Information Security

Syllabus Number 3C327

Special Subjects
Elective 2 credit

MORI, Takuo

1. Course Description

Information security techniques are one of the indispensable techniques and are becoming much more important as an infrastructure of networked societies.

The term "information security" covers very broad fields, from foundational theories such as elementary number theory, algebraic systems, cryptography, and computer science to cryptographic protocols or network protocols in general. In this course, we mainly deal with the latter fields.
This course relates to the diploma policy DP4C.

2. Course Objectives

The goal of this course is that students master the following abilities;

Students can explain the basics of elemental number theory and abstract algebraic systems which construct public key crypto systems and explain the meanings of mathematical expression used in the public key crypto systems.
Students can explain the basic features of secret key or public key crypto systems, block cipher modes of operation and Hash functions, and can process encryption/decryption as for basic crypto systems.
Students can explain the purpose and summaries of information security, cryptographic protocols and network protocols, and explain or execute the processes of basic protocols.
Students can classify malware which is one of the factors of the illegal accesses, and explain the countermeasures against illegal accesses.
Students can explain the summaries, the purposes and the problems of identification, biometric identification.
Students can explain the security evaluation and its standardization.

3. Grading Policy

Grading policy:
Midterm report(50%), Examination(50%).

The way of feedback;
Answers for questions or feedback for the contents of class and examination will be given in a class, through LMS or in office hours.

4. Textbook and Reference

Textbook
宮地充子,菊池浩明編著　IT Text 情報セキュリティ　オーム社、ISBN-13: 978-4274132841

5. Requirements(Assignments)

Before each class, materials related to the class will be published through LMS. Students should download them to their own devices or print them to make it possible to refer to or to take notes.
Students should read these materials and grasp what they do not understand and they understand in an hour.
After each class, student should review the class through tests on the LMS in half an hour.

6. Note

Students can hardly earn credits without submitting the mid-term report. Thus, it is expected students to observe the deadline.
As for the self-learning support, students are expected to utilize materials, such as slides, handouts, and quizzes on the LMS

Before taking this course, students should take the following courses;
Mathematical Logic, Linear Algebra, Discrete Mathematics, Computer Networks, Programming Language Theory, Graph Theory, Introduction to the theory of automata and computation, Software Technologies for Information Systems Development, Web Technology, Digital Signal Processing, Digital Image Processing.

At the same semester with this course, students should take take the following courses;
Laboratory in Computer Science 1, Information Theory, Information System Design, Laboratory on Computer Network.

After taking this course, students should take the following courses;
Laboratory in Computer Science 2, Operating System, Software Engineering, Informatic Sociology, Web Application.

If a student has a question on quizzes or mid-term report or examinations, ask the question in the class or in office hours or through LMS.

This course is a required course, and relates to the mid term 1-3 and 5-1 of the attaining targets for learning and educating, in the JABEE program.

7. Schedule

[1]	Information security, introduction to the information security, threats against information security, countermeasures against threats, cipher systems
[2]	Secret key cryptography, cipher systems, block/stream cipher, the evaluation of ciphers.
[3]	Basic theory of Public key cryptography, digital signature
[4]	Basic theory of Public key cryptography, digital signature 2, cryptographic primitives, a public key cryptography based on the factoring problem.
[5]	Public key cryptography/Digital Signature
[6]	Public key cryptography/Digital Signature, signature schemes with a hash function, signature schemes without a hash function, secret sharing schemes
[7]	Cryptographic Protocols, multi-party protocol, distributed decryption of RSA, group-signature and multi-signature.
[8]	Zero knowledge proofs and its application to the social systems, electronic money, electronic voting
[9]	Network security, client-authentication, Public Key Infrastructure(PKI)
[10]	Internet security, IPSEC, SSL/TLS, S/MIME
[11]	Illegal access, computer viruses, detection techniques of illegal access, targeted threats
[12]	Information hiding, digital watermark, steganography, anonymous channel
[13]	Biometric, the necessity of identification by using biometrics, identification by using information proper to a person
[14]	Computer security certification
[15]	Summary and examination