Seminar 1 Preparation: STRIDE and DREAD tools

Course: MSc Computer Science

Module: Network and Information Security Management

Date: Saturday 21st August 2021

DREAD Threat Modelling:

The DREAD threat model provides a risk rating for a given threat by answering a series of questions. The resulting risk rating can be used to sort risks by their overall threat to the business, highlighting those that need to be investigated with immediate attention. A copy of the DREAD matrix has been included below (Microsoft, 2003).

Rating	**High (3)**	**Medium (2)**	**Low (1)**
Damage Potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information.	Leaking trivial information.
Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
Affected Users	All users, default configuration, key customers.	Some users, non-default configuration.	Very small percentage of users, obscure feature; affects anonymous users.
Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

Score	Risk Rating
12-25	High
8-11	Medium
5-7	Low

Identified Threats (Healthcare):

Threat 1:

Threat Description	Unauthorised user gains access to WiFi Network
Threat Target	WiFi network
Risk Rating	High
Attack Techniques	WiFi Password Brute forcing
Countermeasures	• Explicit Whitelisting • Firewalls

Threat	**D**	**R**	**E**	**A**	**D**	**Total**	**Rating**
Unauthorised user gains access to WiFi Network	3	3	2	3	2	13	High

Threat 2:

Threat Description	Forcing disconnect of management PC from medical mannequin
Threat Target	Medical mannequin host PC
Risk Rating	Medium
Attack Techniques	WiFi Deauthentication
Countermeasures	• Upgrading to 802.11W (2009) standard. • Firewall

Threat	**D**	**R**	**E**	**A**	**D**	**Total**	**Rating**
Forcing disconnect of management PC from medical mannequin	1	3	2	1	1	8	Medium

References:

Meier, J. et al. (2003) Improving Web Application Security: Threats and Countermeasures. Available From: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN [Accessed 21st August 2021].