, Industry and Community Connections**

- Mutually-Beneficial Partnerships
- Career Development
- Lifelong Learning
- Regional Economic Growth



Challenges We are Addressing

- Employment Market-driven enrollments
Perception that “IT is dead” = Falling enrollments
- IT Hybridization; IT Across Content Areas/Careers
- Traditionally autonomous education systems
- “Siloed” departments delivering student services
- Marketing of Schools/Programs
- Coordination, Collaboration, Communication...



Computing Accreditation and IT Curriculum





Overview

- Change in focus of ABET's accreditation standards for computing programs
- ACM's Computing Curricula Series
- Efforts to define a recommended IT curriculum for associate degree programs and to identify a means to accredit community colleges



Basic philosophy shift of ABET

- Formerly accreditation based on criterion and standards
 - A criterion described the underlying principles that **MUST** be met for a program to be eligible for accreditation
 - Standards provided one example of how the criteria can be met
- Current approach focuses on outcomes-oriented accreditation

CAC/ABET General Criteria



- There are criteria for:
 - Objectives, Outcomes and Assessment;
 - Students;
 - Faculty;
 - Curriculum;
 - Technology Infrastructure;
 - Institutional Support and Financial Resources;
 - Program Delivery;
 - Institutional Facilities.

Accreditation Assessment



- What is the program trying to do?
- How well is it doing it?
- How do you measure how well it is doing it?
- How do you use results to continuously improve?



Program Structure

- Outcomes & assessment must be embedded
- Objectives and outcomes
- Evaluation
 - Quantitative & qualitative
 - Assessment tools
- Feedback loop for continuous improvement
 - Not just for the visit (lifestyle change)
 - Annual reports on learning and continuous improvement
- Show a complete cycle

