LEIC/LETI – 2013/14, 2º Teste de Sistemas Distribuídos, 17 de Junho de 2014

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

Grupo I [8v]

Considere um portal de reserva de viagens que permite aos utilizadores comprarem viagens, agindo de intermediário entre turistas e operadoras de viagens.

Quando um cliente - a correr em nome de um dado utilizador, *U* - pede ao portal (*P*) para comprar uma determinada viagem, *P* responde com a seguinte mensagem:

$$P\text{->}U: \underbrace{\{senha\}_{Kx}\ ,\ detalhes\ da\ reserva}_{M},\ \{resumo(M)\}_{Ky}$$

A mensagem acima transporta uma senha secreta que, no início da viagem, o utilizador deverá comunicar à empresa que oferece a viagem para provar que fez a compra, logo tem direito à viagem.

Na mensagem acima, considere que:

- "{}" significa cifragem assimétrica.
- Tanto o portal *P* como cada utilizador *U* dispõem de um par de chaves assimétricas: $K_{pub(P)}$, $K_{priv(P)}$, $K_{pub(U)}$, $K_{priv(U)}$, respetivamente. As chaves públicas foram previamente partilhadas entre os interlocutores de forma segura.

1. Quanto à componente $\{senha\}_{Kx}$:
   a. [0,7v] De entre as chaves $K_{pub(P)}$, $K_{priv(P)}$, $K_{pub(U)}$, $K_{priv(U)}$, a qual corresponde Kx?

   b. [0,8v] Escutando a mensagem que passou pela rede, observou-se o seguinte extrato:
   `TWFuIGlzIGRpc3RpbmdlaXN...`
   É este o resultado retornado diretamente pela função de cifra? Justifique.

2. A componente $\{resumo(senha)\}_{Ky}$ corresponde a uma assinatura digital de chave pública.
   a. [0,7v] De entre as chaves $K_{pub(P)}$, $K_{priv(P)}$, $K_{pub(U)}$, $K_{priv(U)}$, a qual corresponde Ky?

   b. [0,8v] Apresente o pseudo-código do algoritmo que U executa para validar a assinatura que recebe.

   c. [0,9v] Indique um ataque que seria possível caso a mensagem não levasse uma assinatura digital. Seja claro nos passos que o atacante segue para executar o ataque e no benefício que o atacante obteria do ataque. (Nota: não se aceitam ataques que apenas visam o vandalismo.)

d. O uso de um MAC em vez da assinatura digital de chave pública seria possível caso ambos os interlocutores partilhassem uma chave simétrica, K.

i. [0,8v] Em que consistiria o MAC de M? Apresente sucintamente a expressão de cálculo do MAC.

ii. [0,8v] No contexto deste sistema, recomendaria ou desaconselharia essa solução? Justifique.

3. O cliente de U conheceu a chave pública de P num certificado digital de chave pública que obteve numa pesquisa na Web, a partir de um site de origem duvidosa.

a. [0,9v] U tem forma de confirmar que a chave pública contida no certificado é legítima? Se sim, indique os passos que U segue para chegar a essa confirmação. Se não, indique uma alternativa correta.

b. [0,8v] Considere que o certificado que U recebeu foi emitido pela CA_2, que por sua vez é uma sub-CA da CA raiz CA_1. U não conhece CA_2 mas tem instalado o certificado de chave pública de CA_1. Como deve U proceder?

4. [0,8v] Quanto à abordagem seguida para autorizar o acesso às viagens neste sistema, como a classifica: lista de controlo de acessos ou capacidades? Justifique.

Grupo II [4v]

1. Considere uma invocação de um cliente a um serviço em RPC (em qualquer das tecnologias que aprendeu). Considere o pressuposto que pretende tolerar faltas silenciosas do servidor (também designadas por faltas de paragem – crash).

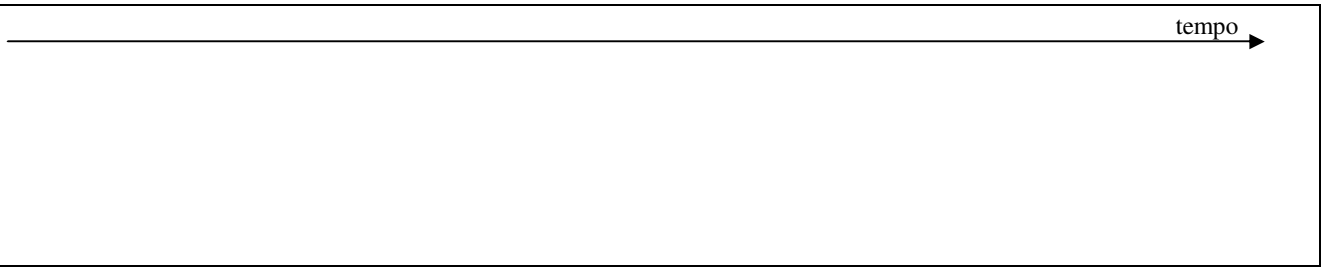
a) [0,7] Explique o que caracteriza uma falta silenciosa.

b) [0,7] Que implicação tem assumir que as faltas dos servidores são silenciosas (e não outro tipo de faltas) no grau de replicação? Justifique com um exemplo.

