Cracking Passwords With GPUS

Tanner Pflager
Colorado State University – CS475
November 2016

It is well known that GPUs perform very well in parallel tasks compared to CPUs. GPUs can perform significantly more FLOPs per second than a CPU, and GPUs are improving at higher rate than CPUs. This has resulted in more applications utilizing the performance in GPUs. However, there are some impacts of this performance that raise concerns in topics such as security especially cryptography.

Cryptographic hash functions rely on complex algorithms to produce unique and one way hashes. Many systems use these hash functions to encrypt passwords. A brute force attempt to decrypt passwords is a class of problem that is parallel in nature. It is very likely that ideal speedup can be achieved on this type of problem. In result, due to the increasing performance of GPUs, it may no longer be computationally infeasible to brute force decrypt a password. In fact, there is a system that can attempt 350 billion passwords per second.

Stricture Consulting Group created a 5 server cluster that can crack any 8 character alphanumerical password using the NTLM cryptographic algorithm (which is included in every version of Windows since 2003) in under 6 hours. That is 95^8 combinations. The 5 server cluster utilizes 25 AMD Radeon HD 6990s. The AMD Radeon HD 6990 has a peak performance of 5.10 TFLOPS, this means the cluster as a whole, excluding the CPUs, has a peak performance of 127.5 TFLOPS. This system was built in 2012 and can be considered outdated.

The Nvidia Tesla P100 has a peak performance of 21.2 TFLOPS, which if placed in a similar system, would have 530 TFLOPS peak performance. A system composed of 25 Nvidia Teslas could attempt more than 1.4 trillion passwords per second. This means an 8 character password could be cracked in 1.5 hours, or a 9 character password could be cracked in a little longer than 5 days. Not to mention that more servers and GPUs could be added to the cluster.

The fact that these kind of systems can be built relatively easy using consumer grade hardware and open source software does pose a significant risk. This really affects everyone. Many people use passwords less than 8 characters, which would take seconds or minutes to crack. Of course this is specific to the NTLM algorithm, but often consumers are unaware to what cryptographic algorithm is being used.

In the future, I predict that cryptographic hash functions will utilize GPUs to generate hashes. The hash functions will require much more computational resources and parts of the hash function will be done in parallel. I also predict that the hash functions will be designed in such a way that they are bandwidth bound. A hash function that is bandwidth bound would take a lot longer to break, because the

performance of any given GPU would be bottle necked and limited by memory accesses.

As parallel computing and hardware advances, society as a whole will have to compromise speed for security by using slower hash functions and longer passwords. Companies will have to reevaluate security policies to better account for advancements in hardware.

Bibliography

Goodin, Dan. "25-GPU Cluster Cracks Every Standard Windows Password" *Ars Technica*. N.p., 09 Dec. 2012. Web. 12 Nov. 2016.

Hagedoorn, Hilbert. "Radeon HD 6990 Review." *Guru3D.com*. N.p., 7 Mar. 2011. Web. 12 Nov. 2016.

@KMoamm. "Nvidia Unveils Pascal Tesla P100 With Over 20 TFLOPS Of FP16 Performance - Powered By GP100 GPU With 15 Billion Transistors & 16GB Of HBM2." *Wccftech*. N.p., 26 Apr. 2016. Web. 12 Nov. 2016.

Oechslin, Philippe. "NTLM Algorithm [Openwall Community Wiki]." *NTLM Algorithm [Openwall Community Wiki]*. N.p., 17 Feb. 2010. Web. 12 Nov. 2016.