TÉCNICO LISBOA

Sistemas Distribuídos

PROJETO • Entrega 3

T_09 • LEIC-T • 2017/2018 • 2.º Semestre

Diogo Redin
84711

Gonçalo Matos
81943

Marta Simões
81947

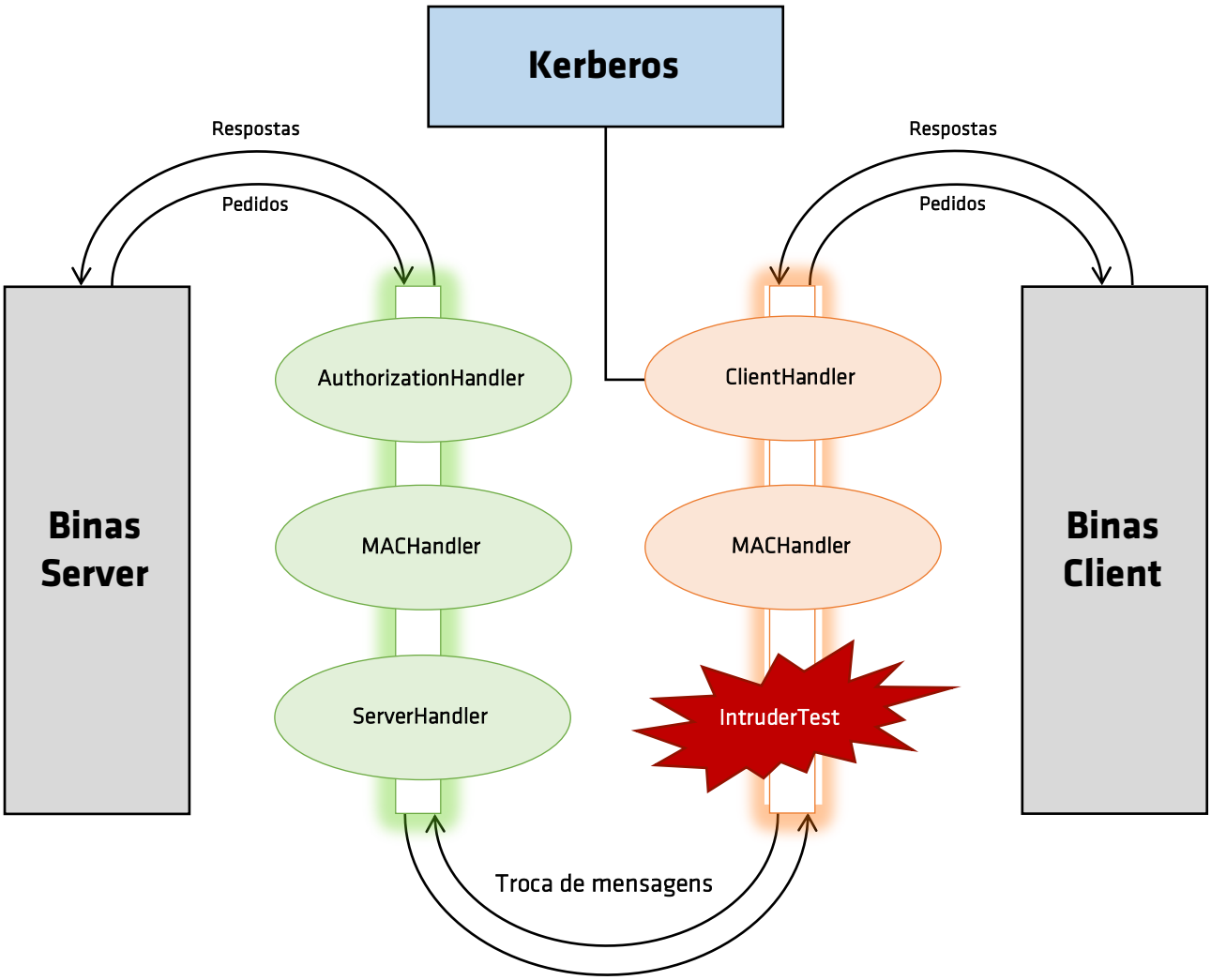

Figura 1 – Modelação da solução implementada.

