Security Across the Computer Science Curriculum

L. Felipe Perrone
perrone@bucknell.edu
Dept. of Computer Science
Bucknell University

Security and Software Assurance in Computer Science Programs

- Many graduate programs seem to offer wide coverage of the subjects with a variety of course offerings.
- Undergraduate programs are not quite there yet. The question is: *"Why not?"*

Undergraduate Programs

We envision three models of instruction for teaching Sec/SwA to undergraduates:

- ***Single-Course:*** A junior or senior elective.
- ***Track:*** A course sequence starting from 1st or 2nd year that adds to the core CS curriculum.
- ***Thread:*** Principles of software assurance and security serve as a unifying theme across the core curriculum.

Justifying the ***Single-Course***

- ***Curricula are already packed.*** This is in part due to the need to cover a variety of principles. Certification requirements add even more pressure.
- ***Resources required are minimal.*** One or two faculty knowledgeable in the subject are enough.

Single-Course

A quick, informal Internet survey in 2005 revealed:

Institution	Department	Course	Prerequisites
Bucknell University	Computer Science	CSCI 379 Topics in Computer Science	CSCI 315 Operating Systems or permission
Dartmouth College	Computer Science	CS38 Security and Privacy	CS23 Software Design and Implementation CS37 Computer Architecture
Denison University	Math and Computer Science	CS 402 Advanced Topics in Computer Science	CS-272 Data Structures and Algorithm Analysis II
Oberlin	Computer Science	CSCI 343 Secure Computing Systems	An introductory programming course or permission
Old Dominion University	Computer Science	CS 472 Network and Systems Security	CS 361 Advanced Data Structures and Algorithms
Richmond University	Math and Computer Science	CMSC 395 Special Topics	CMSC 301 Computer Architecture
Rose-Hulman Institute of Technology	Computer Science and Software Engineering	CSSE 442 Computer Security	CSSE 332 Operating Systems MA 275 Discrete and Combinatorial Algebra I

The *Single-Course* at Bucknell

Introduction to the C Programming Language.
Hands-on (1): Writing code for elementary ciphers.
Elementary Cryptology.
More on Elementary Cryptology.
Hands-on (2): Analyzing and breaking elementary ciphers.
Hands-on (3): Programming a stream cipher.
Block Ciphers.
DES.
Public Key Encryption.
Crypto Hashes.
Hands-on (4): Experimenting with OpenSSL.
Hands-on (5): Programming with OpenSSL Hashes.
Hands-on (6): Using Public Key Encryption.
Hands-on (7): Using Public Key Encryption II.
Public-Key Infrastructures.
Authentication protocols.
Canonical Authentication Protocols.
Buffer Overflows.
Secure Programming Practices I.
Hands-on (8): Secure Programming Practices II.
Writing Secure Code.
Malware: Viruses & Worms.
Malware: Trojans, Rootkits, Spyware, Adware.
Protection in Operating Systems.
User Authentication.
Access Control (MAC, DAC, RBAC, ACL, ACM)
Security Models & Trusted OS design.
Trusted OS design.
Assurance in Operating Systems.
Introduction to Computer Networks.
Network Threats.
Network Threats.
Hands-on (9): Experiments with assessment tools.
Firewalls. Honeypots. (HW5 due)
Intrusion Detection Systems.
Administering security.
Policies and physical security.

Limitations of the ***Single-Course***

- It cannot possibly cover all the fundamentals that the student needs to learn. It’s a pretty loaded course...
- It happens too late in the sequence to create a real awareness to the problems in Sec/SwA.
- It doesn’t demonstrate that principles of Sec/ SwA underlie many topics in Computer Science and can’t be separated from them.
- It is likely to be only minimally effective.

Track

- Provides excellent breadth and depth of topics in Sec/SwA for those students who opt in.
- Its value is recognized by the NSA's certification of *Center of Academic Excellence in Information Assurance Education* (CAEIAE). This seal of approval "could" attract more students and more "really interested" students.

