Interface de Apoio para Ataques de Força Bruta com o *GPU MD5 Crack*

Frederico Schardong[1], Rafael B. Ávila[1]

[1]Curso de Graduação Tecnológica em Segurança da Informação
Universidade do Vale do Rio dos Sinos (UNISINOS)

frede.sch@gmail.com, rbavila@unisinos.br

1. Introdução

A área da Segurança da Informação, embora ainda pouco explore o poder computacional da computação paralela (SCOTT; CLARK; BAGHERI, 2005), ganhou uma significativa ferramenta de apoio com o advento das GPUs. Hoje em dia, a quebra de hashes de senhas pode ser executada em tempo viável por qualquer pessoa que tiver acesso a uma GPU relativamente moderna e tiver em mãos o resultado de uma função de hash, ou seja, uma senha criptografada.

O software *GPU MD5 Crack* (VERNOUX, 2011) é o único software livre que usa GPU para ataque de força bruta ao algoritmo MD5 (RIVEST, 1992). O aplicativo é multiplataforma e é constituído de um executável que recebe parâmetros para definir uma seqüência de geração de senhas, as quais são criptografadas com MD5 e comparadas com o hash original. Sua utilização, entretanto, requer um relativo grau de conhecimento do assunto, pois exige o fornecimento de parâmetros específicos para que a execução tenha êxito.

Como resultado de um trabalho de investigação em plataformas paralelas para ataques de força bruta, no contexto da Segurança da Informação, este artigo apresenta uma primeira contribuição sob forma de uma interface alternativa para o GPU MD5 Crack, onde foram implementados novos parâmetros que facilitam o uso do software, bem como uma interface gráfica que simplifica o seu uso. A motivação para a realização deste trabalho é facilitar o uso da computação paralela para quebras de senha por força bruta, bem como incentivar o uso de softwares livres.

No restante do artigo, a Seção 2 apresenta alguns conceitos de base para o entendimento do trabalho, como o princípio básico dos algoritmos de ataque por força bruta, e algumas iniciativas já existentes. A Seção 3 descreve a contribuição principal do artigo, apresentando a interface gráfica desenvolvida e as alterações realizadas no software. A Seção 4 apresenta os resultados obtidos com a implementação e, por fim, na Seção 5 os autores fazem suas considerações finais.

2. Ataques por Força Bruta e Iniciativas Existentes

Um ataque de força bruta sobre senhas criptografadas com algum algoritmo significa, dentro de um limite pré-estabelecido, gerar todas as senhas possíveis, criptografar cada uma e comparar com a senha criptografada original, até que alguma das senhas geradas e criptografadas seja igual à senha criptografada original (STALLINGS, 2010). O tempo para quebra de uma senha é definido pelos tipos de caracteres usados, pelo tamanho e pelo computador/cluster que está gerando e comparando todas as senhas possíveis.

Podem ser encontrados na literatura diversos trabalhos dedicados à quebra de hashes por força bruta usando computação paralela, porém poucos o fazem utilizando GPU, que é o escopo deste estudo.

O software IGHASHGPU (GOLUBEV, 2009) possui suporte a placas de vídeo da Nvidia com tecnologia CUDA (FARBER, 2011) e da ATI/RADEON, sendo capaz de usar mais de uma GPU na quebra dos hashes. Este aplicativo, entretanto, não possui interface gráfica e é distribuído sob licença fechada.

Nguyen et al. (2010) implementam um aplicativo usando a linguagem CUDA que é capaz de usar computadores que possuem GPUs como se fossem um cluster. O programa, entretanto, não é distribuído de forma pública e a literatura disponível não permite verificar o grau de usabilidade da interface implementada.

O *GPU MD5 Crack* (VERNOUX, 2011) é o único software dentre os encontrados que atende ao propósito da quebra de senhas com GPU e é distribuído de forma aberta, sob licença GPL. O software faz parte da distribuição Linux Backtrack 4 e, até o momento, limita-se a operar com GPUs da Nvidia que possuem a tecnologia CUDA. Ainda, o aplicativo utiliza apenas uma GPU, mesmo que o ambiente forneça mais do que uma. Embora apresente uma implementação eficiente, o software requer que o usuário faça cálculos para prever a quantidade de senhas possíveis para a configuração de quebra desejada, ou seja, é preciso calcular quantas senhas são possíveis para o mapa de caracteres selecionados e tamanho da senha. Outro ponto de dificuldade para o usuário final é que não foi disponibilizada uma interface gráfica multiplataforma, devendo a interação ser feita através de linha de comando.

