# CSE 543
# Information Assurance and Security

## Overview and Concepts

Professor Stephen S. Yau

# *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

# *Sample Project Topics (cont.)*

6. Human factors related to security
7. Malware Analysis for proactive detection and prevention
8. 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
9. Network based solutions for MITM and DDoS attacks
   a) Model based attack detection and prevention
   b) Cryptographic solutions

# *Initial Course Project Proposal*
## *Due February 4, 2014*

1. Project title [8 – 20 words]
2. List of group members
3. Objective [one sentence]
4. Motivation [no more than 50 words]
5. Scope of study [no more than 50 words]
6. Expected major results [in bullet form, about 100 words]
7. For group project, each group member's responsibility
8. A preliminary list of references [***in standard format – authors in the order of appearance, title of the paper or book, publication (title of the journal or conference proceedings or URL website), volume number and date, page numbers inclusive (for journals and conference proceedings)*** ].

# *Interim Course Project Report*
## *Due March 6, 2014*

***Note: The content in this report must be consistent with your approved project proposal. If there is significant deviation, indicate that in the report and subject to approval .***

1. Project title
2. List of group members
3. Introduction
   - Background and Motivation (no more than one page)
   - Your Goals and scope of study of this project (no more than one page)
4. Results
   - The specific tasks you have completed
   - The tasks you will work the next two weeks
   - References each student has read
   - References each student will read, but not yet
5. Detailed Timetable (with major milestones for individual tasks)
6. References (should be complete, references given in standard format)
7. *No more than 15 pages for a group project, including figures and tables.*
8. *No more than 10 pages for an individual project, including figures and tables.*

# *Final Course Project Report*

1. **Deadline**
   1. In-class and Hybrid student group project: ***April 8, 2014***
   2. Online student project: ***April 24, 2014***
2. **Report Format**
   1. ***40 to 60 pages*** for each in-class group project ***(including figures, tables and references)***
   2. ***15 to 25 pages*** for each online student individual project ***(including figures, tables and references).*** For an online student group project, the length may increase appropriately.
   3. Font size and line spacing: 12 point and 1.5 lines spacing
   4. Page size: 8.5"X 11", one column.
3. **Report Content** ***(30 to 60 pages) – for in-class or hybrid group project; for online student project, reduced proportionally)***
   1. **Project title, section & group number, student names and a summary** [all in one page – cover page]
   2. **Introduction** ***(one - two pages)***
      1. Motivation and background
      2. Your goals and scope of study of this project
   3. **Overview of the project** ***(including each member's responsibilites)*** ***(one - two pages)***
   4. **Detailed Results** of each group members ***(20 - 40 pages)****
   5. **Conclusions and Recommendations** ***(usually no figures)*** ***(5 - 10 pages)****
   6. **References** ***(2 - 5 pages)*** ***(Each reference must be numbered and cited in text) (satisfying format)***

# *Additional Guidelines for Final Report*

- Detailed survey results* ***(20 – 40 pages)***
  - Highlights of each approach ***with reference citations***
    - Approach (method or technique)
    - Coverage
    - Summary of experimental or real-world data and analysis
    - Strengths and weaknesses (summary from the references)
- Conclusions * ***(5 – 10 pages)*** ***(in your own words)***
  - Comparison of strengths and weaknesses of all approaches
  - Recommendations, including future work

# *Additional Guidelines for Final Report*

- Detailed research results* ***(20 – 40 pages)***
  - Highlights of your approach ***with reference citations***
    - Approach (method or technique)
    - Coverage
    - Summary of experimental or real-world data and analysis
    - Strengths and weaknesses (summary from the references)
- Conclusions * ***(5 – 10 pages) (in your own words)***
  - Comparison of strengths and weaknesses of all approaches
  - Recommendations, including future work

# *Guidelines for Project Presentation*

- Each student of a group must present one part
- Total presentation of a group project, including short Q/A for clarification ***within 25 minutes***
- Discussions after presentation ***within 10 minutes***
- Focus on
  - Overall project, and highlights of survey results or current state of the art to support you conclusion ***within 15 minutes***
  - Conclusion ***within 10 minutes***

# *Final Individual Course Project Report*

- ***In addition to group report, each student*** must submit an ***individual*** project final report of no more than 10 pages (10 font, two column and single space), including figures.
- The individual project final report must include the following:
  - An ***overview*** of the project, including relevant references in specified format (***in each student's own words***, but the content must be consistent with the group reports of ***all*** the students in the same group)
  - ***Contributions*** made and lessons learned in the project by the student
- ***A satisfactory project, including the individual and group final reports, is required for passing the course***.
- If a student passes the course and wants to include the project report in his/her MCS portfolio, ***only the graded individual final report of the project*** can be used in his/her MCS portfolio.

