The forum discussion was informative, and the viewpoints posted provided additional areas of consideration which can be used to further improve the recommendations made within my initial post.

One area under consideration was that of password management. Students overall agreed with the use of stronger passwords, however, a more objective measure of password strength may be a good topic for further discussion. Smirnov (2021) provided an article which discussed default router passwords within the context of password entropy- an extremely useful measure for password strength. This, in turn, could be further extended through the integration of other password strength criteria such as password lifetimes (Becker et al., 2018), which may be easier to implement in an IoT scenario.

Overall, excellent points were made regarding the notion of DoS mitigation and response. Villar (2021) argued that rapid advancement in hacking techniques and increased DoS attack volumes make it difficult for static systems to respond effectively to DoS attacks, making the use of Artificial Intelligence and Machine Learning a necessity to prevent catastrophic outages. Within the context of my original recommendation, DoS attacks may be better managed through the usage of middleware, but the lack of flexible DoS detection would make it easier for attackers to compromise the middleware itself. Consequently, AI should be given deeper consideration to build a secure and future proof system. Furthermore, in response to my initial post, Justus (2021) posed a valid question to my assertion that DoS attacks can be seen as infrastructural in nature, noting that physical proximity and communication protocols could make it possible for DoS attacks to be carried out against devices directly. I agree that this is a viable attack scenario, and would look to continue the discussion within the context of a DREAD analysis: following the DREAD factors, direct device attacks would be less lethal than internet-based attacks because attackers are forced to be close to the device over some period of time for a DoS to work, making this form of attack hard to scale.

**References**

Becker, I., Parkin, S. & Sasse, M. (2018) 'The rewards and costs of stronger passwords in a university: linking password lifetime to strength', Proceedings of the 27th USENIX Conference on Security Symposium (SEC'18). Baltimore, Maryland, 15-17 August. USA: USENIX Association. 239–253.

Justus, M. (2021) Forum discussion with Shan Swanlow, 19 November.

Smirnov, A. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=285146 [Accessed 29 November 2021].

Villar, A. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=284987 [Accessed 29 November 2021].