ABSTRACT

CYBER-LLAMA-2: Zero-shot MEDICALHARM Threat Modeling Mentor
for Modern Medical Device Cybersecurity, Privacy, and Safety.

Emmanuel Kwarteng

Marquette University, 2024

With the rapid growth of Modern Medical Devices (MMDs) and their increasing connectivity to enhance patient care, concerns about security, privacy, and safety are paramount. If compromised, these devices can expose sensitive patient information and harm patients. Therefore, securing MMDs against cyber-attacks is critical. Threat modeling, mandated by the FDA as a premarket submission requirement in the MMD domain, serves as the first defense mechanism. However, our investigation of 119 participants from various MMD manufacturing companies revealed a need for a tailored threat modeling methodology that considers both patient safety and device complexity. To address this, we present MEDICALHARM, a new methodology combining threat and risk analysis under a single scheme, specifically addressing safety, security, and privacy threats. Our post survey among cybersecurity experts in the MMD domain revealed positive feedback, particularly on its perspective on the integration of cybersecurity, privacy, safety, trust level, and documentation strategy.

Nevertheless, developing a tailored threat modeling methodology is just one facet of the problem. Adopting the MEDICALHARM methodology requires training, which can be a lengthy process considering the previous conventional threat modeling methodologies also took several years to implement. To facilitate this, we developed CyberLlama2, a threat modeling-assisted LLM designed to aid MEDICALHARM in identifying threats. CyberLlama2 acts as a MEDICALHARM mentor, helping adopters perform threat modeling with ease. This specialized model is fine-tuned with a large set of cybersecurity instructions to enhance effectiveness. Our evaluation of CyberLlama2's performance using Rouge, MAUVE, METEOR, CHRF, and WER metrics demonstrates its improved performance over baseline and other cybersecurity models. These results highlight CyberLlama2's potential to significantly enhance threat modeling processes, making it a valuable tool for securing Modern Medical Devices.