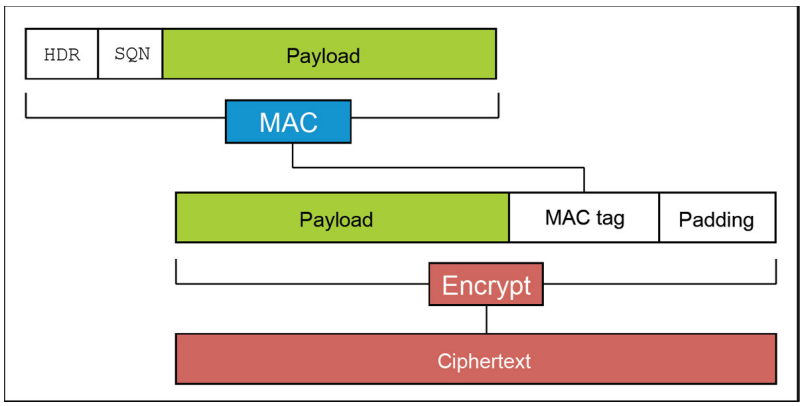
LEIC/LETI 2013/14, Repescagem do 2º Teste de Sistemas Distribuídos, 1/7/14

Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas. Duração: 1h30m

Grupo I [7,3v]

1. Em SSL/TLS, dois interlocutores (cliente e servidor) começam por estabelecer uma chave secreta (simétrica), K, entre eles. Depois da fase inicial, cada mensagem trocada entre ambos passa pelos passos ilustrados na figura seguinte:



(fonte: arstechnica.com)

a. [0,9v] De entre as componentes indicadas na figura, indique qual/quais asseguram os seguintes requisitos (indique "nenhuma" se o requisito não for assegurado neste protocolo).

i. Confidencialidade
ii. Integridade
iii. Autenticidade
iv. Não repúdio

b. [0,7v] Indique de forma clara o que a caixa "MAC" faz.

c. [0,9v] Indique uma vantagem e uma desvantagem de usar SSL/TLS em Web Services, relativamente a implementar segurança ao nível dos *SOAP handlers*.

d. O protocolo descrito acima é precedido por uma fase chamada "TLS handshake protocol", que pode envolver troca de certificados digitais de chave pública do servidor e/ou do cliente.

i. [0,9v] O SSL/TLS usa cifra híbrida. Como está a troca de certificados do "handshake protocol" relacionada com a cifra híbrida usada pelo SSL/TLS?

ii. [0,7v] Quando um cliente recebe o certificado de chave pública do servidor, o cliente precisa de conhecer mais informação para além da que está contida no certificado para o validar? Se sim, qual? Se não, justifique.

2. Considere as 2 primeiras mensagens do protocolo Needham-Schroeder de chave simétrica:

$$1.\ A \rightarrow S:\ \ A, B, N_A$$

$$2.\ S \rightarrow A:\ \ \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_B}\}_{K_A}$$

a. [0,9v] O que é a componente N_A enviada na mensagem 1 e para que serve? Ilustre com um exemplo de ataque que seria possível caso a componente N_A não existisse no protocolo.

b. [0,9v] Indique qual a 3ª mensagem do protocolo (indique emissor, destinatário e conteúdo da mensagem).

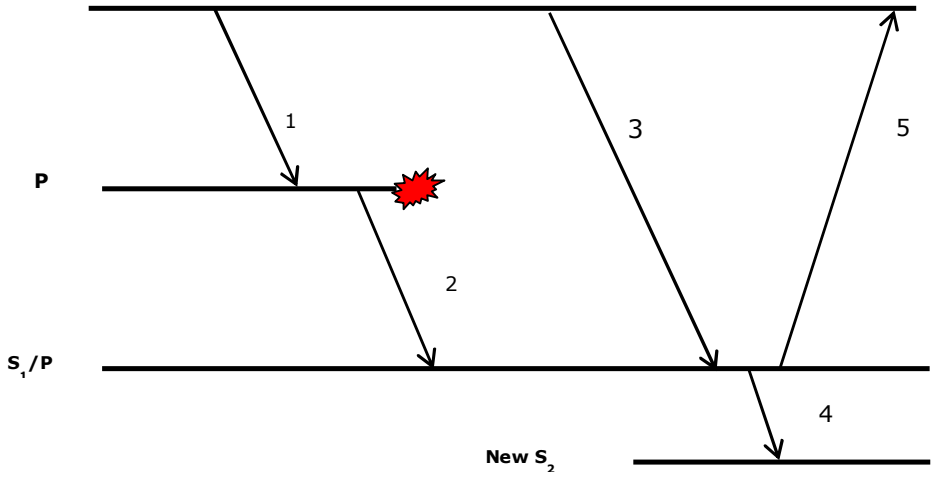
c. Após o protocolo terminar:

i. [0,7v] Quem conhece K_{AB}? Justifique.

ii. [0,7v] O que garante que K_{AB} foi distribuída de forma segura ao(s) interlocutor(es) que indicou na alínea anterior?

Grupo II [5,3v]

1. Considere este diagrama refente à execução do primary backup



a) [0,6v] Explique que mecanismo permite ao cliente detectar a falta e recuperar.

b) [0,6v] Explique como se evita que a operação seja executada duas vezes do servidor S1/P?

c) [0,6v] Qual a razão da existência de New S2 no diagrama. Justifique o que sucederia se não existisse esta componente.

d) [0,6v] Este protocolo garante sequencialidade linear (também chamada linearizabilidade/*linearizability*)? Se sim, justifique. Se não, ilustre com um exemplo.

2) Considere o protocolo de quóruns *quorum consensus* estudado nas aulas, para um sistema em que os serviços são apenas leituras e escritas de valores.

a) [0,6v] Que tipo de faltas dos servidores tolera este sistema?

b) [0,6v] Considere que pretende tolerar dois nós em falta . De quantos nós necessitaria?

c) [0,6v] Considerando o modelo de faltas dos nós, dê um exemplo de uma falta arbitrária. Seja objectivo na descrição da falta.

d) [0,6v] Compare a disponibilidade deste sistema com a de outro baseado em primary backup. **Assumindo que nunca falha mais que uma minoria de réplicas em simultâneo** Justifique.

e) [0,5v] Se o quórum for de pesos, o valor apresentado na alínea b) pode variar?

Grupo III [4v]

1. A maioria dos livros tem um código ISBN (**International Standard Book Number**).

   a) [0,6v] Classifique-o como URL, URN, URI. Justifique a sua classificação.

   b) [0,6v] Poderia utilizá-lo como uma tag de um namespace? Justifique .

2. Um espaço de nomes tem de garantir a unicidade referencial.
   a) Uma possibilidade para garantir essa propriedade baseia-se na utilização da difusão.
      i) [0,7v] Explique como.

      ii) [0,7v] O DNS não utiliza esta técnica, porquê? Justifique.

3. O DNS tem uma arquitectura em que vários servidores contem uma réplica da informação para tornar o serviço mais disponível.
   a) [0,7v] Quando pretende modificar um nome, não se utiliza um mecanismo de transacções atómicas para garantir a consistência. Porquê?

b) [0,7v] O sistema pode dispor de réplicas do servidor principal. A função destes servidores e das caches: (i) é a mesma; (ii) têm funções diferentes; ou (iii) têm algumas análogas e outras diferentes? Justifique.

Grupo III [3,4v]

1. Considere o seguinte programa cliente (em pseudo-código):

```
1 openTransaction();
2 reserva comboio Lisboa – Porto;
3 reserva comboio Porto – Vigo;
4 reserva hotel;
5 closeTransaction();
```

Considere que as linhas 2-4 são invocações remotas a diferentes servidores (S_2, S_3, S_4, respetivamente) e que é usado o protocolo 2-phase commit.

a. [0,9v] Represente num diagrama seguinte as mensagens que são trocadas durante a execução das linhas 1 e 2.

b. [0,9v] Represente no diagrama seguinte todas as mensagens trocadas durante a execução da linha 5, assumindo situação sem falhas nem atrasos.

c. O 2PC usa timeouts:

i. [0,9v] Descreva 2 situações distintas onde, perante timeout, o coordenador ou participante tomam uma decisão unilateral no protocolo.

ii. [0,7v] O facto do 2PC se basear em timeouts significa que o 2PC só funciona corretamente num sistema síncrono? Justifique.