ACM Computing Curricula

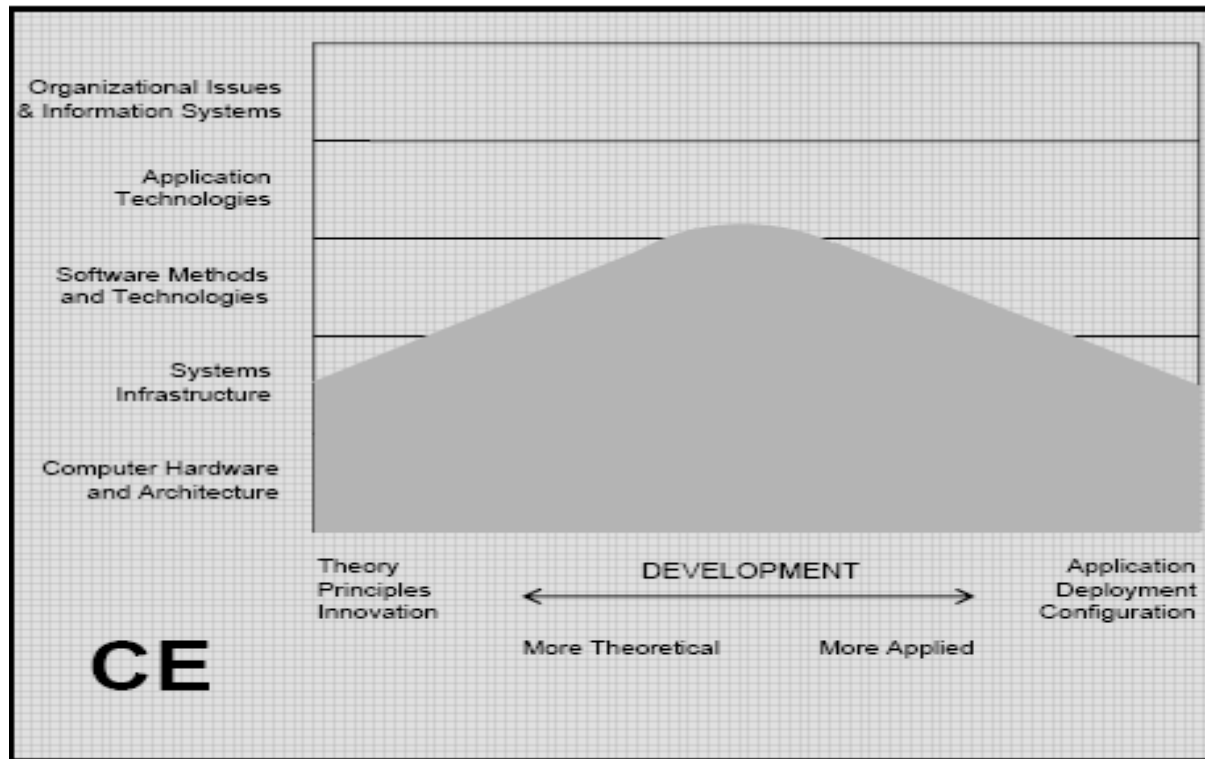
