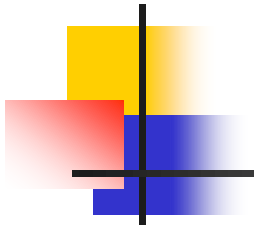

CSE 543
Information Assurance and Security

Introduction

Professor Stephen S. Yau

Fall, 2014

Information Assurance

- Information Assurance (IA) encompasses the ***scientific, technical, and management disciplines*** required to ***ensure information security and quality.***
  - Security techniques as well as organization, operation management and policy, legality, all play important roles.
  - Information quality also contributes to the overall information assurance of information systems and networks.

National IA Program

- The ***National Centers of Academic Excellence in Information Assurance Education (CAEIAE)*** and the ***National Centers of Academic Excellence in Information Assurance Research (CAE-R)*** Programs are outreach programs designed and operated initially by the National Security Agency (NSA) in the spirit of Presidential Decision Directive 63, National Policy on Critical Infrastructure Protection, May 1998.
  - The program is now jointly sponsored by the NSA and the Department of Homeland Security (DHS) in support of the President's National Strategy to Secure Cyberspace, 2003.
  - The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA), and producing a growing number of professionals with IA expertise in various disciplines.
- ASU has been certified as ***both CAEIAE and CAE-R, and is pending re-designation.***

Presidential Decision Directive 63
May 22, 1998

- Explains key elements of the Clinton Administration's policy on critical infrastructure protection
- Intended to take all necessary measures to swiftly eliminate any significant ***vulnerability to both physical and cyber attacks on our critical infrastructures***, especially our ***cyber systems***.
- Ensures the ***continuity and viability of critical infrastructures***, including, but not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services
- Available at: *https://www.fas.org/irp/offdocs/paper598.htm*

President's National Strategy to Secure Cyberspace (Feb. 2003)

- President Bush directed the development of a National Strategy to ***Secure Cyberspace*** to ensure that America has a clear ***roadmap*** to protect its critical infrastructures.
- Provides ***direction*** to the federal government departments and agencies for cyberspace security
- Identifies ***steps*** that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cyber security
- Prevent ***cyber attacks*** against America's critical infrastructures;
- Minimize ***damage and recovery time*** from cyber attacks that do occur.
- Available at: *https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf*

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 IA Concentrations

9: Declared Center for IA education or research

10: Full-time IA faculty

CAE-R Criteria

1. Engagement in serving on technical program committees of IA conferences, editing IA journals, hosting IA conferences and IA workshops, and collaborating with or assisting local government, business, and industry.
2. Producing students' thesis, dissertations, or projects, related to IA.
3. Strong peer-reviewed publications in IA by faculty and students
4. History of research funding related to IA

IA Courses at ASU

- CSE465: Information Assurance
- CSE466/598: Computer Systems Security
- CSE467/598: Data and Information Security
- CSE468/598: Computer Network Security
- CSE469/598: Computer and Network Forensics
- CSE539: Applied Cryptography
- CSE543: Information Assurance and Security
- CSE545: Software Security
- CSE548: Advanced Computer Network Security
- More courses in EE, IE and CIS (Business School)

IA Concentrations in MS and MCS in Computer Science

- A minimum of 15 credits in Information Assurance and related areas are required.
- MS thesis and the project portfolio for MCS must have a major portion of the content in the information assurance area
- For more information: *http://cidse.engineering.asu.edu/forstudent/graduate/computer-science/*

IA Concentration in PhD in Computer Science

- A minimum of 18 credits in Information Assurance and related areas are required.
- PhD dissertation must have a major portion of the content in the information assurance area
- For more information : *http://cidse.engineering.asu.edu/forstudent/graduate/computer-science/*

Benefits from CAEIAE or CAE-R Programs

- Formal recognition from the U.S. government, as well as opportunities for prestige and publicity, for their role in securing our nation's information systems.
- Students attending CAEIAE or CAE-R schools are eligible to apply for scholarships and grants through
  - The Department of Defense (DoD) Information Assurance Scholarship Program
  - The Federal Cyber Service Scholarship for Service Program (SFS) operated by National Science Foundation (NSF)

NSF Federal Cyber Service: Scholarship for Service (SFS)

- Accredited US university or college that has been designated as a CAEIAE or CAE-R Center
- Eligibility
  - ***Domestic full-time students*** enrolled in ***IA Concentration Programs***
- Scholarship:
  - Stipend per academic year (in 2013-14):
    - $20,000 for undergraduate
    - $25,000 for master degree student
    - $30,000 per year for doctoral student
    - Full tuition, books, and travel to approved conferences

NSF Federal Cyber Service: Scholarship for Service (SFS) (cont.)

