1. Course Title (Course Code)

Information Security (2225)

2. Instructor

Hisato Shima

3. Term

Fall 2 (M2 students only)

4. Outline and Objectives

In this course students learn basics of information security, in both management aspect and technical aspect. Students will understand of various types of security incidents and attacks, and learn methods to prevent, detect and react incidents and attacks. Students will also learn basics of application of cryptography which are one of the key technology to implement security functions.

At the last session, teams of students will make presentation of their study project for a topic related to information security.

5. Goals (Attainment Targets)

(1) To become able to explain various Information security threat and controls for it.
(2) To become able to analyze a security incidents and design countermeasures.
(3) To become able to explain information security incident response.
(4) To become able to explain the usage of Common Key cryptography and Public Key cryptography.
(5) To become able to explain the mechanism to protect confidentiality and completeness of data.

6. Correspondence relationship between Educational goals and Course goals

<table>
<tr><th colspan="3">Educational goals</th><th>Course goals</th></tr>
<tr><td rowspan="2">High level ICT skill</td><td colspan="2">Basic academic skills</td><td>(1), (2), (3), (4), (5)</td></tr>
<tr><td colspan="2">Specialized knowledge and literacy</td><td>(2), (3)</td></tr>
<tr><td rowspan="8">Human skill
(Tankyu skill)</td><td colspan="2">Ability to continually improve own strengths</td><td></td></tr>
<tr><td rowspan="4">Ability to discover and resolve the problem in society</td><td>Problem setting</td><td></td></tr>
<tr><td>Hypothesis planning</td><td></td></tr>
<tr><td>Hypothesis testing</td><td></td></tr>
<tr><td>Practice</td><td></td></tr>
<tr><td rowspan="3">Fundamental Competencies for Working Persons</td><td>Ability to step forward</td><td></td></tr>
<tr><td>Ability to think through</td><td>(2), (3)</td></tr>
<tr><td>Ability to work in a team</td><td>(2), (3)</td></tr>
<tr><td colspan="3">Professional ethics</td><td>(2), (3)</td></tr>
</table>

7. Requirements

Fundamentals of Information Networks (achievement of attainment targets is required)

8. Textbooks

None

9. Reference Books

Title: Principles of Information Security
Author: Michael E. Whitman and Herbert J. Mattord
Publisher: Cengage Learning;
ISBN: 1285448367

To understand cryptography in depth
Title: Understanding Cryptography: A Textbook for Students and Practitioners
Author: Christof Paa and Jan Pelzl
Publisher: Springer
ISBN: 3642041000

10. Evaluation

Goals	Evaluation method & point					
	term-end exam	quiz	report	presentation	deliverable	other
(1)		○		○		
(2)		○		○		
(3)		○				
(4)		○				
(5)		○				
Allocation		70		30		

Course Schedule
(Notice) This schedule is a tentative plan, there might be changes, additions, or revisions etc. at the time of delivering the course.

Lesson 1: Overview of Information Security (Lecture, 90 min)

The overview of this course will be explained. Students understand the goal and scope of this course through several examples of security incidents.

1. Orientation (learning objectives, performance evaluation, etc.)
2. What is Information Security?
3. Examples of Information Security Incidents
4. What is Information Security Management

Lesson 2: Basics of Information Security and Human aspects (Lecture, 90 min)

Students learn the three concepts of information security and other basic concepts. Human and Management Aspects of Security measure is explained.

1. Causes of Information Security Incidents
2. The three concepts of Information Security (Confidentiality, Integrity, Availability)
3. Basic terminologies in Information Security
4. Human Aspect of Information Security
5. Social Engineering and Internal Crimes

Lesson 3: Information Security for Server Systems (Lecture, 90 min)

Security Attacks for Server systems will be explained and discuss counter measure for attacks.

1. Attacks to Server Systems connected to the Internet and counter measures
2. Attacks to Web Servers and counter measure
3. Denial of Service Attack
4. Attacks to Network Systems

Lesson 4: Information Security for Client devices (Lecture, 90 min)

Security Attacks for Client devices will be explained and discuss counter measure for attacks.

1. Attacks for Personal Computers and Smart phones, and counter measure
2. How the malicious software intrude the device?
3. What the malicious software does to the system?

Lesson 5: Information Security Risk Management (Lecture, 90 min)

Students learns Risk Management process for Information Systems

1. What is Risk Management process?
2. Identifying Information Assets
3. Identifying Security Risk and evaluation
4. Risk Treatment

Lesson 6: Information Security Risk Management Exercise (Exercise, 90 min)

Students exercises Risk Management process

1. Identifying Information Assets
2. Identifying Security Risks and evaluate them
3. Treatments of identified risks

Lesson 7: Security Risk management as an Organization (Lecture, 90 min)

Students learn how an organization manage security risks, including, establishing policy, security organization and rules.

1. Information Security Governance
2. Information Security Management System (ISMS)
3. Information Security Policy, Standards and Procedures
4. Information Security Evaluation

Lesson 8: Security Incident Response (Lecture 30 min, Exercise 60 min)

Students learn about organization to handle security incidents, and understand how to react to security incidents through exercise

1. What is Security Incident response
2. Computer Security Incident response team
3. Incident response exercise

Lesson 9: Information Security and Cryptography (Lecture, 90 min)

Cryptography is essential technology to protect Information Security. In this section, Students learns about basic concept of cryptography

1. Requirements for Secure Communication
2. What is Cryptography?
3. Classic Cryptography
4. Modern Cryptography

Lesson 10: Common Key Cryptography (Lecture 45 min, Exercise 45 min)

Students learn and exercise Common Key Cryptography

1. Common Key Cryptography algorithms: DES, Triple DES, AES
2. Encryption modes
3. Exercise on Common Key Cryptography

Lesson 11: Public Key Cryptography (Lecture, 90 min)

Students learn about Public Key Cryptography.

1. Key distribution problems of Common Key Cryptography
2. What is Public Key Cryptography?
3. RSA
4. Hybrid encryption

Lesson 12: Public Key Exercise and Recommended Ciphers (Exercise 60 min, Lecture 30 min)

Students exercise Public Key Cryptography and Hybrid encryption. Learn about Standard Ciphers.

1. Exercise of Public Key Cryptography
2. Exercise of Hybrid encryption
3. Recommended Ciphers

Lesson 13: Data Integrity and Digital Signature (Lecture 45 min, Exercise 45 min)

Students learns how to detect unauthorized change of data

1. Integrity of Data
2. Hash Function
3. Digital Signature
4. Exercise of Hash functions and Digital Signature

Lesson 14: Public Key Certificate and PKI (Lecture 45 min, Exercise 45 min)

Students learns about Public Key Certificate and Public Key Infrastructure (PKI)

1. Key Certificate: Digital Signature of Public Key
2. Public key Infrastructure (PKI) and Certificate Authority
3. Exercise on PKI

Lesson 15: Presentation and Discussion (Presentation, 90 min)

Groups of Students will make presentations for the topic they selected and researched. After each presentation, we have Q&A and Discussion session in the class.