Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Vojtěch Trefný**
Osobní číslo:	**A17302**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Bitlocker šifrování disku v Linuxovém prostředí**
Téma anglicky:	**Bitlocker Disk Encryption in the Linux Environment**

Zásady pro vypracování:

1. **Seznamte se s nástrojem Windows Bitlocker pro šifrování disků.**
2. **Popište podporované šifrovací módy a možnosti správy klíčů.**
3. **Analyzujte použitá kryptografická primitiva a jejich atributy.**
4. **Seznamte se s nástrojem a knihovnou libbde a možnostmi přístupu k Bitlocker obrazu disku v prostředí OS Linux.**
5. **Navrhněte a podle možností implementujte nutná rozšíření Linuxových nástrojů pro jednoduchý přístup k obsahu Bitlocker disku.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **FERGUSON, Niels. AES-CBC + Elephant diffuser A Disk Encryption Algorithm for Windows Vista. 2006. Dostupné také z: https://css.csail.mit.edu/6.858/2012/readings/bitlocker.pdf**
2. **ROSENDORF, Dan. Bitlocker: A little about the internals and what changed in Windows 8. 2013. Dostupné také z: http://spi.unob.cz/presentations/23-May/07-Rosendorf%20The%C2%A0BitLocker%C2%A0Schema.pdf**
3. **Library and tools to access the BitLocker Drive Encryption (BDE) encrypted volumes. In: GitHub [online]. 2018 [cit. 2018-11-29]. Dostupné z: https://github.com/libyal/libbde**
4. **CASEY, Eoghan. Handbook of digital forensics and investigation. Boston: Academic, c2010. ISBN 978-012-3742-674.**
5. **CARRIER, Brian. File system forensic analysis. London: Addison-Wesley, 2005. ISBN 978-032-1268-174.**
6. **SOMASUNDARAM, G. a Alok SHRIVASTAVA. Information storage and management: storing, managing, and protecting digital information in classic, virtualized, and cloud environments. 2nd ed. Indianapolis, IN: John Wiley, c2012. ISBN 978-111-8094-839.**
7. **AUMASSON, Jean-Philippe a Matthew D GREEN. Serious cryptography: a practical introduction to modern encryption. San Francisco: No Starch Press, [2017]. ISBN 978-159-3278-267.**

Vedoucí diplomové práce: **Ing. Michal Bližňák, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2018**

Termín odevzdání diplomové práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
garant oboru