

1.1 Computing systems, networks and requirements

Name: _____ Class: _____ Date: _____

Total: 10 marks

KEY WORDS authentication • authorization

Objective

Computing systems, networks and requirements. Supported SL concept preparation; original classroom practice, not an official IB paper or assessed learner work.

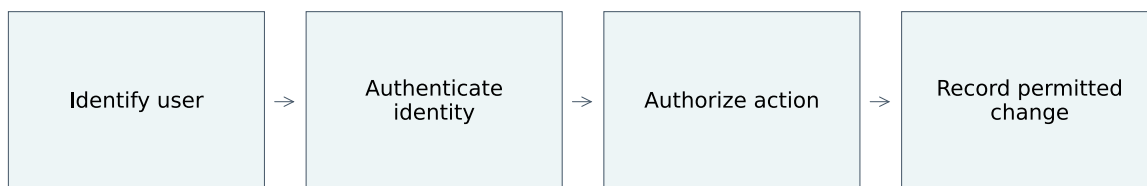
1 Key knowledge and worked examples

■ What would explain this observation?

- A school booking system can calculate correctly and still fail if users lose access or records are disclosed. Success includes the system context.
 - Start with a prediction. State the quantities or features you would compare, then decide what evidence could distinguish two explanations.
-

■ Build the model

- A computer system combines hardware, software, data and people. A network enables communication using protocols. Requirements should distinguish function from constraints such as availability, security and accessibility.
- **authentication** : Checking an asserted identity; **authorization** : Determining permitted actions.



■ Choose evidence that can test it

- Separate authentication from authorization. Authentication checks identity; authorization determines permitted actions. A threat model connects a valuable asset, a possible attack and an appropriate control.
- Use a fictitious school dataset to define users and permissions. Draw data flows, compare validation and verification, and specify tests for normal, boundary and invalid input. Do not use real credentials or student records in exercises.

■ Work from known quantities

- State the known values and their units. Choose the relation because its assumptions fit this case, then rearrange before substitution.
- Known: a file contains 12 megabytes, where this example defines one megabyte as one million bytes. $\text{Bits} = \text{bytes} \times 8 = 12 \times 1,000,000 \times 8 = 96,000,000$ bits. At 8,000,000 bits per second, ideal time = size/rate = 12 s, excluding overhead.

Example:

A 40 million bit file transfers at 5 million bits per second. Find ideal time. Use the same sequence: known quantities → model → relation → substitution → unit and interpretation.

■ Check the conclusion and its limits

- Bandwidth is not actual end-to-end throughput. Encryption does not by itself ensure correct authorization or remove every security risk.
- Return to the original observation. Explain what the result supports, which conditions it assumes, and one way to test a competing explanation.

Warn:

Encryption guarantees that every user has appropriate access permissions. This claim is false: Bandwidth is not actual end-to-end throughput. Encryption does not by itself ensure correct authorization or remove every security risk.

Key:

Computing systems, networks and requirements: Separate authentication from authorization. Authentication checks identity; authorization determines permitted actions. A threat model connects a valuable asset, a possible attack and an appropriate control.

■ Runnable trace and boundary

```
size_MB, rate_Mbps = 20, 10
bits = size_MB * 1_000_000 * 8
if rate_Mbps <= 0:
    raise ValueError("Rate must be positive")
seconds = bits / (rate_Mbps * 1_000_000)
print(seconds)
print(0 / (rate_Mbps * 1_000_000))
```

Expected output:

```
16.0
0.0
```

Decimal MB means one million bytes; multiply by eight before dividing by bits per second. Zero data has zero ideal transmission duration. A nonpositive rate is rejected; actual overhead is outside this arithmetic model.

2 Practice

2.1 Which question concerns authorization? Choose one answer.

- **A** Who are you?
- **B** May this user edit this record?
- **C** What colour is the login screen?

[1]

2.2 A 40 million bit file transfers at 5 million bits per second. Find ideal time. Show the relation, substitution and units.

[2]

2.3 Decide whether this claim is true and justify: Encryption guarantees that every user has appropriate access permissions.

[2]

2.4 Checking an asserted identity: write the technical term.

[1]

3 Exam-style questions

3.1 A 20 MB file uses decimal MB= 10^6 bytes and a 10 Mb/s link. Find ideal time and explain why observed time can be longer. [4]

Solutions

2.1 B Separate authentication from authorization. Authentication checks identity; authorization determines permitted actions. A threat model connects a valuable asset, a possible attack and an appropriate control.

2.2 $\text{time} = \text{size} / \text{rate} = (40 \text{ million bits}) / (5 \text{ million bits/s}) = 8 \text{ s}$.

2.3 False. Bandwidth is not actual end-to-end throughput. Encryption does not by itself ensure correct authorization or remove every security risk.

2.4 authentication. authentication means Checking an asserted identity.

3.1 $\text{Time} = 20 \times 10^6 \times 8 / (10 \times 10^6) = 16 \text{ s}$. Overhead, contention and delays add time. Distinguish bits from bytes and storage capacity from sustained transfer rate.