STRIDE - Threat modelling

The STRIDE threat model ensures that software products maintain the CIA triad

S - Spoofing [Gain unauthorized access]
T - Tampering [Change functionality or corrupt data]
R - Repudiation [Avoid accountability]
I - Information Disclosure [Gain intelligence or misuse information]
D - Denial of Service (DoS) [Make services unavailable]
E - Elevation of Privilege [Execute actions beyond authorized level]

	Type of Threat	What Was Violated
S	Spoofing	Authentication
T	Tampering	Integrity
R	Repudiation	Non-repudiation
I	Information Disclosure	Confidentiality
D	Denial of Service (DoS)	Availability
E	Elevation of Privilege	Authorization

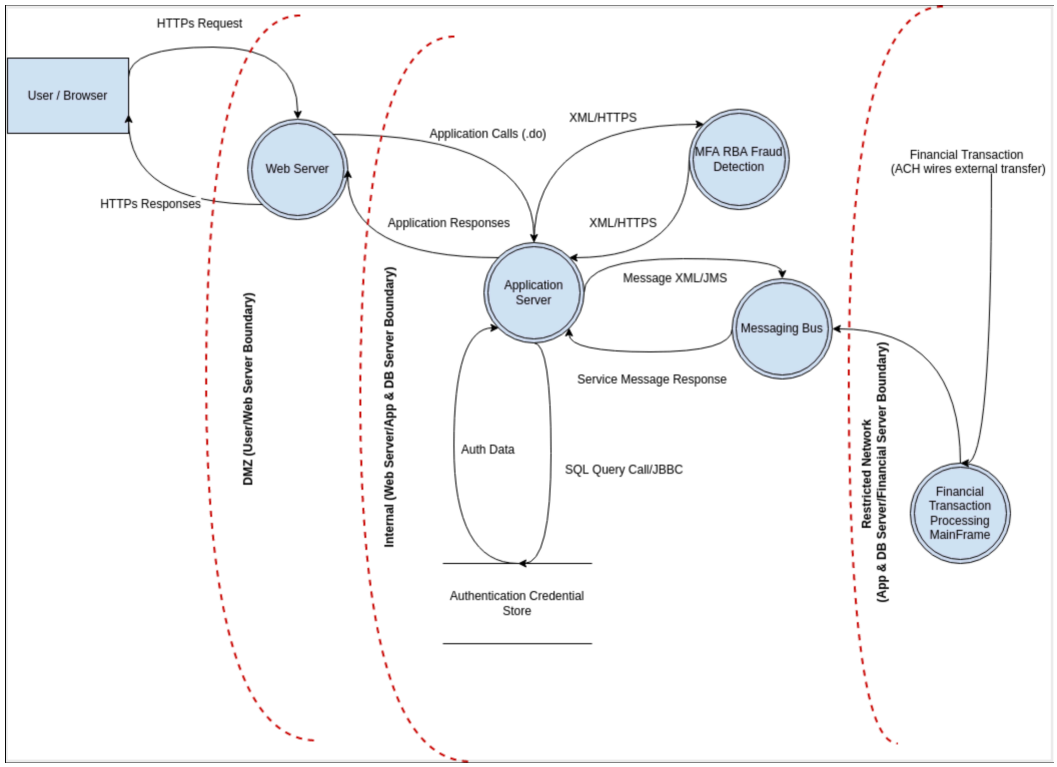
How to Use

1. Identify system components — Use data flow diagrams (DFDs) to outline processes, data stores, data flows, and external entities.
2. Apply STRIDE to each element — For each component in your DFD, consider what threats may apply under each STRIDE category.
3. Document threats — Record the threats, potential impact, and mitigation strategies.
4. Prioritize and mitigate — Rank(by both quality and quantity) threats by risk level and develop controls to address them.

