Aldo:
Computer networks are not the only ones that can be compromised with cybersecurity threats. As the paper "Compromising a Medical Mannequin" demonstrates, medical systems that can be considered as IOT systems can be affected too. The mannequin iStan is a medical device used for training purposes by students at the University of South Alabama. As described, students were able to identify software vulnerabilities that allowed them to perform threats to elevate user privileges by performing a brute force attack (obtaining valid user and password) and denegate service to the software application by simulating false entry signals [Glisson, Andel, McDonald, Jacobs, Campbell, 2015].

Honeypots are an alternative proposed to mitigate brute force and denegation of service attacks in IOT systems that are connected to a network such as medical equipment. Honeypots are security tools that block network access to an attacker and deceive him/her by allowing infiltration to a false image of the real system that allows the network administrator to monitor the activity and personal information of the attacker such as his/her IP address. In the case of the medical mannequin, threats could be identified before the attacker is able to infiltrate the medical equipment [Arif, De Rosal, Eko, Christy, 2019].

Thank you, Aldo, for the informative post. The use of brute force attacks as implemented by the students in the study (Glisson et al., 2015) highlights the vulnerabilities medical devices face. Honeypots are indeed a helpful mitigation strategy to overcome brute force attacks. The increased visibility allows security teams to gather intelligence on the threat actors and plan defences, whereas firewalls fail to prevent this. The amount of time that attackers waste by infiltrating a dummy system means less time to attack the actual system (TitanHQ, 2021). Threat actors can become frustrated and perhaps not consider following on in this process.

An example of this is the Kippo honeypot, which creates a false SSH server (Doubleday et al., 2016). This honeypot is exceptionally detailed, making the attackers attempt redundant. The data collected can map out the attacker's plans, which can later be used for analysis and future staff training. However, there are disadvantages such as cost. The more realistic setup will incur higher costs and the setup can add complexity to the network with more maintenance on SQL databases.

Further vulnerabilities could incur, and this may be used to gain access to the actual data. Therefore a consideration might be to keep the attackers out rather than let them in as that may provide just as valuable information. The honeypot can provide valuable data on the severity of the risk, and this information can be important for discovering vulnerabilities, improving development and improving security policies (Al-Jameel & Alanazi, 2021).

Al-Jameel, S. & Alanazi, A. A. (2021). Honeypots Tools Study and Analysis. Available: http://paper.ijcsns.org/07_book/202101/20210121.pdf [Accessed 17 November 2021].

Doubleday, H., Maglaras, L. & Janicke, H. (2016). SSH Honeypot: Building, Deploying and Analysis. Available: https://thesai.org/Downloads/Volume7No5/Paper_18-SSH_Honeypot_Building_Deploying_and_Analysis.pdf [Accessed 17 November 2021].

Glisson, W., Andel, T., Mcdonald, J., Jacobs, M., Campbell, M. & Mayr, J. (2015). Compromising a Medical Mannequin. Available: https://www.researchgate.net/publication/281487935_Compromising_a_Medical_Mannequin [Accessed 13 November 2021].

Titanhq. (2021). Benefits of Honeypots – There's More to Honeypots Than Wasting Hackers' Time. Available: https://www.webtitan.com/blog/honeypots-how-far-can-you-go-in-wasting-a-hackers-time/ [Accessed 17 November 2021].