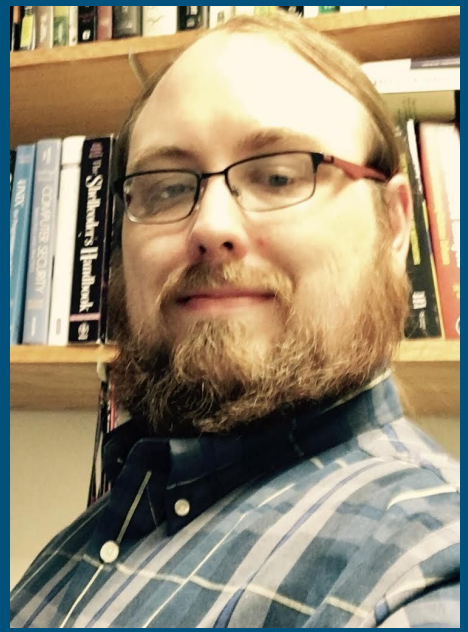
What They're Teaching Kids These Days

Comparing Security Curricula and Accreditations to Industry Needs

Who Are We: Robiam



Rob Olson

Chaim Sanders

- Background
  - Professors at RIT
  - Part of CSec Curriculum Committee
- Interests
  - Web App Sec
  - Education

* The views expressed are our own

RIT TIGERS

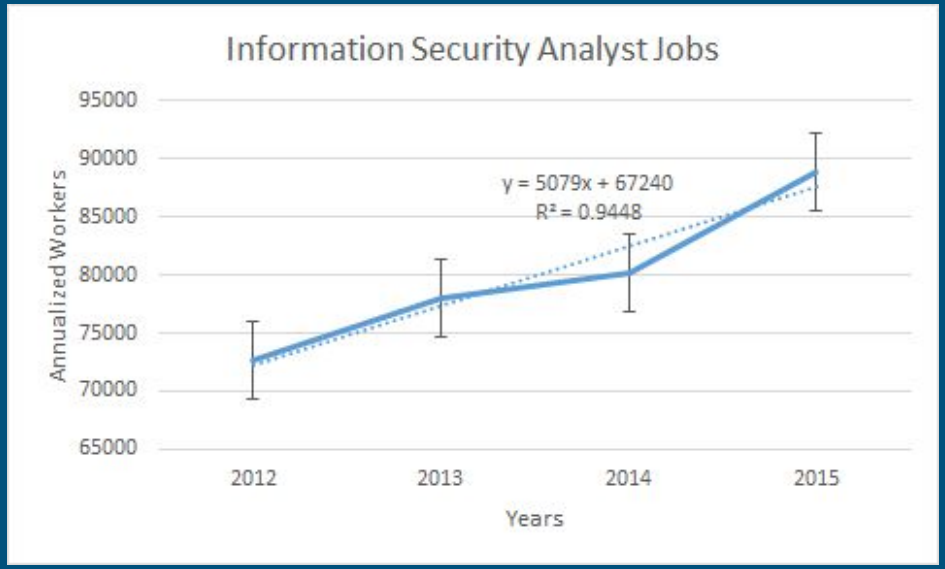
ZEROFOX

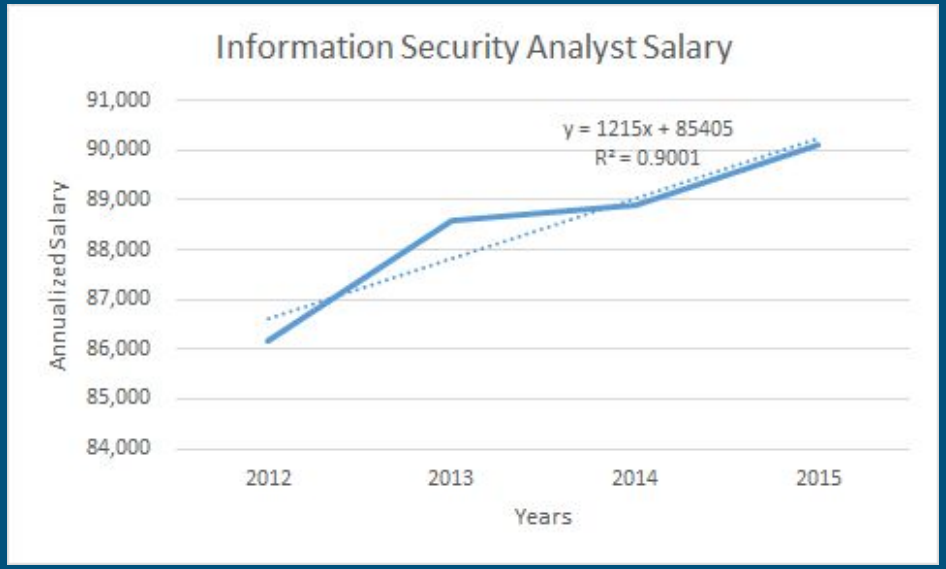
Introduction - Research Questions

- How do universities decide where/if to teach security topics?
- How do universities decide which security topics to cover?
- How/If will cybersecurity education become standardized?
- How do curricula/accreditations map to job functions?
  - Is there a mapping?
  - How does this affect your business and hiring process?

Overview

- Q: Why do we even care about education?
- A: It appears we have a solidly growing field
  - Where do these new workers get their education?





* Bureau of labor and statistics

Wait....

- If that seems low, that's probably because it is.
  - For example - 20,000 people have attended Blackhat/Defcon
- Available data varies greatly

	Currently Employed USA	Jobs Available USA	Currently Employed Global	Jobs Available Global
Cyberseek	779,402	348,975	X	X
Cisco	X	X	X	>1,000,000
Peninsula Press	X	209,000	X	X
CSO Online	X	X	6,000,000*	1,500,000*
Frost and Sullivan	1,692,000	389,000	4,007,000	901,000

* Indicates values predicted for 2019

Education only goes so far...

Upper Echelon Schools*:

- University Central Florida
- Rochester Institute of Technology
- Northeastern University
- Brigham Young University
- University of Maryland
- University of Texas: SA