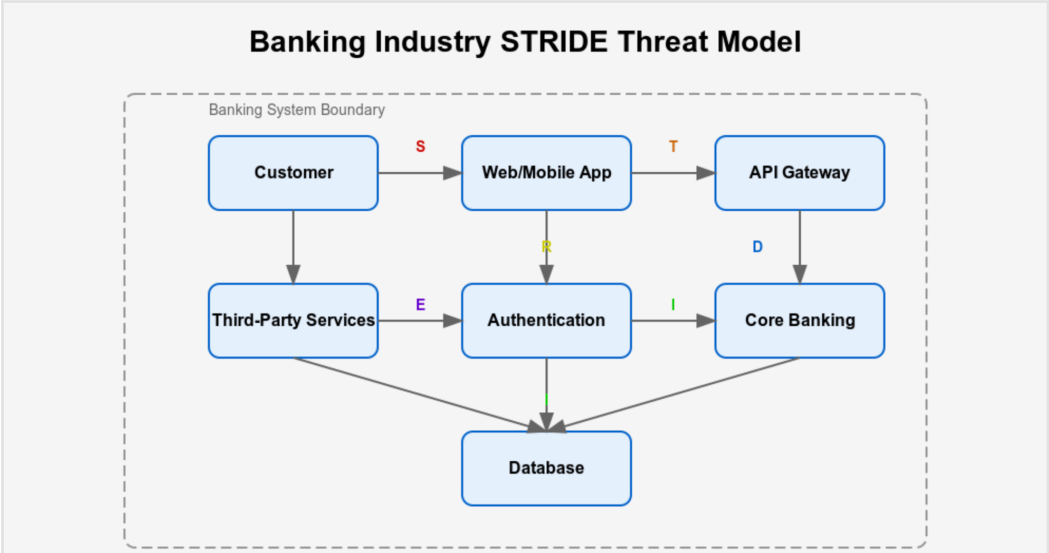
Example: Web Application Login Page

Component	STRIDE Threat	Example
Login Form	S – Spoofing	Attacker fakes a user login
Database	T – Tampering	SQL injection alters records
Logs	R – Repudiation	User denies fraudulent action, logs are incomplete
HTTPS Traffic	I – Info Disclosure	Data leaks via insecure transmission
Server	D – DoS	Attacker floods with traffic
App Backend	E – Elevation of Privilege	Gains admin access via vulnerability

Stride Threat Modeling Data Flow Diagrams



EXAMPLE — Banking Application.



STRIDE Threat Categories in Banking

Type	Threat	Description	Banking Example
S	**Spoofing**	Impersonating someone else	Phishing, credential theft, fake apps
T	**Tampering**	Modifying data or code	Transaction fraud, SQL injection
R	**Repudiation**	Denying performed actions	Denied transactions, poor audit trails
I	**Information Disclosure**	Exposing information	Data breaches, unencrypted records
D	**Denial of Service**	Making systems unavailable	DDoS attacks, service outages
E	**Elevation of Privilege**	Gaining unauthorized access	Broken access controls, IDOR

STRIDE mitigation

Threat	Description	Mitigation Strategies
S – Spoofing	Impersonating another user or system entity	- Multi-factor authentication (MFA) - Strong password policies - Certificate-based authentication
T – Tampering	Unauthorized modification of data or code	- Data integrity checks (e.g., hashing) - Code signing - Access controls and validation
R – Repudiation	Denying the performance of an action without a way to prove it	- Secure and tamper-proof logging - Digital signatures - Audit trails with timestamps
I – Information Disclosure	Unauthorized access to confidential data	- Encryption (in transit and at rest) - Least privilege access - Secure coding practices

D – Denial of Service	Preventing legitimate use of services	- Rate limiting and throttling - Input validation - Use of WAFs/CDNs to absorb traffic
E – Elevation of Privilege	Gaining unauthorized access to higher-level permissions	- Role-based access control (RBAC) - Patch vulnerabilities promptly - Use of sandboxing