Evaluation of Security Risks Using Mission Threads

Work In Progress

Carol Woody, Ph.D. - Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, USA
cwoody@cert.org

Mission threads describe operational process steps required to perform organizational functions. Researchers from Software Engineering Institute (SEI) are exploring the use of mission threads for analysis of operational security risks early in the life cycle to identify design weaknesses and establish confidence for system and software assurance. From a realistic mission thread, multiple system and software relationships and dependencies as well as critical assets and high-impact points of failure can be identified and mitigation approaches developed and validated. SEI has successfully applied this approach for alert originators who plan to use the Wireless Emergency Alerts (WEA) system, a public alerting service offered by the Department of Homeland Security. Mission threads provide a means for identifying and evaluating potential threats in a way that stakeholders can understand the risks and determine appropriate responses.

A mission thread is an end-to-end set of steps that illustrate the technology and people resources needed to deliver expected behavior under a set of conditions and provide a basis for identifying and analyzing potential problems that could represent risks. For each mission step, the expected actions, outcomes, and assets are assembled. Confirmation that the components appropriately respond to expected operational use increases confidence that the system will function as intended even in the event of an attack [1]. An WEA mission thread is shown in Figure 1.

Using a threat modeling technique such as STRIDE which was developed by Microsoft [2] each step is analyzed to determine the assets that need protection and ways in which they can be threatened. The following table provides an example for step 4 when the operator establishes access to the alert origination system in the mission thread shown in Figure 1.

<table>
<thead>
<tr>
<th>Step Description</th>
<th>Assets</th>
<th>STRIDE Threat Identification Examples</th>
</tr>
</thead>
</table>
| Operator attempts to log on to the alert origination system. | - One person  
- Server (valid accounts/authentication information)  
- Logon procedure  
- Logon application  
- Username/password data in database  
- Communications between logon software, server, and alert originator | - Unidentified individual attempts to log on with AOS operator’s information  
- Operator denies having logged on  
- Capture of logon info using key logger or packet sniffer  
- Operator’s account not registered or servers are down  
- Successful logon by an unidentified and unauthorized individual |
From this information, security experts can develop attack scenarios that characterize risks the system needs to be prepared to handle in a form meaningful to mission thread participants. Figure 2 provides an example where an attacker steals a certificate of authentication in Step 4 and uses it to later send valid but illegitimate WEA messages sending people into a harmful situation.

![Figure 2: WEA mission thread risk.](image)

Work continues to further validate this security risk analysis approach and formalize the steps into a standard practice.

References