Introdução

Para a terceira parte do Projeto tínhamos por objetivo impedir que um utilizador malicioso invoque operações que afetem o saldo de outros de utilizadores de forma ilegítima e que possíveis atacantes adulterem mensagens na rede. Para tal, passámos a autenticar as invocações feitas pelos clientes ao servidor, autorizando apenas as que dizem respeito ao cliente autenticado e garantimos a integridade dos pedidos e das respostas.

Kerberos simplificado

Para podermos autenticar as invocações feitas pelos clientes ao servidor, implementámos o protocolo Kerberos simplificado, baseado em *tickets*, que permite identificar os utilizadores de forma segura.

Como o Kerberos usa apenas cifra simétrica, tanto o cliente como o servidor de uma determinada aplicação provam a sua identidade entre si através do acesso a um servidor Kerberos. As mensagens do protocolo Kerberos são protegidas contra ataques de interceção e repetição. A Figura 2 ilustra a interação entre um cliente e o servidor Kerberos.

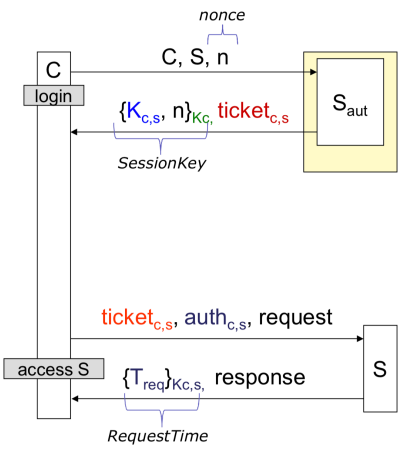

Figura 2 – Interação cliente/Kerberos

Implementação

O essencial da implementação desta parte do Projeto consistiu no desenvolvimento de quatro handlers principais:

- **KerberosClientHandler**: o cliente autentica-se no Kerberos, recebe uma chave de sessão, um ticket, e é criado autenticador.
- **KerberosServerHandler**: o servidor abre e valida o ticket, assim como valida autenticador.
- **BinasAuthorizationHandler**: o servidor verifica se o e-mail do pedido corresponde ao do utilizador autenticado.
- **MACHandler**: é usado pelo cliente para proteger mensagens de saída e pelo servidor para validar mensagens de chegada.

Para além destes quatro handlers principais, recorremos também ao PrettyLoggerHandler, que nos permite observar a estrutura das mensagens de saída e de chegada sempre que é efetuado um pedido. Assim, conforme ilustram as Figuras 3 a 5, o protocolo implementado e o conteúdo das mensagens SOAP são os seguintes:

- **Autenticação**: inicialmente, o cliente autentica-se e são transmitidos pelo header da mensagem:
  - **Ticket**: é criado pelo cliente junto do Kerberos, convertido para CipheredView e adicionado ao header.
  - **Auth**: é criado pelo cliente junto do Kerberos, convertido para CipheredView e adicionado ao header.
- **Integridade**: à medida que os pedidos são efetuados, o MACHandler adiciona um MAC a todos os pedidos sensíveis, que garante que o e-mail do cliente que efetuou o pedido corresponde ao que é usado no servidor.
  - **Geração do MAC**:
    - É o último a ser adicionado ao cabeçalho das mensagens e utiliza a chave de sessão, obtida a partir do ticket, para criar uma string correspondente ao e-mail do pedido (cifrado).
  - **Verificação do MAC**:
    - Server - Tendo recebido um MAC no pedido, verifica se, gerando um novo MAC com a mesma chave de sessão, este corresponde ao já recebido no header.
    - Client – Tendo recebido um MAC na resposta, verifica se, gerando um novo MAC com a mesma chave de sessão, este corresponde ao já recebido no header.

```
T09_Binas
BinasClientApp running
Creating client using UDDI at http://t09:TiRR649@uddi.sd.rnl.tecnico.ulisboa.pt:9090/
Contacting UDDI at http://t09:TiRR649@uddi.sd.rnl.tecnico.ulisboa.pt:9090/
Looking for 'T09_Binas'
Found http://localhost:8070/binas-ws/endpoint
Creating stub...

FAULT TOLERANCE TESTING | SECURITY TESTING
Press (0) to shutdown.
Press (1) to create three users, already registered on Kerberos.
Press (2) to get the credit from those three users.
Press (3) to rent binas for users 1 and 3.
Press (4) to return binas for users 1 and 3.
Press (5) to rent binas for user 2.
Press (6) to return binas for user 2.
Press (7) to rent binas for user alice@T09.binas.org.

Enter Command:
1
alice@T09.binas.org activated.
charlie@T09.binas.org activated.
eve@T09.binas.org activated.
DONE

2
alice@T09.binas.org, credit: 10
charlie@T09.binas.org, credit: 10
eve@T09.binas.org, credit: 10
DONE
```

