UNIVERSITY COMPUTER SCIENCE • EXERCISE SHEET

12.6 Security and professional ethics

Name: _____ Class: _____ Date: _____ **Total: 24 marks**

KEY WORDS threat model

Objective

Build a threat model and answer an ethics call in writing.

1 Key knowledge and worked examples

■ **The model**

Assets x entry points x attackers; each threat paired with a mitigation and a test ✓.

■ **Worked example: the matrix**

3 roles x 6 actions = 18 cells; 4 allowed; 14 denials by default ✓.

2 Practice

2.1 Name BookShare's three entry points. [3]

2.2 How does the search form close its injection row? [3]

2.3 State the professional answer to a data-sale request. [3]

3 Exam-style questions

3.1 The renewal API endpoint accepts a member id and a copy id.

Threat-model it: name the assets touched, the plausible attackers, and two threats (one injection-shaped, one authorisation-shaped). Pair each with a mitigation and its test. Add the endpoint's row to the authorisation matrix (which cells newly allow?). [8]

3.2 The owner asks: "Sell anonymised reading history to advertisers – revenue is tight."

Distinguish this from the earlier raw-history request. State what the codes say about employer preference versus public interest. Give the engineer's written response with its alternatives and its paper trail. [7]

Solutions

2.1

- Web form, API, reminder channel ✓.

2.2

- Parameterised queries plus a length cap – tested by feeding `' OR '1'='1` and asserting zero rows leaked ✓.

2.3

- Documented refusal with alternatives, traceable to a code ✓.

3.1

- Assets touched: loan records, member ids ✓.
- Attackers: opportunistic outsider with the API, an insider testing another member's data, automated scanners ✓.
- Injection threat: crafted ids – mitigation: parameterised inputs and schema validation; test: payload ids return structured errors, zero leakage ✓.
- Authorisation threat: member A renews member B's loan – mitigation: ownership check at the domain boundary; test: cross renewal refused with 403 ✓.
- Matrix: member-renew and librarian-renew cells allow (2 new allows); the rest of the renewal column denies ✓.

3.2

- Distinction: anonymised aggregate with consent is a different artefact from raw per-member history – the harm profile changes (re-identification risk remains the key question) ✓.
- Codes: privacy harm and public interest outrank employer preference; the engineer documents rather than quietly obeys or quietly refuses ✓.
- Response in writing: the concern (re-identification), the conditions under which it is defensible (consent, aggregate thresholds, review), alternatives (sponsorship, grants), and the decision record – the paper trail is the point ✓.