CAEIAE Criteria

1 🚫	Partnerships in IA Education
2 🚫	IA Treated as a Multidisciplinary Science
3	University Encourages the Practice of IA
4	Academic Program Encourages Research in IA
5 🚫	IA Curriculum Reaches Beyond Geographic Borders
6	Faculty Active in IA Practice and Research and Contribute to IA Literature
7	State-of-the-Art IA Resources
8 🚫	Declared Concentrations
9	Declared Center for IA Education or Research
10 🚫	Full-time IA Faculty

Limitations of the ***Track***

- Since not all students opt in, a large number of students will still graduate without the knowledge that the current reality requires. The change in the status quo is not what is needed.
- Not all schools have the resources to implement a track in Sec/SwA (small colleges and universities in particular).

Are the principles of ***Sec/SwA*** fundamental to modern CS?

- OS1 Overview of Operating Systems (2): The identification of potential threats to operating systems and potential threats and the security features design to guard against them.
- OS4 Operating Systems Principles (2): Mutual exclusion as a mechanism for the implementation of access control in trusted operating systems.
- OS5 Memory Management (5): Memory protection as a fundamental mechanism in the design of a trusted operating system.
- NC3 Network Security (3): Fundamentals of cryptography, public-key and secret-key algorithms, authentication protocols, and digital signatures.
- PL2 Virtual Machines (1): Security issues arising from the execution of mobile code.
- PL4 Declarations and Types (3): Type checking as a tool to enhance the safety and the security of a computer program.
- IS2 Search and Constraint Satisfaction (5): Search heuristics as essential components in intelligent intrusion detection systems.
- IM1 Information Models and Systems (3): Information privacy, integrity, security, and preservation.
- SP4 Professional and Ethical Responsibilities (3): Computer usage policies and enforcement mechanisms.
- SP5 Risks and Liabilities of Computer Based Systems (2): Implications of software complexity, and risk assessment and management.
- SP7 Privacy and Civil Liberties: Study of computer based threats to privacy.
- SE6 Software Validation (3): Validation and testing of software systems.
- SE8 Software Project Management (3): Risk analysis and software quality assurance.

Thread

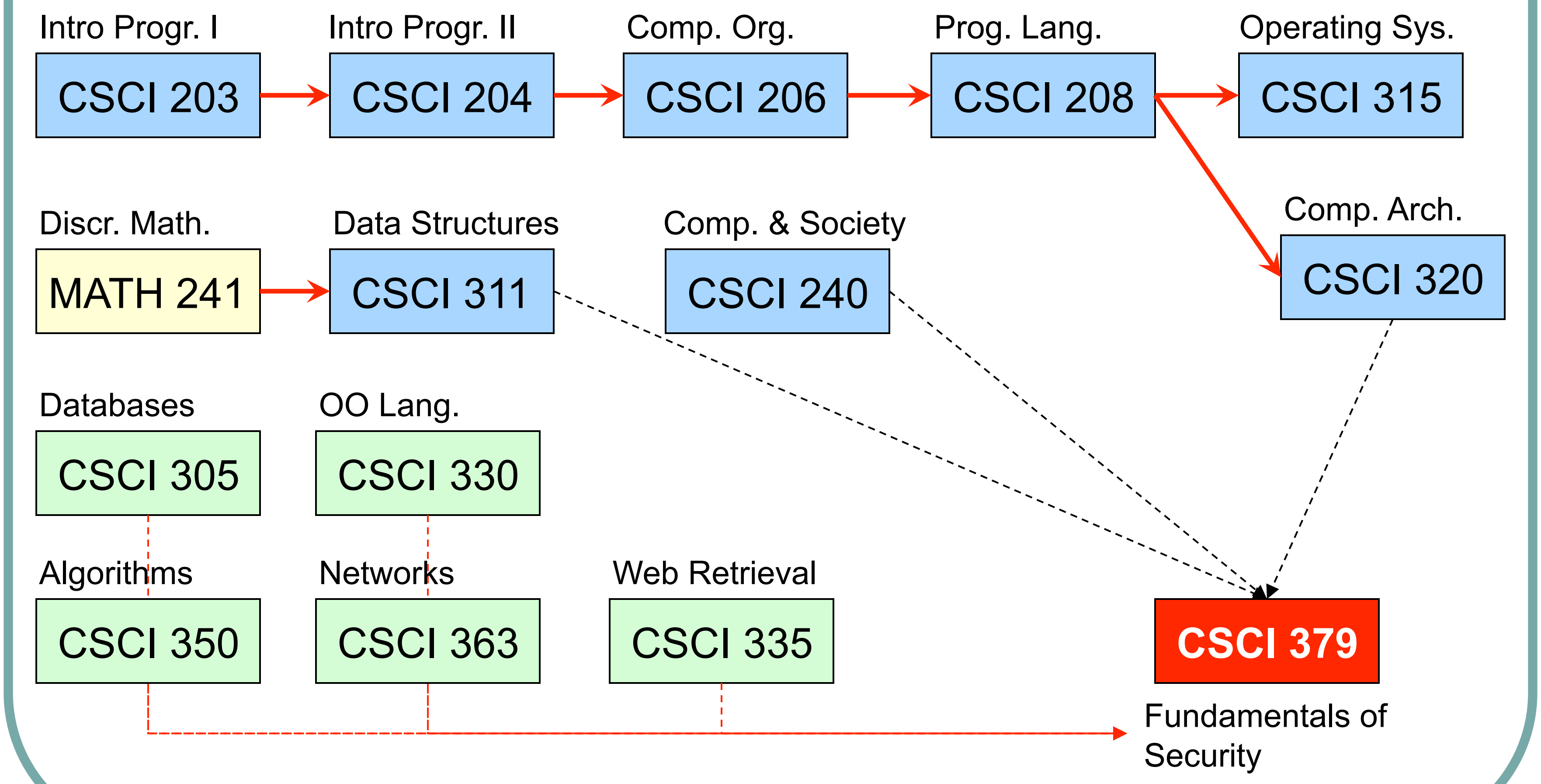
- **Approach:** Address the principles of Sec/SwA as you teach each topic in Computer Science, across different courses, across the entire curriculum (core and electives).

