O Uso de Processamento Paralelo Como Ferramenta de Segurança

Claudio André da Silva Junior
Lactum Informática
02652-080, São Paulo, SP
E-mail: claudio.andre@correios.net.br

Resumo

Nos últimos anos tem-se observado grande avanço no desenvolvimento de processadores e *grids* paralelos, especialmente as modernas placas gráficas ou GPUs, que oferecem enorme capacidade de paralelismo a baixo custo e, além disto, são capazes de executar programas de propósito geral. Este avanço, contudo, pode transformar-se em um problema de segurança, pois, a base de muitas das técnicas da criptografia moderna é a dificuldade computacional de se resolver algum problema. Com o objetivo de analisar o choque de forças entre estes dois entes antagônicos, este trabalho irá mostrar que o avanço da programação paralela nas GPUs permite ganhos de eficiência nas rotinas de quebra de senha que podem oferecer um risco real à segurança de alguns dos mecanismos de controle de acesso baseados em senha.

Palavras-chave*: programação massivamente paralela, segurança da informação, quebra de senha, programação para GPUs.*

1. Introdução

O software se tornou peça fundamental em nossa sociedade nos últimos anos. Como consequência, qualquer falha no software pode causar prejuízos financeiros, de imagem ou até a perda de vidas. Neste contexto, a correta aplicação das disciplinas de segurança da informação é fundamental. Contudo, uma parte importante das técnicas empregadas na criptografia moderna depende de problemas que são computacionalmente onerosos (COSTA; FIGUEIREDO, 2010, p. 66).

Porém, avanços recentes na tecnologia dos processadores têm oferecido ao usuário doméstico acesso ao poder de computação equivalente ao disponível em supercomputadores de poucos anos atrás (TAVARES, 2012). Ainda, as atuais placas gráficas de propósito geral ou GPGPUs (*General Purpose Graphics Processing Unit*), embora caseiras e de baixo custo, contém milhares de núcleos de processamento, são capazes de realizar milhões de operações por segundo (AMD, 2011) e podem ser usadas para executar programas de propósito geral, em contraste com o que ocorria há alguns anos atrás, quando uma placa de vídeo servia apenas como controladora de vídeo.

Então, neste ponto de evolução tecnológica uma dúvida inquietante surge: será que o aumento do poder de processamento destas novas placas gráficas representa um risco a alguns dos métodos de segurança usados atualmente?

Este trabalho demonstrará que é possível utilizar o paralelismo oferecido pelos modernos processadores e placas gráficas, e que este fato aumenta os riscos de uma senha ser quebrada por um atacante qualquer.

2. Objetivos

O objetivo principal é analisar o impacto que o advento das tecnologias de computação paralela podem causar na criptografia. Em especial, estimar o ganho

possível com o uso de GPUs na criptoanálise. Ao final, comprovar que o aumento do poder de processamento e o grande grau de paralelismo oferecido pelas modernas placas gráficas exigirão dos pensadores da área de segurança maior cuidado ao selecionar algoritmos e senhas que sejam capazes de resistir aos ataques vindouros.

3. Metodologia

Realizar-se-á uma revisão da bibliografia que ofereça subsídios à tese central deste trabalho. Em seguida, um estudo exploratório com o uso de experimentos será realizado para comprovar que o comportamento preconizado neste texto é, de fato, o que ocorre em situações reais.

Para tanto, amostras deverão ser geradas, programas paralelos e sequenciais devem ser executados nestas amostras e os resultados devem ser tabulados de forma a se obter regras que possam ser generalizadas. Por fim, os ganhos de desempenho que surgem ao se paralelizar as tarefas de um algoritmo de quebra de senhas serão medidos.

3.1. Ferramenta Utilizada

As rotinas paralelas para auditoria (ou quebra) de senhas foram desenvolvidas em OpenCL (KHRONOS, 2012). Dada sua relevância e atualidade (DREPPER, 2008; ARCH, 2012), os algoritmos selecionados foram: SHA-512 crypt, SHA-256 crypt e raw SHA-512.

Em seguida, o famoso software livre de auditoria de senhas *John the Ripper* (OPENWALL, 2012) foi alterado para incluir esta nova funcionalidade. O resultado foi submetido para a comunidade de desenvolvedores do *John*, e a contribuição aceita e incluída em sua árvore de desenvolvimento (SILVA JUNIOR, 2012a) foi usada para se obter os resultados da execução paralela. O desempenho dos algoritmos tradicionais foi obtido também com o *John the Ripper*, ferramenta já empregada em outros estudos como referência (SPRENGERS; BATINA, 2012).

