Uma janela de oportunidades na computação de alto desempenho

Claudio André da Silva Junior[1]
*claudioandre.br@gmail.com

[1]*Universidade Federal de Alfenas*

Palavras-chave: Computação de Alto Desempenho, Programação Paralela, Segurança da Informação.

Introdução

A evolução da ciência tem demandado modelos e técnicas de computação de altíssimo desempenho. Do projeto de novas substâncias ao planejamento de viagens espaciais, os mais variados ramos científicos têm se beneficiado da evolução tecnológica. Contudo, o acesso a esta tecnologia ainda é limitado pelo seu alto custo.
Neste contexto, este trabalho demonstrará que o uso da linguagem OpenCL e de placas de "vídeo" de uso doméstico, ou GPUs, oferecem ao pesquisador desempenho equivalente ao de um supercomputador.

Metodologia

Consistiu em implementar o algoritmo usado para cifrar senhas em ambiente Linux, o *hash* SHA-512 *crypt*, na GPU AMD Radeon HD 6770. Os resultados obtidos foram, em seguida, confrontados com os oferecidos pelas implementações de referência disponíveis na indústria. As máquinas usadas nos testes podem ser vistas abaixo:

Tabela 1: configuração dos equipamentos.

Equipto	Configuração	Núcleos
C1	Uma CPU AMD Phenom™ II X6 1075T 4 GB RAM	6 núcleos
C2	Uma CPU AMD FX™ 8120 8 GB RAM	8 núcleos
C3	Duas[1] CPUs Intel® Xeon® CPU E5-2670 @ 2.60 128 GB RAM	16 núcleos 32 *threads*

Todos os núcleos de CPU disponíveis foram utilizados para os testes (via *threads*). Os testes foram realizados em equipamentos ociosos. Uma série de 15 aferições foi realizada, as variações entre cada medida não ultrapassou 1% do valor da anotado. Uma GPU, quando em uso, não consome mais que 2% dos recursos da CPU.

Resultados e discussão

Com o uso da técnica em foco, e apesar de seus três anos de idade, a Radeon HD 6770 ofereceu performance superior a todas as CPUs testadas, inclusive, àquelas presentes na máquina C3, de alto custo. Os resultados, mostrados a seguir, foram confirmados em outras GPUs de mercado.

Tabela 2: senhas processadas por segundo por todos os núcleos da CPU (poder de processamento (*)).

Equipamento	Padrão (a)	Otimizado
C1	1617	2254 (b)
C2	1520	2055 (b)
C3	2579	5632 (b)
GPU HD 6770	-	8982 (c)
GPU GTX 570	-	15108 (c)
GPU GTX TITAN	-	20160 (c)

(a) Obtido com a biblioteca Unix crypt(3).
(b) Obtido com a biblioteca OpenSSL de 64bits.
(c) Implementação feita por este trabalho em OpenCL.
(*) Diferenças na arquitetura explicam porque uma CPU com menos núcleos pode superar uma com mais núcleos.

Conclusões

A GPU AMD Radeon HD 6770 foi mais eficaz que as CPUs na resolução de um problema computacional real: um *hash* iterado que demanda muito poder de processamento. De fato, a GPU superou todas as CPUs testadas; superou, inclusive, duas CPUs trabalhando juntas. Portanto, nossa técnica permitiu a um equipamento ultrapassado oferecer mais poder de processamento que um servidor de custo elevado.
Logo, é imperativo que as técnicas aqui discutidas sejam divulgadas de sorte a impedir que limites orçamentários cerceiem a curiosidade de nossos cientistas. O que este trabalho comprova é que nossa técnica aplicada a uma GPU de R$ 200,00 a torna capaz de superar um computador de R$ 10.000,00 na resolução de um problema real.
Além disto, os resultados aqui demonstrados são regra e não exceção. Trabalhos anteriores já comprovaram que outros problemas podem ser resolvidos com ganho na GPU (SILVA JUNIOR, 2014).
Por fim, a contribuição deste trabalho está em aplicar a técnica e comprovar sua eficácia. Também, em compartilhar o código com a comunidade por meio do famoso *software* de auditoria de senhas *John the Ripper*.

Referências

SILVA JUNIOR, C. A. Os riscos de segurança inerentes ao uso dos modernos equipamentos médicos informatizados. In: Congresso Científico-Cultural da Unifal-MG, 2014, Alfenas. **Anais do Congresso**, 2014.

[1] O computador possui duas CPUs e suporta até 32 *threads* simultâneos. Cada CPU custa ± US$ 1.500,00 (Amazon, out/2014).