Licenciatura em Engenharia informática e de Computadores — Alameda
Unidade Curricular de Sistemas Distribuídos — Ano Letivo 2017/2018

Relatório da 3º Entrega do Projeto (P3)

Segurança

Grupo A46

Hélio Domingos
83473

Miguel Regouga
83530

João Pina
85080

Repositório GitHub:

https://github.com/tecnico-distsys/A46-SD18Proj

Segurança

Para garantir que o sistema BINAS é resistente a ataques maliciosos, tais como a adulteração de mensagens de rede e/ou a invocação de operações que afetam o saldo dos utilizadores de forma ilegítima, são aplicados diversos mecanismos de segurança, sob a forma de *handlers.*

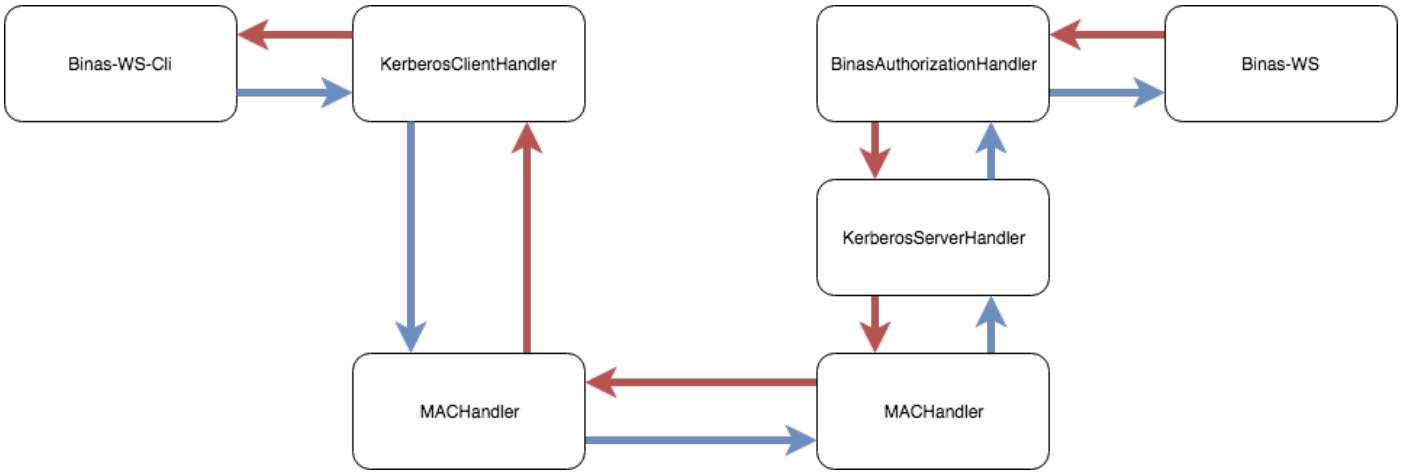

Figura 1 — Solução da segurança

Handlers

Um *handler* é um mecanismo que permite intercetar e aceder diretamente as mensagens SOAP que saem e entram de um cliente (neste caso, Binas-WS-Cli) ou servidor (Binas-WS). Para assegurar a segurança de todo o sistema, foram implementados 4 *handlers* no projeto.

Nome do Handler	Mensagens de chegada (*inbound*)	Mensagens de envio (*outbound*)
KerberosClientHandler	• Recebe *RequestTime* e valida-o.	• Realiza a autenticação do cliente no servidor *Kerberos*; • Recebe chave de sessão e *ticket*; • Coloca *ticket* no cabeçalho da mensagem; • Cria e coloca autenticador no cabeçalho da mensagem.
KerberosServerHandler	• Recebe *ticket* e valida-o; • Recebe autenticador e valida-o.	• Envia *RequestTime*.
MACHandler	• Verifica se o resumo é consistente.	• Cria um resumo do *body* da mensagem e coloca-o no *header*.
BinasAuthorizationHandler	• Verifica se os e-mails do *ticket*, autenticador e pedido de operação são iguais.	

