

Relatório

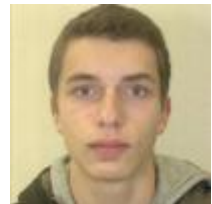
Segurança

Grupo 41

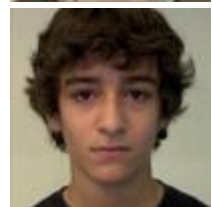


TÉCNICO
LISBOA

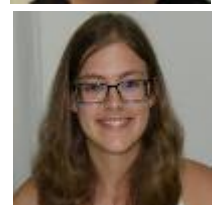
Francisco Sousa nº82037



José Canana nº82039



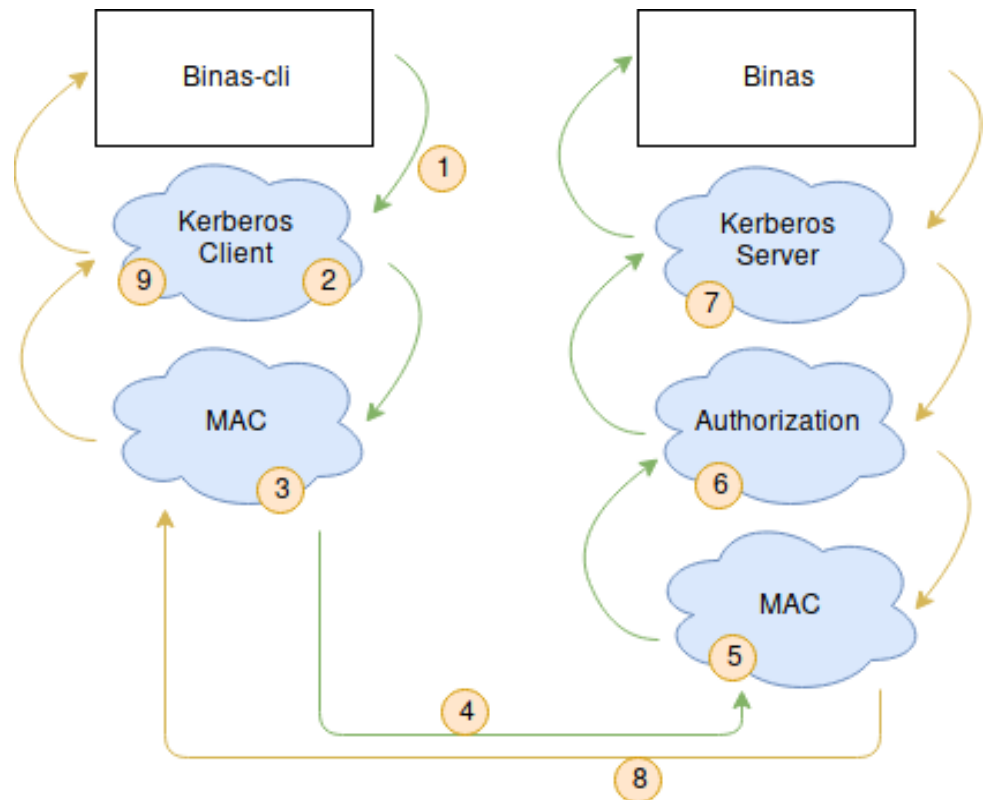
Inês Vilhena nº84593



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 mensagem 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 descriptação 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

```
Invoke ping()...
Message destination: http://localhost:8080/binas-ws/endpoint
2018-05-18T21:35:18.050 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/'>
  1 <SOAP-ENV:Header>
    <t:ticket xmlns:t='http://ticket/'>
      <ticket xmlns:ns2='http://kerby.sdis.tecnico.ulisboa.pt/'>
        <data>Y2dAozfzKTRm+fpJzjbF8tJdID+94VXT/jDK4ehdGyulLbdhIH/exzCog0hkyWl/4nJLyej89v8rRF0xvbd/MG3Sc7TCTpRgHLC4J83McSfSdUHG6CgCOFN2uFnJRtQ71GDhM91/Wz
7Nj/2qe0bKEECXnlq9qTLzBEwEjo0V13EDhJ0xaresoWnaidVxWl6gzg7ghpnZAJ6a1bmYUbaVR9cP3AKExiv5VNBt10hjYF1GzhtKvj636AtF+Zkg3V6/15iuUfQVxfEwo7S2q9EmavHXrd9/fciJY
UYdGkV9/r/0ErSQ6o77Kdo8dMmzVKmePCVpWl1xhGVG+FeTxIEyYeIJ+UHMImZyq8F6uLvbWlviQECfKChUKQguvypENgahIz4v9YdvI218444nFNuIPB5Pw==</data>
        </ticket>
      </t:ticket>
    <t:auth xmlns:t='http://ticket/'>
      <auth xmlns:ns2='http://kerby.sdis.tecnico.ulisboa.pt/'>
        <data>tKPrC140fAygA+SAU+KwXjtKHMDa9LzuHC4EAdjrYLHJjgVudkY7oDbbBA659EU6AHWDFvHOA3T+oKFcjHSZV4mYErTvECT4svgMunoJzEfmmDDIEXicyv0wtf8LgmLXBs6wXSCFq
xv6ieuJq6SeJUcW3XR5pX9tYzSCfaVqzQP8AkZ3cLFBBcTbYLtS4pJZvDe30HMF4uSKULzt0EwXKjCmWek+GLBBEFr0rJmIGlw=</data>
        </auth>
      </t:auth>
    <t:MAC xmlns:t='http://ticket/'>7g3NPxPJSojtEiepI4bAuuhdCYZ82FOCLNM/3jGUUnuU=</t:MAC> 3
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:test_ping xmlns:ns2='http://ws.binas.org/'> 4
      <input_message>client</input_message>
    </ns2:test_ping>
  </S:Body>
</S:Envelope>
2018-05-18T21:35:18.674 INbound 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>
    <rt:requestTime xmlns:rt='http://requestTime/'>
      <cipheredRt xmlns:ns2='http://kerby.sdis.tecnico.ulisboa.pt/'>
        <data>D/afyR6IrsS87HMqmevcKPSB74bcW8010shsULOPvXBcGX3P8YnULFK31eeGLysdZBLt9neuSLTM3FNwQovf3tvtqQn85YSbjGYc8PDhUJFPoQXmEx5nTucquWfu+XuebNMtbsZv
osny7TbFE+fh1DETEU4n600oJogQ/cQyEdsFjxAX5WjZHL1RMu3cLoToahWBxduUjWu0hzz6dDQ==</data>
      </cipheredRt>
    </rt:requestTime>
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:test_pingResponse xmlns:ns2='http://ws.binas.org/'>
      <return>Hello client from T4I_Binas!
Found 0 stations on UDDI.
    </ns2:test_pingResponse>
  </S:Body>
</S:Envelope>
Header element not found.
Caught exception on MACHandler INBOUND : java.util.NoSuchElementException
SERVER AUTHENTICATED
Message source: http://localhost:8080/binas-ws/endpoint
```

