






TÉCNICO LISBOA

Sistemas Distribuídos

Relatório de Segurança – Entrega 3
Grupo T01

Repositório de GitHub:

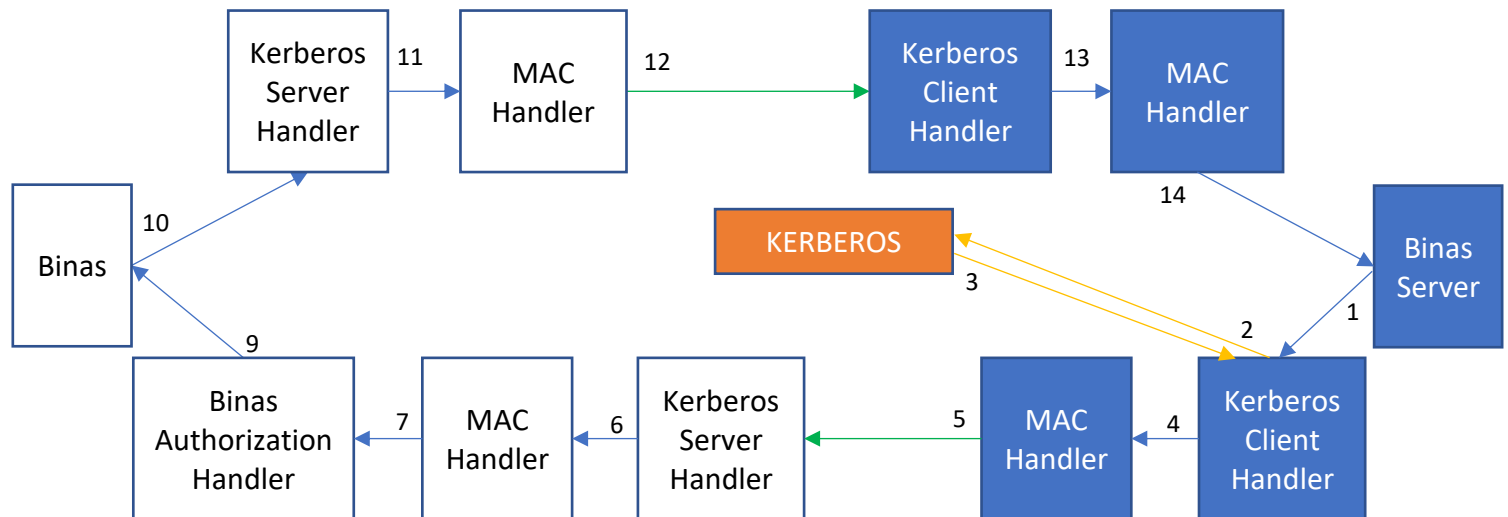
<https://github.com/tecnico-distsys/T01-SD18Proj><https://github.com/tecnico-distsys/T01-SD18Proj>

		77921	Mafalda Gaspar
		84710	Diogo Vilela
		84758	Rafael Ribeiro

Introdução:

Para a terceira entrega utilizou-se a solução da primeira entrega fornecida pelos professores.

Figura da solução de segurança:



Descrição da Figura e Explicação da Solução:

Como se pode observar pela figura, existem quatro *Handlers*.

O *KerberosClientHandler* é o primeiro a ser chamado. O seu objetivo é autenticar-se perante o *Kerberos* e obter o *Session Ticket* e o *Auth*.

O *MacHandler* é o segundo *handler* a ser executado, tendo como objetivo (numa *Outbound Message*) gerar o MAC da mensagem a ser enviada e colocá-lo no cabeçalho da mesma.

O *KerberosServerHandler* é o terceiro *handler* a ser executado. Confirma que o cliente é quem afirma ser ao fazer a validação do *Session Ticket* (verificando que o *email* do servidor no *Session Ticket* é igual ao *email* do servidor que está a receber a mensagem) e do *Auth* (verificando que o *email* do cliente do *Auth* é igual ao *email* do cliente do *Session Ticket*). Obtem também a chave privada conhecida pelo servidor e cliente, que foi utilizada na geração do MAC e que será utilizada na verificação do mesmo quando o *MACHandler* for executado com uma *Inbound Message*.

Quando o *MACHandler* é executado do lado do *binas-ws*, o *handler* verifica se a mensagem foi alterada desde que foi gerada, gerando um MAC da mensagem recebida e comparando-o ao MAC presente no cabeçalho.

O *BinasAuthorizationHandler* é o quinto *handler* a ser executado. Tem como objetivo verificar que o cliente tem a autorização para executar o pedido através da comparação do identificador (no âmbito do projeto, *email* do utilizador) recebido no *Session Ticket*, no *Auth* e no *request* recebido.

Na resposta ao pedido (do *binas-ws* para o *binas-ws-cli*) o *MACHandler* é executado para a verificação da integridade das mensagens e o *KerberosServerHandler* e o *KerberosClientHandler* são executados para a inserção e verificação do *Time Request*.

Não se conseguiu implementar completamente a solução apresentada acima. No momento da entrega, apenas os *KerberosServerHandler* e *KerberosClientHandler* funcionavam corretamente. Os outros *handlers* – *MACHandler* e *BinasAuthorizationHandler* – embora incorretos, estão praticamente completos.

Segurança – Conteúdo das Mensagens:

Quando o *binas-ws-cli* efetua um pedido ao *binas-ws* envia uma mensagem SOAP que contém no *Body* o *email* do utilizador.

Quando a mensagem é capturada pelo primeiro *Handler* – *KerberosClientHandler* – são adicionados dois campos ao cabeçalho, o *Session Ticket* e o *Auth* do cliente.

A partir deste ponto, a análise é teórica, pois a solução não foi implementada com sucesso.

Após esse *handler* terminar, o *MACHandler* é executado e adiciona o *MessageAuthenticationCode* da mensagem a enviar, também ao cabeçalho.

Quando o *binas-ws* responde ao pedido do *binas-ws-cli*, são adicionados o *Time Request* enviado anteriormente pelo cliente e o *MAC* da mensagem.