Dentre os softwares citados nesta seção, todos apresentam praticamente o mesmo desempenho, porém o software implementado por Nguyen et al. (2010) utiliza mais do que uma GPU Nvidia, caso o ambiente forneça. A vantagem do IGHASHGPU dentre os outros é suportar GPUs da ATI/RADEON, enquanto que a principal vantagem do GPU MD5 Crack é ser GPL. A desvantagem encontrada em todos os softwares citados é que nenhum possui interface gráfica, o que motivou o desenvolvimento deste trabalho, conforme detalhado a seguir.

3. Adaptação do GPU MD5 Crack

A partir da versão original do GPU MD5 Crack, foram feitas adaptações no sentido de torná-lo mais fácil ao usuário final, permitindo sua aplicação na verificação de ambientes de rede (ex.: executar o software sobre a base de senhas de usuários), ou mesmo como ferramenta didática no ensino de Criptografia.

A primeira adaptação consiste na implementação de uma interface gráfica multiplataforma para o software. Essa interface solicita quais os tipos de caracteres e tamanho máximo da senha que serão gerados por força bruta na GPU, além do hash MD5 a ser comparado com cada hash gerado. A implementação utiliza a biblioteca GTK+ (KRAUSE, 2007).

Iniciado o processamento, a interface gráfica mostra o real progresso da geração de todas as senhas da configuração selecionada, bem como a quantidade de hashes que são gerados por segundo e o tempo restante para terminar de gerar todas as senhas. A Figura 1 ilustra uma tela da interface, mostrando os campos para a entrada de dados e o progresso da execução.

Na versão original do GPU MD5 Crack, deve-se informar ao executável, via parâmetros, quantas senhas devem ser geradas e qual o *charset* (conjunto de caracteres) escolhido. As possibilidades de charsets são:

- Números
- Letras minúsculas
- Minúsculas e números
- Maiúsculas

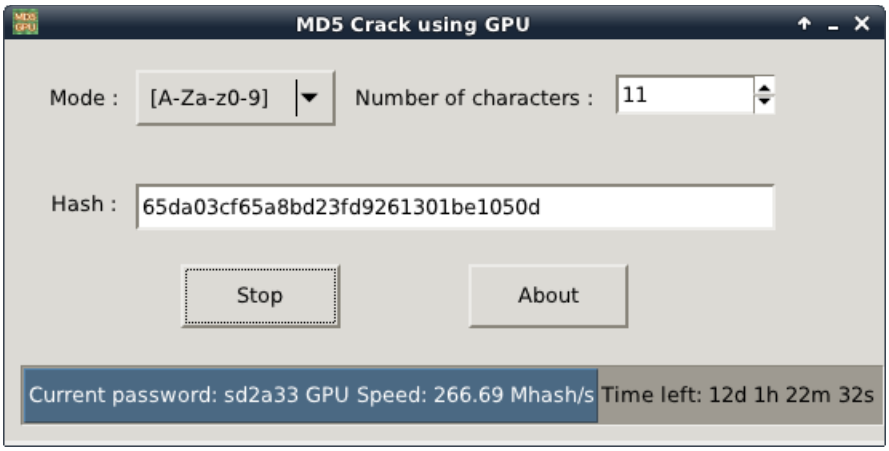

Figura 1. Interface gráfica implementada para o GPU MD5 Crack

- Maiúsculas e números
- Minúsculas e maiúsculas
- Minúsculas, maiúsculas e números
- Todos os caracteres imprimíveis

Essa necessidade de passagem de parâmetros é um dos fatores que mais dificulta o uso do software. Para se ter uma idéia da quantidade de variações possíveis, a Tabela 1 mostra o número de possibilidades de senhas de acordo com o charset escolhido e o tamanho da senha.

