1. Course Code

2225

2. Course Title

G71e: Information Security

3. Teacher

IWAMOTO, Hisashi

4. Term

Fall 2

5. Course Requirements (Courses / Knowledge for this course) and Important Information

None

6. Course Overview and Objectives

In this course, students learn basics of information security, in both management aspects and technical aspects. 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 application of cryptography which are one of the key technologies to implement security.

7. Course Outline

1 Overview of Information Security
2 Basics of Information Security and Human aspects
3 Information Security of IT Systems(Part 1)
4 Information Security of IT Systems(Part 2)
5 Information Security for Web Services
6 Security for Information Networks
7 Information Security Risk Management
8 Information Security as an Organization
9 Information Security and Cryptography. Shared Key Cryptography
10 Public Key Cryptography
11 Completeness of data and Digital Signature
12 Public Key Certificate and PKI
13 Presentation and Discussion
14 Presentation and Discussion
15 Security Incident Response and Course Summary
16

8. Textbooks (Required Books for this course)

None

9. Reference Books (optional books for further study)

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 Paar and Jan Pelzl
Publisher: Springer
ISBN: 3642041000

10. Course Goals (Attainment Targets)

(1) To understand various Information security threats and controls for it.
(2) To understand information security management in an organization.
(3) To understand information security incident response.
(4) To understand the usage of Shared Key cryptography and Public Key cryptography.
(5) To work in a group to research and present about security related topics
(6)
(7)
(8)

11. Correspondence relationship between Educational goals and Course goals

Educational goals of the school			Course Goals
High level ICT skills	Basic academic skills		
	Specialized knowledge and literacy		(1)(2)(3)(4)
Human skill (Tankyu skill)	Ability to continually improve own strengths		
	Ability to discover and resolve the problem in society	Problem setting	
		Hypothesis planning	
		Hypothesis testing	
		Practice	
	Fundamental Competencies for Working Persons	Ability to step forward	
		Ability to think through	(5)
		Ability to work in a team	(5)
Professional ethics			

12. Evaluation

Goals	Evaluation method & point allocation					
	examination	Quiz	Reports	Presentation	Deliverables	Other
(1)		○		○	○	
(2)		○		○	○	
(3)		○			○	
(4)		○			○	
(5)				○		
(6)						
(7)						
(8)						
Allocation		60		30	10	

13. Evaluation Criteria

Examination	
Quiz	Quiz in every week evaluates students understand the key contents of the lectures and materials.
Reports	
Presentation	Studetns research and present a topic he choose. Presentation contents, materials and skill are evaluated by peer reviews by students.
Deliverables	Evaluates the participation and understanding of the excersize in the class
Other	

14. Active Learning

Hourly percentage of active learning within the whole class time		30%
1	Active learning such as problem solving assignment using the knowledge and skills acquired in class.	All the time
2	Active learning such as group works and discussions.	Sometimes
3	Outcome presentations and feedbacks.	Sometimes
4	Students actively make decisions on how the class should be conducted.	Not at all

15. Notes

Class materials are offered as pdf files. Your PC (Windows, Mac or Linux) and the Internet connection are required for the class and homeworks.

16. Course plan

(Notice) This plan is tentative and might be changed at the time of delivery

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

Lesson 2: Basics of Information Security and Human aspects (Lecture 60 min., Exercise 30 min.)

Students learn the various courses of security incidents. In this session, human Aspects of Security incident and their countermeasures are explained. Students also learn the key concepts of information security.

1. Trends of Information Security Incidents
2. Human Aspect of Information Security
3. The Key concepts of Information Security (Confidentiality, Integrity, Availability)
4. Words used in Information Security

Lesson 3: Information Security of IT Systems(Part 1) (Lecture 60 min., Exercise 30 min.)

Security threads for Client devices (such as Personal Computers) and their countermeasures are discussed

1. What is Malware (Computer Virus) ?
2. How a Malware intrudes the system?
3. Social engineering

Lesson 4: Information Security of IT Systems(Part 2) (Lecture 60 min., Exercise 30 min.)

Security threads for Server systems are explained and their countermeasure are discussed..

1. How server systems are attacked?
2. User authentication and password
3. Server Security Protections

Lesson 5: Information Security for Web Services (Lecture 60 min., Exercise 30 min.)

Security threads for Web servers and their countermeasures are discussed

1. Attacks to Web Servers
2. SQL Injection Exercise
3. Denial of Service Attack

Lesson 6: Security for Information Networks (Lecture 60 min., Exercise 30 min.)

Security threads for Computer Networks and their countermeasures are discussed

1. Separation of networks and Firewall
2. Network monitoring and Intrusion Detection
3. Wireless and Wired LAN Security
4. Security of communication over public Internet

Lesson 7: Information Security Risk Management (Lecture 60 min., Exercise 30 min.)

Risk Management process for Information Systems is explained

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

Lesson 8: 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. Security Management for Organization
2. Information Security Management System (ISMS)
3. Security Organization and Responsibilities
4. Information Security Policy, Standards and Procedures
5. Information Security Evaluation

Lesson 9: Information Security and Cryptography. Shared Key Cryptography (Lecture 60 min., Exercise 30 min.)

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

1. Information Security and Cryptography
2. Classic Ciphers
3. Shared Key Cryptography: DES, AES
4. Encryption modes for block ciphers

Lesson 10: Public Key Cryptography (Lecture 60 min., Exercise 30 min.)

Students learn Public key Cryptography and Hybrid Cryptography

1. Key delivery problem of Shared Key Cryptography
2. Public key cryptography, RSA
3. Hybrid cryptosystem
4. Exercise of Cryptography

Lesson 11: Completeness of data and Digital Signature (Lecture 60 min., Exercise 30 min.)

Technology for Integrity. How to detect unauthorized change of data

1. Completeness of Data and Cryptography
2. Hash Functions
3. Digital Signatures

Lesson 12: Public Key Certificate and PKI (Lecture 60 min., Exercise 30 min.)

Technology for Authenticity. Public Key Certificate and Public Key Infrastructure (PKI)

1. Vulnerabilities in using Public Key cryptography
2. Key Certificate: Digital Signature of Public Key
3. Applications of Public Key Certificate

Lesson 13-14: Presentation and Discussion (Presentation, 180 min.)

Students will make presentations for the topic they selected and researched.

Lesson 15: Security Incident Response, Review of the student's presentation and Course Summary (Lecture 60 min., Exercise 30 min.)

Students learn how an organization should react and handle security incidents

1. Computer Security Incident response team (CSIRT)
2. How to Respond to Incidents?
3. Review of the student's presentation
4. Summary of the Course