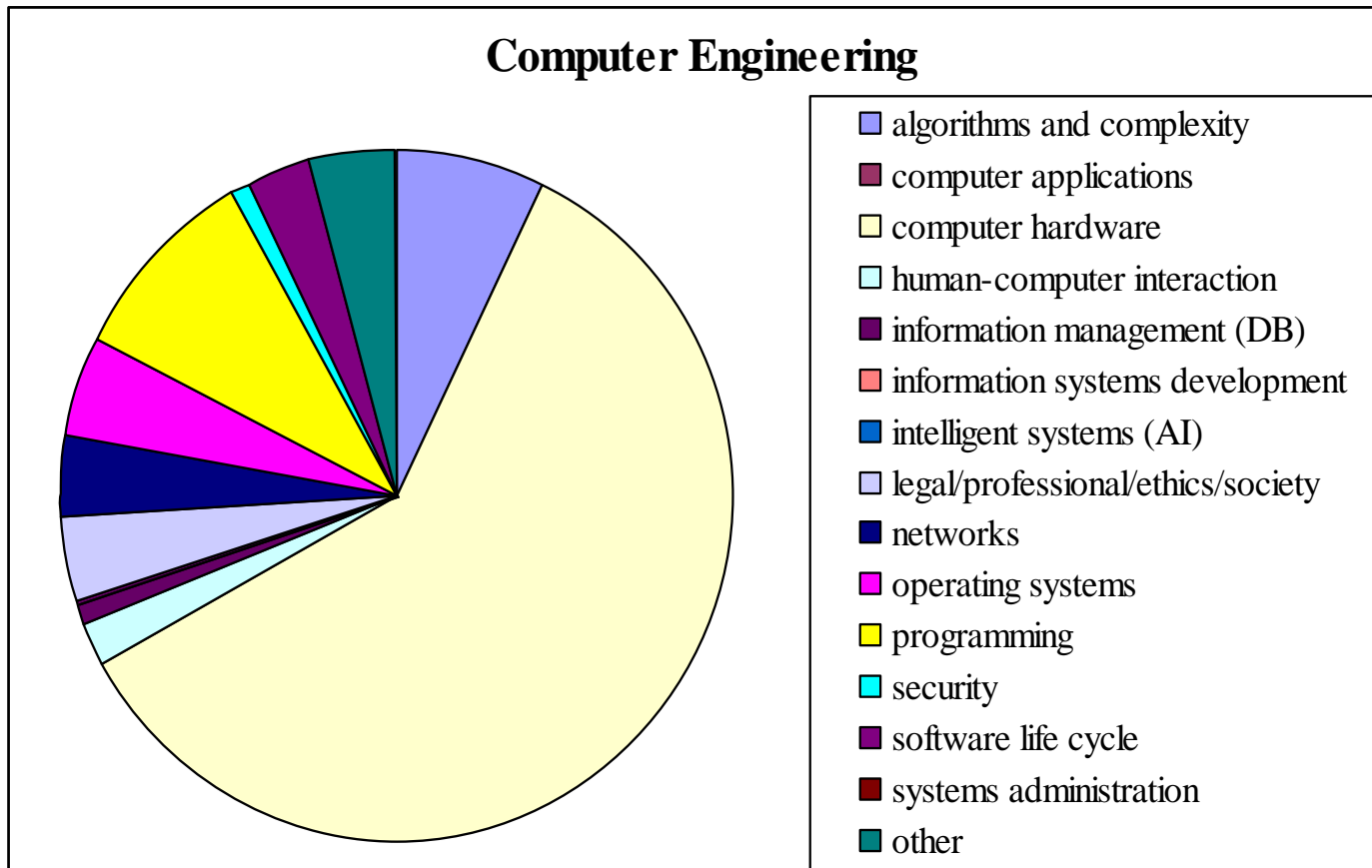