- (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

```
Awaiting connections
Press enter to shutdown
2018-05-18T21:35:18.072 INbound 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/'>
  1 <SOAP-ENV:Header>
    <t:ticket xmlns:t='http://ticket/'>
      <ticket xmlns:ns2='http://kerby.sdis.tecnico.ulisboa.pt/'>
        <data>Y2dAozfzKTRm+fpJzjbF8tJdID+94VXT/jDK4ehdGyulLbdhIH/exzCog0hkyWl/4nJLyej89v8rRF0xvbd/MG3Sc7TCTpRgHLC4J83McSfSdUHG6CgCOFN2uFnJRtQ71GDhM91/Wz
7Nj/2qe0bKEECXnlq9qTLzBEwEjo0V13EDhJ0xaresoWnaidVxWl6gzg7ghpnZAJ6a1bmYUbaVR9cP3AKExiv5VNBt10hjYF1GzhtKvj636AtF+Zkg3V6/15iuUfQVxfEwo7S2q9EmavHXrd9/fciJY
UYdGkV9/r/0ErSQ6o77Kdo8dMmzVKmePCVpWl1xhGVG+FeTxIEyYeIJ+UHMImZyq8F6uLvbWlviQECfKChUKQguvypENgahIz4v9YdvI218444nFNuIPB5Pw==</data>
        </ticket>
      </t:ticket>
    <t:auth xmlns:t='http://ticket/'>
      <auth xmlns:ns2='http://kerby.sdis.tecnico.ulisboa.pt/'>
        <data>tKPrC140fAygA+SAU+KwXjtKHMDa9LzuHC4EAdjrYLHJjgVudkY7oDbbBA659EU6AHWDFvHOA3T+oKFcjHSZV4mYErTvECT4svgMunoJzEfmmDDIEXicyv0wtf8LgmLXBs6wXSCFq
xv6ieuJq6SeJUcW3XR5pX9tYzSCfaVqzQP8AkZ3cLFBBcTbYLtS4pJZvDe30HMF4uSKULzt0EwXKjCmWek+GLBBEFr0rJmIGlw=</data>
        </auth>
      </t:auth>
    <t:MAC xmlns:t='http://ticket/'>7g3NPxPJSojtEiepI4bAuuhdCYZ82FOCLNM/3jGUUnuU=</t:MAC> 3
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:test_ping xmlns:ns2='http://ws.binas.org/'> 4
      <input_message>client</input_message>
    </ns2:test_ping>
  </S:Body>
</S:Envelope>
MESSAGE AUTHENTICATED
ACCESS GRANTED
Caught exception on MACHandler OUTBOUND : pt.ulisboa.tecnico.sdis.kerby.KerbyException: Exception while deciphering view!
2018-05-18T21:35:18.668 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/'>
  5 <SOAP-ENV:Header>
    <rt:requestTime xmlns:rt='http://requestTime/'>
      <cipheredRt xmlns:ns2='http://kerby.sdis.tecnico.ulisboa.pt/'>
        <data>D/afyR6IrsS87HMqmevcKPSB74bcW8010shsULOPvXBcGX3P8YnULFK31eeGLysdZBLt9neuSLTM3FNwQovf3tvtqQn85YSbjGYc8PDhUJFPoQXmEx5nTucquWfu+XuebNMtbsZv
osny7TbFE+fh1DETEU4n600oJogQ/cQyEdsFjxAX5WjZHL1RMu3cLoToahWBxduUjWu0hzz6dDQ==</data>
      </cipheredRt>
    </rt:requestTime>
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:test_pingResponse xmlns:ns2='http://ws.binas.org/'>
      <return>Hello client from T4I_Binas!
Found 0 stations on UDDI.
    </ns2:test_pingResponse>
  </S:Body>
</S:Envelope>
```

