**THREAT MODLING :** A structured process used to identify, analyze, and mitigate potential security threats to a system or application.

Popular Threat Modeling Frameworks :

**STRIDE :** A framework developed by Microsoft that focuses on six categories of threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

[**PASTA**](https://www.google.com/search?sca_esv=fc200b82b34debf5&rlz=1C1ONGR_en-GBIN1074IN1074&q=PASTA&sa=X&ved=2ahUKEwiguOD-w4WPAxVj6jgGHfD6AKUQxccNegUIkQIQAQ&mstk=AUtExfAsXzC0UGuJdATJ3cCHf7eXPw4txXfDs_f2FnfLn1W37BLJFOS0x5JTf_VGGxtsnjSR-pYbNb4uWYhwRmpE0PGONrXUIL14Nc9S2DZDjgijjWLDwYwWspxuew0xvhpiw2VI9FuksTx8x7Ly9vAxLeAlxvXU8Be84I7Uxkpm6X7-XCwjePCLJAqwaRmTXO8rTBVm&csui=3) **:** A seven-stage methodology that aligns business objectives with technical threats through attacker emulation.

[**DREAD**](https://www.google.com/search?sca_esv=fc200b82b34debf5&rlz=1C1ONGR_en-GBIN1074IN1074&q=DREAD&sa=X&ved=2ahUKEwiguOD-w4WPAxVj6jgGHfD6AKUQxccNegUIjgIQAQ&mstk=AUtExfAsXzC0UGuJdATJ3cCHf7eXPw4txXfDs_f2FnfLn1W37BLJFOS0x5JTf_VGGxtsnjSR-pYbNb4uWYhwRmpE0PGONrXUIL14Nc9S2DZDjgijjWLDwYwWspxuew0xvhpiw2VI9FuksTx8x7Ly9vAxLeAlxvXU8Be84I7Uxkpm6X7-XCwjePCLJAqwaRmTXO8rTBVm&csui=3) **:** A threat model that helps in ranking identified threats based on damage potential, reproducibility, exploitability, affected users, and discoverability.

**STRIDE : STANDS FOR**

* **Spoofing:** Impersonating another user or entity.
* **Tampering:** Modifying data or system configurations without authorization.
* **Repudiation:** Denying an action or transaction without proper accountability.
* **Information Disclosure:** Unauthorized exposure to sensitive data.
* **Denial of Service (DoS) :** Preventing authorized users from accessing a system or service.
* **Elevation of Privilege:** Gaining unauthorized access to higher-level system resources.

Here's a comprehensive STRIDE threat modeling analysis for the Amazon Online Shopping System based on the data flow diagram. I've broken it down component-wise and included all possible threats and corresponding mitigations.



### STRIDE Threat Modeling Summary

| **COMPONENT** | **THREAT TYPE** | **THREAT DESCRIPTION** | **MITIGATION STRATEGIES** |
| --- | --- | --- | --- |
| **CUSTOMER** | Spoofing | Impersonation of legitimate users | Multi-factor authentication, CAPTCHA, session management |
|  | Tampering | Altering search criteria or account details | Input validation, integrity checks |
|  | Repudiation | Denying product selection or transaction | Secure logging, digital signatures |
|  | Information Disclosure | Leakage of personal or payment data | TLS encryption, data masking, secure storage |
|  | Denial of Service | Flooding system with requests | Rate limiting, CAPTCHA, anomaly detection |
|  | Elevation of Privilege | Gaining unauthorized access to admin features | Role-based access control, privilege separation |
| **CUSTOMER'S BANK** | Spoofing | Fake bank impersonating legitimate one | Mutual TLS, certificate pinning |
|  | Tampering | Modifying payment requests | Message integrity checks, secure APIs |
|  | Repudiation | Disputing payment transactions | Transaction logging, non-repudiation mechanisms |
|  | Information Disclosure | Exposure of financial data | End-to-end encryption, secure tokens |
|  | Denial of Service | Blocking payment gateway | Redundancy, failover systems |
|  | Elevation of Privilege | Unauthorized access to bank systems | Strong authentication, network segmentation |
| **AMAZON ONLINE SHOPPING SYSTEM** | Spoofing | Fake system mimicking Amazon | Domain validation, secure certificates |
|  | Tampering | Altering product or payment data | Input sanitization, integrity checks |
|  | Repudiation | Denying order placement or payment | Audit trails, secure logs |
|  | Information Disclosure | Leaking customer or supplier data | Data encryption, access control |
|  | Denial of Service | Overloading system with traffic | Load balancing, rate limiting |
|  | Elevation of Privilege | Exploiting vulnerabilities to gain admin access | Patch management, role-based access control |
| **AMAZON'S BANK** | Spoofing | Impersonation of Amazon’s bank | Secure authentication, certificate validation |
|  | Tampering | Modifying payment instructions | Secure APIs, message integrity |
|  | Repudiation | Denying payment processing | Transaction logging, digital signatures |
|  | Information Disclosure | Exposure of transaction details | TLS, secure vaults |
|  | Denial of Service | Disruption of payment services | Redundant systems, DDoS protection |
|  | Elevation of Privilege | Unauthorized access to bank operations | Access control, monitoring |
| **SUPPLIER** | Spoofing | Fake supplier impersonating legitimate one | Supplier verification, secure on boarding |
|  | Tampering | Altering invoices or purchase orders | Document integrity checks, secure communication |
|  | Repudiation | Denying receipt of payment or orders | Signed acknowledgments, audit logs |
|  | Information Disclosure | Leakage of supplier contracts or payment info | Encryption, access control |
|  | Denial of Service | Supplier system unresponsive | Backup suppliers, retry mechanisms |
|  | Elevation of Privilege | Unauthorized access to internal procurement systems | Least privilege principle, supplier access restrictions |