Figure 2.3. Computer Engineering



ACM Computing Curricula

Computer Engineering





ACM Computing Curricula

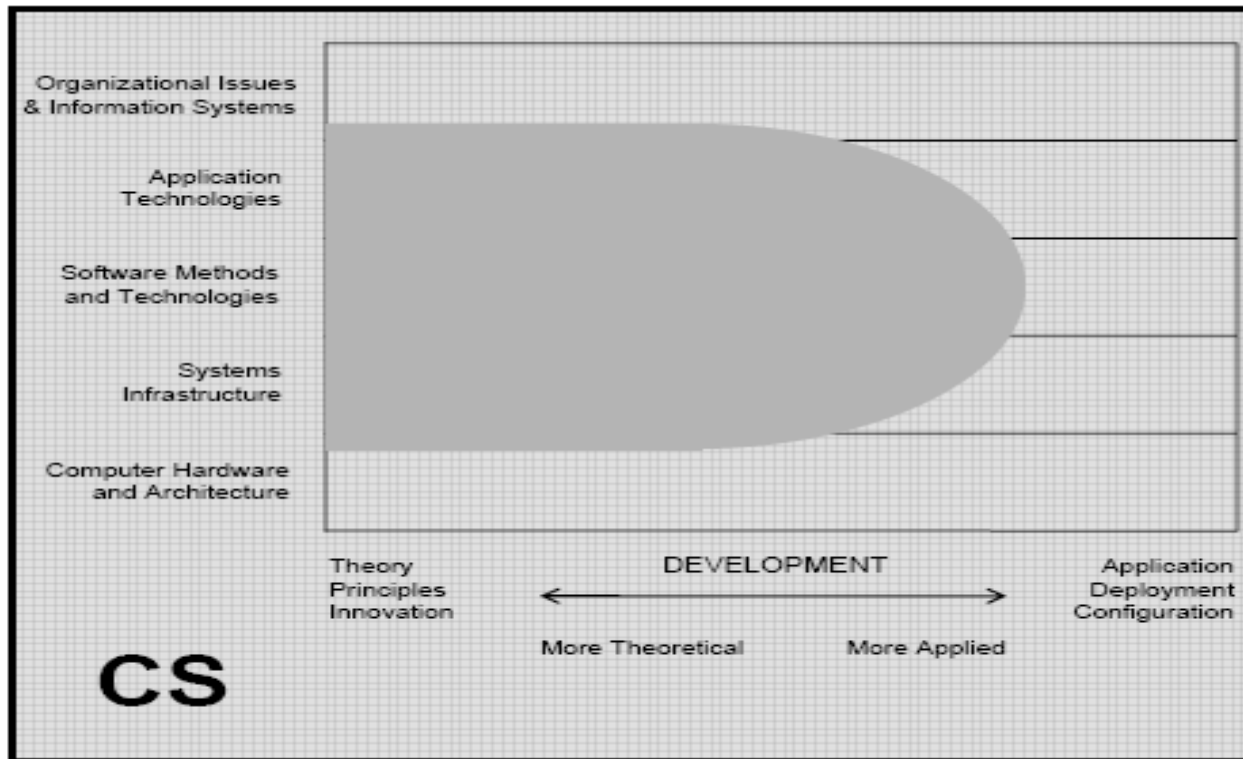
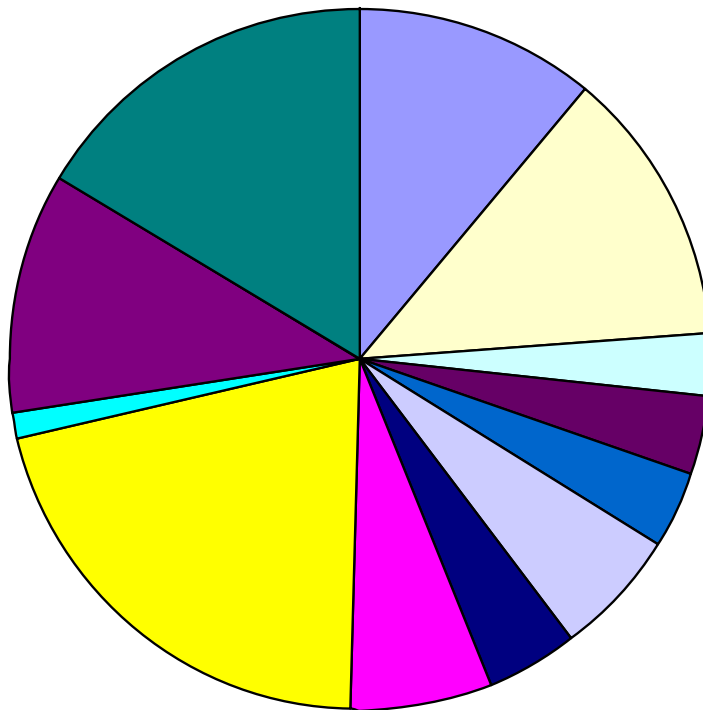