RIT Numbers:

- ~120 new students per year
- ~90 graduates per year

Other School Numbers:

- ??????

* - There is no current comparative criteria for evaluating school security programs

The sum of all fears

- Let's assume 3 out of 4 students graduate
  - Switching majors, Dropping out, etc
- There are **~137* four year schools** with information security programs
- Now let's assume the max **~90 students** graduate per year per school
- At MOST the US is producing **12,330 CSec students** each year (unrealistic)

- If we assume there are **1,128,377** (CyberSeek) total security jobs
  - With the average employee's career being **40 years** (1,128,377/40)
- We need to be producing **28,209 students** - we're not
- Clearly we need to do the absolute BEST with the students we have…
  - How do we do that?

* CAE-CD Accredited Institutions

Outline

- Current Solutions
  - Academic Curriculum
    - Computer Science
    - Information Technology
    - Information Systems
  - Accreditation(ish)
    - ABET
    - NSA
- Upcoming Solutions
  - CSEC 2017
- Recommendations

2013 ACM Curriculum CS Recommendations (In instructional hours)

Knowledge Unit	T1	T2	Rank
Software Dev Fundamentals	43	0	1
Discrete Structures	37	4	2
Algorithms & Complexity	19	9	3
Programming Languages	8	20	4
Software Engineering	6	22	4
Systems Fundamentals	18	9	6
Arch. & Org	0	16	7
Social Issues/Prof. Practice	11	5	7
Operating Systems	4	11	9

Knowledge Unit	T1	T2	Rank
Parallel/Distributed Comp.	5	10	9
Info. Management (DB)	1	9	11
Intelligent Systems	0	10	11
Networking and Comms.	3	7	11
Info. Assurance/Security	3	6	14
HCI	4	4	15
Graphics/Visualization	2	1	16
Comp. Science	1	0	17
Platform-based Dev.	0	0	18

