

Pontifícia Universidade Católica de Campinas Faculdade de Engenharia de Computação - FECOMP

Sistemas Operacionais B – Relatório Experimento

Chamada de sistema e criptografia no kernel Linux

Beatriz Morelatto Lorente RA: 18071597

Cesar Marrote Manzano RA: 18051755

Fabrício Silva Cardoso RA: 18023481

Pedro Ignácio Trevisan RA: 18016568

**Sumário**

1. **Introdução.........................................................................................3**
2. **Algoritmos de criptografia utilizados.................................................4**
3. **Programa de teste.............................................................................5**
4. **Módulo de criptografia.......................................................................6**

**Introdução**

O experimento desenvolvido pretende demonstrar os passos feitos para o desenvolvimento de chamadas de sistema (system calls) que podem armazenar e ler arquivos usando a API criptográfica do kernel. A chamada de armazenamento permite que programas em espaço de usuário possam alocar arquivos cifrados pelo algoritmo AES em modo CBC, e deste mesmo modo a chamada de leitura lê o arquivo cifrado.

**Algoritmos de criptografia utilizados**

Para a cifrar e decifrar a string fornecida pelo usuário foi utilizado o algoritmo AES em modo CBC.

Primeiramente é necessário entender como o algoritmo AES (Advanced Encryption Standard) funciona. O algoritmo consiste em uma criptografia simétrica de blocos de tamanho fixo (utilizamos blocos de 16 bytes, 128 bits). O algoritmo usa uma chave para cifrar e decifrar os blocos e esta também tem 16 bytes.

No modo de criptografia CBC, para cada bloco de texto é aplicado a função XOR com o bloco anterior, garantindo que cada bloco seja dependente um do outro. Para o primeiro bloco, é aplicado um vetor de inicialização, garantindo que cada operação de criptografia seja única. O esquema do algoritmo é representado abaixo:

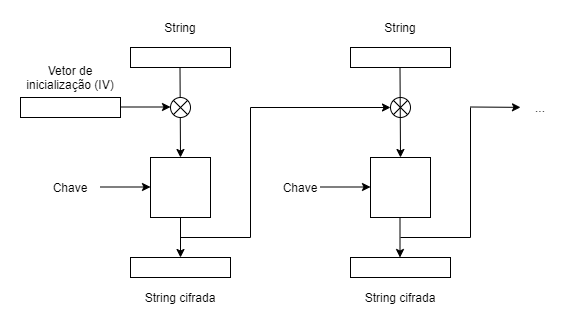


Figura 1 - Esquema do modo de criptografia CBC

Já para o resumo criptográfico foi utilizado o algoritmo SHA1. Consiste em uma função de dispersão criptográfica, considerado bem seguro. O algoritmo produz uma mensagem de dispersão com 20 bytes, que é conhecida como o resumo da mensagem original.

**Programa de teste**

Para testarmos o experimento foi feito um programa em espaço de usuário que se comunica com o módulo. O esquema abaixo representa como essa comunicação é feita.

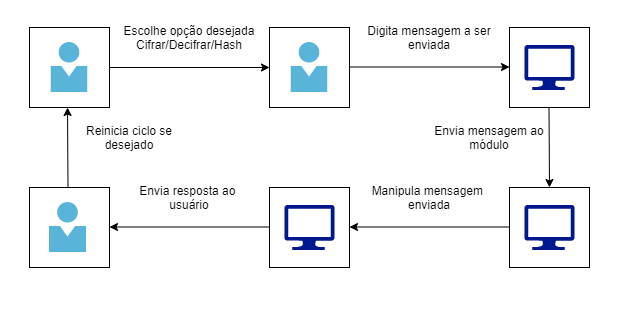


Figura 2 - Esquema do programa de teste

Primeiramente é escolhida a operação que se deseja fazer, ou seja, cifrar, decifrar ou calcular o resumo criptográfico de uma mensagem. Após a escolha o usuário digita qual a mensagem que será enviada ao módulo. Para saber qual operação será feita, foi concatenado as letras ‘c’ (cifrar), ‘d’ (decifrar) ou ‘h’ (hash), no final da mensagem, dependendo da escolha do usuário. Desse modo o módulo pode aplicar adequadamente o algoritmo em cima de uma mensagem, basta ler apenas a última posição da string para isso. Após manipular a mensagem (mais detalhes sobre essa manipulação serão discutidos mais para frente), o módulo devolve a mesma para o programa de teste e este se encarrega de imprimir as informações necessárias. Todo o ciclo pode ser feito novamente caso o usuário deseje.

**Módulo de criptografia**

O funcionamento do módulo de criptografia é bastante simples, ele apenas manipula uma mensagem e envia para o programa de teste. Porém, a manipulação da mensagem não é um processo fácil e diversos erros podem ser cometidos na hora de sua implementação.