Question 1: Security Engineering Basics [20 points]

(a) **[2 points]** Explain the fundamental security design principle *Economy of Mechanism*.

(b) **[4 points]** Explain the Principle of *Psychological Acceptability*.

(c) **[5 points]** Consider the following security scenarios. For each scenario, classify the attack as either an **active attack** or a **passive attack**.

i A network attacker intercepts and records encrypted Wi-Fi traffic between a user and a web server for later analysis.

ii An attacker sends a flood of malformed packets to a web server to make the service unavailable to legitimate users.

iii An attacker secretly monitors keystrokes on a compromised machine without altering system behaviour.

iv An attacker intercepts a legitimate authentication message and later retransmits it to gain unauthorised access to a server.

v An attacker captures network packets to infer communication patterns and user behaviour without changing any data.

(d) **[4 points]** A high-frequency trading platform is required to record every transaction attempt to a centralised, tamper-proof audit server to meet regulatory compliance. During a period of extreme market volatility, the volume of trades increases tenfold. The delay caused by the system waiting for the audit server to confirm each log entry begins to stall trade execution, threatening to cause massive financial losses for clients and crashing the trading engine. To keep the platform online and responsive, the system automatically switches to a ”Performance Mode” that suppresses all non-essential recording of transaction metadata until traffic stabilises.

Identify the two security goals that are in contention in this scenario. Briefly explain how these goals conflict with each other.

(e) **[5 points]** A company enforces the following password policy for its employees:

- Passwords must be exactly 10 characters long.
- The first 9 characters must be lowercase letters (a–z) or digits (0–9).
- The final character must be one of the following special characters: #, $, %, &, or .

Calculate the **entropy** (in bits) of a password under this policy.

Question 2: Authentication and Key Establishment [20 points]

(a) **[3 points]** Explain what a public key certificate is.

(b) **[4 points]** Explain what a root certificate is and how it can be identified.

(c) **[3 points]** Explain the purpose of the root certificate store in an operating system or a web browser.

(d) **[2 points]** The image below shows a common certificate error encountered while browsing the internet. Explain one possible reason for this error.

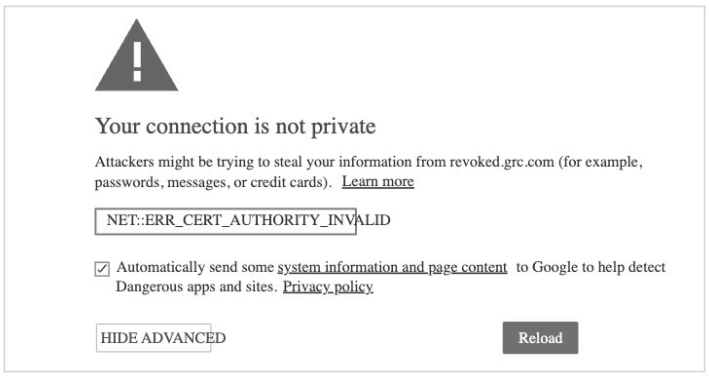


Figure 1: Certificate Error

(e) **[8 points]** Suppose A wants to establish an authenticated session with B. They already share a secret key k, and B has a means to verify A's password p. Consider the following two protocols:

Protocol 1:

$A \to B : \mathrm{Enc}_k(p)$

Protocol 2:

$A \to B : \mathrm{Enc}_k(p), \mathrm{MAC}_k(p)$

i For each of Protocol 1 and Protocol 2, determine whether it achieves the objective of establishing an authenticated session. Justify your answer separately for each protocol. **(4 marks)**

ii Describe a modification to one of the protocols to achieve the objective. **(4 marks)**

Question 3: Public Key Cryptography [20 points]

(a) **[4 points]** Let p be a prime number. Explain what it means for an integer g to be a primitive root modulo p.

(b) **[2 points]** Using a prime number p and a primitive root g of p, define the discrete logarithm problem.

(c) **[8 points]** Suppose A and B are trying to establish a key using the Diffie-Hellman key exchange. The public parameters they are using are $p = 11$ and $g = 2$.

i If A computes their public key as 10, what is A's private key? Explain your calculation. **(2 marks)**

ii If B computes their public key as 7, what is B's private key? Explain your calculation. **(2 marks)**

iii Assuming A and B exchange their public keys, show the calculation A performs to find the shared key and calculate the shared key. **(2 marks)**

iv Assuming A and B exchange their public keys, show the calculation B performs to find the shared key and calculate the shared key. **(2 marks)**

(d) **[3 points]** Explain what *Perfect Forward Secrecy (PFS)* is in the context of cryptographic protocols.