- It's not quite like chopping up Sec/SwA to serve in bite-sized morsels. It's more like using the opportunities that already exist in the CS curricula to teach the fundamental concepts in Sec/SwA.

Thread

- Is this a matter of calling attention to what is already in the curriculum?
  - To some extent it may be, but it invites a careful review of the curriculum to ensure that all the important principles receive the attention they need to receive.
- Is this a way to market the program so as to attract more students?
  - Uh, sure, why not? Higher enrollment is good. Parents and alumni often ask what we're doing about Sec/SwA.
- What is more important, though, is that *all students in the regular degree program will be educated in principles that are of key importance*.

The *Thread* at Bucknell



A few more details

- ***Intro Prog. I:*** input validation, error handling, testing, proper documentation, interface design.
- ***Intro Prog. II:*** testing, proper documentation, interface design.
- ***Comp. Org.:*** buffer overflows, input validation, memory leaks, error handling, hardware mechanisms for protection.
- ***Prog. Lang.:*** type safety, virtual machines.
- ***Op. Sys.:*** virtualization, protection, access control, reference monitor, policies, resource allocation.
- ***Comp. Soc.:*** ethics, privacy, hacktivism, risk assessment, computer crime.

Implementing the ***Thread***

- The extensive coverage requires approval from the entire department.
- Each course needs to be revised to identify the essential opportunities in Sec/ SwA to be addressed in its context.
- Modules, lectures, labs, homework need to be created.
- Faculty need to be trained.

A proposal for ***Thread*** implementation (Xiannong Meng)

- Place the faculty with expertise in Sec/SwA in charge of studying the curriculum and devising new materials.
  - A curricular development grant (summer) could support this work.

- Create a mechanism to allow the faculty who created the new materials to apply them when they are first used.
  - The faculty become “just-in-time” (JIT) resources that are used in all the courses that apply the new materials. They teach the students the topic(s) and show the faculty who “host” them how to use the material.
  - The JIT faculty need to be released from regular teaching duties (course release program) in order to have time to for the new activities.
  - After this setup period, the faculty without Sec/SwA would have been trained “in the house” and the thread could become sustainable.

Thanks

- Questions?
- Feedback?