Sistemas Distribuídos
2017/2018

Projeto, Parte 3
Segurança

RELATÓRIO

Grupo A30

Github: https://github.com/tecnico-distsys/A30-SD18Proj

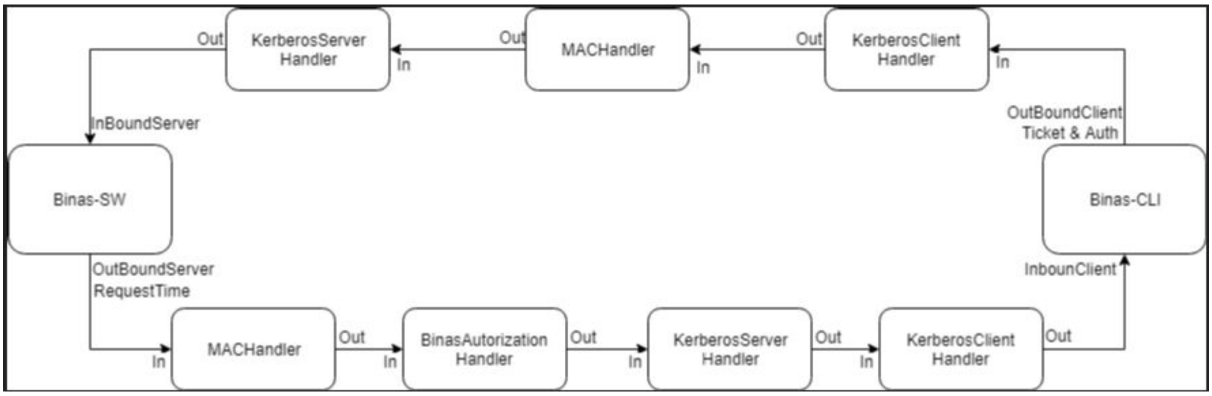
81633 - João Henriques

82343 - Pedro Cunha

83434 - Beatriz Toscano

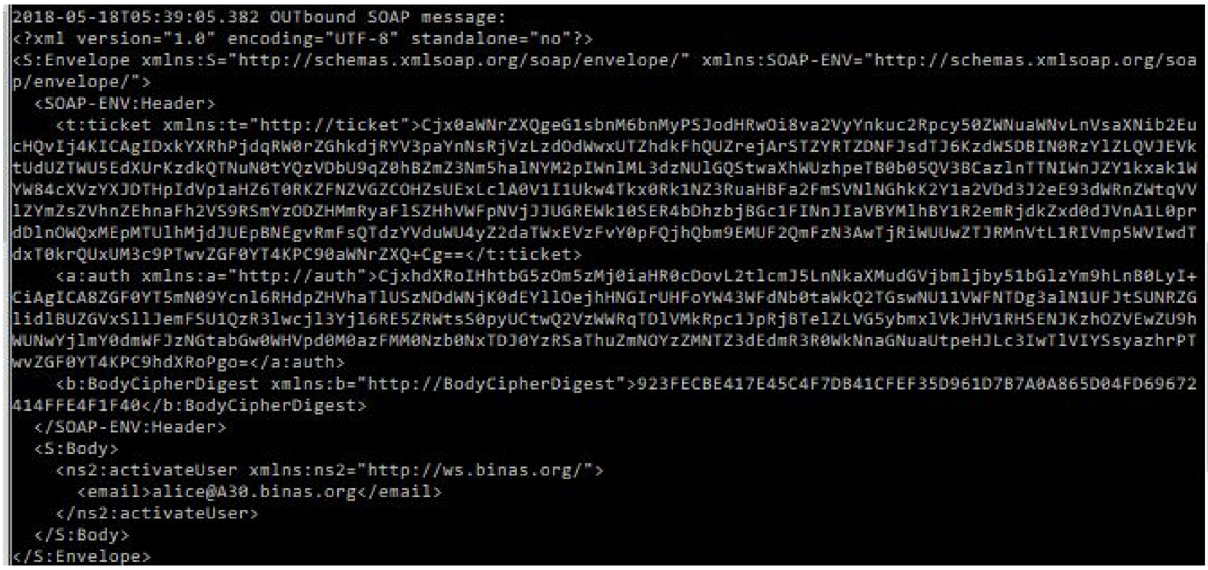
Realizamos a nossa terceira entrega utilizado a solução da primeira entrega apresentada pelo corpo docente da cadeira.

Fizemos o esquema para o exemplo de uma função que implica a utilização do email, mais em particular a activateUser.



