Threat Modelling Glossary

Key Words

STRIDE

Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

STRIDE is a threat classification model developed by Microsoft to help identify potential security risks in a system. It categorises threats into six types.

Threat Category	Description	Example
Spoofing	Pretending to be another user or system to gain unauthorised access.	Phishing attack to steal banking credentials.
Tampering	Modifying data or code to cause unintended behaviour.	Changing transaction values in an API request.
Repudiation	Users denying that they performed an action.	A customer claims they did not make a financial transaction.
Information Disclosure	Exposing confidential data to unauthorised parties.	Database breach leaking customer records.
Denial of Service (DoS)	Disrupting service availability by overloading systems.	DDoS attack on a banking website.
Elevation of Privilege	Gaining unauthorised privileges beyond intended access.	Exploiting a vulnerability to gain admin rights.

DREAD

Damage, Reproducibility, Exploitability, Affected Users, Discoverability

DREAD is a risk assessment model used to prioritise threats by scoring them based on five factors.

Total Risk Score = D + R + E + A + D (max 50). Threats scoring higher numbers are prioritised for mitigation.

Factor	Description
Damage	How severe would the impact be?
Reproducibility	How easily can the attack be replicated?
Exploitability	How simple is it to carry out the attack?
Affected Users	How many users are impacted?
Discoverability	How easy is it to discover the vulnerability?

Threat	D	R	E	A	D	Total Score
SQL Injection	9	8	9	7	6	39 (High)
DoS Attack	6	9	9	10	10	44 (Critical)

CVSS

Common Vulnerability Scoring System

CVSS is a standardised scoring system to measure the severity of security vulnerabilities. It's used to rank and prioritise vulnerabilities based on a numerical score (0-10). CVSS is widely used in vulnerability databases like NVD (National Vulnerability Database).

CVSS Components:

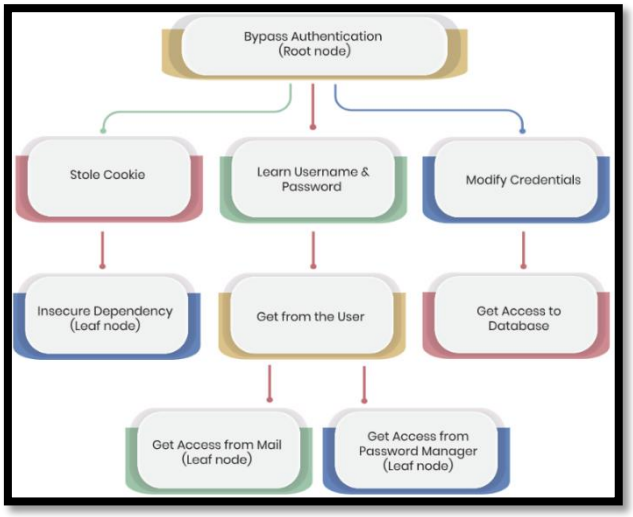
- Base Metrics (Intrinsic Characteristics) – These define the fundamental properties of a vulnerability that do not change over time.
- Threat Metrics (Real-World Exploitability) – These metrics change over time based on active exploitation and fixes.
- Environmental Metrics (Organisation-Specific Factors) – These customise the CVSS score based on an organisation's security priorities.
- Supplemental Metrics (Additional Context) – These provide extra non-scoring details about the vulnerability.

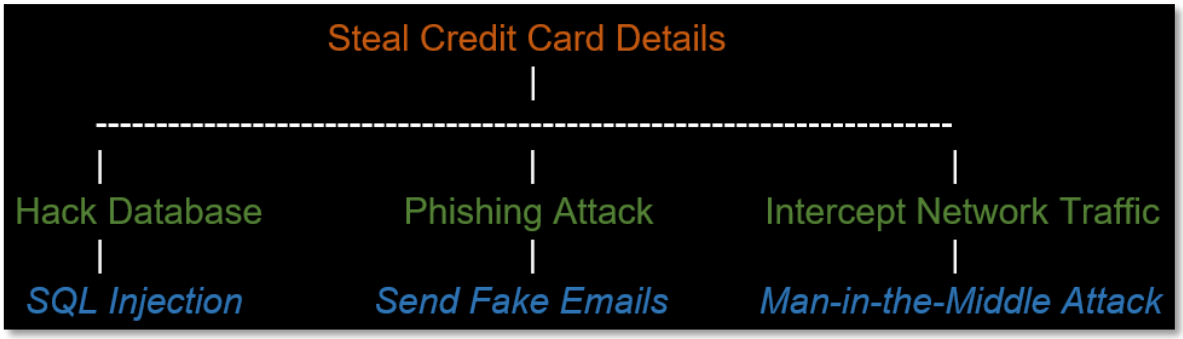
Scoring System CVSS v4.0:

CVSS Score	Severity Level
0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

Attack Trees

Attack trees are a visual representation of possible attack paths that adversaries could take to compromise a system.





