STRIDE Threat Modeling for OpenMetrics

There are 6 categories to consider in a STRIDE model:

The categories are:

1. Spoofing
2. Tampering
3. Repudiation
4. Information Disclosure
5. Denial of Service
6. Elevation of Privilege

Using the STRIDE Model, some threats were identified and classified:

1. Spoofing

- An external entity may try to gain access to data metrics by spoofing or stealing credentials/IP and as a result access is given to the wrong user.

  Attack Options:
  - Password theft by phishing
  - Password crashing by brute force
  - IP spoofing

  Mitigation:
  - Utilizing API tokens, client certificates, or other secure authentication methods.
  - Implementing secure authentication mechanisms for metric producers and consumers (exporters and ingesters).

2. Tampering

- Data flowing from endpoints can be tampered with in transit which can lead to corruption of metrics.
- Metric definitions can be exposed to unauthorized alteration which could result in misinterpretation or misrepresentation of data.

  Mitigation:
  - Use hashes or data signatures for data validation and tamper detection.

3. Repudiation

- Attackers may cover up any evidence of unauthorized actions by altering data logs or information logs.

Mitigation:

- Audit and logging mechanisms to track all system activity and suspicious activity.

4. **Information Disclosure**

- Improperly handling queries may allow an attacker to gain access to information that is not intended for disclosure. E.g. Querying for one metric returns all metrics which are then filtered on the frontend. This data flowing across the access request and response may be sniffed by an attacker.

Mitigation:

- Encryption of sensitive data and access control mechanisms to restrict data accessibility.

5. **Denial of Service**

- An external agent can make so many requests for metrics that it can overwhelm the web server and deny normal user access.
- An attacker can try to overwhelm the data storage by tampering with metric formats to try and store more data than the system can handle.

Mitigation:

- Load balancing and traffic filtering systems to mitigate traffic spikes and spread the load evenly.
- Data tracking mechanisms to track suspicious spikes in data storage.

6. **Elevation of Privilege**

- A user may be able to gain elevated privileges beyond their normal role and modify metrics that they should not have been able to modify

Mitigation:

- Implement the principle of least privilege and role based access control to limit the privileges of users.