Request Session: Threat Dragon

CDT Threats & Risks: Session 2

Matthew Edwards

Oct. 17th, 2019

Goals

- Become familiar with Threat Dragon interface.
- Understand and build system diagrams supported by Threat Dragon.
- Apply STRIDE for threat annotation.

Preliminaries

Github accounts

Sample Model

https://threatdragon.org/

Session Task

1. Form into pairs (STRIDE:TRIKE group members).
2. On Github, create a new project and add a basic README
3. Use the Threat Dragon interface to diagram:
   - A **browser** actor which sends commands and receives responses from ...
   - A process called **DragonDrop** which ...
   - Creates widgets and receives widget code from an external **Widget Factory** process, and ...
   - Writes queries and receives results from a **database**.
   - There is a trust boundary between **DragonDrop** and all other elements.
4. Examine the elements and data flows using the STRIDE approach to look for threats. Discuss!

Stretch Task

1. Find and fork a suitable project on Github `https://github.com/explore`
2. Using ThreatDragon, analyse the code (and/or documentation) to come up with a system diagram.
3. Use the combination of the code, the diagram and the STRIDE approach to identify threats.
4. Review your threats, see if there are mitigations you could suggest.