Attack Libraries

Attack libraries are predefined collections of common attack patterns, vulnerabilities, and exploitation techniques. Attack libraries help organisations identify and prevent known security threats.

Examples of Attack Libraries:

- CWE (Common Weakness Enumeration) – A list of software security weaknesses.
- CAPEC (Common Attack Pattern Enumeration and Classification) – A catalogue of known attack methods.
- MITRE ATT and CK Framework – A knowledge base of real-world adversary tactics and techniques.

Threat Modelling Manifesto

The Threat Modelling Manifesto is a set of principles and values for effective and meaningful threat modelling.

Core Values:

- Find and fix design issues over compliance checklists.
- Collaboration over rigid processes.
- Continuous improvement over one-time reviews.
- Practical application over excessive documentation.

Principles:

- Threat modelling should start early and evolve.
- Everyone can participate in threat modelling.
- Use frameworks but adapt them to your needs.

OWASP Threat Modelling Cookbook

The OWASP Threat Modelling Cookbook is a practical guide for implementing threat modelling. It includes:

- Step-by-step threat modelling methodologies
- Templates and checklists
- Common threats and security best practices
- Integration with Agile, DevOps, and Secure SDLC

The ATT and CK Framework

The MITRE ATT and CK framework is a comprehensive knowledge base that documents real-world cyberattack tactics and techniques.

ATT and CK Framework Components:

- Tactics – The goal of an attack.
- Techniques – Specific methods used to achieve a tactic.
- Sub-techniques – More granular versions of techniques.
- Mitigations – Recommended defensive strategies.

Summary

Concept	Purpose	Use Case
STRIDE	Identifies threats in a system.	Used during system design to categorise risks.
DREAD	Prioritises threats based on risk score.	Helps focus on high-risk threats.
CVSS	Rates vulnerability severity (0-10).	Used in vulnerability management.
Attack Trees	Visual representation of attack paths.	Used in penetration testing and security assessments.
Attack Libraries	Catalogues common attack techniques.	Helps security teams identify threats efficiently.
Threat Modelling Manifesto	Philosophical guide to threat modelling.	Encourages best practices in security design.
OWASP Threat Modelling Cookbook	Practical guide for threat modelling.	Helps development teams implement security.
MITRE ATT and CK	Documents real-world attack techniques.	Used for threat detection, response.

Bibliography

National Cyber Security Centre (NCSC) (no date) *Using attack trees to understand cyber security risk.* Available at: https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk

UK Government (2022) *Conducting a STRIDE-based threat analysis.* Available at: https://www.gov.uk/government/publications/secure-connected-places-playbook-documents/conducting-a-stride-based-threat-analysis

Practical DevSecOps (no date) *What is STRIDE threat model?* Available at: https://www.practical-devsecops.com/what-is-stride-threat-model/

National Institute of Standards and Technology (NIST) (no date) *CVSS vulnerability metrics.* Available at: https://nvd.nist.gov/vuln-metrics/cvss

MITRE Corporation (no date) *MITRE ATT&CK Framework.* Available at: https://attack.mitre.org/

Forum of Incident Response and Security Teams (FIRST) (no date) *CVSS v4.0 User Guide.* Available at: https://www.first.org/cvss/v4-0/user-guide

National Cyber Security Centre (NCSC) (no date) *Using attack trees to understand cyber security risk.* Available at: https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk

MITRE Corporation (no date) *Common Weakness Enumeration (CWE).* Available at: https://cwe.mitre.org/

MITRE Corporation (no date) *Common Attack Pattern Enumeration and Classification (CAPEC).* Available at: https://capec.mitre.org/

Threat Modeling Manifesto (no date) *Threat Modeling Manifesto.* Available at: https://www.threatmodelingmanifesto.org/

Open Web Application Security Project (OWASP) (no date) *OWASP Threat Model Project.* Available at: https://owasp.org/www-project-threat-model/