ACM Computer Science IAS KU Breakdown

IAS. Information Assurance and Security (3 Core-Tier1 hours, 6 Core-Tier2 hours)

	Core-Tier1 hours	Core-Tier2 hours	Includes Electives
IAS/Foundational Concepts in Security	1		N
IAS/Principles of Secure Design	1	1	N
IAS/Defensive Programming	1	1	Y
IAS/Threats and Attacks		1	N
IAS/Network Security		2	Y
IAS/Cryptography		1	N

ACM Elective Security Course Topic List

Topic	Inst. Hours
Machine-level representation of data	1
Human factors and security	3
Foundational Concepts	2
Principles of Secure Design	3
Defensive Programming	5
Threats and Attacks	2
Network Security	6
Cryptography	6
Web Security	4

Topic	Inst. Hours
Security Policy & Governance	2
Introduction (to Network Comm.)	.5
Networked Applications	1
Local Area Networks	.5
Security and Protection	1
Language Translation and Exec.	1
Security Policies, Laws, and Computer Crimes	1

ACM Curriculum Recommendations for IT

Knowledge Unit	Hrs	Rank
IT Fundamentals	25	4
HCI	20	11
Info. Assurance/Security	23	5
Information Management	34	3
Integrative Prog. & Tech.	23	5
Math and Statistics	38	1
Networking	22	8

Knowledge Unit	Hrs	Rank
Programming Fundamentals	38	1
Platform Technologies	14	12
Sys. Admin. & Maintenance	11	13
System Integration & Architecture	21	10
Social & Professional Issues	23	5
Web Systems and Tech.	22	8

ACM Curriculum Recommendations for IS

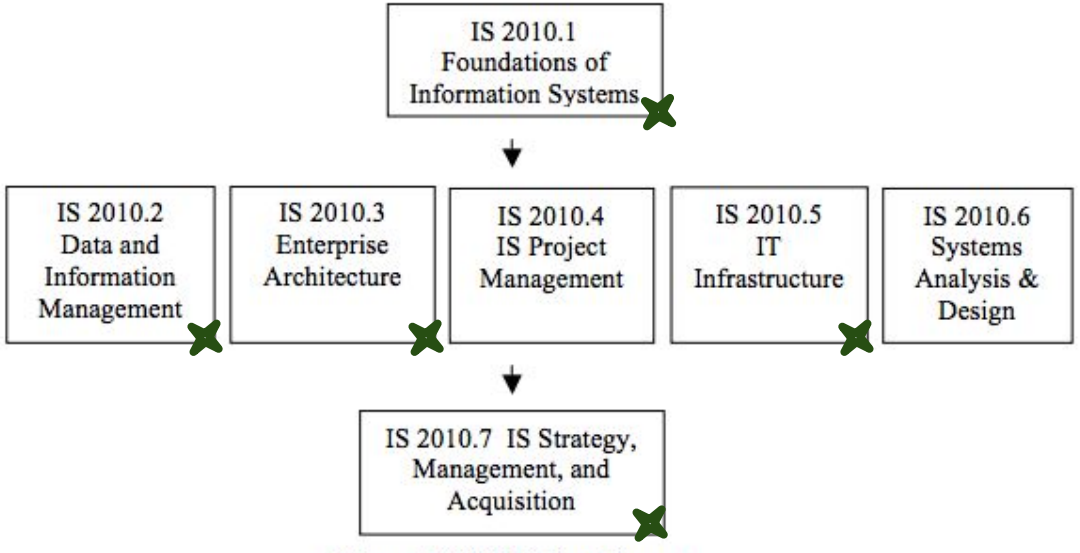


Figure 7: IS 2010 Core Courses

Sample Elective Courses

Application Development
Business Process Management
Enterprise Systems
Introduction to Human-Computer Interaction
IT Audit and Controls
IS Innovation and New Technologies
IT Security and Risk Management