Figure 2.4. Computer Science



ACM Computing Curricula

Computer Science



- algorithms and complexity
- computer applications
- computer hardware
- human-computer interaction
- information management (DB)
- information systems development
- intelligent systems (AI)
- legal/professional/ethics/society
- networks
- operating systems
- programming
- security
- software life cycle
- systems administration
- other



ACM Computing Curricula

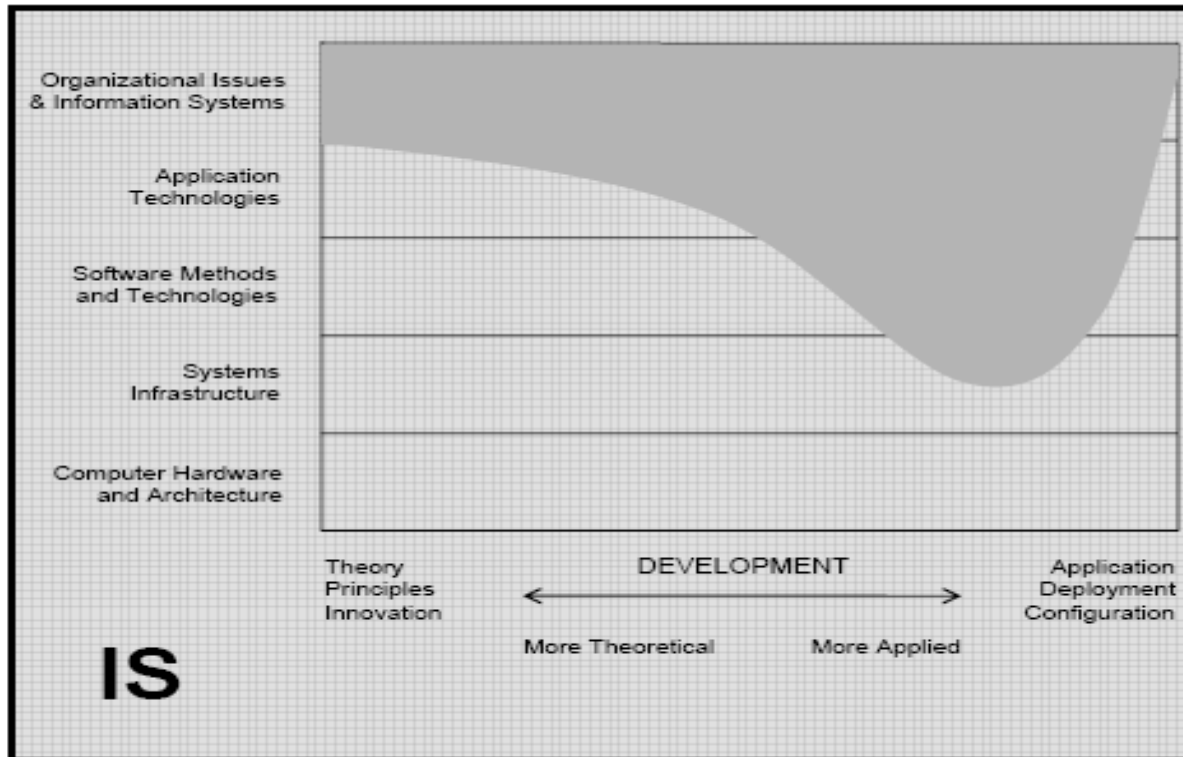
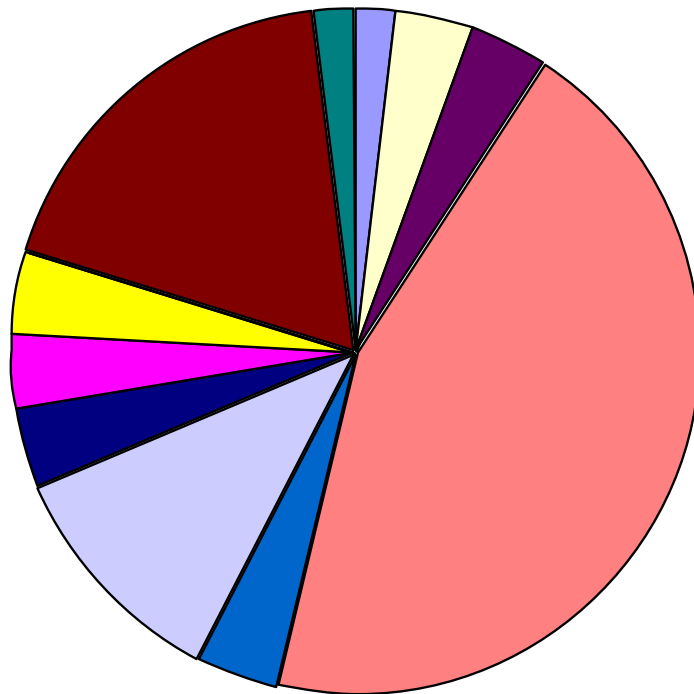


