PEER- RESPONSE

I agree with your arguments that tampering with medical mannequins affects the training of medical students, which leads to incorrect diagnosis and treatment of patients. Technology is taking over the production and operation of medical training devices like a mannequin, prone to cyber threats. The iStan medical mannequin is prone to DOS attacks that affect TCP network protocol and brute force attacks tampering with 802.11 wireless transmissions responsible for communication between the mannequin and the control panels. When the mannequin is tampered with during the production stage, it comprises the teaching, learning of medical professionals, and the investigation of these devices.

The attacks against the medical mannequin are preventable by using a network firewall. This network firewall will hinder attacks from DOS that make the iStan front-end software Muse unavailable. The firewall helps install a certain number of allowed incomplete TCP requests for a specific destination. It is possible through a resilient architecture, hardware, bandwidth, and outsourcing. The attacks cannot continue since when the permitted number is attained, they are not processed until they are completed or when time runs out.

Disabling the Wi-Fi Protected Setup feature mitigates attacks from brute force on 802.11 wireless transmissions within the radio range. It is possible because the attackers do not access the Wi-Fi network, and it is impossible to attack while not in the same radio range. The regular passwords for connectivity and control are discouraged from having better protection of medical training equipment. When the medical training equipment is protected against cyber threats and vulnerabilities, the training and teaching of medical students will not be tampered with and will not be cases of incorrect diagnosis and treatment of patients.

Reference List

Anon, Network dos attacks. *Network DoS Attacks | Junos OS | Juniper Networks*. Available at: <https://origin-www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/topic-map/security-network-dos-attack.html> [Accessed March 16, 2022].

Anon, Security tip (ST15-002). *CISA*. Available at: <https://www.cisa.gov/uscert/ncas/tips/ST15-002> [Accessed March 16, 2022].

Glisson, W.B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. and Mayr, J., 2015. Compromising a medical mannequin. *arXiv preprint arXiv:1509.00065*.

Kartch, R., 2016. Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response. *Software Engineering Institute, Carnegie Mellon University*.