Tabela 1 — Especificação da funcionalidade dos handlers

Autenticação de Utilizadores

O servidor *Kerberos* guarda os dados de autenticação dos utilizadores de um determinado sistema. Antes de poder interagir com o servidor, o cliente deve solicitar ao servidor Kerberos um ticket e uma chave de sessão, de forma a poder comunicar com o servidor.

O servidor *Kerberos* autentica o utilizador e gera o ticket e a chave de sessão caso este esteja autorizado a comunicar com o servidor para o qual pediu autorização; caso não esteja, é lançada uma exceção.

Controlo de Acessos

Para garantir a frescura da mensagem, antes de enviar um pedido ao servidor, o cliente regista o momento de criação do pedido; é depois cifrado dentro do autenticador e é enviado junto deste para o servidor. O servidor envia-o de volta na resposta ao cliente e o cliente deve verificar se são iguais, assegurando assim que a resposta corresponde ao pedido efetuado.

Ao receber um pedido, o servidor compara os e-mails presentes no *ticket*, autenticador e operação desejada — caso sejam todos iguais, é confirmado que o cliente tem acesso aos dados que está a pedir. Caso contrário, não é permitido o acesso ao cliente e é enviada uma exceção para o cliente.

Integridade dos Pedidos e Respostas

Para garantir a integridade dos pedidos e respostas, é adicionado ao cabeçalho de cada mensagem um MAC (*Message Authentication Code*). Este código é calculado com uma função de resumo aplicada ao corpo da mensagem, sendo também utilizada para este fim a chave de sessão gerada pelo *Kerberos*, que é usada tanto pelo cliente como pelo servidor.

Ao chegar ao destino, o MAC é recalculado utilizando também o corpo da mensagem *inbound* e é comparado com o MAC original. Caso sejam iguais, então está garantida a integridade da mensagem. Em caso contrário, é lançada uma exceção, uma vez que o corpo da mensagem pode ter sido alterado indevidamente.

Mensagens SOAP

Uma mensagem SOAP é um documento XML que contém um envelope (que identifica o dito documento como uma mensagem SOAP). Esse envelope é constituído por um cabeçalho, um corpo (que contém informação de pedidos e respostas) e um elemento *fault* opcional (que contém erros e informações do estado do sistema).

