

Zadání bakalářské práce

Řešitel: **Večeřa Vojtěch**

Obor: Informační technologie

Téma: **Obnova hesel archivů ZIP s využitím GPU**
Password Recovery of ZIP Archives Using GPU

Kategorie: Bezpečnost

Pokyny:

1. Seznamte se s architekturou a implementací nástroje Wrathion.
2. Analyzujte techniky šifrování archivů ZIP a 7-ZIP.
3. Navrhněte rozšíření nástroje Wrathion o podporu dosud nepodporovaných metod šifrování archivu ZIP a modul pro archivy typu 7-ZIP.
4. Navržené rozšíření implementujte (včetně kódu pro akceleraci pomocí GPU).
5. Proveďte měření výkonu nástroje na nově přidaných formátech a výsledky porovnejte s konkurenčními nástroji.
6. Zhodnoťte dosažené výsledky.

Literatura:

- PHONG, Pham H. Password recovery for encrypted ZIP archives using GPUs. In: *SoICT'10. Proceedings of the 2010 Symposium on Information and Communication Technology*. New York: ACM 2010. s. 28-33. ISBN 978-1-4503-0105-3.
- MENEZES, Alfred J., VAN OORSCHOT, Paul C., VANSTONE, Scott A. *Handbook of Applied Cryptography*. Boca Raton (Florida): CRC Press 1999. 810 s. ISBN 978-8189836122.
- A další dle dohody s vedoucím.

Pro udělení zápočtu za první semestr je požadováno:

- Body 1 až 3.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese

<http://www.fit.vutbr.cz/info/szz/>

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Hranický Radek, Ing.**, UIFS FIT VUT

Datum zadání: 1. listopadu 2015

Datum odevzdání: 18. května 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
602 00 Brno, Božetěchova 2

doc. Dr. Ing. Dušan Kolář
vedoucí ústavu