universidade de aveiro

SEGURANÇA

1º Semestre

Secure Messaging Repository System

Grupo : P4G2

Fábio Cunha - 76677
João Amaral - 76460

- **Estabelecimento de uma chave de sessão temporária**

Antes de se estabelecer qualquer troca de mensagens é necessário o estabelecimento de uma chave de sessão entre o cliente e o servidor que mais tarde, quando a sessão terminar, devem ser descartadas de modo a não comprometer o conteúdo cifrado.

Para o estabelecimento de chaves de sessão entre um cliente e o servidor decidimos implementar o processo de Diffie-Hellman em conjunto com autenticação de valores na forma de uma assinatura digital (também conhecido por STS - Station-to-Station). Neste processo o cliente gera o valor Ya (Ya= α^a mod q) e o servidor o valor Yb (Yb=α^b mod q), que são os seus valores públicos de DH, sendo a e b valores secretos e gerados aleatoriamente. Na comunicação, o cliente começa por enviar ao servidor um quadruplo composto por o valor Ya, a sua chave de assinatura pública, o seu certificado de chave pública e uma assinatura digital do valor Ya produzida a partir da chave privada de assinatura do cliente. O servidor então irá realizar a validação da chave pública recebida pelo cliente usando para isso o certificado de chave pública recebido. Caso a mesma esteja válida então o servidor irá usa-la para realizar a verificação da assinatura digital de Ya (assinatura que foi produzida a partir da chave privada de assinatura do cliente). Assim, se se verificar que a assinatura é válida, comparando o valor obtido na decifra com o existente na assinatura, então o servidor pode comprovar que o valor que recebeu Ya foi realmente criado pelo cliente e não por um impostor. De seguida o servidor irá enviar um quadruplo, semelhante ao recebido anteriormente, ao cliente, sendo este composto por o seu valor calculado Yb, a sua chave pública, o seu certificado de chave pública e uma assinatura digital do valor Yb. O cliente irá então realizar o mesmo processo de validação de chave e assinatura e caso estas se confirmem, pode-se dizer que a chave simétrica de sessão K (K=a^ab mod q) obtida por ambos é uma chave de sessão válida e que apenas ambas as entidades conhecem.

No entanto é ainda necessário assegurar a propriedade PFS (Perfect Forward Secrecy). Esta é garantida se no final da sessão as chaves correspondentes da sessão, tanto do cliente como do servidor, sejam esquecidas assim como os segredos que as originaram, a e b, usados na geração de Ya e Yb e ainda esquecer o estado que possa persistir do gerador de número pseudo-aleatório usado pelo algoritmo. Assim, se esta propriedade for garantida, alguém que tenha guardado toda a informação trocada durante esta sessão, mesmo tendo acesso a todas as chaves de longo prazo de ambos os interlocutores, este não irá conseguir reconstruir as chaves de sessão usadas nesta comunicação e deste modo não conseguirá decifrar qualquer conteúdo trocado posteriormente com o servidor. A única maneira possível seria então através de uma pesquisa de força bruta ("brute force") no domínio da chave de sessão.

- **Cache de validade de chaves públicas**

De modo a evitar a validação do certificado de chave pública do cliente de todas as vezes que é trocada uma mensagem usando esta, optamos por fazer caching da validade do certificado durante a sessão (durante a troca de valores de Diffie-Hellman), assumindo assim que este não irá revogar durante a sessão. Quando a sessão termina o servidor esquece a validade do certificado e na próxima comunicação, isto é, numa nova sessão, será necessário voltar a validar esta e de novo guardar o resultado obtido desta validação. Um outro modo poderia ser realizando a validação de chave pública dentro de um período de tempo definido, por exemplo, de minuto a minuto.

- **Validação de certificados de chave pública do Cartão de Cidadão**

Para validar os certificados de chave pública do Cartão de Cidadão vão ser feitos pedidos ao servidor e a entidade emissora, o qual vai responder se o certificados está válido ou não.

