The context of this research (article) derbies how medical devices comfortably creates room for vulnerabilities as medical services dependency on technology increases. Effort in the past has concentrated majorly on individual breaches and their technical knowledge around medical devices. However, there has been concerns around the vulnerabilities in the technical devices used in the medical industry as well as uncertainty of the possibility of intentional failure of this devices.

According to Glisson et al. (2015) the greatest security threats is that of inadequacy of policies and technique leading to difficulty in deciding if a breach was intentional or malicious.

  Glisson et al. (2015) Also highlighted the impact of vulnerabilities around training facilities if not detected can lead to wrong assessment from professionals as a result of inaccuracies within the medical devise. This concerns led to investigations around the possibility of compromising a mannequin system In a medical training environment and vulnerabilities like brute force attack and denial of service where detected around network communications and controlling computer.

As already known that denial of service attacks targets the disruption of network service and connectivity, there are many ways these can be mitigated against. According to Mahjabin et al. (2017) this could be achieved by using prevention filter which when applied to routers ensures only legitimate traffic have access and another type could be the ingress filters which prevent traffic with spoofed IP to enter a protected network.

Brute force attack is known case of multiple attempts to gain unauthorized access, and this can be mitigated against by using some methods like Limiting login attempts, using two factor authentications, Restricting access to authentication url (Anon, 2019).

Reference:

Anon. (2019) What is a Brute Force Attack & How to Prevent Them. Available from: https://sucuri.net/guides/what-is-brute-force-attack/ [Accessed 14 November 2021].

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Available from: https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf [Accessed 14 November 2021].

Mahjabin, T., Xiao, Y., Sun, G., Jian, W. (2017) A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks.*13(12): 1-33. Available from: [**https://journals.sagepub.com/doi/pdf/10.1177/1550147717741463**](https://journals.sagepub.com/doi/pdf/10.1177/1550147717741463)