Prof. Ing. Jiří Šafařík, CSc.

Faculty of Applied Sciences

University of West Bohemia

**Review of Dissertation Thesis**

**Digital Forensics: The Acceleration of Password cracking**

**submitted by Radek Hranický**

**at Faculty of Information Technology, Brno University of technology**

The thesis has 202 pages (appendices and bibliography included) written in English and has been submitted in 2021.

Subject of the submitted thesis is acceleration of password cracking for digital forensics and addresses distributed password cracking and probabilistic password models. As digital forensics became a new part of forensic science, time new methods coming from computer science are needed at the same. So, the subject of the thesis is up to date and is vital part of computer science without doubt.

Author formulates research goals in the Chapter 1 accompanying with brief background. To me, to study characteristics of existing cracking tools and study the methods for the time-space attacks are rather means used to achieve the goals. On the other hand, to propose algorithms and strategies for distributed password cracking, evaluate the solution, propose improvements of methods utilizing the knowledge about existing passwords and their experimental verification are well stated goals.

In Chapter 2 are given the essential principles of password cracking. These are described in a well-arranged way. Next, the use of parallel and distributed computing to increase performance is described in Chapter 3. This includes related work and definition of requirements for distributed cracking solution author intends to focus on. Then, the frameworks for distributed computing are introduced and evaluated. Author decided to use BIONC what I consider as good choice. Next logical step is the choice of cracking engine. After defining criteria and evaluation of cracking tools, author decided to use hashcat tool what is good choice as well. Next, the workload distribution in cracking tasks among multiple nodes is discussed. Here, author gives related work together with distribution in Fitcrack, author's distributed cracking systems which is introduced later in section The Architecture of Fitcrack. There is a lot of forward references in the text of the thesis, e.g., on pp. 53, 54 there are four. Beside the related work based on extensive study of literature, approx. 200 references, in this chapter author describes proposed distributed password cracking system Fitcrack incorporating dictionary attacks, brute-force attacks, hybrid attacks, PCFG attacks and PRINCE attacks as well. Conducted experiments proved usefulness of proposed improvements.

Further, author deals with probabilistic password models exploiting. After analysis of related work, author proposed improvements of current approach. These are faster “password generator”, automation of calculation of keyspace for given PCFG, modification of existing PCFG grammar and solution for PCFG-based cracking in distributed environment. Set of experiments considering parallel PCFG cracking, grammar filtering and distributed PCFG cracking were conducted. Results showed possible improvements and brought new findings for future work.

Formally, the thesis has very good quality containing only few spelling mistakes. I would expect list of abbreviations.

Without doubts, author has done a lot of work and covered many issues of distributed password cracking. Results of the thesis were published in three journal papers and four conference paper, all indexed in WoS. This is above-average for doctoral students. The author’s work enhanced methods and tools for distributed password cracking.

I recommend the thesis for defence.

Plzeň 8.12.2021