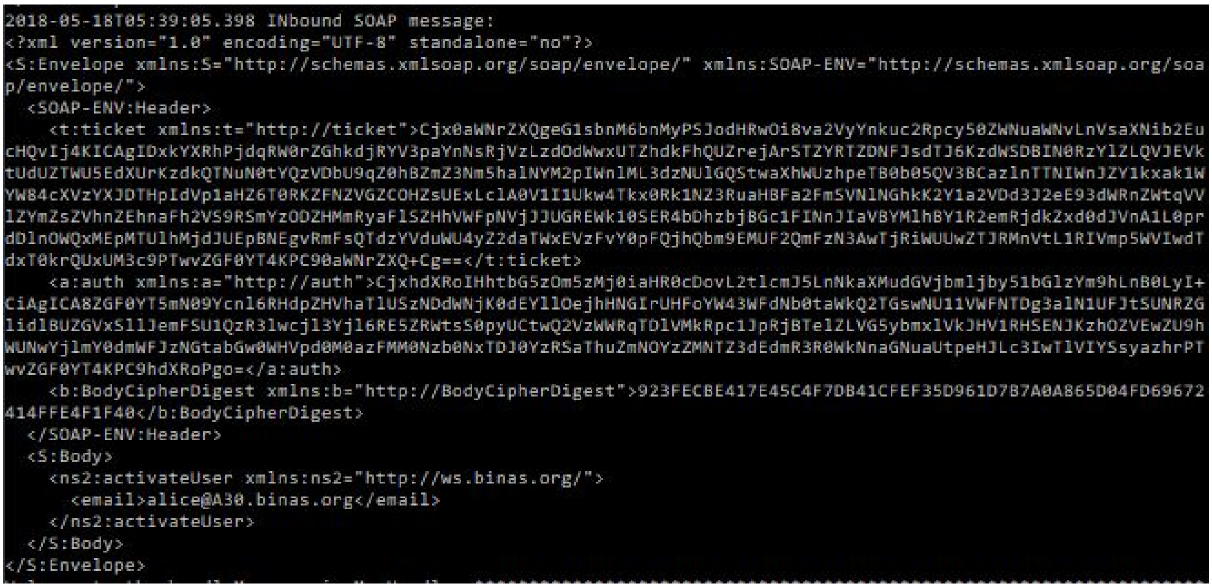
- KerberosClientHandler:
  - OutboundElement:
    - Através do Kerberos cifra o ticket e o auth, envia essa informação agora cifrada no SOAP num novo header;
  - InboundElement:
    - Através do Kerberos decifra o requestTime, gera um novo e compara-os;
- KerberosServerHandler:
  - OutboundElement:
    - Através do Kerberos cifra o requestTime e envia os no SOAP;
  - InboundElement:
    - Através do Kerberos decifra o ticket e o auth e cifra requestTime;
- BinasAuthorizationHandler:
  - OutboundElement:
    - Compara o email presente no SOAP Body com o email referente ao Auth e ao Ticket;
  - InboundElement:
    - Compara o email presente no SOAP Body com o email referente ao Auth e ao Ticket;
- MACHandler:
  - OutboundElement:
    - Codifica a mensagem (SOAP Body) e envia a chave e a mensagem;
  - InboundElement:
    - Codifica o SOAP Body e compara o com a mensagem, usando a chave recebida no SOAP, de modo a verificar se a informação foi corrompida ;

No MACHandler para gerar o body cifrado, usamos a sessionKey gerada no KerberosClientHandler, a qual enviamos através do SOAPCotntext. Se for detectada alguma infração, num dos handleres é enviada uma RuntimeException para o binas-cli.



```
2018-05-18T05:39:05.382 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/soa
p/envelope/">
  <SOAP-ENV:Header>
    <t:ticket xmlns:t="http://ticket">Cjx0aWNrZXQgeG1sbnM6bnMyPSJodHRwOi8va2VyYnkuc2Rpcy50ZWNuaWNvLnVsaXNib2Eu
cHQvIj4KICAgIDxkYXRhPjdqRW0rZGhkdjRYV3paYnNsRjVzLzdOdWwxUTZhdkFhQUZrejArSTZYRTZDNFJsdTJ6KzdWSDBIN0RzYlZLQVJEVk
tUdUZTWU5EdXUrKzdkQTNuN0tYQzVDbU9qZ0hBZmZ3Nm5halNYM2pIWnlML3dzNUlGQStwaXhWUzhpeTB0b05QV3BCazlnTTNIWnJZY1kxak1W
YW84cXVzYXJDTHpIdVp1aHZ6T0RKZFNZVGZCOHZsUExLclA0V1I1Ukw4Tkx0Rk1NZ3RuaHBFa2FmSVNlNGhkK2Y1a2VDd3J2eE93dWRnZWtqVV
lZYmZsZVhnZEhnaFh2VS9RSmYzODZHMmRyaFlSZHhVWFpNVjJJUGREWk10SER4bDhzbjBGc1FINnJIaVBYMlhBY1R2emRjdkZxd0dJVnA1L0pr
dDlnOWQxMEpMTUlhMjdJUEpBNEgvRmFsQTdzYVduWU4yZ2daTWxEVzFvY0pFQjhQbm9EMUF2QmFzN3AwTjRiWUUwZTJRMnVtL1RIVmp5WVIwdT
dxT0krQUxUM3c9PTwvZGF0YT4KPC90aWNrZXQ+Cg==</t:ticket>
    <a:auth xmlns:a="http://auth">CjxhdXRoIHhtbG5zOm5zMj0iaHR0cDovL2tlcmJ5LnNkaXMudGVjbmljby51bGlzYm9hLnB0LyI+
CiAgICA8ZGF0YT5mN09Ycnl6RHdpZHVhaTlUSzNDdWNjK0dEYllOejhHNGIrUHFoYW43WFdNb0taWkQ2TGswNU11VWFNTDg3alN1UFJtSUNRZG
lidlBUZGVxSllJemFSU1QzR3lwcjl3Yjl6RE5ZRWtsS0pyUCtwQ2VzWWRqTDlVMkRpc1JpRjBTelZLVG5ybmxlVkJHV1RHSENJKzhOZVEwZU9h
WUNwYjlmY0dmWFJzNGtabGw0WHVpd0M0azFMM0Nzb0NxTDJ0YzRSaThuZmNOYzZMNTZ3dEdmR3R0WkNnaGNuaUtpeHJLc3IwTlVIYSsyazhrPT
wvZGF0YT4KPC9hdXRoPgo=</a:auth>
    <b:BodyCipherDigest xmlns:b="http://BodyCipherDigest">923FECBE417E45C4F7DB41CFEF35D961D7B7A0A865D04FD69672
414FFE4F1F40</b:BodyCipherDigest>
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:activateUser xmlns:ns2="http://ws.binas.org/">
      <email>alice@A30.binas.org</email>
    </ns2:activateUser>
  </S:Body>
</S:Envelope>
```

