Hodnocení vedoucího bakalářské práce

Student: Večeřa Vojtěch
Téma: Obnova hesel archivů ZIP s využitím GPU (id 18211)
Vedoucí: Hranický Radek, Ing., UIFS FIT VUT

1. **Informace k zadání**
   Práce navazuje na projekt Sec6Net, konkrétně na vykázaný prototyp nástroje Wrathion, který slouží pro obnovu hesel s možností akcelerace pomocí GPU. Cílem bylo analyzovat existující techniky kryptografického zabezpečení archivů ZIP a 7z, doplnit existující modul pro ZIP o podporu dalších metod zabezpečení a vytvořit nový modul pro formát 7z. Student rozšířil stávající modul o formát SecureZIP šifrovaný pomocí AES, který je zabezpečen odlišným způsobem než dosud podporovaný WinZIP, či starší PKZIP. Pan Večeřa dále navrhl a implementoval modul pro formát 7z. Nový modul podporuje několik variant zabezpečení, které se liší podle toho, zda jsou komprimována, či šifrována pouze data souborů, či také jejich hlavičky, apod. Praktický přínos programových výstupů student prokázal experimentálně pomocí výkonových měření, přičemž nechybělo ani porovnání s konkurenčními nástroji. Zadání tedy považuji za splněné.
2. **Práce s literaturou**
   Student aktivně čerpal jak z doporučené literatury, tak z dalších materiálů, které si sám dohledal. Zejména náročné bylo pochopení struktury a zabezpečení formátu 7z, který jeho autor, Igor Pavlov, popisuje jen velmi stručně a detailnější dokumentace zde není k dispozici.
3. **Aktivita během řešení, konzultace, komunikace**
   Student byl během řešení aktivní, práci se mnou konzultoval. Dohodnuté termíny dodržoval a na konzultace docházel obvykle připraven. Oceňuji také pomoc při demonstraci nástroje Wrathion na dni otevřených dveří.
4. **Aktivita při dokončování**
   Ačkoli k implementaci varianty pro GPU se student dostal relativně pozdě, práce byla dokončena v dostatečném předstihu a byla se mnou řádně konzultována.
5. **Publikační činnost, ocenění**
   -
6. **Souhrnné hodnocení** **velmi dobře (B)**
   Aktivitu studenta hodnotím jako nadprůměrnou. Pan Večeřa pracoval cílevědomě a průběžné výsledky pravidelně konzultoval. Řešení vyžadovalo nejen důkladné pochopení technologie OpenCL, ale především vnitřní struktury a zabezpečení formátů SecureZIP a 7z. Zejména detailní pochopení formátu 7z považuji za netriviální úkol, především z důvodu neexistující dokumentace. Práci studenta bohužel degraduje prodleva při implementaci kódu pro GPU, množství prezentačních a jazykových nedostatků při závěrečné korektuře a neúspěšná implementace podpory slibovaného 3DES šifrování formátu SecureZIP. Absenci podpory 3DES nicméně nepovažuji za nijak fatální, neb tato šifra je dnes považována za překonanou a u formátu ZIP je spíše raritou. I přes zmíněné nedostatky práci hodnotím jako velmi dobrou.

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

V Brně dne: 30. května 2016

.....
podpis