Threat Modeling - Known Mitigations

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat** | **Property** | **Threat Definition** | **Mitigations** |
| **Spoofing** | Authentication | Spoofing threats involve an adversary creating and exploiting confusion about who is talking to whom. Spoofing threats apply to the entity being fooled, not the entity being impersonated. Thus, external elements are subject to a spoofing threat when they are confused about what or whom they are talking to. | To authenticate principals:   * Windows authentication (NTLM) * Kerberos authentication * Windows or Live ID authentication * PKI systems such as SSL/TLS and certificates * IPsec * Digitally signed packets   To authenticate code or data:   * Digital signatures * Message authentication codes * Hashes |
| **Tampering** | Integrity | Tampering threats involve an adversary modifying data, usually as it flows across a network, resides in memory, on disk, or in databases. | * Windows Discretionary Access Control Lists * Windows Mandatory Integrity Controls * Digital signatures * Message authentication codes |
| **Repudiation** | Non-repudiation | Repudiation threats involve an adversary denying that something happened. | * Strong authentication * Secure logging and auditing * Digital signatures * Time stamps * Trusted third parties |
| **Information disclosure** | Confidentiality | Exposing information to someone not authorized to see it. | * Encryption * ACLS |
| **Denial of service** | Availability | Deny or degrade service to users. | * Windows Discretionary Access Control Lists * Filtering * Quotas and rate limits * Authorization * High-availability designs |
| **Elevation of privilege** | Authorization | Gain capabilities without proper authorization. | * Windows Discretionary Access Control Lists * Group or role membership * Privilege ownership * Permissions * Input validation |