SOAP Envelope do KerberosClientHandler - outboundElement



```
2018-05-18T05:39:05.398 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/soa
p/envelope/">
  <SOAP-ENV:Header>
    <t:ticket xmlns:t="http://ticket">Cjx0aWNrZXQgeG1sbnM6bnMyPSJodHRwOi8va2VyYnkuc2Rpcy50ZWNuaWNvLnVsaXNib2Eu
cHQvIj4KICAgIDxkYXRhPjdqRW0rZGhkdjRYV3paYnNsRjVzLzdOdWwxUTZhdkFhQUZrejArSTZYRTZDNFJsdTJ6KzdWSDBIN0RzYlZLQVJEVk
tUdUZTWU5EdXUrKzdkQTNuN0tYQzVDbU9qZ0hBZmZ3Nm5halNYM2pIWnlML3dzNUlGQStwaXhWUzhpeTB0b05QV3BCazlnTTNIWnJZY1kxak1W
YW84cXVzYXJDTHpIdVp1aHZ6T0RKZFNZVGZCOHZsUExLclA0V1I1Ukw4Tkx0Rk1NZ3RuaHBFa2FmSVNlNGhkK2Y1a2VDd3J2eE93dWRnZWtqVV
lZYmZsZVhnZEhnaFh2VS9RSmYzODZHMmRyaFlSZHhVWFpNVjJJUGREWk10SER4bDhzbjBGc1FINnJIaVBYMlhBY1R2emRjdkZxd0dJVnA1L0pr
dDlnOWQxMEpMTUlhMjdJUEpBNEgvRmFsQTdzYVduWU4yZ2daTWxEVzFvY0pFQjhQbm9EMUF2QmFzN3AwTjRiWUUwZTJRMnVtL1RIVmp5WVIwdT
dxT0krQUxUM3c9PTwvZGF0YT4KPC90aWNrZXQ+Cg==</t:ticket>
    <a:auth xmlns:a="http://auth">CjxhdXRoIHhtbG5zOm5zMj0iaHR0cDovL2tlcmJ5LnNkaXMudGVjbmljby51bGlzYm9hLnB0LyI+
CiAgICA8ZGF0YT5mN09Ycnl6RHdpZHVhaTlUSzNDdWNjK0dEYllOejhHNGIrUHFoYW43WFdNb0taWkQ2TGswNU11VWFNTDg3alN1UFJtSUNRZG
lidlBUZGVxSllJemFSU1QzR3lwcjl3Yjl6RE5ZRWtsS0pyUCtwQ2VzWWRqTDlVMkRpc1JpRjBTelZLVG5ybmxlVkJHV1RHSENJKzhOZVEwZU9h
WUNwYjlmY0dmWFJzNGtabGw0WHVpd0M0azFMM0Nzb0NxTDJ0YzRSaThuZmNOYzZMNTZ3dEdmR3R0WkNnaGNuaUtpeHJLc3IwTlVIYSsyazhrPT
wvZGF0YT4KPC9hdXRoPgo=</a:auth>
    <b:BodyCipherDigest xmlns:b="http://BodyCipherDigest">923FECBE417E45C4F7DB41CFEF35D961D7B7A0A865D04FD69672
414FFE4F1F40</b:BodyCipherDigest>
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:activateUser xmlns:ns2="http://ws.binas.org/">
      <email>alice@A30.binas.org</email>
    </ns2:activateUser>
  </S:Body>
</S:Envelope>
```

SOAP Envelope do KerberosServerHandler - inboundElement

Estas mensagens dizem respeito ao pedido de ActivateUser entre o Binas-Server e o Binas-Cliente.