Accepted Manuscript

Mimic computing for password recovery

Bin Li, Qinglei Zhou, Xueming Si

PII: S0167-739X(17)32043-5
DOI: https://doi.org/10.1016/j.future.2018.02.018
Reference: FUTURE 3989

To appear in: *Future Generation Computer Systems*

Received date : 11 September 2017
Revised date : 16 January 2018
Accepted date : 12 February 2018

Please cite this article as: B. Li, Q. Zhou, X. Si, Mimic computing for password recovery, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.02.018

Mimic Computing for Password Recovery

Bin Li[a,*], Qinglei Zhou[b], Xueming Si[a]

[a]State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, Henan, China
[b]School of Information Engineering, Zhengzhou University, Zhengzhou 450001, Henan, China

Abstract

The recovery of encrypted information based on password authentication is an important mechanism to maintain network security. As a result, many password recovery systems have been developed. However, those systems are inefficient and energy intensive because they are primarily optimized for CPUs and GPUs. Inspired by a new computing model, namely, *mimic computing* – a hardware/software co-designed computing model that can dynamically reconfigure appropriate system structures based on application features – we propose a novel password recovery system. The design of such a system is non-trivial and includes several challenges: (1) how to build high-performance password recovery reconfigurable algorithms; (2) how to partition the hardware and software for password recovery; (3) how to optimize resource utilization and power consumption; and (4) how to improve the scalability. We present our insights, design decisions, and implementation details to address these challenges. Our extensive experiments show that the newly designed password recovery system significantly outperforms traditional CPU-based and GPU-based systems in terms of both efficiency and energy consumption. In particular, our system is 27.81 and 4.23 times faster than CPU-based and GPU-based systems in terms of password cracking, and our system consumes 14.97 and 5.97 times less energy than CPU-based and GPU-based systems.

Keywords: mimic computing, password recovery, hardware/software co-design, energy efficiency

1. Introduction

Encryption technology is widely used in many types of information service systems, such as PC terminals, server and mobile terminals, network forums, and micro-blogs. Although image, visual and fingerprint authentication methods have been applied to authenticate user identity, the human-memorable text password authentication mechanism is still widely used for its convenience and very low cost. At the same time, today's popular password encryption algorithms up to 200 kinds, and the analysis of different cryptography and recovery algorithms is essential to recover encrypted information and systems. The diversity of encryption algorithms, the timeliness of applications and the density of computation contribute to the high demand for computing capacity and solution of various encryption algorithms.

Password recovery is a computationally intensive task that requires high-speed parallel computing. However, the existing computing architecture and computing ability face challenges meeting the needs of password recovery applications. Traditional CPU architecture password recovery is limited by its computational speed for cryptographic algorithms and can only crack passwords with low complexity. To this end, abundant research has addressed GPU[1–9]and FPGA[10–20]. However, many shortcomings remain. Although GPU implementation accelerates password recovery, GPUs have high power consumption and low energy efficiency ratios and are not suitable for large-scale use. By contrast, the implementation of FPGA focuses too much on algorithm itself and does not address how to effectively partition and layout the algorithm. And scalability is poor, which leads to variable FPGA algorithm performance. There is still space to improve clock frequency and resources. Moreover, when faced with complex applications, FPGA routing resources occupy more chip area, resulting in performance degradation, increased power consumption, and serious efficiency problems.

The above-mentioned work is only for a single application whose structure is simple. There is no unified framework for multiple algorithms in the password recovery domain that takes into account the performance, efficiency and flexibility of the computing system. Therefore, the development of a high-performance and dynamic variable recovery algorithm in the field of password recovery through innovative technology is an urgent challenge.

With the rapid development of high-performance computing, reconfigurable technology is gaining increasing attention. Reconfigurable architecture has a high speedup ratio, flexible programmability, and other advantages and has been widely used in many areas[21–23]. Mimic computing[24] relies on reconfigurable technology to achieve high-performance and efficient computing. It starts from innovations in architecture and in-depth analysis of the relationships among the application, structure and performance to provide high-efficiency computing in several typical fields. Moreover, mimic computing proposes the concept of "application determines the structure, structure determines the efficiency". In mimic computing, the applica-

*Bin Li
Email address: cctvlibin@163.com (Bin Li)