1. Transferência de arquivos pela rede e criptografia

Israel Silva Barbará , Paulo Ferreira

Centro de Desenvolvimento Tecnológico – Universidade Federal de Pelotas (UFPEL) Caixa Postal 354 – 96001-970 – Pelotas – RS – Brasil

*Resumo. A transferencial de arquivos deve ser feita de forma a garantir integridade e segurança de dados ,essa integridade se da por meio de criptografia. A criptografia usada foi o modelo PGP (pretty good privacy ) , onde o objeto é criptografado usando criptografia simétrica e a chave é criptografada usando criptografia de chave publica e chave privada, o sistema usa também um sistema de certificação onde é criptografado com chave privada a assinatura do host . É usado também um sistema de de hash MD5 para verificar a integridade do arquivo passado.*

***1.*Introdução**

Com o crescente uso das redes de computadores para se comunicar , surgem métodos de proteção de dados devido ao crescente numero de ataques a usuários .

Confiança na integra dos dados , integridade para que os dados possam trafegar sem ser corrompidos devido a problemas na rede ou a interferência por usuários mal intencionados , para resolver esse tipo de problema é usado criptografia para que os pacotes possam trafegar na rede sem que outros usuários além do remetente e destinatário possam ter acesso .

***2.Programa e estrutura***

O programa esta dividido em 2 arquivos :

pedido.rb. Esse programa representa o lado do usuário , este faz um pedido para um arquivo x no diretório do servidor , e processa esta resposta.

Filetranfer.rb . É o host onde vai ser feito o processamento do arquivo pedido , este arquivo que foi pedido pelo cliente é criptografado e enviado para o cliente.

**3.*Criptografia usada***

O programa Filetransfer.rb implementa criptografia simétrica AES de 256 bits para criptografia do arquivo , logo é aplicado na chave uma criptografia de chave publica do cliente na chave , esse processo visa desempenho já que a criptografia simétrica é muito mais rápida do que a criptografia de chave publica e privada , É aplicada uma certificação também para que o usuário possa confirmar que o pacote recebido foi devidamente enviado pelo servidor onde foi feito o pedido, para isso o servidor criptografa uma assinatura com sua chave privada , assim quando o cliente descriptografar saberá que o pacote enviado tem origem no servidor, uma hash md5 foi implementada para evitar erros de integridade no arquivo.

O formato seguido pelo pacote a ser enviado pelo servidor esta descrito a baixo :

Pacote = certificado / chave / iv / arquivo / hashMD5 O programa pedido.rb recebe este pacote , e precisa processa -lo para chegar no arquivo que foi pedido originalmente , o programa verifica o certificado , se a assinatura bate com a que foi setada na inicialização do programa , então o programa segue o fluxo , logo ele precisa descriptografar a chave com a sua chave privada para garantir autenticidade e confidenciabilidade do pacote já que somente o cliente pode descriptografar a chave criptografada com a chave publica , a partir da chave mais o iv aplica-se a descriptografia com chave simétrica para chegar no texto original , neste texto original é aplicado a hash , o que acarreta num resultado , este resultado vai ser comparado com a hash passada pelo servidor afim de verificar se não houve mudanças no pacote no caminho.

***4.Conclusão***

As técnicas de criptografia garantem um meio seguro de comunicação fazendo possível aplicações que necessitam sigilo , como operações bancarias .

O uso das 4 técnicas somadas , criptografia de chave simétrica , chave publica e privada mais o uso da hash garantem que os pacotes trafeguem pela rede de forma a sempre receberem o objeto mandado pelo remetente .