Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **BC. MICHAL KUBÍČEK** **Oponent:** **Ing. Ladislav Vyskočil**

Studijní program: **Informační technologie**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2023/2024**

Téma diplomové práce: **Vylepšenie bezpečnosti hesiel pomocou generatívnych modelov**

Hodnocení práce:

Cílem diplomové práce bylo popsat problematiku bezpečnosti hesel a navrhnout a implementovat nástroj pro generování hesel za využití generativních modelů, k jehož dosažení bylo třeba splnit několik bodů, jejichž přesná specifikace byla součástí zásad uvedených v zadání práce. Diplomová práce je napsána ve slovenském jazyce. Po jazykové stránce nebyly nalezeny žádné pravopisné, nebo stylistické chyby. Text práce je zpracován srozumitelně. Po formální stránce je práce vhodným způsobem řazena do navazujících logických celků a doplněna komentáři i odkazy na odpovídající literární či elektronické zdroje. Diplomová práce obsahuje přiměřené množství obrázků, tabulek a příloh.

V teoretické části byla velmi rozsáhle provedena literární rešerše problematiky bezpečnosti hesel, která obsahovala popis zranitelností a možných typů útoků, ochrany heslem s různými typy autentizací, zahrnující 2FA/MFA ověřování, SSO, Biometrickou autentizaci a Token-Based autentizaci. Dále byla popsána politika hesel a její doporučení, šifrování a ukládání hesel, použité metody HASH, Salting a Peppering. V této části byla zmíněna i správa a obnova hesel, psychologie tvorby hesel, uživatelské návyky a chyby, také popis sociálního inženýrství a phishingu pro neoprávněné získání hesel. Poslední kapitola teoretické části popisuje úvod do generativních modelů a jejich typy.

Úvod praktické části je zaměřen na analýzu existujících řešení, zahrnující praktické testy síly hesel generovaných v jednotlivých aplikacích. Další kapitola se zabývá analýzou datových sad s uniklými hesly. Byl proveden výběr sad hesel a s pomocí nástroje Password-Strength byla v prostředí Python provedena analýza těchto sad s prezentací výsledků analýzy. Poté byl proveden výběr generativního modelu za využití analýzy použitelnosti a pro nejlepší vlastnosti vybrán model LSTM. Následně byl prakticky popsán postup při trénování generativního modelu. Další kapitola se zabývá vyhodnocením bezpečnosti a obsahuje praktické ukázky útoků na hesla při použití Brute Force, slovníkového útoku, Keyloggeru a Hashcatu. Následuje přehledné vyhodnocení bezpečnosti hesel vytvořených zvoleným generativním modelem, zahrnující i podrobnou analýzu. Poslední část praktické části se zabývá implementací nástroje pro generování hesel pod OS Windows za použití jazyka C# v prostředí Visual Studio, která zahrnuje grafický návrh, popis principu funkce aplikace, postup tvorby i popis a demonstraci výsledné aplikace „MiKUB-Generator“.

Diplomová práce je velmi rozsáhlá a podrobně popisuje celou problematiku bezpečnosti hesel i navržená řešení. Všechny body zadání diplomové práce byly splněny v plném rozsahu, a proto ji doporučuji předložit k obhajobě

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 15. 5. 2024 Podpis oponenta diplomové práce