

Exame (Recurso)

Linguagens e Modelos de Concorrência e Segurança

15 Julho 2008

I

1. Considere os seguintes processos CCS:

$$\begin{aligned} USER &\triangleq \overline{\text{login}}.DO \\ DO &\triangleq \overline{\text{use}}.\overline{\text{logout}}.done.USER \\ MAC &\triangleq \text{login}.LOOP \\ LOOP &\triangleq \text{use}.LOOP + \text{logout}.MAC \\ SYS &\triangleq (\text{new } \text{login}, \text{use}, \text{logout})(USER \mid MAC) \end{aligned}$$

- (a) Explique que sistemas $USER$, MAC e SYS estão a modelar.
(b) Seja

$$WORLD \triangleq done.WORLD$$

Indique justificando se $WORLD \sim SYS$.

- (c) Seja $MACC \triangleq (\text{new } \text{use})MAC$. O sistema $MACC$ é idêntico a MAC , mas a acção use fica restrita ao sistema.
(1) Escreva em CCS uma especificação $SPEC$, o **mais simples** possível, e que caracterize o comportamento de $MACC$, isto é tal que $MACC \sim SPEC$.
(2) Indique se $MACC$ pode atingir uma situação de bloqueio (deadlock).

2. Considere a seguinte especificação CCS:

$$SPEC \triangleq AliceHasIt.SPEC + BobHasIt.SPEC$$

$SPEC$ especifica o comportamento observável de um sistema $GROUP$ constituído por dois processos concorrentes, $ALICE$ e BOB , que competem pelo uso de um recurso. Quando tem o recurso em seu poder, $ALICE$ emite a mensagem $AliceHasIt$, quando tem o recurso em seu poder, BOB emite a mensagem $BobHasIt$. Implemente o sistema $GROUP$ com base em três processos independentes, $ALICE$, BOB e

$$RESOURCE \triangleq \overline{\text{get}}.\overline{\text{release}}.RESOURCE$$

Mostre a equivalência entre a especificação e a implementação usando a ferramenta MWB e envie a sua solução por email.

II

1. Considere um sistema constituído por dois processos *MARIA* e *MANEL* que apenas apresentam um canal público livre *public*. *MARIA* e *MANEL* pretendem, através de um protocolo de comunicação conveniente, chegar a acordo sobre um identificador (um nome / nonce) novo, não existente previamente, e que no fim seja apenas conhecido de ambos. Tanto *MARIA* como *MANEL* podem apenas usar o canal *public* uma única vez.
 - (a) Apresente um modelo em PI do sistema considerado sob a forma de uma especificação sequencial simples, sem usar composição paralela.
 - (b) Apresente um modelo em PI em que *MARIA* e *MANEL* são representados por processos independentes concorrentes.
 - (c) Mostre como exprimir as seguintes propriedades do sistema que descreveu na alínea (b).
 - O sistema tem sempre menos que 2 threads independentes.
 - O sistema pode atingir um estado de bloqueio (deadlock).
 - O sistema possui inicialmente dois threads independentes e qualquer um desses threads tem possibilidade de usar o canal *public*.
 - O sistema atinge um estado em que tem exactamente duas componentes partilhando um nome privado.
 - (d) Verifique as propriedades acima na ferramenta SLMC, **interpretando os resultados**, e envie a sua solução por email.

III

Considere o seguinte protocolo criptográfico entre dois principais *A* e *B* e um servidor *S*. O protocolo usa criptografia simétrica e criptografia assimétrica em diferentes interações. Inicialmente, *A* e *B* conhecem a chave pública PK_S de *S*.

$$\begin{aligned} A \rightarrow S &: idb, \{K_a\}_{PK_S} \\ S \rightarrow B &: ida \\ B \rightarrow S &: ida, \{K_b\}_{PK_S} \\ S \rightarrow A &: idb, \{K_b\}_{K_a} \end{aligned}$$

O objectivo é que os dois principais *A* e *B*, após executar o protocolo partilhem uma nova chave simétrica KAB' , conhecida apenas por ambos (e pelo servidor, que é assumido como confiável).

Considere a propriedade de confidencialidade seguinte: *se no fim do protocolo A e B trocarem mensagens cifradas com as chave K_b , o conteúdo de tais mensagens não poder ser adquirido por nenhum atacante em tempo útil.*

1. Modele o sistema numa variante adequada do modelo SPI.

Justifique se o seu modelo satisfaz a propriedade de confidencialidade indicada em cima. Modele o sistema na ferramenta Proverif e verifique a propriedade de confidencialidade referida (envie a sua solução por email).