- **Processo de criação de conta**

Para criar uma conta ou caixa de mensagens no servidor um utilizador necessita de enviar a este uma mensagem do tipo CREATE. Nesta mensagem o campo <uuid> corresponde ao digest do certificado de chave pública. No campo <other attributes> deverá estar presente a chave pública de autenticação, o certificado desta, assim como a chave de assinatura digital do utilizador. Deverá também estar presente o certificado de chave pública das mesmas para que o servidor as possa validar. Esta informação irá ser guardadas no campo <secdata> do “perfil” do cliente cujos dados a guardar devem estar propriamente assinados com a chave privada do Cartão de Cidadão.

A mensagem CREATE após ser criada do lado do cliente é cifrada com a chave temporária de sessão e enviada ao servidor que irá então decifrar e guardar os dados recebidos.

- **Validação das mensagens cliente-servidor**

Cada mensagem trocada entre o cliente e o servidor deve ser validada através do processo de MAC (Message Authentication Code), mais concretamente HMAC, tirando partido da chave simétrica de sessão acordada entre os dois.

- **Processo de cifra de mensagens cliente-servidor**

Todas as mensagens trocadas entre o cliente e o servidor deverão ser cifradas usando a chave de sessão acordada entre os dois no inicio da mesma, recorrendo ao algoritmo de AES (Advanced Encryption Standard) e ao modo de .

- **Processo de decifra de mensagens cliente-servidor**

Do mesmo modo do processo da cifra, na decifra tanto o cliente como o servidor decifram a mensagem trocada usando a chave de sessão pré estabelecida, que apenas estes dois conhecem.

- **Processo de cifra de mensagens entre clientes**

O processo de cifra de mensagens funciona em 2 passos. O primeiro trata da cifra do conteúdo da mensagem (campo <msg>) após ser convertido para base64, usando uma chave simétrica (AES) que é escolhida por quem iniciou a comunicação. Esta chave simétrica é então cifrada usando a chave pública do destinatário (RSA) de modo a poder ser distribuída seguramente. Para cada mensagem enviada deve ser gerada uma nova chave simétrica. As chaves públicas dos destinatários fazem parte da informação de segurança existente no “perfil” de cada utilizador .

- **Processo de decifra de mensagens entre clientes**

O processo de decifra funciona também em 2 passos. O destinatário da mensagem, ao recebê-la, decifra-a usando a sua chave privada (RSA). Após a decifrar irá obter a chave simétrica, assim como a mensagem cifrada por esta. Deste modo pode então decifrar a mensagem usando a chave simétrica e obter o conteúdo original da mensagem.

- **Processo de validação de chave públicas**

A validação das chaves públicas é realizado através da validação do certificado de chave pública que é enviado em conjunto da chave pública do remetente.

- **Controlo de integridade das mensagens**
    - MAC criado a partir da chave de sessão
    - Validação de certificados de chave pública dos utilizadores em cada sessão
    - Validação do certificado de chave pública do servidor pelos utilizadores
    - Validação da assinatura digital nas trocas de valores no processo de Diffie-Hellman

- **Algoritmos usados**
    - AES + Modo de cifra CTR/OFB
    - RSA
    - SHA-2 (SHA-256/SHA-512)
    - Diffie-Hellman + validação dos valores públicos trocados (assinatura digital)

- **Chaves de cifra**
    - Servidor - Par de chaves assimétricas
    - Utilizador - Par de chaves assimétricas (assinatura e autenticação) do Cartão de Cidadão
    - Servidor/Utilizador - Chave temporária de sessão simétrica

- **Validação e integridade (autenticadores de dados)**
    - Validação na geração da chave de sessão - Assinatura digital criada com a chave privada dos interlocutores (cliente-server)
    - Validação na troca de mensagens cliente-cliente - Assinatura digital com a chave privada de assinatura do cartão do cidadão do remetente.
    - Validação na troca de mensagens cliente-servidor - HMAC