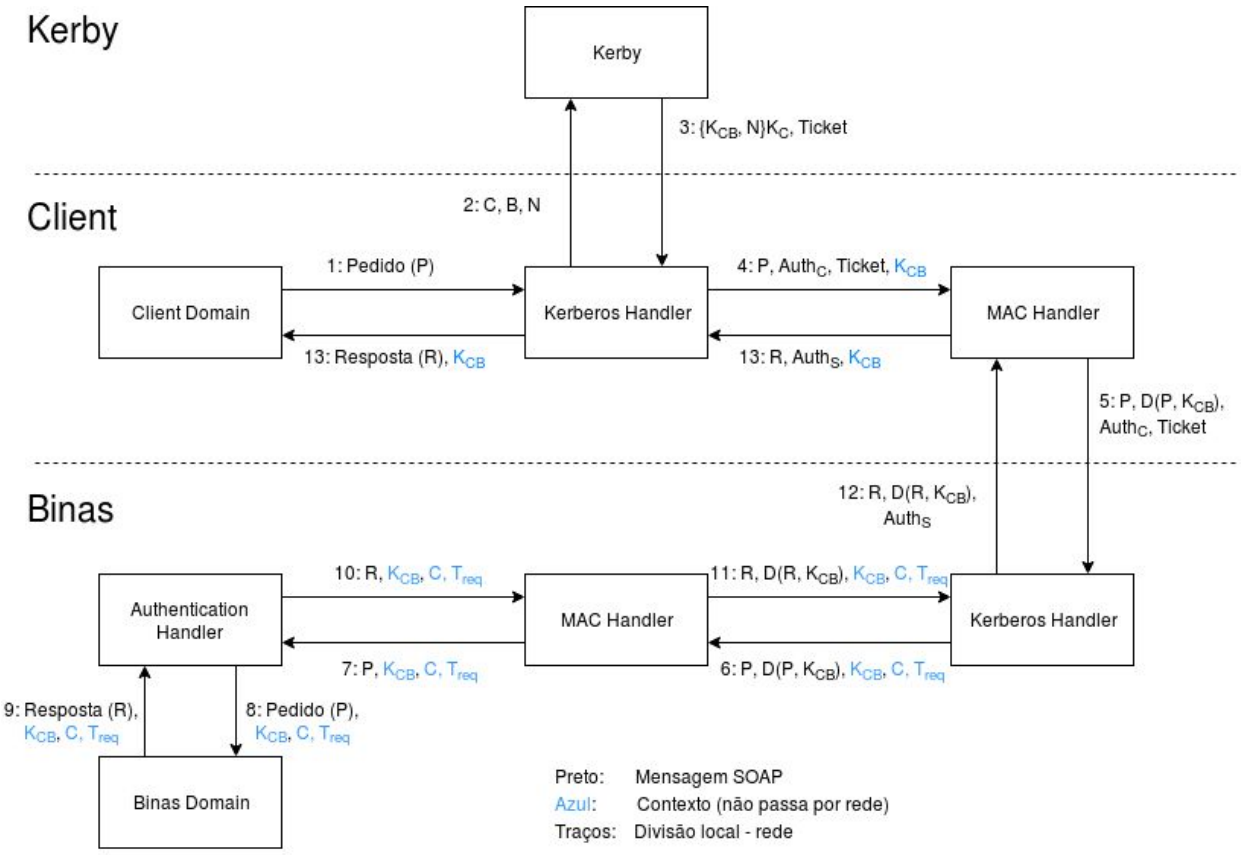
TÉCNICO LISBOA

Sistemas Distribuídos

Terceira Parte: Segurança

Grupo A17		https://github.com/tecnico-distsys/A17-SD18Proj
		
83448	83475	83504
Dorin Gujuman	Hugo Guerreiro	Manuel Vidigueira



- Sequência normal de envio de pedido. Nota: 2 e 3 só são executados se o Ticket anterior estiver expirado.

Kerberos Handler (Client)

Outbound

- Input: P (pedido/operação)

Caso não tenha um ticket ou este esteja expirado, gera um nonce (N), contacta o servidor Kerby e obtém novo ticket. Decifra a outra parte da resposta do Kerby usando K_C (gerada através da password em properties), verificando se o nonce retornado foi o enviado no pedido do Ticket, e guarda K_{CB} em contexto. Gera $Auth_C$ usando o tempo de sistema atual (milissegundos) e coloca-o, juntamente com o Ticket, no header da mensagem SOAP.

- Output: P, $Auth_C$, Ticket; Em contexto: K_{CB}

Inbound

- Input: R (resposta), $Auth_S$; Em contexto: K_{CB}

Decifra $Auth_S$ usando K_{CB} e verifica se o tempo é igual ao tempo enviado anteriormente em $Auth_C$.

- Output: R; Em contexto: K_{CB}

MAC Handler (Client)

Outbound

- Input: P, $Auth_C$, Ticket; Em contexto: K_{CB}

Gera um MAC usando P e K_{CB}, e coloca-o no header da mensagem SOAP.

- Output: P, D(P, K_{CB}), $Auth_C$, Ticket; Em contexto: K_{CB}

Inbound

- Input: R, D(R, K_{CB}), $Auth_S$; Em contexto: K_{CB}

Gera um MAC usando R e K_{CB} e compara com o MAC recebido, aceitando se igual.

- Output: R, $Auth_S$; Em contexto: K_{CB}

Kerberos Handler (Server)

Outbound

- Input: R, D(R, K_{CB}); Em contexto: K_{CB}, C, T_{req}

Gera $Auth_S$ usando o T_{req} em contexto e coloca-o no header da mensagem SOAP.

- Output: R, D(R, K_{CB}), $Auth_S$; Em contexto: K_{CB}, C, T_{req}

Inbound

- Input: P, D(P, K_{CB}), $Auth_C$, Ticket;

Decifra ticket usando K_B, põe K_{CB} em contexto e decifra $Auth_C$. Verifica que e-mail de $Auth_C$ corresponde ao e-mail no Ticket e põe-o em contexto (C). Verifica que T_{req} está dentro do intervalo de tempos do Ticket, que é mais recente que o último T_{req} que este cliente enviou (evita replay attacks), e que a sua "idade" é inferior um tempo fixo[1]. Põe T_{req} em contexto e guarda-o como sendo o mais recente.

- Output: P, D(P, K_{CB}); Em contexto: K_{CB}, C, T_{req}

MAC Handler (Server)

O comportamento é semelhante para o MAC Handler (Server), diferindo no conteúdo do corpo da mensagem usado para gerar o MAC (input P em vez de R, e vice-versa).

Authentication Handler (Server)

Outbound

- Input = Output

Não executa comportamento

Inbound

- Input: P; Em contexto: K_{CB}, C, T_{req}

Compara o e-mail C com o e-mail que consta na operação (pedido P), rejeitando se diferente.

- Output: P; Em contexto: K_{CB}, C, T_{req}

[1] Margem de manobra (menor possível) de tempo entre o envio (aproximadamente) da mensagem e a sua chegada. Valor utilizado ronda 1000 ms.