Introduction to Software Security
Chapter 2.4:
Microsoft DREAD Threat Classification

Elisa Heymann
elisa@cs.wisc.edu

Barton P. Miller
bart@cs.wisc.edu

Loren Kohnfelder
loren.kohnfelder@gmail.com

DRAFT — Revision 3.0, August 2023.

Objectives

- Learn about the DREAD threat classifications.
- See how DREAD assigns scores to its various threat categories.

Overview

The DREAD methodology[1] was developed at Microsoft, starting with Jason Taylor of the Internet Explorer team, and published in 2003 in a book by Howard and LeBlanc[2].

DREAD is less of a threat modeling methodology than it is a threat classification system.. It provides a ranking for a threat in each of the five categories:

1. **D**amage potential
2. **R**eproducibility
3. **E**xploitability
4. **A**ffected users
5. **D**iscoverability

The categories contrast with STRIDE and can be considered complementary to STRIDE. Where STRIDE talks about how the threat causes its damage, DREAD focuses more on the effect and consequences of the threat.

Details

Each category ranks the threats ranked on a scale of 0 to 10, and the total ranking is the sum of the ranks in each of the five categories. The scores are interpreted as follows:

Damage potential:

0 - Indicates no damage caused to the organization
5 - Information disclosure has occurred
8 - Non-sensitive user data has been compromised

[1] Jayanthi Manikandan, “DREAD Threat Modeling Methodology”, Microsoft, March 2003. https://www.practical-devsecops.com/dread-threat-modeling/
[2] Michael Howard and David LeBlanc, **Writing Secure Code**, 2nd edition, Microsoft Press, 2003.

9 - Non-sensitive administrative data has been compromised
10 - The entire information system has been destroyed

Reproducibility:

0 - Difficult to replicate the attack
5 - Complex to replicate the attack
7.5 - Easy to replicate the attack
10 - Very easy to replicate the attack

Exploitability:

2.5 - Indicates that advanced programming and networking skills needed to exploit the vulnerability
5 - Available attack tools needed to exploit the vulnerability
9 - Web application proxies are needed to exploit the vulnerability
10 - Indicates the requirement of a web browser needed to exploit the vulnerability

Affected Users:

0 - no users affected
2.5 - Chance of fewer individual users affected
6 - Few users affected
8 - Administrative users affected
10 - All users affected

Discoverability:

0 - Indicates hard to discover the vulnerability
5 - HTTP requests can uncover the vulnerability
8 - Vulnerability found in the public domain
10 - Vulnerability found in web address bar or form

DREAD helps in prioritizing threats by assigning a value to them, where the highest scoring threats would be the most critical and must be prioritized in mitigation.

Summary

Inside Microsoft, DREAD has been superseded by STRIDE, but is still used by a variety of companies and government organizations. Where the STRIDE model describes threat categories, DREAD focuses on their severity and impact, so DREAD is a threat scoring system, in some ways like CVSS (described in Chapter 6.5.1). The STRIDE model is used during the design phase to anticipate what threats might exist for the system being designed. The DREAD is used to describe threats that are already known. In many ways, the two approaches are complementary.

Exercises

1. Find a threat to a real or theoretical software component and then describe the threat by assigning a score for each of DREAD threat categories..