STRIDE Threat Modelling

Dr Rosanne English

What is STRIDE?

- A framework for discussing and classifying threats
- Designed to support developers in considering common threats

STRIDE Threat Modelling Breakdown

Spoofing

Tampering

Repudiation

Information disclosure

Denial of service

Elevation of privilege

Spoofing

THREAT	Spoofing
PROPERTY	Authentication
DEFINITION	Masquerading as something or someone else
EXAMPLE	Phishing website or e-mail

Tampering

THREAT	Tampering
PROPERTY	Integrity
DEFINITION	Unauthorised modification of data
EXAMPLE	Unauthorised modification of salary in a database

Repudiation

THREAT	Repudiation
PROPERTY	Non-repudiation
DEFINITION	Refusal to accept responsibility for an action
EXAMPLE	Claiming an e-mail from an individual’s address was not sent by them

Information Disclosure

THREAT	Information Disclosure
PROPERTY	Confidentiality
DEFINITION	Exposure of confidential information to unauthorised parties
EXAMPLE	Password leaks

Denial of Service

THREAT	Denial of Service
PROPERTY	Availability
DEFINITION	Service unavailable to legitimate users when it should be available
EXAMPLE	Flooding HTTP requests

Escalation of Privilege

THREAT	Escalation of Privilege
PROPERTY	Authorisation
DEFINITION	Individual or process capable of actions they do not have authorisation for
EXAMPLE	User with read only permissions escalates privileges to write capability

Applying STRIDE

- Consider the potential threats for each element under the STRIDE model
- Record details of threats as you progress
- Record any assumptions

STRIDE Mitigation

- Spoofing - Authentication
- Tampering - Data protection
- Repudiation - Non-repudiation
- Information disclosure - Confidentiality
- Denial of Service - Availability
- Elevation of privileges - Authorisation

STRIDE

POSITIVES

- Provides a framework to consider possible threats
- Helps identify common vulnerabilities in systems and processes

LIMITATIONS

- May not be comprehensive
- A pro-active approach to considering common threats