Sistemas Distribuídos

Entrega 3 – Segurança

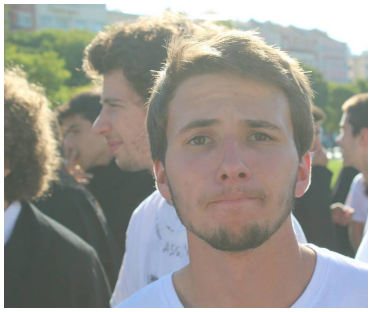
2017/2018

Grupo A37

https://github.com/tecnico-distsys/A37-SD18Proj

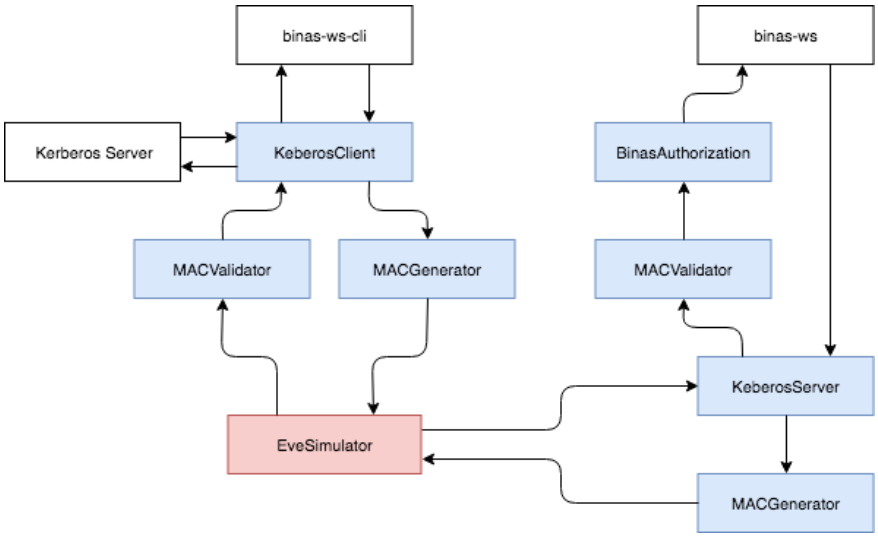
Francisco Pereira, 76196

Diogo Freitas, 81586



João Rodrigues, 83483

Figura de Segurança:



Nota: Todos os handlers (indicados a azul e vermelho) intercetam mensagens em ambos os sentidos. No entanto, de modo a proporcionar uma melhor compreensão da lógica por detrás da implementação deste projeto, indica-se na figura que alguns destes apenas recebem/enviam quando nenhuma ação é tomada.

Handlers:

- **KerberosClientHandler –** Permitindo a execução do protocolo Kerberos através da comunicação com um servidor Kerberos, tem como objetivo garantir a autenticidade do cliente. Para tal, aquando do envio de uma mensagem ao binas, gera um autenticador (*Auth*) e ir requisita um Ticket ao servidor Kerberos, através de um email sabido previamente estar registado no servidor em questão. Após conclusão destas tarefas, adiciona tanto o *Auth* como o Ticket enquanto *headers* à mensagem SOAP. Se, por outro lado, estiver a receber uma mensagem para o cliente, então valida o *requestTime* presente num *header*, lá colocado pelo binas de modo a garantir a frescura da mensagem.
- **KerberosServerHandler –** Ao receber uma mensagem para envio ao cliente, gera um *requestTime*, associando-o a um *header*. Isto permite garantir ao cliente de que esta resposta corresponde a um pedido feito recentemente, importante para garantir a frescura da mensagem. Recebendo uma mensagem para o binas, o objetivo passa por fazer a validação do Ticket e do *Auth* presentes nos *headers* da mensagem SOAP, lá colocados pelo KerberosClientHandler, verificando se consegue desencriptar o ticket com a sua chave, aceder à *sessionKey*, utiliza-la para aceder ao *Auth* e, finalmente, verificar a frescura da mensagem através do marcador temporal que encontra dentro do *Auth* e verificar se o cliente discriminado no *Auth* bate certo com o do Ticket.
- **MACGeneratorHandler –** Caso esteja a receber uma mensagem que vai fora, o objetivo do *handler* é a verificação da integridade da mensagem. Para tal, calcula o resumo do SOAPEnvelope(*body* + *headers*), gerando assim um MAC, adicionando-o à *header* correspondente. e gerado o *header* correspondente.
- **MACValidatorHandler –** Recebendo a mensagem, o objetivo deste *handler* é ir verificar que o MAC que vem com a mensagem está correto, garantindo assim que a mensagem recebida é exatamente igual à enviada pelo cliente/binas. Para tal, retira o *header* do MAC de forma a poder recalcular o MAC da mensagem enviada inicialmente. Se o resultado obtido for igual ao MAC recebido, então é comprovada a integridade da mensagem.

- **BinasAuthorizationHandler –** Recebendo a mensagem, o objetivo deste *handler* passa por garantir que qualquer pedido que envolva autenticação de um utilizador corresponda ao mesmo utilizador discriminado no *Ticket*, impedindo assim que um utilizador, na posse de um *Ticket* válido com um dado email, não faça pedidos ao binas em nome de outro utilizador.
- **EveSimulatorHandler –** Este *handler* será usado na demonstração do projeto e só entrará "em ação" para demonstrações de ataques ao sistema, alterando a mensagem SOAP a ser trocada entre o cliente e o binas.

