Collaborative Discussion

Contents

Response to Ian Wolloff

Hi Ian,

I enjoyed the quote by Dan Farmer, which sums up that security is not an issue if no devices operate.

In your post, it refers to using 2FA as a mitigation technique against brute force attacks. 2FA is a reasonable consideration since it usually requires a user's biometric data for confirmation, making 2FA much better than mere passwords. Do you think, in the context of medical devices, such an authentication system is viable? For example, in order for a blood glucose monitor to communicate with a patient observation server, it might not be reasonable to expect each nurse assigned to monitor a patient, to provide 2FA to the device. In this case, OAuth 2.0, though, does support the concept of a Device Authorisation Flow (https://auth0.com/intro-to-iam/what-is-oauth-2/), so I wonder if, in the context of medical devices, OAuth 2.0 may be a better substitute to 2FA?

Response to Shan Swanlow

Hi Shan,

I enjoyed the reference to difficulties surrounding the use of encryption in (medical) devices given the power requirements, potential vulnerabilities in the encryption algorithms, and computation power of these devices. In this regard, the reference to Hedayatipour & McFarlane (2021) was a good read. I am pretty interested in the

statement in the post, "a strong device password is easy to create". This is entirely agreeable, though. In the context of the paper by Glisson et al. (2015), do you see the enforcement of a password policy being external to the mannequin? Another intriguing statement in the post is the DoS attacks are primarily infrastructure concerns. Does the argument hold if attackers can gain access to (medical) devices directly, for instance, if the device exposes functionality over radio waves and not via internet-based communications?

References

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin.