

MODELIRANJE VARNOSTNIH GROŽENJ S POMOČJO GENERATIVNE UMETNE INTELIGENCE

Nika Jeršič¹, Muhamed Turkanović¹, Tina Beranič¹

¹ Fakulteta za elektrotehniko, računalništvo in informatiko, Koroška cesta 46, 2000 Maribor

nika.jersic@um.si, muhamed.turkanovic@um.si, tina.beranic@um.si

Modeliranje informacijsko varnostnih groženj in ranljivosti je ključni postopek za prepoznavanje, razvrščanje in zmanjševanje tveganj v programski opremi, sistemih IT in organizacijskih procesih. V ta namen so bili razviti različni okviri in metodologije, ki se osredotočajo na posebna področja uporabe in pristope k varnostni analizi. Čeprav celovita uporaba teh metod omogoča boljši pregled nad varnostnimi tveganji, se v praksi pogosto srečujemo z izzivi, kot so dolgotrajni postopki in zapletenost izvajanja. V tem prispevku predstavimo nekaj najpogostejše uporabljenih varnostnih okvirov in raziščemo, kako lahko veliki jezikovni modeli prispevajo k avtomatizaciji in pospešitvi postopka modeliranja informacijsko varnostnih groženj. Osredotočili se bomo na njihovo sposobnost prepoznavanja morebitnih ranljivosti, analiziranja vzorcev varnostnih incidentov in predlaganja blažilnih ukrepov, kar lahko bistveno izboljša učinkovitost in dostopnost varnostnih ocen v organizacijah. V okviru analize smo preučili uspešnost različnih obsežnih jezikovnih modelov, vključno s ChatGPT, Perplexity, CoPilot in Gemini, pri prepoznavanju varnostnih groženj. Prav tako smo primerjali, kako posamezna orodja pomagajo pri prepoznavanju, modeliranju in preprečevanju groženj ter kako natančna in uporabna so pri zagotavljanju varnostnih priporočil.

Ključne besede: Kibernetika varnost, analiza ranljivosti, modeli analiziranja ranljivosti, jezikovni modeli

USING LARGE LANGUAGE MODELS TO MODEL SECURITY THREATS

Information security threat and vulnerability modelling is a key process for identifying, classifying and mitigating risks in software, IT systems and organisational processes. Various frameworks and methodologies have been developed for this purpose, focusing on specific application areas and approaches to security analysis. Although the comprehensive application of these methods provides a better overview of security risks, in practice we are often faced with challenges such as lengthy procedures and

complexity of implementation. In this paper, we present some of the commonly used frameworks for information security threat modelling and explore how large language models can contribute to their automation and speed of generation. We will focus on their ability to quickly identify potential vulnerabilities, analyse patterns of security incidents and suggest mitigating actions, which can significantly improve the efficiency and accessibility of security assessments in organisations. As part of our analysis, we examined the performance of various large-scale language models, including ChatGPT, Perplexity, CoPilot and Gemini, in identifying security threats. We have also compared how each tool helps to identify, model and prevent threats, and how accurate and useful they are in providing security recommendations.

Keywords: Cybersecurity, vulnerability analysis, vulnerability analysis models, language models