CSF Tools

STRIDE-LM Threat Model

Introduction to STRIDE-LM

The process of threat modeling can be very beneficial in determining how to best protect a computer application or network. The purpose of the threat modeling is to evaluate the system from the perspective of a potential attacker, then select appropriate controls for reducing the risk of those attacks.

STRIDE is a popular threat model originally developed at Microsoft. It is an acronym for six classifications of threats to systems:

1. **Spoofing** – Impersonating another user or system component to obtain its access to the system
2. **Tampering** – Altering the system or data in some way that makes it less useful to the intended users
3. **Repudiation** – Plausible deniability of actions taken under a given user or process
4. **Information Disclosure** – Release of information to unauthorized parties (e.g., a data breach)
5. **Denial of Service** – Making the system unavailable to the intended users
6. **Elevation of Privilege** – Granting a user or process additional access to the system without authorization

Practitioners at Lockheed Martin noted that STRIDE was developed primarily to address engineering and development projects, rather than network defense. To make the model more applicable to the latter, they added a seventh classification:

7. **Lateral Movement** – Expanding control over the target network beyond the initial point of compromise.

STRIDE-LM Components

ID	Threat Vector	Desired Property	Framework References
S	Spoofing	Authentication	• PR.AC-1: Identities and credentials are issued,... • PR.AC-6: Identities are proofed and bound to... • PR.AC-7: Users, devices, and other assets are... • PR.PT-1: Audit/log records are determined,...
T	Tampering	Integrity	• PR.AC-2: Physical access to assets is managed and... • PR.DS-1: Data-at-rest is protected • PR.DS-2: Data-in-transit is protected • PR.DS-6: Integrity checking mechanisms are used... • PR.DS-8: Integrity checking mechanisms are used... • PR.IP-3: Configuration change control processes... • PR.MA-1: Maintenance and repair of organizational... • PR.PT-1: Audit/log records are determined,...

ID	Threat Vector	Desired Property	Framework References
			• PR.PT-2: Removable media is protected and its use... • DE.CM-2: The physical environment is monitored to... • DE.CM-4: Malicious code is detected • DE.CM-5: Unauthorized mobile code is detected • DE.CM-7: Monitoring for unauthorized personnel,...
R	Repudiation	Non-repudiation	• PR.AC-1: Identities and credentials are issued,... • PR.AC-6: Identities are proofed and bound to... • PR.AC-7: Users, devices, and other assets are... • PR.PT-1: Audit/log records are determined,...
I	Information Disclosure	Confidentiality	• PR.DS-1: Data-at-rest is protected • PR.DS-2: Data-in-transit is protected • PR.DS-5: Protections against data leaks are... • PR.IP-6: Data is destroyed according to policy • PR.PT-2: Removable media is protected and its use...
D	Denial of Service	Availability	• PR.DS-4: Adequate capacity to ensure availability... • PR.IP-4: Backups of information are conducted,... • PR.PT-5: Mechanisms (e.g., failsafe, load...
E	Elevation of Privilege	Least Privilege	• PR.AC-4: Access permissions and authorizations... • PR.PT-3: The principle of least functionality is... • DE.CM-4: Malicious code is detected

ID	Threat Vector	Desired Property	Framework References
			• DE.CM-5: Unauthorized mobile code is detected • DE.CM-7: Monitoring for unauthorized personnel,...
LM	Lateral Movement	Containment	• PR.AC-3: Remote access is managed • PR.AC-5: Network integrity is protected (e.g.,... • PR.AC-6: Identities are proofed and bound to... • PR.MA-2: Remote maintenance of organizational... • PR.PT-3: The principle of least functionality is... • PR.PT-4: Communications and control networks are... • DE.CM-1: The network is monitored to detect... • DE.CM-6: External service provider activity is... • DE.CM-7: Monitoring for unauthorized personnel,... • RS.MI-1: Incidents are contained

STRIDE-LM elements and countermeasures

Further Reading

- Using the STRIDE-LM Threat Model to Drive Security Control Selection
- Sunburst Visualization of Threats to Controls