2. O protocolo de primary backup, que aprendeu nas aulas teóricas, com dois servidores tolera uma falta silenciosa de um servidor.
   a) [0,7] Que pressuposto ou pressupostos tem esse protocolo sobre as faltas da rede?

   b) Um dos pressupostos é que o sistema é síncrono, o que implica que todas as mensagens e processamento são executados dentro de um período máximo de tempo.
      i) [0,7] Dê um exemplo de uma situação em que o sistema falha se eliminar este pressuposto.

      ii) O protocolo de quórum (*quorum consensus*, ensinado nas aulas) tolera o funcionamento assíncrono do sistema.
         (1) [0,7] Explique com um exemplo.



         (2) [0,5] Como compara o grau de replicação deste protocolo com o primary backup?

Grupo III [4v]

Excerto do IDL

```
program BANCOPROG {
  version BANCOVERS {
    ……;
  } = 1;
} = 0x20000005;
```

Excerto do programa de ligação ao servidor

```
void main (int argc, char *argv[]){
  CLIENT *cl;
  int a, *result;
  char* server;
  server = argv[1];
  cl = clnt_create(server, BANCOPROG, BANCOVERS, "tcp");
  if(cl == NULL) {
      clnt_pcreateerror(server);
      exit(1);
  }
  ……
}
```

1. O excerto de programa acima implica a utilização de um serviço de nomes.
   a) [0,6] Explique qual a função deste serviço de nomes no Sun-RPC.

   b) [0,6] Este serviço é uma alternativa ao DNS ou este continua a ser necessário? Justifique.

   c) Considerando o nome do serviço (`BANCOPROG, BANCOVERS):`
      i) [0,4]Como o classifica quanto ao âmbito? Justifique.

      ii) [0,5] Do ponto de vista das propriedades dos nomes, indique **duas** diferenças relevantes entre este nome e o URL que é utilizado na invocação dos Web Services.

2. Considere a frase: "a disponibilidade do serviço de nomes pode determinar a disponibilidade de um serviço"
   a) Com o conhecimento que tem da invocação de serviços em Web Services, **apresente um exemplo**:
      i) [0,4] De uma forma de utilização dos Web Services que esta frase não tem sentido.

      ii) [0,4] De uma forma de utilização dos Web Services em que a frase tem sentido.

   b) [0,5] Que técnica(s) conhece para mitigar o problema da disponibilidade dos serviços de nomes? Explique como o DNS a utiliza.

3. [0,6] Uma preocupação nas soluções de tolerância a faltas é que não invalidem propriedades de soluções centralizadas. Uma dessas propriedades é a serialização das operações. Acha que a arquitetura que referiu do DNS garante esta propriedade? Justifique.

Grupo IV [4v]

Considere o seguinte programa transacional, que efetua um conjunto de reservas de viagens sobre diferentes operadores. Assuma que o protocolo de terminação atómica é o 2-phase commit (2PC).

```
1 Boolean reservarViagens(List<Reserva> reservas) {
2  tx = openTransaction();
3  for each (Reserva r in reservas) {
4    Endpoint e = r.obterOperador();
5    if (e.reservarViagem(r, tx) == false) {
6      abortTransaction(tx);
7      return false;
8    }
9  }
10 closeTransaction(tx);
}
```

1. [0,7v] Indique uma razão que levou o programador a incluir as linhas 3-9 numa transação.

2. [0,7v] Indique que linhas correspondem a invocações sobre o coordenador do 2PC.

3. [0,8v] A transação distribuída pode abortar caso o programa chegue à linha 6. Há outras situações em que a transação distribuída aborte? Se não, justifique. Se sim, indique uma dessas situações em detalhe.

4. Assuma que o método é chamado com reservas no argumento, geridas pelos servidores A, B e C, respetivamente.
   a. [0,9v] Ao chegar à linha 10, qual o estado que cada processo (coordenador, A, B e C) mantém associado à transação distribuída? Justifique.

Coordenador:

Servidores A, B, C:

   b. [0,9v] Apresente num diagrama as mensagens que são trocadas quando a linha 10 se executa. Assuma um cenário em que o servidor A está em falha silenciosa durante o seu exemplo todo; todos os outros servidores estão corretos.