# ELEC0138: Security and Privacy Coursework 1

## 1. Introduction and Objectives

In today's digital landscape, where data is a critical asset, ensuring security and privacy is paramount. This document aims to define a threat model and potential security or privacy attacks to address risks associated with malicious attackers, employees, and theft of payment information, regarding to online databases in marketing scenarios.

## 2. Asset Identification

Considering a marketing scenario, in which various commercial data is collected / aggregated (via terminal devices), sent / retrieved (from central databases, via secured network), and processed locally at specified device(s). The following aspects could be focused on:

Terminal devices as IoT instantiations;

Database security: access management and attack prevention by network traffic inspection;

Data processing: against data/model poisoning

Distributed learning applications;

potential privacy implications of information exposure

## 3. Threat Model

### Threat: Malicious Attacks

- Vulnerabilities: Exploiting vulnerabilities in the database access service.

- Likelihood: Low, but significant impact if successful.

- Impact: Loss of service /poisoned data/model, leading to the loss of critical functions, sensitive info. Exposure, leading to degraded reputation.

- Protection: Implement measures such as network isolation, application-layer threat prevention, identity and access management (IAM), and regular security updates to mitigate risks.

### Threat: Employees Misperformance

- Vulnerabilities: Internal database access service vulnerabilities.

- Likelihood: Relatively Low.

- Impact: Loss of service or leakage of sensitive data.

- Protection: Utilize Role-Based Access Control (RBAC), enforce the Least Privilege Principle, and employ data encryption to restrict unauthorized access.

### Threat: PII-contained data exposure during network transporting

- Vulnerabilities: network transportation & encryption vulnerabilities

- Likelihood: Moderate

- Impact: Data breaches, financial loss, reputational damage.

- Protection: Implement robust encryption algorithms, intrusion detection systems (IDS), and stringent access control mechanisms to safeguard payment information.

### Threat: Mis-usage of data … …

## 3. Data Sources and Attacks Set-Up

To assess and simulate potential attacks, we will utilize various data sources including network traffic logs, system logs, application logs, and data flow diagrams.

Data could be accessed via online databases (Kaggle etc.) or simulated if possible (de-private);

Set up a Linux vm for testing & performing attacks, reusing code snippets given in lectures.

-tcpreplay, pcap(s), python files (for later processing)

Possible attacks as listed:

Ddos (tcp,dos, http…)

Man-in-the-middle

Brute-Force (password leakage)

(possible memory overflow vulnerability, but no-code supported)

…

## 4. Assess Impact and Prioritize Threats

### Assessment Criteria:

- Impact: Evaluate the severity of each threat based on potential consequences such as data loss, financial loss, legal implications, and reputational damage.

- Likelihood: Assess the probability of each threat materializing based on historical data, industry trends, and internal vulnerabilities.

- Feasibility: Consider the technical feasibility and resources required for attackers to exploit vulnerabilities.

- Mitigation Cost: Estimate the cost associated with implementing security measures to mitigate each threat.

### Prioritization:

1. Malicious Attacker: High impact, low likelihood, but critical to mitigate due to potential loss of service.

2. PII-contained data exposure during network transporting: relatively high impact, moderate likelihood, remedies may take time (update issues)

3. Employees: Low impact, low likelihood, but essential to prevent insider threats and data leakage.

By prioritizing threats based on impact, likelihood, and feasibility, organizations can allocate resources effectively to mitigate risks and enhance security posture. Regular risk assessments and proactive security measures are crucial to adapt to evolving threats and protect sensitive data effectively.