# Information Assurance (IA)
## Overview and Concepts

- Concepts
- Principles & strategies
- Techniques
- Guidelines, policies & laws

# *Basic Concepts  of Information Assurance*

# *Information Forms and States*

- **Information Forms**
  - Hard copy
  - Softcopy
  - Records of formal and informal meetings
  - Telephone conversations
  - Video teleconferences
  - ……..
- **Information States**

  Transmitted, processed, stored

# *Threats and Vulnerabilities*

- A *threat* is a ***potential occurrence*** that can have an undesirable effect on the system assets or resources
- A *vulnerability* is a ***weakness*** that makes a threat to possibly occur

# *Four Categories of Threats*

- ***Disclosure***: Unauthorized access to information
  - Snooping
- ***Deception***: Acceptance of false data
  - Alteration
  - Spoofing
  - Denial of receipt
- ***Disruption***: Interruption or prevention of correct operations
  - Alteration
- ***Usurpation***: Unauthorized control of part of a system
  - Alteration
  - Spoofing
  - Delay
  - Denial of Service

# *Necessary Protection*

- Protect ***working areas*** from outside intrusion or theft
- ***Key equipment*** in secure rooms, and make sure it works properly
- Review ***programs*** carefully to detect potential malicious logic
- Keep track of all ***sensitive files, documents, conference records, experiment results***, which may be on printed papers. stored in magnetic storage media, CDs or DVDs.
  - Protect them from unauthorized access.
  - Backup this information periodically in case of system failure
- Encrypt ***sensitive information*** during storage or transmission
- Obfuscate ***sensitive data*** during processing
- Choose good ***passwords*** and change them periodically
- Report ***abnormal actions*** immediately

# *DoD Definition of Information Assurance*

Information Assurance (IA) is information operations (IO) that protect and defend information and information systems by ensuring their ***availability***, ***integrity***, ***authentication***, ***confidentiality*** *and* ***nonrepudiation***.

# *Information Characteristics*

***Availability*:**

Timely and reliable access to data and information services for authorized user.

***Integrity*:**

Protection against unauthorized modification or destruction of information

***Authentication*:**

Security measure designed to establish validity of transmission, message, or originator, or means of verifying an individual’s authorization to receive specific categories of information

# *Information Characteristics (cont.)*

***Confidentiality*:**

Assurance that information is not disclosed to unauthorized persons, processes, or devices.

***Nonrepudiation*:**

Assurance that sender of data is provided with proof of delivery to recipient, and recipient is provided with proof of sender's identification.

***Privacy*:**

Ability and/or right to protect certain ***personal data***; extends ability and/or right to prevent invasion of ***personal information or space***. Extends to ***families***, but not to legal persons, such as corporations, organizations, schools

# *Information Characteristics (cont.)*

***Secrecy*:**

Refers to the effect of mechanisms used to limit number of principals who can access information, such as cryptography or computer access control

***Denial of Service*:**

Mechanisms which prevent legitimate user from using the system.

# *Information System*

- Information system consists of
  - Computer systems and networks
  - Information
  - Operating environments

# *INFOSEC*

- ***INFOSEC***: Information Systems Security
  - Protection of information systems against *unauthorized access* to, or *modification of, information*, whether in storage, processing or transit, and against *denial of service* to authorized users or provision of *service to unauthorized users*, including those measures necessary to detect, document, and counter such threats.

# *OPSEC*

- ***OPSEC*: Operations Security**
  - A *process* that determines *what information* adversaries can obtain or piece together from observation and to provide *measures* for reducing such vulnerabilities to acceptable levels

# *Other Important Terms*

- ***Rainbow Series***
  - A series of computer security standards published by US government in 1980s and 1990s describing a process of evaluation for ***trusted systems***.
  - Originally published by DoD Computer Security Center, and then by the National Computer Security Center. Total 35 books have been published
  - Nicknames based on the colors of their covers. For example, the first book of the series and the most well-known book is The DoD Trusted Computer System Evaluation Criteria (DoD 5200.28-STD) in 1983, which is often referred to as ***"The Orange Book"***

# *Other Important Terms (Cont.)*

- ***Indicators:***
  - Profile indicator – normal activities
  - Deviation indicator – different from normal activities
  - Tip-off indicator – drawing attention to information that otherwise might pass unnotices.