ACM IS Security Courses

IT Security and Risk Management

1. Intro to InfoSec
2. Inspection
3. Protection
4. Detection
5. Reaction
6. Reflection
7. Risk Assessment Frameworks
8. Security Engineering
9. Physical Aspects
10. Security in Connected Systems
11. Policy and Management Issues

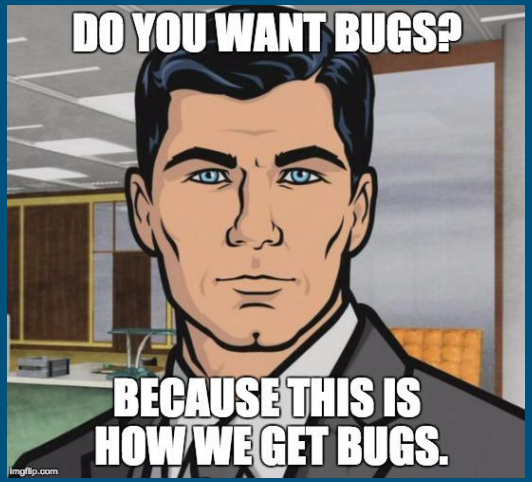
IT Audit and Controls

1. Need for Audit and Controls
2. IT Risk. Business Procs/BC
3. Auditing Ethics
4. Undertaking an Audit
5. Controls
    a. Physical
    b. Network
    c. Access Controls

    .etc
6. Control Assessment

ABET Requirements: Computer Science

- Computer Science (1 ⅓ years: 40 credits)
  - *Fundamentals of algorithms*
  - *Data structures*
  - *Software design*
  - *Concepts of programming languages*
  - *Computer organization and architecture*
- Mathematics (½ year: 15 credits)
  - *Discrete Math*
  - *Other hours may be courses such as linear algebra, statistics, probability, etc.*
- Science (½ year: 15 credits)
  - *Science courses that require laboratory work (chemistry, physics, etc.)*



ABET Requirements: Information Technology

Coverage of the fundamentals of

1. the core information technologies of human computer interaction, information management, programming, networking, web systems and technologies. **[IT]**
2. **information assurance and security. [IT]**
3. system administration and maintenance. **[IT]**
4. system integration and system architecture. **[IT]**

Advanced course work that builds on the fundamental course work to provide depth. **[IT]**

ABET Requirements: Information Systems

- Information Systems (1 year: 30 credits)
  - Coverage of…
    - Fundamentals of application development
    - Data management
    - Networking and data communications
    - **Security of information systems**
    - System analysis and design
    - Role of IS in the organization
  - Advanced coursework that builds on fundamentals to provide depth
  - Quantitative analysis and methods, including statistics

ABET Requirements vs Learning Outcomes

ABET Discipline	Requires Security	Assesses Security Learning Outcomes
Computer Science	No	No
Info. Technology	Yes	Maybe
Info. Systems	Yes	No

ABET Learning Outcomes: General and CS

(e) “An understanding of professional, ethical, legal, **security** and social issues and responsibilities.” **[General]**

(j) “An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices.” **[CS]**

(k) “An ability to apply design and development principles in the construction of software systems of varying complexity.” **[CS]**

ABET Learning Outcomes: Information Technology

(j) “An ability to use and apply current technical concepts and practices in the core information technologies of human computer interaction, information management, programming, networking, and web systems and technologies.” **[IT]**

(k) “An ability to identify and analyze user needs and take them into account in the selection, creation, evaluation, and administration of computer-based systems.” **[IT]**

(l) “An ability to effectively integrate IT-based solutions into the user environment.” **[IT]**

(m) **“An understanding of best practices and standards and their application.”** **[IT]**

