

## Posudek oponenta bakalářské práce

**Student:** Tobiáš Pavel  
**Téma:** Digitální steganografie pro spustitelné soubory (id 20401)  
**Oponent:** Bidlo Michal, Ing., Ph.D., UPSY FIT VUT

1. **Náročnost zadání** průměrně obtížné zadání
2. **Splnění požadavků zadání** zadání splněno

Práce měla za cíl návrh a realizaci aplikace pro ukryvání textové informace ve spustitelných souborech typu ELF a to konkrétně s využitím metody ekvivalenčních tříd a substituce instrukcí strojového kódu. Typ ukryvané informace a použitá steganografická metoda byly výsledkem volby studenta. Zadání bylo splněno.
3. **Rozsah technické zprávy** je v obvyklém rozmezí
4. **Prezentační úroveň předložené práce** 90 b. (A)

Práce je velmi dobře čitelná a srozumitelná, oceňuji zajímavé širší shrnutí historie steganografie a postupnou logickou návaznost na problematiku využívající moderní informační technologie.
5. **Formální úprava technické zprávy** 85 b. (B)

Text obsahuje pouze menší množství překlepů a gramatických chyb, jinak je na vysoké úrovni.
6. **Práce s literaturou** 100 b. (A)

Práce cituje (na BP vyšší) množství referencí z různých oborů, které jsou relevantní či alespoň částečně souvisejí s řešenou problematikou. Citační stránka práce je na vysoké úrovni.
7. **Realizační výstup** 90 b. (A)

Student využil moderních prostředků dostupných v prostředí Python 3, což značně usnadnilo řešení řady situací, volba tohoto jazyka je tedy opodstatněná. Ačkoliv je interpretovaný Python co do výkonnosti řádově méně efektivní než standardní implementace (např. v C), což se zde projevilo při stegoanalýze větších souborů (o velikosti řádově v MB), student provedl NAD RÁMEC ZADÁNÍ profilaci kódu a předložil analýzu, která umožnila výslednou realizaci značně zefektivnit.

Ve věci analýzy výsledků bych např. uvítal, kdyby byla podstatná data (např. kapacita souboru, využití kapacity ukrytou informací apod.) součástí výpisu ke konkrétně zapracované zprávě a ne pouze obecně a souhrnně s nutností spustit příkaz k tomu určený.

Z formálního hlediska všechny zdrojové soubory aplikace, přiložené na CD, postrádají identifikaci autora či instituce, není tedy jasný jejich původ, nicméně popis v technické zprávě dává tušit, že jsou dílem studenta. Žádné další nástroje třetích stran zřejmě nebyly potřeba.
8. **Využitelnost výsledků**

Jedná se o aktuální téma potenciálně využitelné v oblasti bezpečnosti IT.
9. **Otázky k obhajobě**
  1. Jakým způsobem je ošetřeno zpracování textu využívajícího různá kódování (např. UTF8 - kód s obecně proměnnou délkou značek)?
  2. Nevadí pro praktické použití, že binární kód, uvažovaný pro ekvivalenční třídy a zmiňovaný na str. 10, není prefixový?
  3. Jakými konkrétními prostředky byl proveden parsing výstupu algoritmu na základě regulárních výrazů?

**10. Souhrnné hodnocení**

**90 b. výborně (A)**

Celkově jde o kvalitní bakalářskou práci řešící zajímavé téma s potenciálem dalšího rozšíření. Student adekvátně zhodnotil poměrně náročnou oblast, na základě toho navrhl a kvalitně implementoval vlastní řešení a to navíc na základě dodatečné analýzy dále zoptimalizoval. Proto navrhuji hodnocení stupněm A.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 28. května 2018

.....  
podpis