**Introduction**

There is no better time to talk about protecting the medical industry from cyber thread than now. In December 2020, IBM warned the governments and organisations about the attacks targeted towards the corporations critical to the circulation of COVID-19 vaccines (CBC, 2020).

Last few weeks, students were actively engaged in a collaborative discussion generating a vast amount of ideas, views and solutions. This summary post is developed based on the learning through the discussions and team activities conducted for preparing the seminar titled "STRIDE and DREAD tools".

**Background**

The research paper Compromising a Medical Mannequin discusses various cybersecurity gaps identified in the domain of medical devices. As part of the core research, a team of undergraduate computing student team was given access to a medical training mannequin and challenged to compromise within a semester (four months). Students carried out brute force attacks and a denial of service (DoS) attack. Brute force attacks were executed using BackTrack 5 from a live CD and using a virtual machine configuration. The denial of service attack was performed through a network protocol.

**Threat Modeling (STRIDE and DREAD)**

Security threat modelling tools such as STRIDE and DREAD can be used to assess the potential threats and possible impact so that the solution can be secured before implementation.

STRIDE is a thread modelling tool and acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Security specialists can use this framework and mnemonic to identify the potential security threats and address those gaps before implementation. The STRIDE provides a structured method to identify all possible threats. However, prioritising the issues for remediation is not supported by STRIDE.

DREAD is a different thread modelling tool, and this acronym stands for discoverability, reproducibility, exploitability, affected users, and damage. Unlike STRIDE, DREAD can be used to prioritise security threats. First, each factor (e.g. discoverability) for a given security threat can be given a score (for example, 1 to 10). Then, the overall level of risk for the security threat is calculated by dividing the total factors by the number of factors. A higher score represents a high level of threat. Usually, during prioritisation, security threats with higher scores should be addressed first.

Using STRIDE, organisations can identify the inventory of threats and remediation activities can be prioritised using DREAD.

**Vulnerability 1: Brute Force Attack**

Risks related to Brute force attacks can be mitigated by implementing various technical controls. For example, enforcing strong passwords with password complexity, implementing an account lockout policy with a limited number of login attempts and configuring time delays between login attempts are simple but effective technical controls. In addition, implementing security verification questions and enabling multi-factor authentication are a few other technical controls that can minimise the risks related to brute force attacks (O'DRISCOLL, 2020).

In addition, robust security awareness training can be utilised to manage the risks associated with brute force. Till also highlighted that security awareness training can be leveraged to manage the risks related to social engineering attacks (Langbein, 2021)

**Vulnerability 2: Denial of Service Attack**

Hardening wireless systems using industry security benchmarks such as the Center for Internet Security (CIS) security benchmark can help to address the threads related to denial of service attacks. In addition, restrict access to the network by filtering the media access control (MAC) address will minimise the risks associated with denial of service attacks (CISA, 2020).

As Anum highlighted, solutions like firewalls also can be utilised to manage the risks related to Denial of Service Attacks (Rashid, 2021).

**Conclusion:**

Organisations should use systematic approaches to identify security threats and prioritise remediation activities. As noted above, each security threat can be remediated using various security solutions. Organisations must perform a comprehensive assessment considering each solution, pros, cons and limitations before selecting appropriate security solutions.

**References:**

CBC. (2020) Cyberattacks target COVID-19 vaccine distribution effort. Available from: https://www.cbc.ca/news/world/coronavirus-vaccine-distribution-ibm-warns-hackers-1.5826602 [Accessed 30 May 2021].

CISA. (2020) Securing Wireless Networks. Available from: https://us-cert.cisa.gov/ncas/tips/ST05-003 [Accessed 30 May 2021].

Glisson, W. B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. and Mayr, J. (2015) 'Compromising a Medical Mannequin'.

Langbein, T. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=256170 [Accessed 30 May 2021].

O'DRISCOLL, A. (2020) What is a Brute Force Attack? Examples & How to Avoid Attacks. Available from: https://www.comparitech.com/blog/information-security/brute-force-attack/ [Accessed 30 May 2021].

Rashid, A. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=256232 [Accessed 30 May 2021].