4. Panorama

É fato que o software participa do dia a dia das pessoas. Empiricamente verificável, também, que estes sistemas são vulneráveis e vários esforços têm sido feitos para entender e minimizar estas deficiências (DINEI; CORMAC, 2007).

Somado a isto, um grande avanço ocorreu nos últimos anos no desenvolvimento de tecnologias de processamento paralelo: a proliferação de CPUs dotadas de vários núcleos de processamento, o notável desenvolvimento das GPUs (TAVARES, 2012), a maior densidade de núcleos de processamento por chip (AMD, 2011), etc.

Embora nem todos os algoritmos conhecidos sejam facilmente paralelizáveis, sem dúvida, alguns o são. Mesmo considerando-se que, eventualmente, alguns não sejam paralelizáveis, a possibilidade de executá-los de fato, ou seja, fisicamente, ao mesmo tempo junto com outros programas representa um ganho na diminuição do tempo total necessário à execução de qualquer conjunto de programas.

Para coroar todos estes avanços, surgiu em meados dos anos 2000 o OpenCL (KHRONOS, 2012). Trata-se de um padrão aberto, livre de *royalties* para programação paralela heterogênea, pensada para atender os processadores multinúcleo recentes. Dentre estes se incluem, de forma não-exclusiva, as CPUs Intel e AMD, GPUs AMD, NVIDIA e Intel, processadores de sinal, entre outros.

5. Resultados

Em consonância com o esperado, ficou comprovado que há ganho de desempenho ao se

paralelizar a execução dos algoritmos de quebra de senha em uma placa gráfica (GPU). O ganho oscila, normalmente, de 5 a 10 vezes aquele obtido com uma CPU de mesma faixa de preço. Em alguns casos, contudo, usando-se a GPU Radeon HD 7970, uma das mais rápidas do mundo (AMD, 2011), este ganho superou em 20 vezes (SILVA JUNIOR, 2012b) a performance de uma CPU topo de linha no mercado.

5.1. Experimentos Realizados

Abaixo, na Tab. 1, veem-se os resultados dos experimentos realizados com o algoritmo SHA-512 crypt, o mais complexo para esta paralelização. Em seguida, um algoritmo semelhante em sua estrutura, mas que opera apenas com inteiros de 32-bits, precisão nativa nas GPUs testadas. Por fim, uma função de *hash* rápido, o raw SHA-512.

Tabela 1. Resultados experimentais da utilização de programação paralela em GPU.

Algoritmos	Um núcleo CPU [1] AMD FX™-8120	Oito núcleos CPU [2] AMD FX™-8120	Radeon HD 6770	NVIDIA GTX-570
SHA-512 crypt	367 c/s[3]	2.055 c/s[3]	2.428 c/s[3]	11.520 c/s[3]
SHA-256 crypt	300 c/s[3]	1.761 c/s[3]	6.103 c/s[3]	14.400 c/s[3]
Raw SHA-512	1.839.000 c/s[3]	7.409.000 c/s[3]	18.811.000 c/s[3]	24.576.000 c/s[3]

[1]: Usando programação tradicional, ou seja, apenas um núcleo da CPU é utilizado.
[2]: Todos os oito núcleos disponíveis são usados ao mesmo tempo, via programação paralela.
[3]: Quantidade de senhas avaliadas por segundo.

Na Tab. 2 é possível visualizar o quanto uma placa gráfica mediana é mais rápida que uma CPU de oito núcleos.

Tabela 2. Análise do ganho obtido em uma placa NVIDIA GTX-570.

Algoritmos	Um núcleo CPU [1] AMD FX™-8120	Oito núcleos CPU [2] AMD FX™-8120	NVIDIA GTX-570	Ganho
SHA-512 crypt	367 c/s[3]	2.055 c/s[3]	11.520 c/s[3]	31,4x / 5,6x
SHA-256 crypt	300 c/s[3]	1.761 c/s[3]	14.400 c/s[3]	48,0x / 8,2x
Raw SHA-512	1.839.000 c/s[3]	7.409.000 c/s[3]	24.576.000 c/s[3]	13,4x / 3,2x

[1]: Usando programação tradicional, ou seja, apenas um núcleo da CPU é utilizado.
[2]: Todos os oito núcleos disponíveis são usados ao mesmo tempo, via programação paralela.
[3]: Quantidade de senhas avaliadas por segundo.

Mesmo o algoritmo mais refratário ao uso na GPU mostrou, de forma inequívoca, que há um ganho ao se utilizar OpenCL nas GPUs para acelerar o desempenho. Além disto, é importante ressaltar que a placa GTX-570 é apenas uma placa intermediária que está à venda no Amazon por cerca de $ 250,00 dólares americanos (AMAZON, 2012).

