ABSTRACT

Security Attack Analysis (SAA) is a crucial activity in Security Threat Oriented Requirements Engineering (STORE), where threat modeling is conducted to identify potential attacks. Inaccurate SAA can result in flawed security requirements, often due to the performer's lack of knowledge and experience. Large language models (LLMs) have demonstrated remarkable capabilities in solving domain-specific problems when integrated effectively. However, integrating an LLM into the SAA process remains a challenge, especially when employing the multi-agent approach, as it requires strategizing on the orchestration approach and addressing LLM inherent issues, such as hallucination. This study introduces Security Attack Analysis Support (SAAS), a process that employs an LLM-based multi-agent approach to support the engineers in performing SAA. We propose and implement two distinct SAAS designs, each utilizing a unique orchestration approach, and additionally incorporate prompt engineering and structured inputs for both designs. We conducted an expert judgement to assess the effectiveness of both SAAS designs and analyzed the feedback using grounded theory. The results show that both proposed designs have effectively performed SAA in accordance with the scope of the project, with each design offering its own strengths and weaknesses.

Keywords: large language model, requirement engineering, security, requirement engineering, software security.