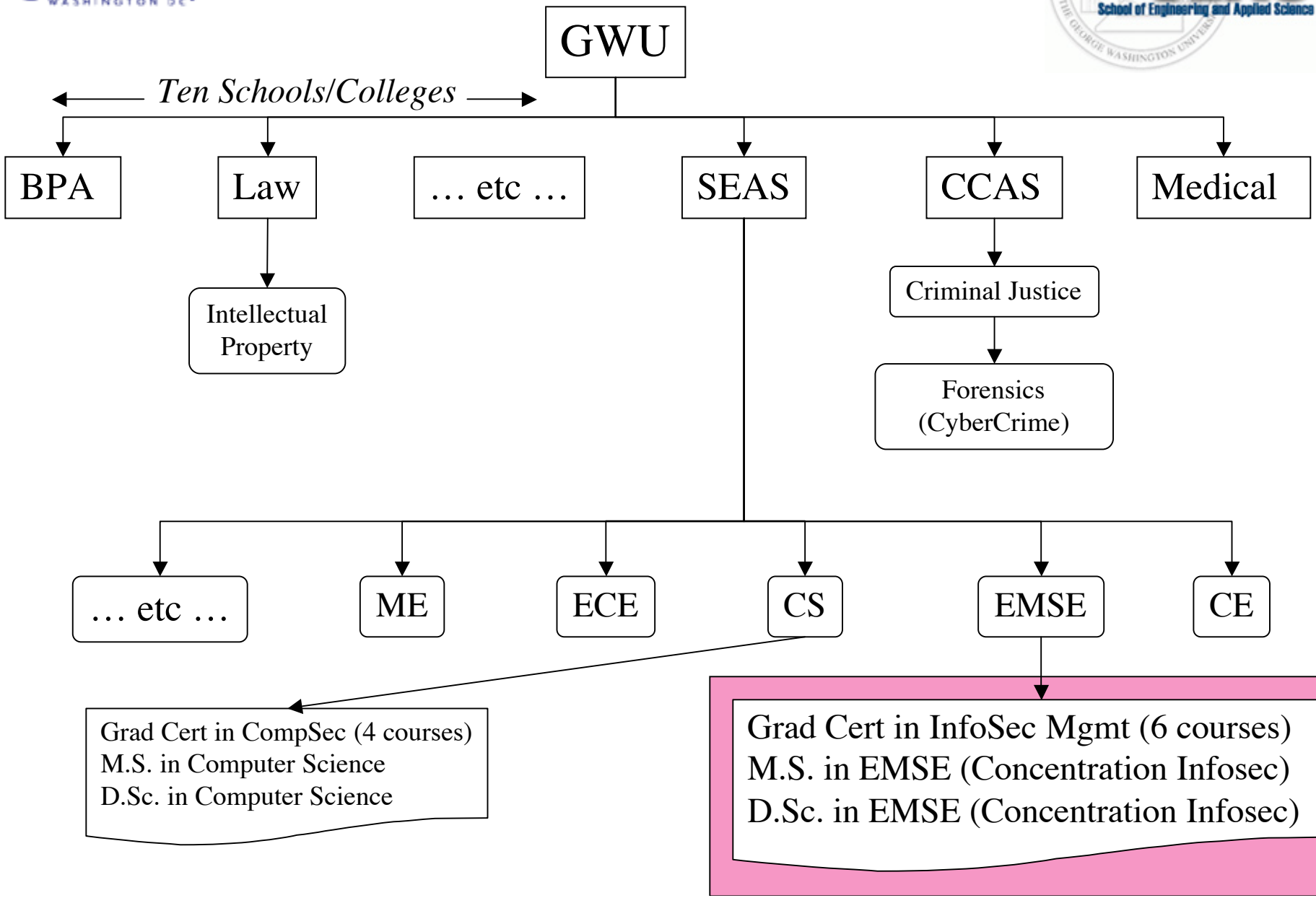
Establishing and Maintaining a Cybersecurity Program: The GWU EMSE Experience

Julie J.C.H. Ryan, D.Sc.
Assistant Professor
Engineering Management and System Engineering
School of Engineering and Applied Science
The George Washington University

Context Diagram



The EMSE Program

- History:
  - Began in 1996 with a single class
    - Intro and Overview of Information Security
  - By 1998, had a six class Graduate Certificate Program
    - 18 graduate credit hours
  - By 2001, had a handful Doctoral students
    - Expecting the first one to finish up Spring 2003
  - Effective Fall 2002, MS in EMSE with a Concentration in Infosec Mgmt
    - 36 graduate credit hours, Certificate Program classes comprise core
- To date (Summer 2002):
  - 619 students taken the intro class
  - 135 have completed the Graduate Certificate Program
  - Approximately 100 currently enrolled in Graduate Certificate Program

