Relatório

Segurança

Grupo 41

Francisco Sousa nº82037

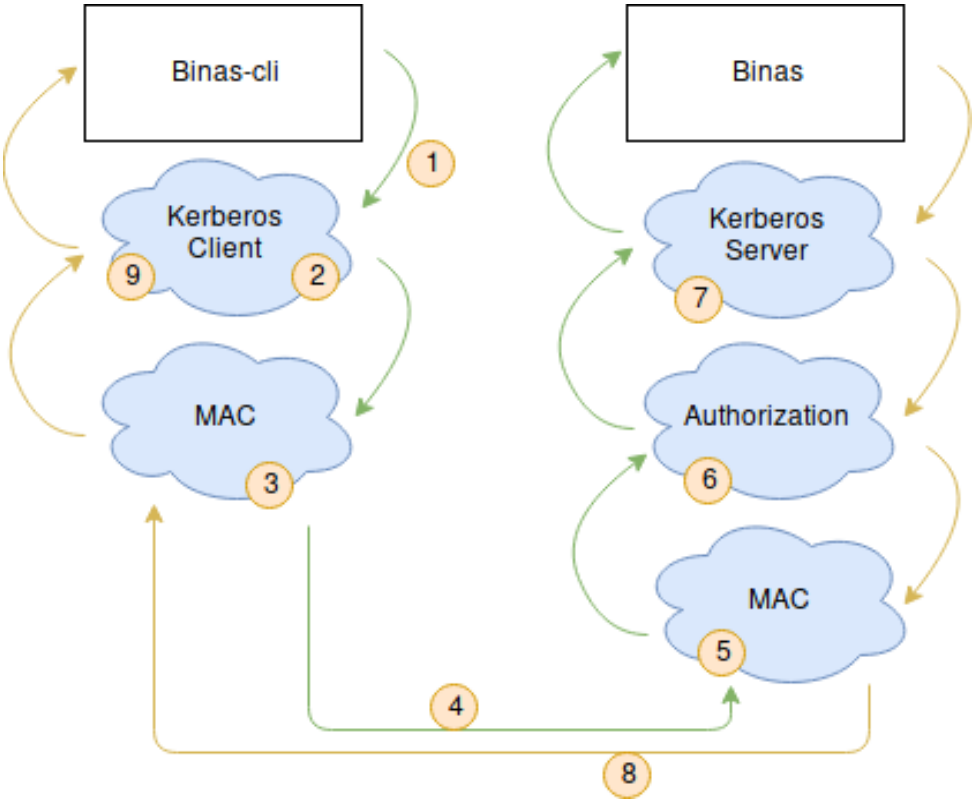
José Canana nº82039

Inês Vilhena nº84593

Descrição Kerberos

A figura ilustra a implementação feita pelo grupo, utilizada na resolução desta entrega.

Para simplificar o trabalho a realizar não iremos utilizar servidores TGS particulares, isto é, serão os handlers do Binas-ws a realizar as operações de validação e autenticação dos *users*.



(1) O pedido feito pelo utilizador é processado pelo KerbyClientHandler, que utiliza a password fornecida para pedir um Ticket que tem uma validade de 30 minutos e contem a Chave de Sessão (sessionKey).
(2) É utilizada a clientKey para decifrar a sessionKey. O ticket e a auth cifrados são ambos colocados no header da SOAPMessage.
(3) O conteúdo do SOAPbody é encriptado e adicionado ao header da SOAPMessage.
(4) A messagem é enviada pela rede. É aqui que a mensagem está sujeita a ataque.
(5) O conteúdo do SOAPBody é analisado pelo MACHandler verificando que a mensagem é a mesma q foi encriptada no passo 3, garantindo assim que não foi alterada na rede.
(6) É feita, pelo AuthorizationHandler, a verificação que o email que realizou o pedido ao Kerberos é o mesmo que enviou a mensagem, garantindo que o utilizador que fez o pedido é também um utilizador activado.
(7) É feita a desencriptação doTicket utilizando a ServerKey, e a auth é validada. Fica também aqui guardado o RequestTime do pedido.
(8) Depois de concluído o pedido no servidor, é enviado pela rede uma resposta que contem o RequestTime.
(9) KerberosClient verifica se o RequestTime recebido é igual ao do pedido, verificando que o Server que forneceu uma resposta é o mesmo a que foi feito o pedido.

SOAPMessage do lado do Cliente

.

(1) Ticket encriptado.
(2) Autenticação encriptada.
(3) Mac encriptada.
(4) Body da soap message com o pedido realizado pelo cliente.
(5) Header da soap message recebida pelo cliente com o TimeRequest vindo do servidor.

SOAPMessage do lado do Servidor