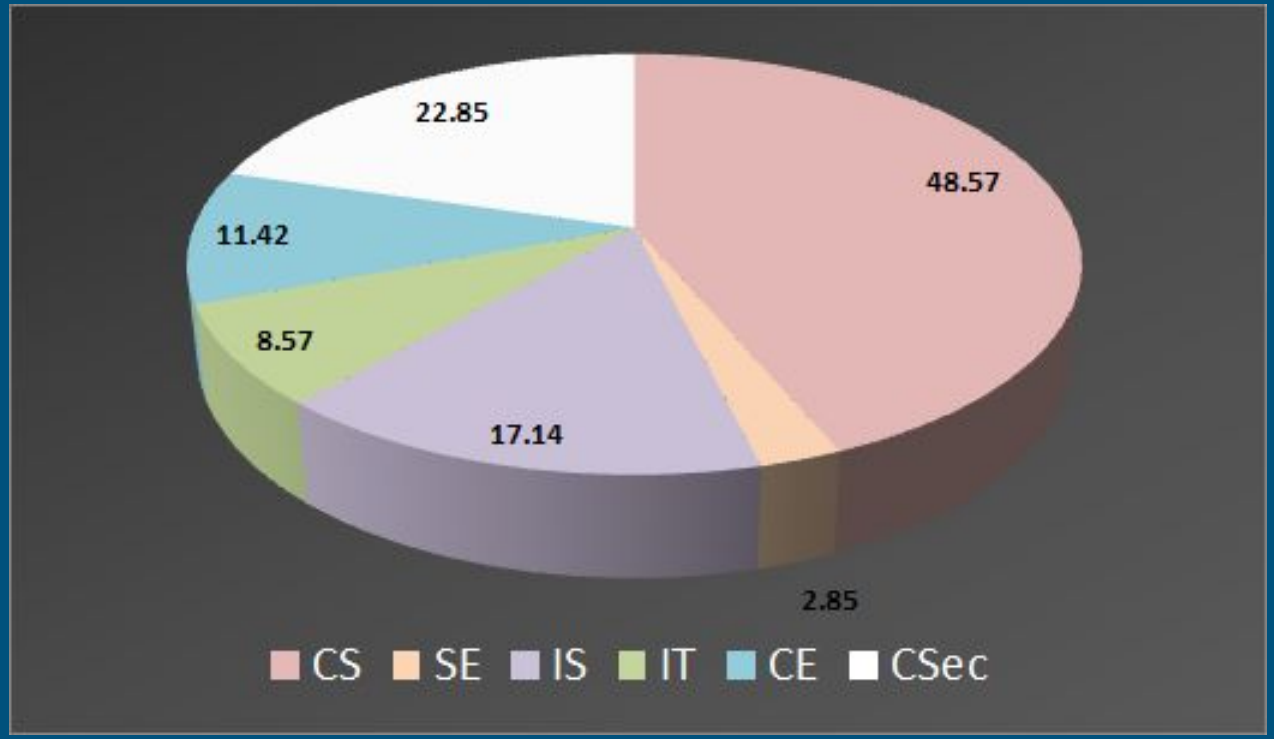
(n) “An ability to assist in the creation of an effective project plan.” **[IT]**

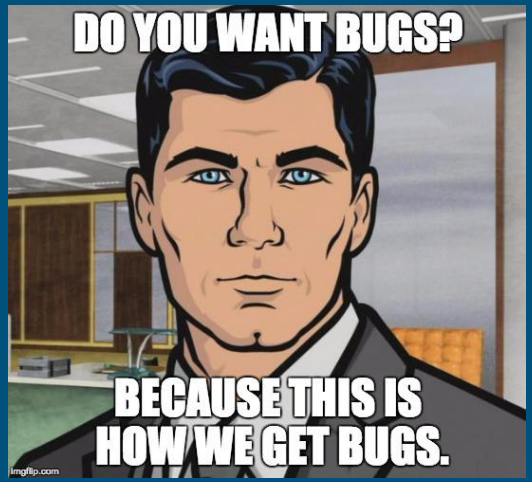
ABET Learning Outcomes: Information Systems