The Classes

- The Graduate Education Certificate (also the MS Core)
  - EMSE 218: Intro & Overview
    - Everything at a micron deep
  - EMSE 315: Law
    - Contracts, Case law, torts, ethics, etc
  - EMSE 312: Protect (minus Crypto)
    - Personnel, Physical, Ops, Computer, Network, etc
  - EMSE 313: Crypto
    - All crypto, all the time
  - EMSE 314: Detect
    - Audit, monitor, IDS, etc
  - EMSE 316: React/Correct
    - Biz continuity, crisis mgmt, recovery
- The MS Electives (2 of…)
  - EMSE 317: Cybercrime
    - Criminal law, forensics processes
  - EMSE 318: Info Ops
    - Effect of global economy on security
  - EMSE 319: Emerging Issues
    - Wireless security
  - EMSE 320: E-Commerce
    - How to, how to secure
- The EMSE Core requirements for all MS tracks
  - EMSE 212: Mgt of Tech Orgs
  - EMSE 260: F&A for Engr Mgrs
  - EMSE 269: Decision Theory
  - EMSE 283: Systems Engineering

Topics Covered

- The short list:
  - Threats
  - Vulnerability assessments
  - Risk management
  - Secure computing
  - Operational security
  - Admin security
  - Policy
  - Law
  - Ethics
  - Network security
  - Life cycle management
  - Personnel security
  - History of computer security
  - History of comms security
  - Crypto, crypto, crypto
- And more….
  - Common Criteria
  - Rainbow series
  - Auditing
  - Monitoring
  - Intrusion detection systems
  - Crisis management
  - Business continuity planning
  - Resource allocation
  - Security engineering
  - Malicious software
  - Trust
  - Passwords
  - Authentication
  - Access control
  - And still more

What We Don't Teach

- Computer Science
  - Not a single line of code generated
  - Not a single algorithm developed
- Electrical Engineering
  - Not a single circuit analyzed
- Hands on skills
  - Not a single firewall configured
  - Not a single system administrated
- Hacking
  - Cover the theory in advanced classes but forbid them to do it
- BUT!
  - We do teach them why each and every element of those specialties is a critical component of security engineering and management

Why and How

- Why
  - Huge requirement for education of non-computer science types
    - Weapons acquisition managers
    - Program managers of all other sorts
    - The other engineers increasingly required to work with IT
    - Senior executives forced to deal with security issues
    - Business types in the IT workforce with no computer science background
  - Strongly believe in the systems engineering approach to security in operational environments
    - Solution in real world is not a computer science problem
- How
  - Started small, built over time
  - Used the feedback from students on what worked and what didn't
    - Continually modify course approach and content

Challenges

- Textbooks
  - Lots of good books out there but not any one just right for our purposes
    - Too much computer science, too much math, too much focus on protection
    - Couldn't make the students buy 10 books for one class
    - Wrote our own, currently in rewrite
      - Expect to have rewrite done end of summer
- Students Knowledge Base
  - No math, darn little science, incredibly weak writing skills
  - Can't assume a core base of KSA!!!
    - What's going wrong at the undergraduate level?
  - Have incorporated basic skill instruction into program:
    - Plagiarism 101
    - Writing 101
    - Speaking 101
    - Logic 101

A Particular Challenge

- Institutional and Professional Liability
  - Duty of due care required of educational institutions and professors
    - Legislation, Regulations, Common law
  - Educators have a clear duty to anticipate dangers
  - Educators have a clear duty to protect students from injury
  - Duty may extend to third parties who are foreseeable victims
- What can go wrong?
  - Students might get busted
    - Hacking, illicit intercept of comms, exceeding authorized access
  - Civil liability in non-criminal cases
  - Other ills
    - Insider trading, ITAR violations, disclosure of trade secrets, copyright violations, etc etc etc
- Defenses include security engineering of course offerings
  - Policies, procedures, technologies, practices, and warnings

Contact Information

Julie J.C.H. Ryan, D.Sc.
1776 G. Street NW #110
Washington DC, 20052
jjchryan@seas.gwu.edu
http://www.seas.gwu.edu/~infosec/

The George Washington University is an NSA Certified Center of Academic Excellence in Information Assurance Education and meets the Federal Training Standards for Information Systems Security Professionals (NSTISSI 4011). We offer Graduate Certificate, Master's, and Doctoral level education in Information Security Management for professionals from all educational backgrounds. GWU is located in the heart of Washington DC very near the White House and other government offices.