TU Clausthal

Abschlussvortrag Masterarbeit Rashad Elmogsi

„Exploring LLMs Capabilities for Password Generation“

Passwords remain the most widely used method for securing digital accounts, yet users often struggle to create ones that are both strong and compliant with security policies. This leads to weak passwords, reuse, and poor adherence to industry standards. Large Language Models (LLMs) such as ChatGPT, Gemini, and LLaMA offer a new approach to password generation. This study investigates how LLMs can create secure, memorable, and policy-compliant passwords across various domains like banking, education, social media, and e-commerce. Structured prompt engineering, along with two widely-used password strength assessment tools zxcvbn and FuzzyPSM are employed to evaluate the complexity, randomness, and memorability of passwords generated by LLMs. The results indicate that well-designed prompts enable LLMs to produce high-quality passwords that meet modern security requirements. In addition, an analysis of hardcoded passwords found in public GitHub repositories provides insight into real world practices, compliance issues, and potential vulnerabilities. The findings suggest that with appropriate prompting, LLMs can be valuable tools for enhancing password generation and security practices.

Betreuer der Arbeit:	Prof. Dr. Mohammad Ghafari, Dr. Mohammad Abboush
Datum:	Mittwoch, 02. Juli 2025, 11:00 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/rooms/fdg-iaq-jqo-nhr/join