Unit 1

Collaborative Discussion

Compromising a Medical Mannequin

The paper presented by Glisson et al. (2015) highlights several vulnerabilities found in medical devices. Vulnerabilities such as medical identity theft, denial of service, use of unencrypted data (Halperin et al., 2008), unencrypted processing data (Malasri et al., 2009), as well as threats to the solution (overcome by brute force attacks) and the supported network protocol (overcome by denial of service). Sametinger et al. (2015) consider a medical device security-critical if the device processes or communicates data (often) via sensors. Security-critical devices are a threat because they may facilitate incorrect decisions by other devices or medical staff, which may have severe consequences for a patient.

To mitigate medical device vulnerabilities consists of both software and hardware aspects. All software must be developed using secure software development techniques, which involves detailed domain knowledge and training. Mitigating brute force attacks over Wi-Fi includes delaying beacon frames and mapping a client's MAC address (Hafiz & Ali, 2014). General brute force mitigation employs complex password length and character set policies, lockout, and refresh policies. Other considerations also include the use of "honeypot accounts" (Herley & Florêncio, 2008). Step to mitigate Denial of Service attacks may involve use of "fuzzy reasoning" in firewalls (Naik & Jenkins, 2016), configuring firewalls to monitor (and drop) a surge of ICMP and UDP packets from an IP address, rerouting targeted traffic to invalid IP addresses, use of private medical networks (Kumari et al., 2020; Gritzalis et al., 2001) or spam and content filtering.

References

Glisson, W.B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J., (2015). Compromising a medical mannequin. *arXiv:1509.00065*.

Gritzalis, D. Gritzalis, C. Moulinos, & J. Iliadis, S. (2001). An integrated architecture for deploying a virtual private medical network over the Web. *Medical informatics and the internet in medicine* 26(1):49-72.

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., & Maisel, W. H. (2008). “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses,”. *2008 IEEE Symposium on Security and Privacy*. IEEE Computer Society:129-142.

Hafiz, M.M. & Ali, F.H.M. (2014). Profiling and mitigating brute force attack in home wireless LAN. *International Conference on Computational Science and Technology (ICCST):*1-6.

Herley, C. & Florêncio, D. (2008). Protecting financial institutions from brute-force attacks. *IFIP International Information Security Conference*:681-685.

Kumari, K.A., Padmashani, R., Varsha, R. & Upadhayay, V. (2020). Securing Internet of Medical Things (IoMT) using private blockchain network. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm:305-326.*

Malasri, K., & Lan, W. (2009). Securing Wireless Implantable Devices for Healthcare: Ideas and Challenges. Communications Magazine 47(7):74-80.

Naik, N. & Jenkins, P., (2016). Fuzzy reasoning-based windows firewall for preventing denial of service attack. *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*:759-766.

Sametinger, J., Rozenblit, J., Lysecky, R. & Ott, P. (2015). Security challenges for medical devices*. Communications of the ACM* 58(4):74-82.