EECS 711 Security Management and Audit

Instructor: Dr. Fengjun Li

Spring 2016

Outline

- Course Introduction
  - Overview
  - Objective
  - Logistics
- What is security management?
  - Outline of the course
  - Our first assignment

Course Overview

- What is this course about?
  - “*information security in the modern organization is a management problem, and not one that technology alone can answer*”
  - We cover the pure technical side of information security in EECS710, EECS712, EECS765, and EECS866.
  - Now we look at this problem from a completely different perspective.

Course Overview

- What is the importance of security management?
  - Human is the weakest link in information security
  - Technical solutions are available – not always correctly adopted.
    - Example: in the past many years, most password breaches are caused by SQL injection (and XSS) attacks
    - Simple technique, simple control, turned out to be very effective
    - Why?
  - Again: “*information security in the modern organization is a management problem*”

Course Objectives

- The course is aimed at imparting knowledge and skill sets that are required to assume the responsibilities of security administrations and management of security of an enterprise information system.

Course Objectives

- Understand the basic issues, concepts, principles, and mechanisms in security management
  - Understand security and contingency plans
  - Understand security policies, models and practices
  - Understand risks – risk assessment and control
  - Understand legal, compliance and certification issues
- Identify real-world security issues and propose solutions

Time & Location

- Time: Wednesday 6:10 pm – 9:00 pm
- Room: BEST 235
- Instructor
  - Fengjun Li, Assistant Professor at EECS
  - fli@ku.edu, please add **[EECS711]** in email subject
  - Office hour: Wed 5:00 – 6:00 pm or by appointment
  - BEST 250G or Nichols 239
- We don’t have a TA/grader

Course Structure

- Lectures
  - Descriptive: what is out there.
  - Critical: what is wrong with …
- In-class discussions
  - Based on real-world cases
  - What is wrong, how to solve it
- Homework: approximately five
- Projects: several mini-projects
- Two exams

Prerequisites

- EECS 710 – Information security
  - Understand security concepts and mechanisms
  - Understand cryptography primitives
  - Understand the “big picture” of security research

Text

- Whitman, Michael E., and Herbert J. Mattord. *Management of Information Security*. Cengage Learning; 3rd edition.
- Research articles (provided on Blackboard)

Using Course Website

- Course website is online
  - http://www.ittc.ku.edu/~fli/eecs711/index.html
- Provide overview of
  - Course syllabus
  - Course schedule
  - Projects
    - Team info
    - Instructions for projects

Using Blackboard

- Materials are available on Blackboard
  - Lecture slides
    - Lecture slides for each class are uploaded ahead of time
      - Well, sometimes they're uploaded shortly before or after the class …
    - If you miss a class, please read the lecture notes and come to see me at office hours
  - Reading materials
  - Project assignments
  - Homework assignments
- We maintain a discussion forum on BB
- Sharing information with email list

Grading

- Homework: 10%
- In-class case study: 10%
- Team projects: 30%
- Exam 1: 25%
- Exam 2: 25%
- Class participation: ±1%

Grading Logistics

- Grade scale: A: >=90%; B: >=75%; C: >=60%; D/F: below 60%.
- Grade dispute
  - Contact me within one week of returned grade
- Late Policy
  - Get instructor’s approval before missing a class, otherwise you need to show proof of emergency (e.g., doctor’s notes)
  - Late assignment will be accepted with a 20% reduction in grade for each day late by.
  - Final project presentation: not accepted.

Policies

- Academic Integrity!
    - Discussing homework with other is encouraged
    - However, all written material and programs must be individual work unless otherwise instructed
        - Please include something like “I have discussed this homework with ...”. There’s absolutely no penalty for doing this.
    - Always reference your source of information
    - Zero tolerance for cheating or copying other people’s work
    - It’s your responsibility to follow the University academic honesty policy

Course Outline

- Security planning
  - organizational planning
  - Contingency planning
- Security policies and operations
  - Security policies
  - Organizational security program
  - Security models and practices
- Risk assessment and control
- Personnel, law and ethics

Project Groups

- You are expected to work in groups of three
- You will do:
  - In-class practices
  - Course projects

In-class Case Study

- In-class practices: security case-study
  - One student will present a real-world security case
  - Students discuss in groups: what happened (from security management perspective)? what was wrong? how to properly handle this case? how to avoid this in the future?
  - One group will present their findings
  - The other groups are expected to challenge the presenters

Assignment 1: CS Task 1

- Explore news reports
- Collect stories of security breaches in the past 5 years
- Identify three stories that are very different from each other. For each story:
  - Give a one-sentence summary of the case
  - Explain (in no more than two sentences) why you pick this case
  - List URLs (no more than three) to news reports about this case
  - Submit to Blackboard

Course Projects

- Three projects. In each project, you will be given a business scenario, in which you are expected to design security policies, mechanisms, etc.
- In each project, we assign three teams into three roles:
  - “The Boss Team”: articulates the scenario, explain the requirements, make assumptions, makes clarifications at the request of the security team.
  - “The Security Team”: the information security manager in the enterprise: designs security policies, instructions, mechanisms, etc, as requested by the boss team.
  - “The Inspector Team”: examines the outputs from the other teams, challenges their work.