Enforcing Digital Forensics Readiness in Wireless Medical Networks Using Artificial Intelligence

CEPHAS MPUNGU

Computer Science, Middlesex University, London, UK

The Covid-19 Pandemic was catastrophic for almost every organisation. This forced many organisations, especially healthcare, to hastily restructure their business operation models through the development and adaptation of systems that support remote working. Cybercriminals on the other hand embraced this opportunity to maximize, leverage and execute more attacks. Most of these attacks were targeted at Wireless medical networks to exfiltrate sensitive data in form of vaccine-related research and personal medical records. Wireless Medical Networks(WMNs) are connections/communications initiated between medical devices without the use of network cables or wires. WMNs use radio-wave communication which makes them more susceptible to attacks compared to wired medical networks. The National Cyber Security Centre (NCSC) cited increased cyberattacks like phishing, SQL injections, zero-day exploits, malware, fraudulent websites and hacking during the lockdowns. The reason for this was that business organisations invested little towards securing remote-work underlying technologies. In the advent of the aforementioned attacks, it is imperative that an organization's Incident Response team is well prepared to launch a digital forensics investigation.

This needs to be done systemically and formally and so every organisation should be undoubtedly placed to carry out such investigations (atminimal cost or interruption to its day-to-day business) by having Digital Forensics Readiness (DFR). DFR is an integral part of an organisation's compliance with dataprotection requirements, especially to aid in data breach investigations and also denotes an organisation's good corporate governance and due diligence. This presentation focuses on the development of a proactive, secure, and streamlined approach to DFR using Artificial intelligence(AI) at the SIEM(Security Information and Event Management) level, among other recommendations. The presentation first discusses threats to wireless medical networks. It then undertakes a systematic review of previously proposed digital forensics frameworks and identifies challenges. Finally, it proposes a novel conceptual framework for Digital Forensics Readiness (DFR) for wireless medical networks that (aims to) addresses the challenges using AI. The framework contributes to the enforcement of evidential data integrity whilst also securing wireless networks. Wireless medical networks will be used as a case study but the conceptual framework can be applied to other domains.

Keywords: digital forensics, artificial intelligence