Cliente -> Servidor

```
Message destination: http://localhost:8080/binas-ws/endpoint
2018-05-18T19:58:32.158 OUTbound SOAP message:
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http:/
/schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header>
      <ticket xmlns="http://ws.binas.org/">Cjx0aWNrZXQgeG1sbnM6bnMyPSJodHRwOi8va2VyYnkuc
2Rpcy50ZWNuaWNvLnVsaXNib2EucHQvIj4KICAgIDxkYXRhPk1WUjJUS1c0dDRUY0NFSDJBREZ3V2kwUTNhT2p
QcEV5M1lDZnFFcjVMQnBtTElkRnEyMm1DYmhmNjdPTnBjL2tEUzFuaitITE1icXN6SVpXSTQ2RTBOUHhsZDE3Y
mRBQTlJcFJBY3d1STUyN2VpVXdENGtPSmV1cVVKSkR5RU9kNm1laGg2bXk5c2tNbWthNG5KUXBoM0ZIaDdsRTR
RZGxuUzlGZEJUNHJhQnJnRkplTmV6V2NJUXByUDg2OW9yOUhNRjNSRHFwOStrQ3FORHNKU1lhdlRCWFh1anhWO
XMwSDFpdytaT2YxTm9BeHJwNmtmV2tRNXZsVzNsckJLb2tETTJCV0h2M0grQm1Qcnd5MFVLczEzQnpJb1MrTWZ
4QUVoaHdHQnYzSUhHeTR5bG96akFKK1p3U2wvdTJKL1hkaGpJeThiUUNMR2FWMTViNXVBYWNLTkM5TlNiWHQrM
mtRZnNmNWtHTXhzZkJ0Ry91M1BJcXdIWTNCSy82NTVCOTl6bjJvanJBWGxXY2JnL0t0ZWYxZ3c9PTwvZGF0YT4
KPC90aWNrZXQ+Cg==</ticket>
      <authenticator xmlns="http://ws.binas.org/">CjxhdXRoZW50aWNhdG9yIHhtbG5zOm5zMj0iaH
R0cDovL2tlcmJ5LnNkaXMudGVjbmljby51bGlzYm9hLnB0LyI+CiAgICA8ZGF0YT5VU29KMVIxSHFwMWVDamgv
dmFYaVZwVnpuN2dhTDFwSWlPYzl6cDVNa1JQeEJvVDNSK31sQ2hlWkt3Mk9EZExpcmlXazk3UFdJSGtkOGVtQ0
5BSU1SOHovT28ydU94bUtTbHZYLzJYMFROcEpIS1NrVzQ2OEZpQ1RFRGo2YmdFWTN2UWJOL1N5azNlbWQ3N3Zq
R0s3Vm1paElrV1hBOHJ5ZTA0MWlCUnFhKzErVzZGR3BWVVdsQnI4a3g4NlFMV0JGSVozNVhDRU5zOHNBTktsTk
5ybElqMGpFR1BSSmJiUW4ydEUxQkFLK0g0PTwvZGF0YT4KPC9hdXRoZW50aWNhdG9yPgo=</authenticator>
      <mac xmlns="http://ws.binas.org/">zOIffISR9G/DdqoE3ucaVq+RUCXp+f6eV0mjPVYZ01g=</ma
c>
   </SOAP-ENV:Header>
   <S:Body>
      <ns2:test_ping xmlns:ns2="http://ws.binas.org/">
         <input_message>client</input_message>
      </ns2:test_ping>
   </S:Body>
</S:Envelope>
```

Figura 2 — Mensagem SOAP, enviada do cliente para o servidor

Numa mensagem que é enviada do cliente para o servidor, o cabeçalho contém o *ticket*, o autenticador e o MAC, sendo que o corpo contém a operação pedida pelo cliente.

Servidor -> Cliente

```
2018-05-18T19:58:33.893 OUTbound SOAP message:
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http:/
/schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header>
      <reqtime xmlns="http://ws.binas.org/">CjxyZXF0aW1lIHhtbG5zOm5zMj0iaHR0cDovL2tlcmJ5
LnNkaXMudGVjbmljby51bGlzYm9hLnB0LyI+CiAgICA8ZGF0YT5Dcm1DaFhHa2dWSi8xOVRPazArQUhlNDllVV
hoU1lON3V6S1NRZ1MyOTZSTGsvbGdCQk1lZ1BGZTBTc3Y2OWZoQ1dCRXNCOEVBQndJVi9jLytua0tneG5maVcr
Z3BSZ3MxRjM0SDRkSzJqeC91UERkdG9wb1J6ejNxYWxtNkZmMXJUaFV6NDl6VWxtNEtSTzBPSXJ1MHhlZU8xVH
4vSUZ3Q1h1ODhEWVZnc2pPUWljeGt5cjBkVWhiVkUraDU4MEdPR3ZlQVVrbDlTSDVOUnlIS1o5bnlBPT08L2Rh
dGE+CiwvcmVxdGltZT4K</reqtime>
      <mac xmlns="http://ws.binas.org/">RU7zVkE2K964ZMyFOlaASFVX/dkZ1y/AFxySqdRIFW8=</ma
c>
   </SOAP-ENV:Header>
   <S:Body>
      <ns2:test_pingResponse xmlns:ns2="http://ws.binas.org/">
         <return>Hello client from A46_Binas!
Found 0 stations on UDDI.
</return>
      </ns2:test_pingResponse>
   </S:Body>
</S:Envelope>
```

Figura 3 — Mensagem SOAP, enviada do servidor para o cliente

No caso de uma mensagem enviada pelo servidor e recebida pelo cliente, o cabeçalho contém apenas o *RequestTime* e o MAC, sendo que o corpo contém a resposta ao pedido.