**Sunday April 10, 2022**

# EAST WEST UNIVERSITY

**Department of Computer Science and Engineering**
**B.Sc. in Computer Science and Engineering Program**
**Midterm-2 Examination, Spring 2022 Semester**

| | |
|---|---|
| **Course:** | **CSE487 Cybersecurity, Law and Ethics, Section-1** |
| **Instructor:** | **Rashedul Amin Tuhin, Senior Lecturer, CSE Department** |
| **Full Marks:** | **30 (15 will be counted for final grading)** |
| **Duration:** | **80 minutes** |

**Notes:** There are **FOUR** questions, answer ALL of them. Course Outcome (CO), Cognitive Level, Mark, for each question are mentioned at the right margin.

The exam contains **complex engineering problems**, EP4: Familiarity of issues, EP5: Extent of applicable codes, EP6: Extent of stakeholder involvement and conflicting requirements

The invigilator and the examiner reserve the right of not accepting the answer script, in any case of (not limited to) non-compliance, late submissions, cheating and misbehavior.

---

**Q1.** John joined as the Chief Technical Officer (CTO) of an organization called ACME INC last month. His organization has many servers, containing sensitive data and mission-critical services. Often a number of hacking attempts take place, which are blocked by the firewall regularly. ACME has Annual Maintenance Contracts (AMCs) with three companies (say X, Y, and Z), one for the servers (storage), one for the core network infrastructure (switch, router, firewall), and one for the peripheral devices (power unit, precision AC, firefighting equipment). The three companies X, Y, and Z perform routine maintenance every four months (April, August, and December). **[CO3, C3, Mark: 05]**

Last week, John received an email from Alice (the contact person from company Y), that they are going to install a security update on one of the firewalls. Alice also emphasized that the current version of the software is prawn to a newly discovered vulnerability, and without the security update, the overall system will be vulnerable. On Monday around 13:00, an employee, named Bob, from company Y, came to install the update. Bob showed his photo ID, which matched with his face. Bob also called of Alice from his phone and gave the phone to John, and Alice confirmed that Bob was sent from company Y. Being convinced after the conversation, Bob was allowed to enter the datacenter to install the security update. Within 15 minutes, Bob finished his work, made a courtesy visit with John, said goodbye and left around 14:00. On Wednesday around 23:00, the whole system of ACME was attacked, and a considerable amount of data was modified and destroyed, bypassing the firewall.

**Identify** the reasons why such attacks succeeded this time, and how it could be prevented in future.

**Q2.** With the help of a diagram, **explain** the *Kerberos* authentication protocol. **[CO3, C3, Mark: 10]**

**Q3.** **Explain** the general mechanism of a DDoS attack. **Discuss** at least two types of DDoS attacks, with prevention mechanisms. **[CO3, C3, Mark: 05]**

## Principles of Data Collection and Use [EP4, EP5, EP6]

**Q4.** Assume that ACME INC is a renowned pharmaceutical company in Bangladesh, who are planning to produce a new drug for Hepatitis C. The treatment of Hepatitis C is costly. You are assigned to perform a feasibility study that requires a survey of the Hepatitis C patients, and their financial capabilities of affording the treatment. **[CO3, C3, Mark: 10]**

Based on the survey data, the pharmaceutical company will decide the scale of production of the drug. The brand value of pharmaceutical company is remarkable and can not be compromised.

**Applying** the principles for data collection and use, create the informed consent document to collect the legal consent of the participants of the survey.

Use reasonable assumptions, if necessary.