(j) “An understanding of and an ability to support the use, delivery, and management of information systems within an Information Systems environment.“ **[IS]**

- Likewise here, we see no mention of “security”

Breakdown By Discipline





NSA CAE-CD/Versus CAE-CO/Versus CAE-R

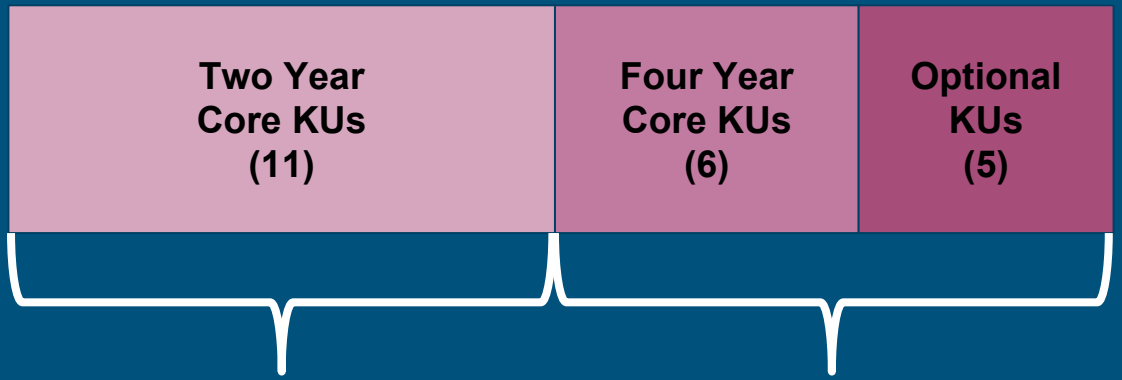
The NSA has its own cyber education designation (170 schools have 1 of 3)

- CAE-CD (Cyber Defense) - High level security blue team*
- CAE-CO (Cyber Operations) - State Sponsored Offense*
- CAE-R (Cyber Defense Research) - Cybersecurity Academics*

“Students attending CAE-CDE and CAE-R schools are eligible to apply for scholarships and grants”

NSA CAE-CD Curriculum Requirements

- Two Types of Universities
  - 2 Year
  - 4 Year
- Two Types of Knowledge Units
  - Required
  - Optional



NSA CAE-CD Curriculum: Core KUs

2 Year Core		4 Year Core (Includes 2 Year Core)
Basic Data Analysis	IT System Components	Databases
Basic scripting or programming	Networking Concepts	Network Defense
Cyber Defense	Policy/Legal/Ethics/Compliance	Network Technology and Protocols
Cyber Threats	System Administration	Operating Systems Concepts
Fundamentals of Security Design Principles		Probability and Statistics
IA Fundamentals		Programming
Intro to Crypto		

NSA CAE-CD Curriculum: Operational KUs

Advanced Cryptography	Software RE	Industrial Control Systems	Data Administration	System Certification and Accreditation	Embedded Systems
Algorithms	Software Sec. Analysis	Mobile Technologies	Database Management	Digital Forensics (Specialties)	Hardware Reverse Engineering
Data Structures	Secure Prog. Practices	Network Security Administration	Digital Comms	Intrusion Detection	Hardware & Firmware Sec
Low Level Programming	Software Assurance	OS Hardening	IA Compliance	Overview of Cyber Operations	RF Principles
Intro to Theory of Comp	Systems Programming	Virtualization Technology	IA Standards	Penetration Testing	Forensic Accounting
Low Level Programming	Advanced Network Technologies	Wireless Sensor Networks	Secure Prog. Management	System Security Engineering	Fraud prevention
OS Theory	Analog Telecomm.	Cloud Computing	Security Risk Analysis	Secure Prog. Practices	Independent/Directed Studies
QA/Functional Testing	IA Architectures	Cybersecurity Mgmt/Planning	Supply Chain Security	Vulnerability Analysis	

NSA CAE-CD Learning Outcomes

- Nothing too crazy
- Outcomes for Intro to Cryptography (For example)

- Students will be able to identify the elements of a cryptographic system.
- Students will be able to describe the differences between symmetric and asymmetric algorithms.
- Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
- Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.