Figure 2.5. Information Systems



ACM Computing Curricula

Information Systems



- algorithms and complexity
- computer applications
- computer hardware
- human-computer interaction
- information management (DB)
- information systems development
- intelligent systems (AI)
- legal/professional/ethics/society
- networks
- operating systems
- programming
- security
- software life cycle
- systems administration
- other



ACM Computing Curricula

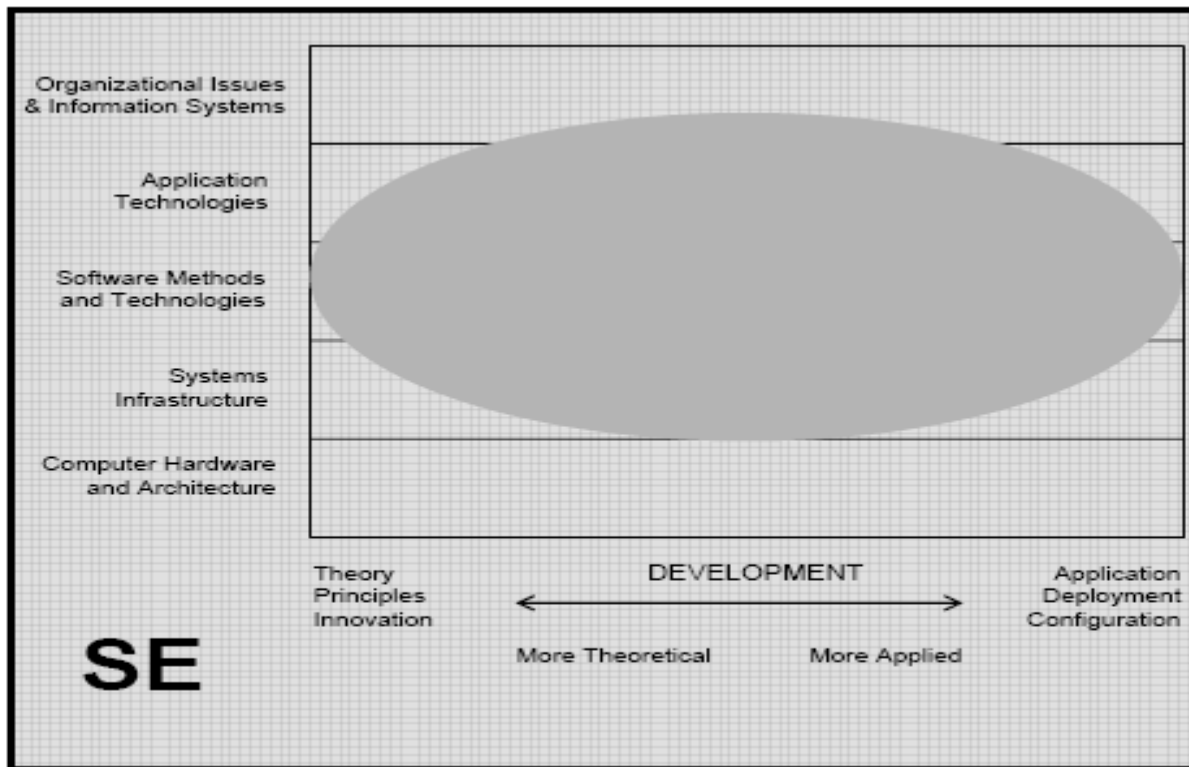
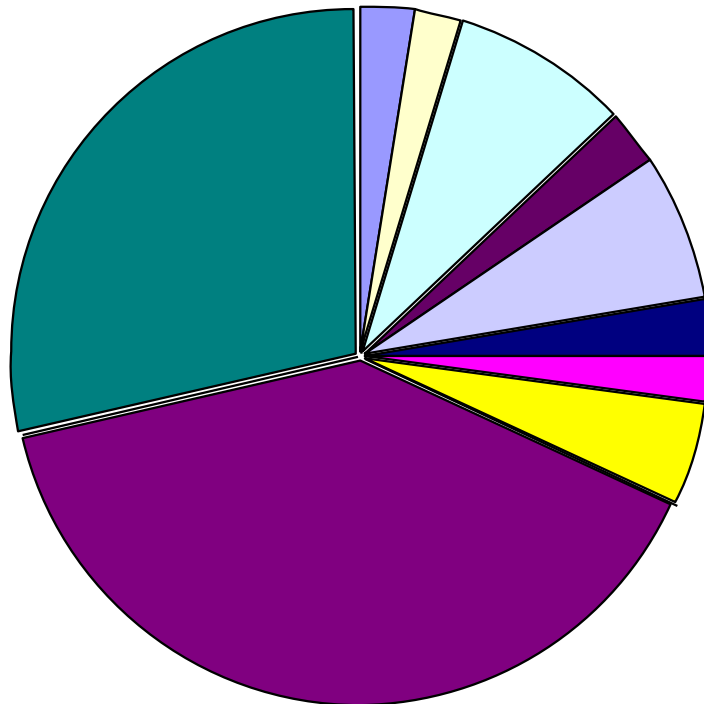


Figure 2.7. Software Engineering



ACM Computing Curricula

Software Engineering



- algorithms and complexity
- computer applications
- computer hardware
- human-computer interaction
- information management (DB)
- information systems development
- intelligent systems (AI)
- legal/professional/ethics/society
- networks
- operating systems
- programming
- security
- software life cycle
- systems administration
- other