6. Conclusão

Foi possível adaptar um software preexistente, o famoso *John the Ripper,* para utilizar as placas gráficas como unidades de processamento. Os algoritmos desenvolvidos foram testados em dispositivos diversos, de diferentes fabricantes, incluídos NVIDIA, AMD e Intel, e se mostraram aptos em todos eles.

O aumento de performance foi medido e os ganhos auferidos foram consistentes, apesar da CPU usada como referência ser uma placa topo de linha e das GPUs serem tecnologicamente medianas, logo, financeiramente acessíveis. Mesmo com esta configuração, a diferença de desempenho foi notória.

Desta forma, embora o impacto da computação paralela ainda não tenha sido totalmente sentido pelos especialistas em criptografia, é inegável que a ameaça representada pelo processamento paralelo se fará sentir em um futuro próximo. Já há casos em que algoritmos têm sido desaconselhados por seus autores em vista desta evolução (CVE, 2012).

Ademais, não bastassem os ganhos em discussão neste trabalho, é sempre bom lembrar que os usuários não selecionam senhas particularmente seguras (DINEI; CORMAC, 2007). E esta conjunção de fatores é um alerta que não pode ser ignorado por cientistas e técnicos responsáveis pela segurança.

Portanto, a força das atuais mecanismos de segurança deve ser posta à prova usando as novas técnicas disponíveis de programação paralela, de forma que apenas os mecanismos mais adequados permaneçam em uso.

Por fim, após analisar o investimento necessário e os resultados obtidos, este trabalho sugere que outros algoritmos, das mais diversas áreas, sejam adaptados de sorte a utilizar as possibilidades oferecidas pela programação paralela. A relação custo-benefício se mostrou muito satisfatória.

Referências

AMAZON. *GeForce GTX 570*. 2012. Disponível em: <http://www.amazon.com/MSI-N570GTX-TWIN-FROZR-PCI-Express/dp/B008809SUM/ref=sr_1_4?ie=UTF8&qid=1345921999&sr=8-4&keywords=gtx-570>. Acesso em 20/08/2012.

AMD. *AMD Launches World's Fastest Single-GPU Graphics Card – the AMD Radeon™ HD 7970*. Califórnia: AMD, 2011. Disponível em: <http://www.amd.com/us/press-releases/Pages/amd-launches-worlds-fastest-2011dec22.aspx>. Acesso em 15/02/2012.

ARCH. *SHA password hashes*. 2012. Disponível em: <https://wiki.archlinux.org/index.php/SHA_password_hashes>. Acesso em 20/02/2012.

COSTA, C. J; FIGUEIREDO, L. M. *Introdução à Criptografia*. Niterói: UFF, 2010.

CVE, E. B. *CVE-2012-3287*. 2012. Disponível em: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3287>. Acesso em: 20/08/2012.

DINEI, F. CORMAC, H. *A large-scale study of web password habits*. In WWW '07: Proceedings of the 16th international conference on World Wide Web, pages 657–666, New York, NY, USA, 2007. ACM

DREPPER, U. *Unix crypt using SHA-256 and SHA-512*. 2008. Disponível em: <http://www.akkadia.org/drepper/SHA-crypt.txt>. Acesso em: 15/02/2012.

KHRONOS. *OpenCL - The open standard for parallel programming of heterogeneous*

systems. Oregon: Khronos Group, 2012. Disponível em: <http://www.khronos.org/opencl/ >. Acesso em: 04/04/2012.

OPENWALL. *John the Ripper password cracker*. 2012. Disponível em: <http://www.openwall.com/john/>. Acesso em: 05/01/2012.

SILVA JUNIOR, C. A. *OpenCL SHA*. 2012a. GitHub. Disponível em: <https://github.com/magnumripper/magnum-jumbo/pull/78>. Acesso em: 20/08/2012.

SILVA JUNIOR, C. A. *OpenCL SHA-256*. 2012b Openwall. Disponível em: <http://openwall.info/wiki/john/OpenCL-SHA-256>. Acesso em: 20/08/2012.

SPRENGERS, M. BATINA, L. *Speeding up GPU-based password cracking*. 2012. In SHARCS 2012: Special-purpose Hardware for Attacking Cryptographic Systems, pages 35–54, Washington, D.C., USA, 2012. CERG.

TAVARES, A. *A revolução das GPUs no Brasil e no mundo*. 2012. Disponível em: <http://www.lncc.br/eventoSeminario/eventoconsultar.php?vMenu=&idt_evento= 946>. Acesso em: 15/02/2012.