1. STRIDE

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Jegeib. (2022, August 25). *Threats - Microsoft Threat Modeling Tool - Azure*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

1. **Core Element of Microsoft SDL**: The Threat Modeling Tool is an integral part of the Microsoft Security Development Lifecycle (SDL), emphasizing its importance in the security development process.
2. **Early Identification and Mitigation of Security Issues**: The tool enables software architects to identify and mitigate potential security issues early in the development process, making it more cost-effective and reducing the overall development cost.
3. **Designed for Non-Security Experts**: The tool is user-friendly and designed with non-security experts in mind, facilitating threat modeling for all developers by providing clear guidance on creating and analyzing threat models.
4. **Answering Critical Security Questions**: The Threat Modeling Tool helps in addressing crucial security-related questions, like how attackers can alter authentication data, the impact of unauthorized access to user profile data, and the consequences of denying access to critical databases.
5. **Utilization of the STRIDE Model**: Microsoft employs the STRIDE model within the tool to categorize different types of threats, thereby simplifying security conversations. This model includes Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
6. **Descriptions of Threat Categories in STRIDE**:
    - **Spoofing**: Illegal access and use of another user's authentication information.
    - **Tampering**: Malicious modification of data, either stored or in transit.
    - **Repudiation**: Situations where users deny their actions without a trace.
    - **Information Disclosure**: Exposure of information to unauthorized individuals.
    - **Denial of Service (DoS)**: Attacks that make a service unavailable to legitimate users.
    - **Elevation of Privilege**: Unauthorized users gaining privileged access.
7. **Enhancing System Security and Reliability**: By addressing these different types of threats, the tool not only improves system security but also contributes to the system's overall availability and reliability, essential for maintaining robust and secure software systems.