ACM Computing Curricula

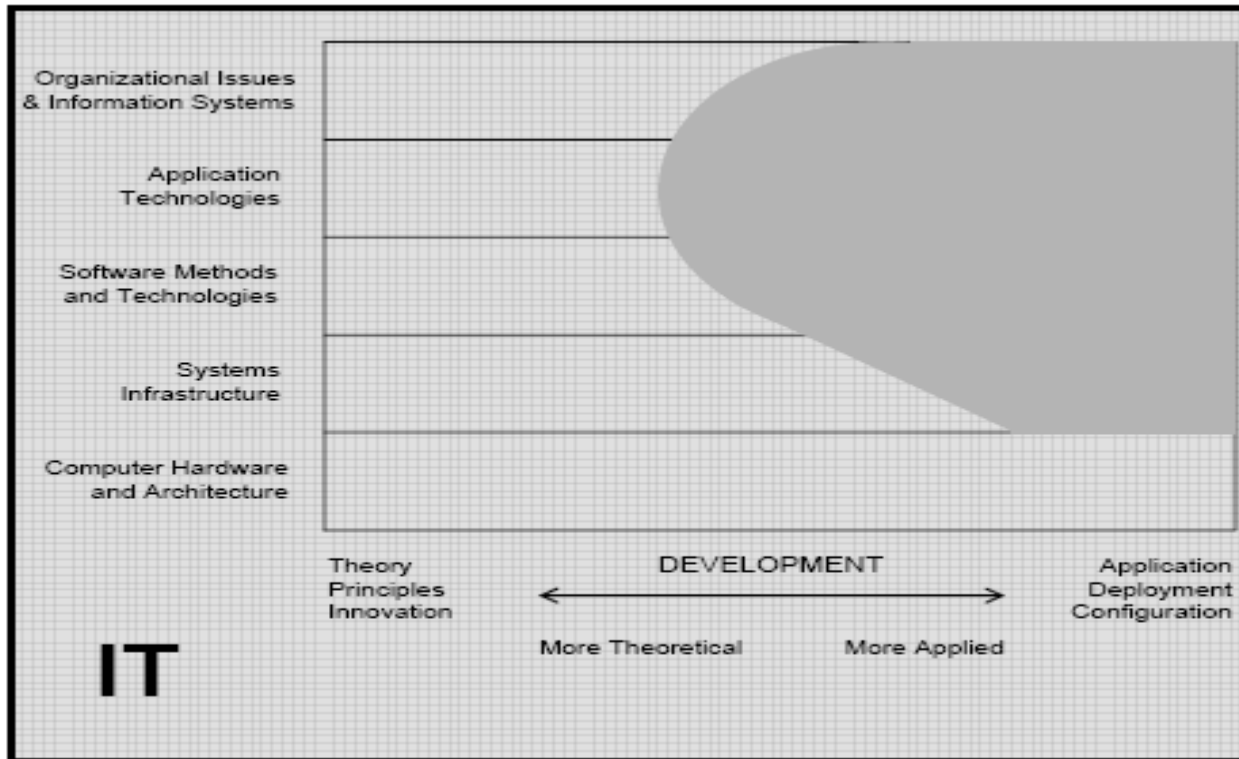
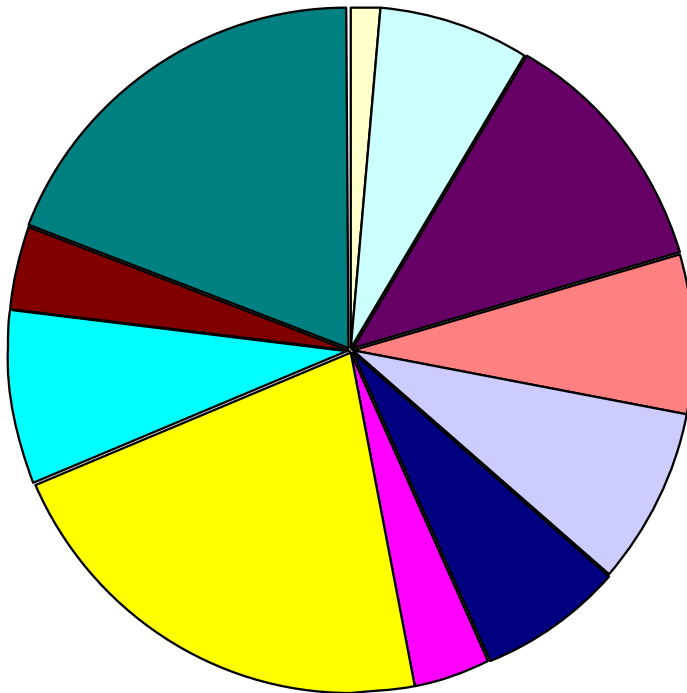


Figure 2.6. Information Technology



ACM Computing Curricula

Information Technology



- algorithms and complexity
- computer applications
- computer hardware
- human-computer interaction
- information management (DB)
- information systems development
- intelligent systems (AI)
- legal/professional/ethics/society
- networks
- operating systems
- programming
- security
- software life cycle
- systems administration
- other

IT Development



- IT Accreditation and curriculum evolved together
 - Goal was to develop an accreditable discipline for 4-year schools with ABET structure as framework
 - 2-year committee formed to help identify how to better create connections



4-Year IT Curriculum: Summary

- Same structure as CS document
- Central part: Body of Knowledge (BOK)
 - Twelve knowledge areas (KAs): **(blue = IT Pillar)**
 - IT Fundamentals
 - **Human-Computer Interaction**
 - **Information Assurance & Security**
 - Information Management
 - Integrative Programming & Technologies
 - Math and Statistics for IT
 - **Networking**
 - **Programming Fundamentals**
 - Platform Technologies
 - System Administration & Maintenance
 - System Integration & Architecture
 - Social & Professional Issues
 - **Web Systems & Technologies**

