The given article serves as a good introduction to how security must be managed within the context of healthcare devices. As the authors discuss, due to the device's use case, the attack surface is predominantly within the area of networking and communication. The majority of threats exist in this area because it leads to the most dangerous consequences- for example, relaying fraudulent information (or insufficient information) from a device can cause a health practitioner to make an error in judgement, and in the case of sending fraudulent information to a medical device responsible for managing a patient's vitals through medication, the patient could be harmed. Additional concerns exist due to the fact that data can also be misused to track and identify individuals. In the article, the area of networking and communication was compromised through a brute-force attack and a denial-of-service (DoS) attack.

Wearable communications can be made more secure through various means. The mannequin in the article fell victim to compromise due to its usage of an easily computable password, although additional consideration must be given to related aspects such as data transmission. Encrypting transmitted data is an effective approach for preventing data interception, however, encryption is currently a balancing act between power consumption, latency, and security. Coelho et al. (2019) discussed the use of encryption algorithms which are more energy efficient and have a lower computation time than more conventional encryption algorithms (viz. AES), however, these algorithms have potential vulnerabilities. The authors conclude that more research is required in this area, and more recently, Hedayatipour & McFarlane (2021) proposed a hardware-based, low-power encryption scheme which is appropriately protected from additional situational attacks.

Authentication is an additional area of concern, which must be managed appropriately to prevent impersonation or the compromise of devices and accounts. Mo et al. (2020) presented an improved version of an existing authentication system which preserves account safety even in the case of device theft, a man-in-the-middle attack, or attempts at device/user impersonation.

Finally, mechanisms to protect from DoS attacks must also be considered. Lomotey et al. (2017) proposed an architecture for medical IoT data, which made it possible to detect and prevent attempts at carrying out a denial-of-service attack on an IoT platform (but not the devices themselves). Sicari et al. (2018) proposed an architecture which makes it possible to detect denial-of-service attacks against IoT middleware, although the amount of time for recovery from a DoS attack remained an area to consider for future research.

In a real-world scenario, it can therefore be argued that protecting against the vulnerabilities exploited on the mannequin (and medical devices at large) relies on the usage of a strong device password, a robust encryption scheme, and some mechanism to detect and/or prevent against DoS attacks. A strong device password is easy to create, however, encryption would be harder to implement for a medical device due to energy requirements. Energy-efficient proposals for encryption have yet to prove their reliability, and thus the usage of a more proven algorithm (such as AES) would be preferred, even though it comes at the cost of higher energy requirements. Lastly, DoS attacks are an infrastructural issue, which can be handled more effectively by introducing some form of middleware to guarantee device uptime- the greatest risk of a DoS attack on a medical device would be that the device is too overloaded to collect data, causing a medical record to be incomplete. Facilitating communication through middleware would prevent this threat because it adds an additional layer to device communication, ensuring that devices cannot be compromised directly and therefore can continue to collect data, even if said data cannot be processed by the middleware. If this transpired, it would also be possible for the device to simply keep that data until the middleware recovers.

**References**

Coelho, K., Damião, D., Noubir, G., Borges, A., Nogueira, M. & Nacif, J. (2019) Cryptographic Algorithms in Wearable Communications: An Empirical Analysis. IEEE Communications Letters 23(11): 1931-1934. DOI: http://doi.org/10.1109/LCOMM.2019.2937782

Hedayatipour, A. & McFarlane, N. (2021) An Encryption Architecture Suitable for on Chip Integration With Sensors. IEEE Journal on Emerging and Selected Topics in Circuits and Systems 11(2): 395-404. DOI: http://doi.org/10.1109/JETCAS.2021.3077023

Jiaqing, M., Wei, S. & Weisheng, P. (2020) An Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems. Wireless Communications and Mobile Computing. DOI: https://doi.org/10.1155/2020/5686498

Lomotey, R., Pry, J., Sriramoju, S., Kaku, E. & Deters, R. (2017) 'Wearable IoT Data Architecture', 2017 IEEE World Congress on Services (SERVICES). Honolulu, Hawaii, June 25-30. New Jersey: IEEE. 44-50.

Sicari, S., Rizzardi, A., Miorandi, D. & Coen-Porisini, A. (2018) REATO: REActing TO Denial of Service attacks in the Internet of Things. Computer Networks 137: 37-48. DOI: https://doi.org/10.1016/j.comnet.2018.03.020