

POSUDEK KVALIFIKAČNÍ PRÁCE

posudek oponenta bakalářské práce

Autor: Petr Samec

Název práce: Využití databází hacknutých uživatelských hesel jako nástroje pro zlepšení zabezpečení uživatelských účtů

Specializace studijního programu: ITE - Informační technologie a e-learning

Datum odevzdání: 4.7.2023

Posudek vyhotovil: Mgr. Václav Dobiáš, Ph.D.

Odborná úroveň práce:	A
Popsání cílů a metod:	B
Věcné chyby, terminologie:	A
Kvalita teoretické části práce, citace:	A
Rozsah a kvalita praktické složky práce:	B
Struktura práce, formální úroveň:	B
Grafická a jazyková úroveň, chyby psaní:	A

Vlastní přínos autora:

Student do Bobříka informatiky implementoval nástroj, který porovnává zadané heslo s databází ukradených hesel. Pokud je zadané heslo v databázi ukradených hesel, pak je uživateli doporučena změna hesla. Při změně hesla je měřena jeho síla pomocí studentem navržené metriky. Tento výrazně praktický přínos práce je navíc sepsán do poměrně povedené závěrečné práce. Kvalitu práce dále zvýrazňuje použití statistických metod, pomocí kterých jsou dokazovány hypotézy. Hlavní překážkou v dosažení všech cílů práce byl nízký počet zachycených hacknutých hesel.

Hlavní nedostatky práce:

Největší nedostatek práce spatřuji v algoritmu výpočtu síly hesla. Použitý algoritmus z mého pohledu ignoruje základní kombinatorické principy. Kdy po přidání dalšího písmene je připočítána jistá hodnota. Reálně ale počet pokusů potřebných k prolomení takového hesla pomocí brute force techniky narůstá exponenciálně. Což jasně ukazuje tabulka na straně 17. Příkladem může být heslo sestávající z 12 malých znaků. Takové heslo je prolomitelné maximálně za 7 dní. Podle studentovy metriky má takové heslo hodnocení 60 bodů. Heslo o 14 znacích je prolomitelné za 12 let, podle studentovy metriky má ale pouze 70 bodů.

Této akademické diskusi by jistě výrazně prospělo, pokud by student provedl korelační analýzu výsledků dosažených pomocí jeho metriky a další jiné metriky. Výsledky jiné metriky má student již uvedeny v kapitole 3. 4.

Mezi další slabé stránky práce patří nedostatečný popis metod práce. Ku příkladu jsem v kapitole 1. 2 nenalezl počet učitelů, u kterých bylo analyzováno jejich heslo. V textu jsem také nenalezl informaci popisující proti jakým typům útoků je metrika navržena. Což je v protikladu s teoretickou částí, ve které student popsal celkem 30 různých typů útoků.

Práce dále vykazuje problémy s tokem textu.

Otázky pro obhajobu a náměty do diskuze:

Čím si vysvětlujete nízké počty zachycených hacknutých hesel.

Prosím o dopočítání korelace mezi výsledky dosaženými studentovou metrikou a nějakou další metrikou.

Práci doporučuji uznat jako bakalářskou.

Navrhuji hodnocení stupněm: velmi dobře



Místo, datum a podpis: České Budějovice, 16.8.2023

Vysvětlivky:

Při celkovém zhodnocení může autor posudku dát jednotlivým položkám hodnocení různou váhu.

A – vysoká úroveň (precizní teoretická část, kvalitní řešerše, bohatá a správně citovaná literatura, bez chyb psaní, výstižné formulace, kvalitní grafika, velký rozsah prací, velice inovativní práce, správná volba metody výzkumu, kvalitně zpracované výsledky výzkumu)

B – standard (teoretická část bez chyb, správně a přesně popsán cíl a metoda práce, průměrná odborná úroveň, standardní rozsah práce, s málo překlepy, vzhledem k rozsahu přiměřený počet drobných chyb, správné popisy v grafech, nepřesné citace v textu, chudší literatura – použití převážně 1- 2 zdrojů)

C – slabší úroveň (cíle a metody popsány nepřesně nebo neodpovídají realitě práce, menší rozsah práce, nepřesná terminologie, chybějící vysvětlení hlavních pojmů, malý rozsah práce, nepříliš inovativní a nosné, nedostatečné zdroje, použití převážně jednoho hlavního zdroje, chudá literatura, četné překlepy a slabší grafická úroveň, větší množství méně podstatných chyb, nejasná metoda a analýza výzkumu)

N – nevyhovující (chybějící nebo velmi stručné a formální popsání cílů a metod, malý rozsah práce, částečně opsáno v teoretické části, slabá terminologie, není patrný vlastní přínos, slabá úroveň vyjadřování, nejasné používané pojmy, malý rozsah praktické složky práce, závažné chyby ve výzkumu, nevyhovující grafická úroveň, mnoho hrubých chyb a překlepů, odbyté)