Tabela 1. Número de possibilidades para cada charset e tamanho de senha

Charset	1 char	2 chars	3 chars	4 chars	5 chars	6 chars
0-9	10	100	1.000	10.000	100.000	1.000.000
a-z	26	676	17.576	456.976	11.881.376	308.915.776
a-z0-9	36	1.296	46.656	1.679.616	60.466.176	2.176.782.336
A-Z	26	676	17.576	456.976	11.881.376	308.915.776
A-Z0-9	36	1.296	46.656	1.679.616	60.466.176	2.176.782.336
A-Za-z	52	2.704	140.608	7.311.616	380.204.032	19.770.609.664
A-Za-z0-9	62	3.844	238.328	14.776.336	916.132.832	56.800.235.584
All	95	9.025	857.375	81.450.625	7.737.809.375	735,091,890,625

Para interagir com a interface gráfica, foi feita uma nova adaptação ao software, através da substituição dos parâmetros originais por novos parâmetros, os quais têm o objetivo de informar quantos dígitos serão gerados e os charsets a serem usados. A partir desses parâmetros é calculada a quantidade de senhas possíveis conforme a Tabela 1 e essa informação é passada ao algoritmo original.

4. Resultados Obtidos

O software foi testado em uma Nvidia GTX 285M, que possui 128 núcleos e um total de 576 GFLOPS. Nessa configuração, foram gerados em média 240 milhões de hashes por segundo, com picos de 266.69 milhões de hashes por segundo.

A fim de verificar que as adaptações não interferiram no desempenho do software, foram comparados os desempenhos das versões adaptada e original. Os

resultados obtidos foram iguais nas duas situações.

Por fim, para efeito de verificação do ganho proporcionado pela GPU, foi implementado um algoritmo semelhante, utilizando linguagem C e a biblioteca POSIX Threads, o qual foi executado nos oito núcleos de uma CPU Intel I7-740QM. Neste caso, o desempenho médio ficou em torno de 1 milhão de hashes por segundo, levando à conclusão de que a GPU é cerca de 240 vezes mais rápida para a realização desta tarefa.

5. Considerações Finais

O uso da computação paralela, principalmente de GPU, para a quebra de algoritmos de hash, apresenta um excelente desempenho em comparação com a CPU normal. Os resultados obtidos nos experimentos comprovam que a geração de hashes na GPU é centenas de vezes mais rápida que na CPU. A partir desse resultado, é possível cogitar que as próximas gerações de GPUs devem tornar fracos até os algoritmos atualmente considerados fortes (SHA-2 e outros).

Com a criação de uma interface gráfica multiplataforma para o software GPU MD5 Crack, é facilitado e simplificado o seu uso. Na adaptação do software, os novos parâmetros criados simplificam o atual uso do software, impedindo que o usuário tenha que calcular a quantidade de senhas que o software deve gerar.

O uso do GPU MD5 Crack com a interface gráfica permite que administradores de redes possam testar a força da senha dos seus usuários em seus serviços, e até as suas próprias como administradores, possibilitando assim, estabelecer uma política de geração de senhas mais fortes. Para fins didáticos a interface gráfica facilita a visualização do software em execução, estimulando o seu uso para testes de tempo de quebra de senhas e até mesmo na recuperação de senhas perdidas.

6. Referências

FARBER, R. **CUDA Application Design and Development**. [S.l.]: Elsevier, 2011.

GOLUBEV, I. **IGHASHGPU**. Disponível em: <http://www.golubev.com>. Acesso em: dez. 2011.

KRAUSE, A. **Foundations of GTK+ Development**. [S.l.]: Apress, 2007.

NGUYEN, D. H.; NGUYEN, T. T.; DUONG, T. N.; PHAM, P. H. Cryptanalysis of MD5 on GPU Cluster. In: International Conference on Information Security and Artificial Intelligence (ISAI2010), Chengdu, China, 2010. **Proceedings...**

RIVEST, R. **The MD5 Message-Digest Algorithm**. RFC 1321. [S.l.: s.n.], 1992. Disponível em: <http://www.ietf.org/rfc/rfc1321.txt>. Acesso em: dez. 2011.

SCOTT, L. R.; CLARK, T.; BAGHERI, B. **Scientific Parallel Computing**. Princeton: Princeton University Press, 2005.

STALLINGS, W. **Cryptography and Network Security**. 5th. ed. [Sl.]: Prentice-Hall, 2010.

VERNOUX, B. **MD5 GPU Crack**. Disponível em: <http://bvernoux.free.fr/md5/index.php>. Acesso em: dez. 2011.