**Types of attacks :**

**1. Flooding**

The **flooding attack** overwhelms a server or network with an excessive number of requests or data. In HTTP/3, this can happen through:

* Opening multiple **QUIC connections** or sending a large number of simultaneous streams.
* Sending legitimate-looking requests at a very high volume, depleting server resources (CPU, memory, or bandwidth).

**Impact:**

* Denial of Service (DoS) for legitimate users.
* Exhaustion of server resources.

**2. Stream Reuse**

The **stream reuse attack** exploits the multiplexing feature of HTTP/3. In this protocol, multiple streams can run independently over a single QUIC connection.  
Attackers might:

* Reuse closed streams to inject malicious messages.
* Exploit vulnerabilities in stream management to interfere with legitimate streams.

**Impact:**

* Disruption of legitimate streams.
* Possibility to inject corrupted or malicious data.

**3. Settings Attacks**

**Settings attacks** target the connection parameters negotiated during HTTP/3 setup. Attackers can:

* Manipulate **SETTINGS frames** to disrupt the server configuration.
* Send unexpected or illegal parameter values to trigger errors or exploit security flaws.

**Impact:**

* Denial of Service by misconfiguring the server.
* Exploitation of bugs or vulnerabilities in HTTP/3 implementations.

**4. Desync Attacks**

**Desynchronization (Desync) attacks** exploit mismatches or inconsistencies in how clients and servers handle data. These attacks:

* Inject malicious or incomplete data into a connection, exploiting mismatched processing between client and server.
* Enable **HTTP Request Smuggling**, where a malicious request is hidden within another.

**Impact:**

* Execution of unauthorized commands.
* Bypassing security controls.

**5. Traffic Decryption**

This attack aims to decrypt the data exchanged between the client and server, despite HTTP/3 using strong encryption (TLS 1.3).  
Attackers may use:

* **Man-in-the-Middle (MITM)** techniques to intercept and analyze encrypted traffic.
* Exploits in TLS implementation or key management.

**Impact:**

* Unauthorized access to sensitive data.
* Compromise of user confidentiality.

**6. 5G MitM**

A **Man-in-the-Middle (MITM)** attack in 5G networks involves:

* Intercepting HTTP/3 traffic on 5G networks using malicious devices or exploiting interconnection vulnerabilities.
* Leveraging the high speed and capacity of 5G to target sensitive data.

**Impact:**

* Spying on communications.
* Injecting malicious content into traffic.

**7. Interconnection Attacks**

**Interconnection attacks** target the points where different systems or networks using HTTP/3 are connected:

* Exploiting weaknesses in the links between servers or services.
* Disrupting the flow of data between interconnected networks.

**Impact:**

* Disruption of operations in interconnected systems.
* Exposure of data to external threats.

**8. Web Fingerprinting**

**Web fingerprinting attacks** analyze HTTP/3 traffic to identify specific patterns or signatures from users or servers.  
Attackers can:

* Monitor requests, responses, and multiplexing patterns to deduce client information (browser, OS, etc.).
* Use this information for targeted attacks.

**Impact:**

* Loss of user anonymity.
* Facilitation of future targeted attacks.

**9. Break Multiplexing**

In HTTP/3, multiplexing allows multiple requests to be sent simultaneously over a single connection. A **break multiplexing attack** attempts to:

* Disrupt this capability by blocking or interfering with specific streams.
* Exploit bugs in stream handling to cause unpredictable behavior.

**Impact:**

* Performance degradation.
* Partial Denial of Service (DoS).