4-Year IT Curriculum: Body of Knowledge



- Each KA has core hours assigned
 - Core hours = lecture hour equivalent
- 314 Total Hours for 4-year; 212 for 2-year
 - For 3-semester-credit-hour courses:
 - Just under 7 courses
 - Does include math, but not other courses, such as technical communications, application domain (specialization), advanced courses
- CS has 280 in their BOK

SIGITE 2-Year Committee



SIGITE 2-Year Process



IAS2. Security Mechanisms (Countermeasures)					
1		X	X	X	
2		X	X	X	Explain 2 factor authentic
3		X	X	X	
4		X	X		
5		X	X		Remove: from perspectiv
6		X	X		Remove: eg...(y)
7		X	X	X	
8		X	X		
9		X	X	X	
10		X	X		
11					
12		X			Describe how pkc works
13					
14					
15					

SIGITE 2-Year Process



IAS2. Security Mechanisms (Countermeasures)				
1	X	X	X	
2	X	X	X	Explain 2 factor authentic
3	X	X	X	
4	X	X		
5	X	X		Remove: from perspectiv
6	X	X		Remove: eg...(y)
7	X	X	X	
8	X	X		
9	X	X	X	
10	X	X		
11				
12	X			Describe how pkc works
13				
14				
15				

SIGITE 2-Year Process



IAS2. Security Mechanisms (Countermeasures)				
1	X	X	X	
2	X	X	X	Explain 2 factor authentic
3	X	X	X	
4	X	X		
5	X	X		Remove: from perspectiv
6	X	X		Remove: eg...(y)
7	X	X	X	
8	X	X		
9	X	X	X	
10	X	X		
11				
12	X			Describe how pkc works
13				
14				
15				

SIGITE 2-Year Process (cont.)



IAS2. Security Mechanisms (Countermeasures)		
1. Describe the three key factors involved in authentication and how they are used to verify identity and grant access to a system.	X	
2. Explain the process and value of two-factor authentication.	X	Explain 2 factor authentication (y)
3. Describe the characteristics of an effective password.	X	
4. Describe and compare physical access control to logical access control.	X	Define physical access control and logical access control
5. Identify the key types of biometric information utilized in authentication from the perspectives of accuracy, intrusiveness and efficiency.	X	Remove: from perspective...(y)
6. Describe the differences between symmetric and asymmetric cryptosystems, e.g., number of keys required, the types of algorithms used, etc.	X	Define symmetric/asymmetric
7. Explain what is meant by integrity, confidentiality, and authentication.	X	Add non-repudiation
8. Describe how cryptosystems offer 1) Confidentiality, and 2) Authentication		
9. Describe digital signatures and certificates	X	
10. Describe how a public key infrastructure (PKI) works	X	Reword as introductory
11. Describe the DES and 3DES algorithms		
12. Demonstrate how public-key cryptography works by the use of public and private keys		
13. Describe the AES algorithm		
14. Describe the differences between block and		

SIGITE 2-Year Process (cont.)



IAS2. Security Mechanisms (Countermeasures)

Minimum core coverage time: 5 hours

Topics:

Cryptography

Cryptosystems

Keys: symmetric & asymmetric

Performance (software/hardware)

Implementation

Authentication

Three key factors: "Who you are, what you have, what you know"

Bio-authentication (use of biometrics)

Two-factor authentication

Core learning outcomes

1. Describe the three key factors involved in authentication and how they are used to verify identity and grant access to a system.
2. Explain the process and value of two-factor authentication.
3. Describe the characteristics of an effective password.
4. Describe and compare physical access control to logical access control.
5. Identify the key types of biometric information utilized in authentication.
6. Describe the differences between symmetric and asymmetric cryptosystems.
7. Define integrity, confidentiality, authentication and non-repudiation.
9. Describe digital signatures and certificates.
10. Define public key infrastructure (PKI).

Elective learning outcomes:

1. Describe the single sign-on authentication process and problems related to using and implementing this technology.
2. Compare key access control and authentication mechanisms (Kerberos, RAS, etc.).
3. Compare the advantages and disadvantages of centralized access controls to decentralized access controls.



Contact Information

- Deborah Boisvert,
deborah.boisvert@umb.edu