Figura 3 – Interação cliente/Kerberos

```
<?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>
    <Details xmlns="http://ws.binas.org/">
      <TimeRequest>CjxieXRlc1JlcXVlc3RUaW1lIHhtbG5zOm5zMj0iaHR0cDovL2tlcmJ5LnNkaXMudGVjbmljby5pbGlzYm9hLnB0LyI+CiAgICA8ZGF0
ZE11eDZOK20zOERtT1llMTZCd0lEYUo5eTqzaTdYVlVXMzR6bEc1MjJpS2hINndWUnRqUjNzTFVKZ3F1ZHlxVHY2bjRIM1BZbE9EeWY2dnpvUGJDTHdhMWt2UXB0
RWUhYRExnV3VyZDZOU2l0emRWUW9NQXZJcXQwcWlPdkRySEhkdzZlWFh1SzB6QllSSGZ4aStkQ3pOa1FzQk8vc1FnV2RwQVdHcTM4emt5WmV3PT08L2RhdGE+Cjw
TimeRequest>
      <Mac>8AF3DC3013DAAA3A5F157185C2DEEEBCCEED5CFF8CAE19AD66BBE3BB7F0CFC25</Mac>
    </Details>
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:rentBinaResponse xmlns:ns2="http://ws.binas.org/"/>
  </S:Body>
</S:Envelope>
```

Figura 4 – Mensagem *outbound*

```
<?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>
    <Details xmlns="http://ws.binas.org/">
      <Auth xmlns="http://ws.binas.org/" xmlns:ns2="http://kerby.sdis.tecnico.ulisboa.pt/">
        <data xmlns="">nJTKRDb/LxyYpYUb9Ew0rbJxxOPCRSNV0ZpfomwCcKeyoXCHtowkZHh2PomKDPRMuQYvfpKlb87Q/qxx1s0O8pGgfUS3nKlt9hFQV85B4TdJTc/lk
h+QX/pCkwHQRswd1W78mtJiogtA2+tAPyVvomuL01xjSDyacRXslvsLe4SLXAfsfoVVQG4jppzWcbQuXCyzqfO8pS2UD024M0twLdhsUC4=</data>
      </Auth>
      <Ticket xmlns="http://ws.binas.org/" xmlns:ns2="http://kerby.sdis.tecnico.ulisboa.pt/">
        <data xmlns="">p9X1STfx9dolyERJ3allLfhBNaHqQ26TDoICwiGCf3icrHrcbvUCXba6lAvrtY0s0JFk65RyrlfNLEbP/iunC/r0JqdO9HXc4dZnKn1Q2MLF182mC
eCPkCZfkiGJdx33/UItbSKo4EnBjaqTnRErE7Gf5jzPtnb67i4LDBL6DkEqTNt6EunGZ/G0jfLSVkyKRgK/38CecQq8OE1t0gXRb8DK/96R7fFBOqOUhQ65CVvv0btbb/YDJeWyJ
hGtAcon36kpeOKwjYn505HLxzD3wIIQKjTZ+5r/BWbB378M5o1mywJ4BxmAldmKrkXp8XF8CIikxKlUab8V4svxsNtT+zdUA4NGucH1A04y34P1sok4Ed+D8vySVBw==</data>
      </Ticket>
      <Mac>8AF3DC3013DAAA3A5F157185C2DEEEBCCEED5CFF8CAE19AD668BE3BB7F0CFC25</Mac>
    </Details>
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:rentBina xmlns:ns2="http://ws.binas.org/">
      <stationId>T09_Station1</stationId>
      <email>alice@T09.binas.org</email>
    </ns2:rentBina>
  </S:Body>
</S:Envelope>
```

Figura 5 – Mensagem *inbound*