**Peer Response 1**

Context: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285108>

Hi Lukman,

This was an informative post that raises some interesting topics for discussion. DDoS detection in the field of medical/IoT devices is different to conventional DDoS detection because of how different the network patterns are: conventional web browsing is highly random because individuals take different amounts of time to browse, while IoT devices behave more consistently because they send data at regular intervals (Doshi et al., 2018). Based on this, do you think that it would be easier to detect a DDoS on an IoT network? Academics are currently focused on using Artificial Intelligence to solve this problem, however, knowing the context of this situation (i.e. knowing that medical devices might have serial numbers, that data transmission can be one-way, and so on), artificial intelligence might not be necessary because foreign communications can be detected, based on whether the communications match existing rules and patterns. Practically speaking, creating a lightweight rules-based system could filter out foreign communications, and could prevent a DDoS entirely. What do you think?

Proper authentication is also an interesting topic to consider. Since the devices are manufactured, they might have known features such as serial numbers or MAC addresses. They also might have identifying information on their software. This could make multi-factor authentication a viable solution for preventing brute force attacks, because the three factors of authentication could be modified to fit an IoT context. The three factors are "something you know", such as a password, "something you have", such as a one-time PIN, or "something you are", which might be a fingerprint (Pearson, 2011). What are your thoughts on this approach?

**References**

Doshi, R., Apthorpe, N. & Feamster, N. (2018) 'Machine Learning DDoS Detection for Consumer Internet of Things Devices,' *2018 IEEE Security and Privacy Workshops (SPW)*. San Francisco, California, 24 May. New Jersey: IEEE. 29-35.

Pearson. (2011) Understanding the Three Factors of Authentication. Available from: https://www.pearsonitcertification.com/articles/article.aspx?p=1718488 [Accessed 18 November 2021].

**Peer Response 2**

Hi Hendrik,

I enjoyed reading your points regarding WiFi security, and based on your recommendation of 802.1x, I also discovered that 802.1x is separate to WiFi security protocols such as WPA and WEP- such security protocols are more related to guaranteeing data confidentiality, while 802.1x is intended to secure the process of authentication on a wireless network (Cisco, 2009), making it possible to mix and match security protocols and authentication schemes. Based on this, what security protocol do you think would be worth implementing alongside 802.1x in a case similar to this one? For instance, a university might want to connect a mannequin to its own network (or a subnet), but this would introduce a large amount of risk if not done in a secure manner. Reddy & Srikanth (2019) discuss the security of the WPA/WPA2/WPA3 and WEP protocols, but find that all have vulnerabilities to some degree, and in most cases, have reproducible steps available for exploiting these vulnerabilities. In light of this, would you consider any other means of securing the network apart from protocols? I think a case could be made for finding other ways of securing the device, such as relying on a wired connection between the mannequin and a computer, and ensuring that the computer in question would not be able to communicate with the WiFi network.

**References**

Cisco. (2009) FAQ on Cisco Aironet Wireless Security. Available from: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/68583-FAQ-Wireless-Security.html [Accessed 19 November 2021].

Reddy, B. & Srikanth, V. (2019) Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 5(4): 28-35. DOI: http://doi.org/10.32628/CSEIT1953127