Introduction to modern cryptography and information security

Special Subjects
Elective 2 credit

MORI, Takuo

1. Course Description

Information security covers broad fields, from the cryptography to practice information networks or systems. In this course, we aim at understanding systematically the way to deal with security problems which may happen in practical information systems, from basic.

This course relates to the diploma policy 1, 4 of the division of informatics science, graduated school of Teikyo University.

2. Course Objectives

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

Students can explain how to prevent from unauthorized accesses, and show basic countermeasures against unauthorized accesses.
Students can explain how to protect Web-applications, and show basic countermeasures against attack to the Web-applications.
Students can explain the operation principles of malware, and show basic countermeasures against malware.
Students can explain the operation principles of intrusion detection/protection systems(IDS/IPS) and, how to introduce them.
Students can show basic access control techniques and choose appropriate ones according to the situation.
Students can explain information security protocols.
Students can explain foundations of constructing/operating information systems.
Students can outline basics of Information Management Systems.
Students can explain new trends in information security technology.
Students can explain and write basic cyber-security programmings.

3. Grading Policy

Grading policy: Examination(100%)

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

4. Textbook and Reference

Textbook
佐々木良一監修、電子情報通信学会編　現代電子情報通信選書「知識の森」　ネットワークセキュリティ　オーム社、ISBN-13: 978-4274215179
Reference
Justin Seitz著, 青木 一史 訳, 新井 悠 訳、一瀬 小夜訳、岩村 誠訳、川古谷 裕平訳、星澤 裕二訳　サイバーセキュリティプログラミン　―Pythonで学ぶハッカーの思考　オライリージャパン、ISBN-13: 978-4873117317

5. Requirements(Assignments)

Before each class, materials for each class will be published through the LMS. Each student should download materials to one's own device or
print them out on paper so that you can refer to them and write on them.

After reading through these materials for about 1 hour and 30 minutes, each student shoud identify what you have understood and what you have not understood.

Take about 1 hour and 30 minutes to check your understanding with the test on the LMS and review.

6. Note

In order to earn credits in this course, students must submit two reports and take the examination.

Students should have basic (at least, undergraduate level) knowledge of the following source,
Mathematical logic, Algebraic systems, Elementary number theory, Complexity theory, Network technology, Programming language, Database theory.

After taking this course, students should take Quantum Information Science.

7. Schedule

[1] A trends in network security
[2] Unauthorized access1 -Password Cracking-
[3] Unauthorized access2 -Basics of Web-application security-
[4] Unauthorized access 3 -Injection, XSS-
[5] Unauthorized access 4 -CSRF, Buffere-overflow, Drive-by-download-
[6] Malwares
[7] Intrusion detection/protection systems.

[8] Access control1 -An introduction to the access control-

[9] Access control2 -Identification, Firewall-
[10] Information security protocols
[11] Construction/Operation of information security systems
[12] Information security management systems
[13] New Trends in network security1 -APT/IPv6-
[14] New Trends in network security2 -Threat to smart phones/tables-
[15] Cyber security programming