- Obligations:
  - Scholarship recipients will be required to ***serve in the Federal Government for one calendar year for each year of scholarship***
  - During summer break, ***internship*** in National Laboratories and Federally Funded Research and Development Centers (FFRDCs).

CSE 543 Course Overview

- One of core courses in the IA Concentration programs
- Covers most of the required information items in NSTISSI-4011 and CNSSI-4012
- Objective: Provides basic and comprehensive understanding of the problems of information assurance (IA) and the solutions to these problems.

Prerequisites and reference book

- Knowledge of information systems, computer networks and their operations are required to be successful in this course.
- *Principles of Information Security*, 4th edition, by M. E. Whitman and H. J. Mattord, Thomson Course Technology, 2011
- Additional references in current literature, such as papers and other books.

Course Description

- ***Basic Concepts and Techniques***
  - IA overview: concepts, trends, and challenges
  - Security and privacy principles and guidelines
  - Security and privacy strategies, and mission assurance
  - Physical and personal security
  - Evaluating systems for functionality and assurance
  - Firewalls and VPN
  - Cryptography and steganography
  - Authentication protocols & access control mechanisms
  - Malware
  - Computer crimes & forensics

Course Description (cont.)

- ***IA Policy, Management, Legal and Ethical Issues***
  - IA policy
  - Administrative security controls
  - Contingency and disaster recovery planning
  - IA management
  - IA certification & accreditation
  - CISSP certification
  - IA risk analysis and management
  - State, US and international standards/jurisdictions and laws and authorities related to IA

Other Course Information (cont.)

- **Class Schedule:**
  - ***Time: Th 6:00 – 7:15 p.m***. for hybrid section
    Line #88526 (Hybrid) Room BYAC 110
- **Instructor:** Professor Stephen S. Yau
  - E-mail: ***yau@asu.edu***
  - Office hours: TTh 1:30 –2:30 p.m. and by appointments
  - Office: BYENG 488
- **Teaching Assistant**: Jia Yu
  - E-mail: jiayu2***@asu.edu***
  - Office hours: Th 2:30 –3:30 p.m. and by appointments
  - Office: BYENG 487

Other Course Information (cont.)

- **Background Survey**
  - Survey form must be completed before ***Saturday, August 30, 2014*** (have to use your ASU email account to access the form)
- **Evaluation**

	#	%
Examinations	2	60%
Assignment	1	10%
Course project:	1	30%

Course Project

- Hybrid classes:
  - Group project, each group having 5 or 6 students
  - Group project presentation at the end of the semester.

Course Project Timeline

- Initial project proposal due: ***September 11, 2014***
- Project proposal finalized: ***September 18, 2014***
- Project interim progress report due: ***October 16, 2014***
- ***Group final project report*** due: ***November 13, 2014***
- Presentations:
  - Each student is required to make a part of presentation on the group course project
  - Presentation slides in electronic format must be submitted by noon on the presentation day

Sample Project Topics

1. Security and privacy in IoT (Internet-of-Things) environments
   a) Ambient intelligence for security and privacy in IoT
   b) Autonomous control for security and privacy in IoT
2. Trust management and Sybil detection in social networks
3. Privacy in social networks
4. Situation awareness in cyber space for security
5. Trustworthy data sharing in collaborative computing environments
6. Human factors related to security

Sample Project Topics (cont.)

7. Security in Software Defined Network
   a) Malicious behaviors analysis
   b) Load balancing
8. Malware Analysis for proactive detection and prevention
9. Cloud computing and service-based systems:
   a) Vulnerability assessment and intrusion detection
   b) Risk analysis and risk management
   c) Information dispersal and data hiding for cloud
   d) Confidentiality and integrity assurance
10. Network based solutions for MITM and DDoS attacks
    a) Model based attack detection and prevention
    b) Cryptographic solutions