NSA CAE-CO Curriculum: Core KUs

1. Low Level Programming
2. Software Reverse Engineering
3. Operating Systems Theory
4. Networking
5. Cellular and Mobile Technologies
6. Discrete Math and Algorithms
7. Overview of Cyber Defense
8. Security Fundamental Principles
9. Vulnerabilities
10. Legal
    a. Includes just war theory and Hague/Geneva Conventions

NSA CAE-CO Curriculum: Optional KUs

1. Programmable Logic
2. Wireless Security
3. Virtualization
4. Cloud Security/Cloud Computing
5. Risk Management of Information Systems
6. Computer Architecture (includes Logic Design)
7. Microcontroller Design
8. Software Security Analysis
9. Secure Software Development
10. Embedded Systems
11. Digital Forensics
12. Systems Programming
13. Applied Cryptography
14. Industrial Control Systems
15. UX/HCI
16. Offensive Cyber Operations
17. Hardware Reverse Engineering

NSA CAE-CO Learning Outcomes

Some make sense…

Outcome: Students will have a **thorough understanding of operating systems theory and implementation.** They will be able to understand operating system internals to the level that they could **design and implement significant architectural changes to an existing OS.**

NSA CAE-CO Learning Outcomes

Some aren’t bad...

Outcome: Students will be able to describe user associations and routing in a cellular/mobile network, **interaction of elements within the cellular/mobile core**, and **end-to-end delivery of a packet** and/or signal and what happens with the hand-of at each step along the communication path. They will be able to explain differences in core architecture between different generations of cellular and mobile network technologies.

NSA CAE-CO Learning Outcomes

Some are… out there.

Outcome: Students will be able to write a functional, stand-alone assembly language program such as a basic telnet client **with no help from external libraries**.

Upcoming ABET Revisions

- General Revisions
  - Curriculum must cover security somewhere “in a manner appropriate to its discipline”
- CS Revisions
  - Requiring three electives from a list
    - Security isn’t on the list, but networking and operating systems are.
- IT Revisions
  - Security is no longer listed as a fundamental topic
- IS Revisions
  - Security is removed as a topic studied during the year of IS coursework

Future Curriculum Guidelines/Accreditation

- ACM is working on a new set of curriculum standards for cybersecurity
  - ACM is getting input from other academic/research organizations, such as IEEE.
  - Most recent draft is v0.75, released in mid June.

- ABET is developing at least one new accreditation for cybersecurity
  - The major push seems to be coming from the Computing Accreditation Committee (CAC)
  - Available information tracks the ACM curriculum being developed
  - Tentative timeline:
    - Finalized by Fall 2018
    - Accreditation process beginning in 2019

ACM CSEC 2017 Curriculum Breakdown

Primary Knowledge Areas

1. Data Security
2. Software Security
3. System Security
4. Human Security
5. Organizational Security
6. Societal Security

Cross-Cutting Concepts

1. Confidentiality
2. Integrity
3. Availability
4. Risk
5. Adversarial Thinking

CSEC 2017 (v 0.5) Topics

Data Security	Software Sec.	System Sec.	Human Security	Org. Security	Societal Security
InfoSec Fund.	Fund. Design Principles	Availability	Ident. Mgmt	Security Policy/Governance	Cybercrime
Cryptography	Practice	Authentication	Social Eng.	Analytical Tools	Cyber law
	Documentation	Access Controls	Social Networks	System Admin.	Ethics
		Secure Sys Design	HCI	Cybersec. Planning	Policy
		Comp. Network Defense	Fund. Sec. Design Principles	Security Program Mgmt	Privacy
		Reverse Eng.		Sec. Awareness	Intellectual Prop.
		Cyber Physical Systems Sec.		Risk Mgmt	Prof. Responsibility
		Digital Forensics			Social Responsibility
					Global Impacts

