American Public University System - A Multi-Disciplinary Approach to Cybersecurity Education

Dr. Clay Wilson, CISSP
Program Director, Cybersecurity Studies
American Public University System

Overview

- About American Public University System (APUS)
- What is a Multi-Disciplinary Approach?
- What Problems does it help solve?
  - Complex Malicious Code
  - Cascade Failures for Infrastructures
  - Hackers Bypass Defensive Technologies
- Problems require a Multi-Disciplinary Education
  - Management and Coordination of Cybersecurity Technologies
- APUS Goal for Cybersecurity Education
  - Summarized Admission Requirements
  - Overview of the APUS Cybersecurity Program
  - APUS Offers Undergrad Certificates
- APUS awarded National Certifications for Cybersecurity Education

About APUS

- Founded in 1991 as American Military University (AMU) by James P. Etter, USMC
- Fully-online; intended for military and working adults with focus on counter-terrorism, military intelligence
- In 2002 expanded to American Public University System, adding American Public University for public service courses, i.e. criminal justice and national security
- APUS accredited by the Higher Learning Commission, North Central Association

About APUS (con't)

- Today more than 100,000 students from all 50 states/DC and 100+ countries
- Approximately 53% active-duty all branches; 47% civilian or other military
- Recent Awards
  - US News & World Report 2014 Online Rankings: APUS Undergraduate Programs Rated Among Best in Overall Quality
  - First Three-Time Recipient of Sloan Consortium Effective Practice Award

About APUS (con't)

Some of the Organizations that Partner with APUS --

- Education Institutions of all Military Service Branches
- Department of Homeland Security
- FBI
- Lockheed Martin Center for Security Analysis

- and many other universities and organizations

What is a Multi-Disciplinary Approach to Cybersecurity?

Definition of Multi-Disciplinary – cooperation and participation across different sectors to solve problems.

Why is a Multi-Disciplinary approach to Cybersecurity now important?

- Sometimes, skill-centered specialists cultivate a traditional boundary around their expertise.
- This can be a restrictive way of finding solutions to a problem.
- Cybersecurity is being hit with **newer types of problems** that bypass traditional boundaries

What Problems does a Multi-Disciplinary Approach Help Solve?

Problem #1 – Cyberattacks are becoming more complex.

- Complexity shows in newer, advanced persistent threats that defeat increasingly sophisticated cybersecurity defensive technologies.

- Cybersecurity experts are always playing catch up after newer methods of cyberattack are discovered.

Complex Malicious Code Operates Undetected for Years

Complex malicious code can reside and operate undetected inside computers for years before discovery.

- The STUXNET malicious code operated inside Iranian nuclear facilities for several years before it was eventually discovered.
- The new SNAKE malicious code, recently announced as a new discovery inside Ukrainian computers, may also have infected other computers worldwide and operated secretly for the past several years.

Cascade Failures May Connect Critical Infrastructures

Problem #2 - Critical infrastructures are subject to complex cascade-failures due to vulnerabilities in other distantly-related infrastructures.

- During Sandy, the hospitals in New Jersey lost electricity when the local power utility flooded.
- When Hospital backup diesel generators ran out of fuel, filling stations had no electricity to pump fuel into delivery tankers.

Hackers Bypass Defensive Technology – Attack Users

Problem #3 - Hackers defeat sophisticated technical cybersecurity defenses by directly targeting the users instead of the computers.

- With ‘Phishing attacks’, users are tricked by email attachments, or by false web sites, that enable hackers to steal personal secrets and passwords.

Problems Require a Multi-Disciplinary Education

Problems of Complexity, Cascade Failures, and Targeted Users now require a multi-disciplinary approach to cybersecurity education.

– Leaders in all professions, all disciplines must develop a "cybersecurity mindset".

> The ACM Education Board in 2013 acknowledged that "a **system-wide perspective** has become an important part of cybersecurity education, and that education must be multi-disciplinary, to include many sectors."

Management and Coordination of Cybersecurity Technology

Traditional cybersecurity education courses were initially designed to expand the technical skills of technology experts.

- Management and Coordination of technology must now be emphasized in Cybersecurity Education.
- Cybersecurity Education must now range across many sectors, not focus just on the development and operation of security technology.

APUS Goal for Cybersecurity Education

Leaders in All Disciplines need Cybersecurity Education to help manage and coordinate technology for cybersecurity -

Business	Education
Public Safety	International Relations
Environmental Science	Space Studies
Sports and Healthcare	Transportation and Logistics

Students may enroll in the APUS Cybersecurity Program with an IT certificate, or ***with a non-technical work background***

APUS Admissions Requirements

Students enrolling for Cybersecurity must meet ***one*** of these requirements ---

- Undergraduate degree in Information Technology or a related field

  or

- Undergraduate IT Certificate

  or

- FIVE years of ***work experience*** at the senior level ***in Criminal Justice, Emergency Management, Intelligence, Homeland Security or other non-technical background***

APUS Cybersecurity Programs

- First half of the graduate cybersecurity program focuses on network security, information assurance, cybercrime, and digital forensics. Second half of grad program focuses on policies, practices, perspectives of different disciplines, including emergency management, homeland security, intelligence, law and ethics, risk management and cyber warfare.

- The capstone course is a multi-disciplinary group project where individual participants represent different sectors, agencies, and disciplines.

- Graduate certificates are available in:
  - Cybercrime
  - Digital Forensics
  - Information Assurance
  - Information Systems Security

- Undergraduate certificates also available in:
  - Digital Forensics
  - Information Assurance
  - Homeland Security
  - National Security
  - Emergency Management

APUS Awarded National Certifications for Cybersecurity Education

2013 - APUS received two National Training Standards certifications for Information Systems Security Professionals from the Committee on National Security Systems (CNSS)

NSTISSI no. 4011 and CNSSI no. 4013

2014 - APUS is also applying for the CAE/IA/CD designation from DHA and NSA.

For Further Information

Clay Wilson, Phd, CISSP
Program Director, Cybersecurity Studies
American Public University System
cwilson@apus.edu

Undergraduate programs
http://www.amu.apus.edu/lp2/cybersecurity/bachelors.htm
Graduate programs
http://www.amu.apus.edu/lp2/cybersecurity/masters.htm