T2 - Segurança de Sistemas

Giovane Milani[1], Vinícius R. Boff[1]

[1]Engenharia de Software - Pontifícia Universidade Católica do Rio Grande do Sul(PUCRS) - Porto Alegre - RS - Brasil

{giovane.milani, vinicius.rech} @edu.pucrs.br

1. Introdução

Este trabalho tem como objetivo simular a troca de mensagens seguras entre o grupo e o professor, implementando parte do processo HTTPS, e explorando conceitos de segurança de sistemas aprendidos durante o semestre, como geração de chaves e comunicação de chaves utilizando Diffie-Hellman e criptografia de mensagens usando AES no modo CBC. Ele é dividido em duas etapas principais: a geração da chave de sessão e a troca segura de mensagens.

A etapa inicial consiste na implementação do protocolo Diffie-Hellman para estabelecer uma chave compartilhada de forma segura. A segunda etapa envolve a decifração de uma mensagem criptografada enviada pelo professor, a inversão dos caracteres dessa mensagem e seu reenvio em formato criptografado.

2. Geração e troca da chave

Para realizar a geração da chave, usamos os valores de p e g do enunciado e escolhemos um valor aleatório maior que 30 dígitos e menor que p para o valor de a, que é chave privada. Com isso, calculamos o valor de A, que é a chave pública, com A = ga mod p. Enviamos o valor da chave pública para o professor, que nos respondeu com a chave pública dele e uma mensagem em hexadecimal.

Com a chave pública do professor e para gerar a senha de comunicação, calculamos o valor de V, com V = B^a mod p. Depois, calculamos o hash com SHA256 do valor de V e pegamos os 128 bits menos significativos para usar como senha.

3. Descriptografando a mensagem

Para realizar a tarefa de descriptografia da mensagem recebido, utilizamos a implementação do *AES (Advanced Encryption Standard)* presente na biblioteca "pycryptodome", que permite a parametrização da chave de criptografia, vetor de inicialização da mensagem, e o modo que, no nosso caso, é o *CBC (Cipher Block Chaining)*.

Inicialmente, separamos os primeiros 16 bytes da mensagem recebida, que será utilizado como IV neste processo. Após, inicializamos o objeto AES, inicializado a partir da função new, e então descriptografamos a mensagem. A partir dos bytes resultantes deste processo, foi possível aplicar o padding utilizando PKCS7, e então obter a mensagem correta em texto plano.

```
def decrypt_aes_cbc(key, iv, ciphertext):
    cipher = AES.new(key, AES.MODE_CBC, iv=iv)
    original_message = unpad(cipher.decrypt(ciphertext), AES.block_size)
    return original_message

received_message = bytes.fromhex("f14c3e...6f84f4")

iv = received_message[:16]
encrypted_text = received_message[16:]

decrypted_text = decrypt_aes_cbc(key, iv, encrypted_text)
```

4. Criptografando a resposta

Um processo parecido foi utilizado para criptografar a mensagem de resposta, utilizando a implementação da mesma biblioteca.

Para realizar a tarefa estipulada, primeiramente invertemos a mensagem descriptografada no passo anterior para obter a mensagem que será enviada, e geramos aleatoriamente um novo vetor de inicialização. Para construir a string completa para a mensagem, aplicamos então o padding, seguindo o PKCS7. Ambos estes valores, juntamente com a chave de criptografia, foram utilizados para o encriptamento da mensagem utilizando a função contrária ao *decrypt*, da mesma biblioteca.

Após este processo, foi necessário adicionar o IV ao início do array de bytes, e então transformá-lo em hexadecimal, encontrando assim o seguinte valor, que foi enviado como resposta do problema:

“96AD0CDFA37E0A9779FEB56D8DD0F3CDC001BEAB6E892D5BF78A7F422AC05ACFD44EBDBB971914A71D2C20B72E4565E52C1CA6361CD045F1911A93791BDA0879”

5. Conclusão

A realização deste trabalho foi uma excelente oportunidade para aprofundar o entendimento sobre protocolos de segurança amplamente utilizados no mundo real. A implementação do protocolo Diffie-Hellman para troca de chaves seguras e o uso do algoritmo AES no modo CBC permitiram explorar de forma prática conceitos fundamentais de segurança de sistemas. Essas experiências práticas são essenciais para consolidar o aprendizado teórico e compreender como esses protocolos são aplicados em situações reais, como na comunicação segura pela internet.

6. Link para vídeo

Abaixo, segue o link para a apresentação do trabalho realizada pelos participantes: `https://youtu.be/KGglv0QNcu4`