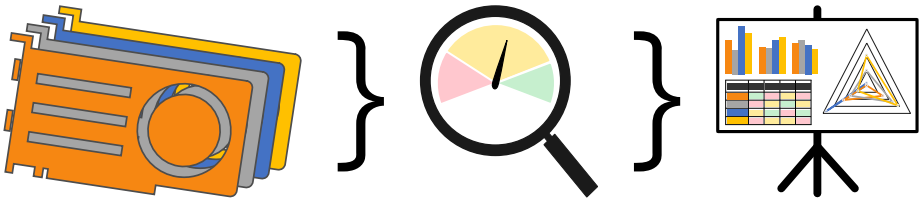
BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2019
http://excel.fit.vutbr.cz

Selecting the right GPU for password recovery

Vojtěch Večeřa



Keywords: password recovery — hashcat — GPU — benchmarks — HW acceleration — OpenCL
Supplementary Material: *N/A*

*xvecer18@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

Extended abstract

Cryptography surrounds us every day from phone unlocking to logging into websites, and far more. Each such system should store only the protected forms of the passwords. Hashing functions are cryptographic functions capable of securing user passwords before transmission or a storing.

The password recovery process takes password candidates and exposes them to the hashing function used by the system of origin. Then, it compares the computed value to the value recovered from the system. This process is easily parallelizable and can take advantage of Field-Programmable Gate Arrays (FPGAs), Graphics Processing Units (GPUs), Application Specific Integrated Circuits (ASICs), and other parallel platforms. Although, the GPUs are the most popular in the password recovery field.

The hashcat is a password recovery tool taking advantage of Open Computing Language (OpenCL) and Single Instruction Multiple Data (SIMD) platforms. It supports a wide variety of hashing algorithms and different common attack types.

Design of Benchmarks

This paper proposes a set of benchmarks and tests aiming to stress the system and test the recovery speeds of different attack types as well as other attributes like temperatures and power consumption. The tests and benchmarks focus on four main categories:

- Speeds of all algorithms.
- Dictionary/mask attack comparison.
- System stability.

Test-bed Configurations

CPU Intel Core i7-6700 @ 3.40 GHz,
RAM - 2x 16GB KINGSTON 2400MHz DDR4 CL16,
SSD - Samsung 850 EVO 256GB,
PSU - 2x EVGA SuperNOVA 1600 G2, 80+ GOLD,
Motherboard - Asus ASRock H110 Pro BTC+,
Fans - 3x Delta 190 CFM,
Chassis - custom-made U4 standard rack chassis.

Selected GPUs

The gaming GPUs are the most commonly used accelerators in the field as they provide decent speeds and decent prices. The selected cards are Nvidia's GTX 1050Ti 4G, GTX 1060 6G, GTX 1070Ti, GTX 1080Ti, RTX 2080Ti, and AMD RX 580 8G.

Evaluation

Speed benchmarks of all algorithms

The performance is one of the most important aspects of when buying new cards. The results show that Nvidia RTX 2080Ti outperforms GTX 1080Ti by 124.9% on average across both kernel types and all algorithms.

Speed of dictionary and mask attacks

The results show the attack speed differences between fast and slow hashing algorithms. Where speed dif-

ferences for fast algorithms are a significant while for slow algorithm insignificant. Also, the results show the maximal speed limits of fast algorithms.

Stability of the systems

The GPUs do not overheat in the custom chassis throughout the tests and benchmarks, and Power Supply Units (PSUs) provide enough power to the system components to remain stable and well powered.

Power consumption

The power consumption measurements confirm the values provided by the card manufacturers.

Initial and operation costs

The GPU prices and their power consumption differ greatly which results in significant overall costs differences for long-term usage. Visualization of computed hashes per 1 Euro of total costs shows how significant or non-significant are the purchase and operational costs.

Conclusions

This is an extended abstract of a paper proposing set of benchmarks for examining GPU models and evaluating measured data.

The data show the Nvidia RTX 2080Ti as the model to go for if the person, company or institution has got the budget for it. Then, the performances of Nvidia GTX 1070Ti and Nvidia GTX 1080Ti are quite similar with 1070Ti beating 1080Ti when it comes to all costs. Finally, the AMD alternative (RX 580) to Nvidia GTX 1060 shows promising for its similar performance but lower initial price. Although, AMD model has got higher power consumption and becomes less relevant for over three years usage.

The future topics of interest could be a speed comparison using motherboards with different supported Peripheral Component Interconnect Express (PCI-e) lanes. It may also be interesting to analyze the effects of password modification rules on dictionary attack recovery speeds and searching for the number of rules required to match mask attack speeds.