CSEC 2017 (v 0.75) Topics

Data Security	Software Sec.	System Sec.	Human Security	Org. Security	Societal Security
Data Integrity & Authentication	Fund. Design Principles		Awareness and Understanding	Policy/Governance	Cybercrime
Digital Forensics			Social Eng.	Analytical Tools	Cyber law
Access Control			Personal Compliance	System Admin.	Cyber Ethics
Cryptography			Ident. Mgmt	Cybersec. Planning	Policy
Secure comm. protocols			Social Behavioral Privacy	Sec. Prog. Mgmt	Prof Responsibility
Cryptanalysis			Personal Data Priv./Sec.	Personnel Security	Global Impacts
Privacy			Usable Security	Risk Mgmt	Digital Forensics
Storage Security				Security Ops	Privacy
					Social Responsiblity

Interesting Changes Between v0.5 & v0.75

- The most extensively developed sections seem to be societal and organizational security.
- Most system security topics have been distributed elsewhere
- v0.75 has an heavy emphasis on cyber-warfare related concepts in societal security, including covering the following sub-topics:
  - Military vs civilian cyber law as a law sub-topic
  - Just war theory as an ethics sub-topic
  - Cyberwar strategy as a policy sub-topic
  - Cybersecurity and statecraft as a policy sub-topic
  - Cyber-in-war vs cyberwar as a policy sub-topic
  - Cyberspace Operations (mentions military ops as a policy sub-topic)
  - Law of armed conflict as a global impacts sub-topic

Designation to Job Mappings

Accreditation(ish) Agency	Program Title	Appropriate Jobs
ABET	Computer Science	Developers ***(AT BEST)***
ABET	Information Technology	System/Network Admins
ABET	Information Systems	Non-technical analyst roles, auditing
ACM/ABET	CSEC 2017 (v0.5)	Generic security analyst
ACM/ABET	CSEC 2017 (v0.75)	Non-technical analyst roles
NSA	CAE-CD	Generic high level blue team (high level variance)
NSA	CAE-CO	State sponsored offense

Conclusions

- Most graduates get security in CS/IT/IS/CE degrees
- NSA, ACM, and ABET are the prime influencers of future trends in security education
  - Security is going to be it’s own thing rather than baked in
  - Looks like a practical CISSP spread out over 4 years
  - It’s probably a good thing to not have NSA be the only players in this space
- Most curricula or accreditation standards are geared towards generic blue team work
  - NSA CAE designations may be influencing CSEC 2017
- No curricula or accreditation standards geared to industry offense
- ABET is going to have a hard time breaking into this field.

General Recommendations

- Need significantly better metrics and tracking of metrics
  - Number of security graduates and class sizes
  - Learning outcome assessment methodology
  - Data about internships/co-ops and student clubs
- There should probably be a more tangible incentive for accreditation other than recruiting students to universities.
- Industry should be more involved in shaping the curriculum
  - CSEC 2017 has open comment periods where anyone can contribute
    - https://www.csec2017.org/

Academic Recommendations

- Certifications should be used to fulfill the requirements of CAE-CD
  - Only IT and CSEC are prepared for new requirements
  - Other options also make sense
    - 37% of institutions offer a Masters in Security
    - 17% of institutions offer a minor in Security
- The NSA CAE-CO content is a best fit for CS, CE, or custom
  - Almost certainly not in IS
- Accrediting bodies should consider offense in addition to defense
  - NSA CAE-CO doesn’t meet industry needs

Questions?

Contact:

Rob: rboics@rit.edu (@nerdprof)

Chaim: csanders@zerofox.com

Data:

Online: http://csecprograms.com

Github: https://github.com/csanders-git/csecprograms