Seminar 1: STRIDE & DREAD tools

During this seminar, we will use the Microsoft STRIDE & DREAD tools (Meier et al., 2003). Read the paper and review the lecture cast, and then based on **your** response in Collaborative Learning Discussion 1, answer the questions below:

Q: Use a 3 level DREAD rating where 0 = no risk and 3 = maximum risk.

The Microsoft DREAD model is a risk assessment model that assigns values to various risk factors identified by various threats.

- **D.** *Damage. Potential effect of a threat.*
- **R.** *Reproducibility. How easy is it to reproduce the threat?*
- **E.** *Exploitability. How difficult is it to create the threat?*
- **A.** *Affected Users. Which users are affected by the threat?*
- **D.** *Discoverability. How easily was the threat discovered?*

Table 1 Classification of DREAD risk factors between 1 and 3. "0" represents No Risk and is excluded.

Risk Rating	**Risk Factor**		
	1 (Low)	2 (Medium)	3 (High)
Damage	This vulnerability leads to other vulnerabilities.	Sensitive data compromised but service still available.	Data modified or service unavailable.
Reproducibility	Seen as once-off.	Threat reproducible on same network or direct access to machine.	Threat reproducible over internet.
Exploitability	Requires a victim's intervention.	Advanced networking and programming skills required.	Exploited with available tools.

Affected Users	Less than half of the users are affected.	More than half of users are affected.	All users are affected.
Discoverability	Difficult to discover.	Discovered by publicly available information.	Discovered by browser window or tool command output.

Table 2 Classification of threats according to DREAD

Risk Rating	**Risk Factor** (0 = No Risk, 3 = Max Risk)	
	Threat: **Denial of Service**	Threat: **Brute Force**
Damage	**3**	**3**
Reproducibility	**3**	**3**
Exploitability	**3**	**3**
Affected Users	**2***	**2***
Discoverability	**3**	**3**
DREAD Score	**14**	**14**

***** *“2” was assigned because of localised testing by students. However, in a real-world scenario this would be ranked as “3”.*

Q: Which is the risk with the highest rating? What assumptions have you made?

All risk ratings (except the “Affected Users” rating) have a maximum-security severity based on the following assumptions:

Table 3 Assumptions for Denial-of-Service threat

	Risk Factor	Assumption
Damage	3	The mannequin can stand-in for a real-world person who has attached medical device(s) that may be required to administer life-saving medication at timed intervals.
Reproducibility	3	The attack was able reproduced via bootable DVD and over the network in a virtual machine. The virtual machine could represent an attacker's machine in a different location or country.
Exploitability	3	The threats were easily exploited by students using readily available tools. They did not require in-depth knowledge of the mannequin and easily attacked the mannequin within a few hours.
Affected Users	2	For this rating, the assumption is that the users affected are limited because only the students are attempting to attack the mannequin.,
Discoverability	3	The assumption is that the students understand the outputs of each tool to proceed with each step of attack. In essence, an attacker could "investigate" each interesting piece of information as sensitive information like the router Personal Identification Number (PIN) was easily viewable in the command tool window.

References

Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. & Murukan, A. (2003). *Threat Modelling*

OWASP Foundation (2021). Threat Modelling Process. Available from https://owasp.org/www-community/Threat_Modeling_Process [Accessed 1 Dec. 2021]