(e) **[3 points]** Explain how the Diffie-Hellman key exchange can be used to achieve Perfect Forward Secrecy.

Question 4: Network Security [20 points]

(a) **[12 points]** A firewall sits between an internal network and the Internet. The internal network uses the public IP address range 203.10.45.0/24. The firewall has two interfaces: `inet` (connected to the Internet) and `lan` (connected to the internal network). Consider the following firewall rule table:

Rule	Iface	Src IP	Dst IP	Proto	Src Port	Dst Port	State	Action
A	inet	external	203.10.45.10	TCP	*	80	New	Accept
B	inet	external	203.10.45.10	TCP	*	443	New	Accept
C	lan	203.10.45.0/24	external	TCP	*	80	New	Accept
D	lan	203.10.45.0/24	external	TCP	*	443	New	Accept
E	lan	203.10.45.0/24	external	UDP	*	53	New	Accept
F	*	*	*	*	*	*	Est.	Accept
G	*	*	*	*	*	*	*	Drop

For each statement below, indicate whether it is **TRUE** or **FALSE** and provide a brief explanation justifying your answer. Where applicable, reference the specific rule(s) involved in your reasoning.

a) This is a stateful firewall. **(2 marks)**

b) An external host can initiate an SSH connection to any internal host on the network. **(2 marks)**

c) An internal host at 203.10.45.50 can browse HTTPS websites on the Internet. **(2 marks)**

d) The web server at 203.10.45.10 can accept incoming HTTP and HTTPS connections from the Internet. **(2 marks)**

e) An external host can send a DNS response (UDP port 53) to an internal host at 203.10.45.100. **(2 marks)**

f) An internal host at 203.10.45.20 can send a file to another internal host at 203.10.45.30 using any protocol. **(2 marks)**

(b) **[4 points]** In IPSec, there are two main security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). Briefly explain the main difference between AH and ESP in terms of the security services they provide.

(c) **[4 points]** Explain how TLS 1.3 achieves 1-RTT (one round-trip time) communication during the handshake, compared to TLS 1.2 which requires 2-RTT. In your answer, focus on the role of Diffie-Hellman key exchange parameters in the initial handshake. You may use a diagram if required.

Question 5: Web security and Software Security [20 points]

(a) **[5 points]** A popular e-commerce platform allows users to submit product reviews. An attacker submits a review for a high-traffic item that includes a malicious JavaScript payload within the text field. Whenever any customer or site administrator views that product's page, the script executes automatically in their browser, attempting to steal their session cookies and redirect them to a fraudulent login page.

i. Identify the **exact type of attack** happening in this scenario. Briefly justify your answer. **(3 marks)**

ii. Suggest a remediation strategy to prevent this attack. **(2 marks)**

(b) **[4 points]** Explain the Same-Origin Policy (SOP) and discuss its role as a fundamental security mechanism in web browsers.

(c) **[4 points]** A web application takes user input from a search bar and inserts it directly into a database query string: `"SELECT * FROM products WHERE name = '" + user_input + "';"`. Explain how an attacker could exploit this using SQL Injection (SQLi) to bypass authentication or leak data.

(d) **[4 points]** Recently, it was discovered that a common Python library used in Large Language Model (LLM) applications was found to have a backdoor installed. If a company or developers were using this infected version of the `litellm` library, it could harvest their login tokens and exfiltrate them to an external server. The attack originated as a legitimate-looking update to the library, where the attacker had exploited vulnerabilities in the developer's build tools to gain unauthorized access to the official publishing account.

i. Identify the type of attack happening here. Briefly justify your answer. **(2 marks)**

ii. Suggest a mitigation strategy to reduce the risk of such attacks in practice. **(2 marks)**

(e) **[3 points]** Explain how stack canaries help mitigate buffer overflow attacks.

Additional space Use this space if you need additional room for your answers. If you use it, make sure to reference it in the original answer space; otherwise, this space will not be marked.

Additional space Use this space if you need additional room for your answers. If you use it, make sure to reference it in the original answer space; otherwise, this space will not be marked.