Nota: Foram utilizados dois MACHandlers distintos (um para gerar e outro para validar) de modo a garantir integridade, não apenas do *Body* da SOAPMessage, mas também dos h*eaders*. Assim, caso os *Headers* sejam alterados, a mensagem não irá chegar ao binas/cliente. Uma alteração dos *headers* poderia ser do interesse de atacantes caso fossem utilizados *headers* para outros fins que não de segurança, como os presentes. Outro caso que é assim evitado é o de receção de uma mensagem cujos *headers Ticket* e *Auth* foram alterados para outros igualmente válidos, sem nunca ter sido alterado o *Body* da mensagem. Caso isso acontecesse, o binas iria receber pedidos que não necessitassem de um email (como o listStations), mas estaria a receber um *Ticket* e um *Auth* que não correspondiam ao cliente que realmente enviou a mensagem.

Mensagens:

Mensagem enviada para o binas de pedido de ativação de um utilizador:

```
2018-05-18T19:04:33.896 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>
    <kerby:auth xmlns:kerby="http://ws.binas.org/">8D91AD300964F90A7D0A970A8AEA12B512DD66FFC6F593DB1DE5FACD427DC7CC6FF8AA068A49457F9BF5DCC9082E8DDE481BE1FB4AAE51048A4D6C62287A864EF30FC7E57FE9BAAEF46F8F0414278558F598E77934B33D418E89792944349CE57BD36E8C5739B4120EC416511B2253AE28290E12C605F965D50F7B456DA734BFBB827A84B9DF9B60B591A60BDDB50E76EA8AABDB6C4E574403F53C2BE1290C558100640B7CA46C89B732D03C8E28397C</kerby:auth>
    <kerby:ticket xmlns:kerby="http://ws.binas.org/">AB55C97A873CD3E3782BC2CB83392252B16848C8308557B467EDC9FBF98F20803478E9A459F41EC772F73FEABF42235569BBA24AED35A5F96EEE54FAA29A3149D5B60C683C87A2E05938B83C2D26626780676A6A7492A4AD401447D846B28A2DDEB0F639762D387BE1FB6C8F6C26A9D6C9F0C8B72544D1957E0A0B3CCC5D9E888B6732051B8017D500570541DF80C276761BDD79139984A8E1861F9AC96B07A96573F2C9D9B4A1505D3A12E36CCEB76DC39ABA11CF5234886170E59908E9AB128419FB53D2289784ABA5F851A7018C992AEC3AE1066F64E33F7099C80762D8943333A55E3C28E76EB61F7ABEEB977BF8E3C283DA389A5210EC25E85304B3D53635F358C30CA5A02CDDB2E5DAEF70728E1A7B8503219A07346B71B936F6731AB33EC53CBCE07FFDF4BCD736EAEC2C5D4E</kerby:ticket>
    <kerby:MAC xmlns:kerby="http://ws.binas.org/">88BA7011CD7DE9C27E3ECF617DDB91A76BD30689F5B573CF9BD30B4A91D13653</kerby:MAC>
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:activateUser xmlns:ns2="http://ws.binas.org/">
      <email>alice@A37.binas.org</email>
    </ns2:activateUser>
  </S:Body>
</S:Envelope>
```

<kerby:auth>: *Header* contendo o *Auth* correspondente ao protocolo Kerberos
<kerby:ticket>: *Header* contendo o *Ticket* correspondente ao protocolo Kerberos
<kerby:MAC>: *Header* contendo o resumo da mensagem a ser enviada (excepto o próprio MAC)

Resposta do binas:

```
2018-05-18T19:04:34.296 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>
    <kerby:requestTime xmlns:kerby="http://ws.binas.org/">7237AD3550A876428D1994B22C34F09F02723003FDA2741646DFAE03972899CC8944F5944D052B4F8F63A4E52D2FB758FB3522C18E0F92EF90880C1B24D62837E24176D9D46D504FF4402674DC32B1D88903762A3DB30C32055BB3D066D271CCFC7D82C843694D1FC8B1F3D4F067A730403FA8CFD2BE77028143F22751AEE71C1E0570FAC18CB96A214BC318848A4C32F6C13CAC9EDCD9D19C3B0E8618F860D6</kerby:requestTime>
    <kerby:MAC xmlns:kerby="http://ws.binas.org/">B41B1E54A9A9457C44D2C130CFDF08FC6AA684D6F024D28CB5CA57C5FF6D0BE4</kerby:MAC>
  </SOAP-ENV:Header>
  <S:Body>
    <ns2:activateUserResponse xmlns:ns2="http://ws.binas.org/">
      <user>
        <email>alice@A37.binas.org</email>
        <hasBina>false</hasBina>
        <credit>10</credit>
      </user>
    </ns2:activateUserResponse>
  </S:Body>
</S:Envelope>
```

<kerby:requestTime>: *Header* contendo o *requestTime* correspondente ao protocolo Kerberos
<kerby:MAC>: *Header* contendo o resumo da mensagem enviada pelo binas (excepto o próprio MAC)