Security Forum
Using Quantitative Analysis in System Threat Modeling
Project Charter

Status: Ballot for Approval
Revision level: V1.0
Date: 14 Feb. 2022

Project Description

Threat Modeling is an important part of creating secure systems. It allows us to proactively assess attack patterns (referred to as threats) that exploit vulnerabilities. However, threat modeling analysis today depends on a qualitative risk analysis in order to rate the likelihood and impact of an attack. The qualitative nature of the analysis makes explaining and justifying business rationale for improvements difficult in the eyes of business stakeholders.

There is an opportunity to incorporate the Open FAIR™ quantitative risk analysis framework in threat modeling to produce more objectively defensible results. The goal is to improve understanding of the risk of the system that is being threat modeled so that a more objective comparison can be performed with other options, with the intent of selecting the most effective one relative to cost.

We propose the creation of an objective methodology to analyze a system with a number of potential mitigations ("what if" approach). This will allow identifying the "right" combination with the intent of optimizing the acceptable risk against operational and implementation variables – like cost and time. This will enable us to select the most effective approach, as compared to various alternatives. This will be compatible with any number of threat modeling approaches.

Goals of this Project

The goal of this project is to integrate Open FAIR quantitative risk analysis in threat modeling. The rationale for this is to provide a more standardized, objective approach to managing risk that stems from developing insecure systems.

This project does not aim to offer guidance on how to threat model or which approach to threat modeling should be used.

It behooves us to put forth guidance for the security community so that the value of threat modeling efforts is directly tied to business outcomes related to risk reduction.

Project Value Proposition

A. Include quantitative analysis in threat modeling as a means of producing enterprise business rationale for mitigations against attack patterns, considering the direct effects on the system in scope and the organization.

B. Use Open FAIR to analyze risk both before and after consideration of potential mitigations of the overall solutions, identifying a balance of mitigations and impact in terms of reduced risk and considering impact on Threat Agent

C. Inform the security community of the benefits of quantitative risk analysis and communicating value in a business context, advocating for use of quantitative analysis

Project Deliverable

The Open Group Guide (a single document) containing the following:

A. Mapping of terminology between Open FAIR and threat modeling to connect domains and facilitate acceptance and understanding by both communities, providing a framework to integrate concepts.

   a. Context of current threat modeling domain, existing frameworks relevant to threat modeling, and high-level overview of current approaches, both offensive and defensive

B. Threat modeling process guide that describes quantitative analysis as a means of objectively selecting the best mitigations across the system in scope to prioritize reduction of enterprise risk, describing how to use the framework.

   a. Emphasis on defensibility and consistency while remaining pragmatic

   b. Consideration of limits of quantitative analysis in terms of complexity and overconfidence in estimates

   c. *Possibility of including commentary on how to use*

C. Use cases to validate the approach and define intended users of the document, demonstrating contextual value for using quantitative analysis in threat modeling.

   a. High-level mapping of several threat vectors

Project Personnel

A. Stakeholders
   a. The governing stakeholders of the project are:
      i. The Open Group
      ii. The Security Forum

B. Team
   a. The project team will be drawn from members of The Open Group Security Forum and invited experts. The project leadership will be selected through the normal procedures of The Open Group.
   b. The Project Facilitator(s) will be Altaz Valani and Simone Curzi.

Project Methodology

This section describes the project methodology, which includes:

A. Approach
   a. Project Facilitators Altaz Valani and Simone Curzi, along with a small team, will produce an initial draft document, including an overview of the problem being solved and the purpose of the document and providing an overview of the content of each section for initial approval by the Project Team.
   b. After giving initial approval, the Project Team will work to review and revise the document, focusing on one section at a time, with the authors making revisions between meetings based on feedback and comments.

c. After review and revision by the Project Team, the authors will apply any final changes before the document goes through formal Security Forum Review.

B. Roadmap
   a. Document development (8+ weeks)
      i. 4-6+ weeks – Initial draft document creation
      ii. 2 weeks – Initial Project Team input
      iii. 2-6+ weeks – Project Team review and revision

   b. The Open Group publication process
      i. Forum Review (8+ weeks)
         1. 1 Week – Announcement
         2. 2 Weeks – Review
         3. 1-3+ Weeks – Resolve Change Requests (CRs), implement revisions, and ballot to approve for publication (or to approve to proceed to Company Review)
            a. 75% approval required (If White Paper/Guide)
            b. *Potential for more time needed if many CRs submitted*
         4. 4+ Weeks – Publication *(tentative timeline; skip if proceeding to Company Review)*
            a. Technical Editor review and editing
            b. VP Approval for document to proceed to Executive Approval
            c. Executive Approval
            d. Publication

C. Governance
   a. Governance of the initiative will be The Open Group standard policy and procedures.
   b. The Project will reside within the Security Forum's Security and Risk Management Working Group.

D. Approval
   a. Project deliverables will be approved by The Open Group. The Project Charter will be approved through the normal mechanism of The Open Group.