Ambientes de Execução Seguros
2º Semestre, 2021/22

1º Exame
29 de junho de 2022

- Todas as perguntas têm a mesma cotação.
- A duração total do exame é de 3 horas.

1. Um dos mecanismos fundamentais de uma *Trusted Computing Base* (TCB) é a existência de mecanismos de hardware e software que permitem concretizar um monitor de controlos de acesso, o qual terá como reponsabilidade a proteção de recursos partilhados do sistema. Explique como é que os sistemas operativos (software) exploram funcionalidades do hardware, nomeadamente do CPU, para concretizar este monitor de controlo de acesso.

2. Explique por que razão uma aplicação não pode interferir arbitrariamente com as estruturas de dados guardadas em memória pelo núcleo de um sistema operativo.

3. Explique que informação é que um sistema operativo normalmente usa para controlar o acesso de um processo a um ficheiro.

4. Considere os espaços de nomes do Linux (Linux *namespaces*), nomeadamente o de processos. Explique de que forma o mesmo pode ser usado como mecanismo de segurança.

5. Explique, de uma forma sucinta mas objetiva, o que distingue uma contentor LXC de uma máquina virtual executada sobre um determinado sistema operativo.

6. Explique que tipo de controlo se consegue realizar com o mecanismo AppArmor.

7. Certas aplicações podem ter interesse em descobrir se estão a executar num ambiente suportado por uma máquina virtual. Explique de que forma podem fazer essa descoberta.

8. O mecanismo SGX da Intel permite executar partes de aplicações em ambientes protegidos, denominados enclaves. Estes enclaves podem comunicar com o exterior através de funções especiais, desginadas por *ecalls* ou *ocalls*. Explique por que razão estas funções são especiais.

9. Os enclaves SGX possuem duas identidades: a sua própria e a do seu assinante, ou selador (*sealing identity*). Explique:
    a. Como se calculam estas duas identidades?
    b. Qual é o seu interesse no âmbito da produção de chaves para uso interno dos enclaves?

10. Considere o mecanismo ARM TrustZone. Como é que o mesmo garante a proteção da memória RAM usada pelo *Secure World*?

11. Explique como funcionava o modelo de *secure boot* proposto no âmbito do AEGIS (não precisa de referir o processo de recuperação).

12. Explique os princípios fundamentais para a atestação do arranque de um sistema computacional.

13. Segundo a TCPA (*Trusted Computing Platform Alliance*), há dois modos de arranque (*boot*): autenticado/confiável (*authenticated/trusted*) e seguro (*secure*). Explique as diferenças entre ambos.

14. Explique em que consiste um arranque sob avaliação (*measured boot*) dos sistemas operativos Windows.

15. Um arranque seguro via UEFI (UEFI *secure boot*) garante a correção dos módulos de *firmware* carregados durante o arranque de um sistema através de registos colocados em bases de dados locais, sendo uma delas a dbx (*blacklist*). Explique para que serve e como é usada esta base de dados.

16. O mecanismo de *hash extends* (dispersões extendidas) é usado pelo TPM como base para atestação. Explique:
    a. Como funcionam?
    b. Por que razão são uteis para atestação?

17. Cada uma das 4 hierarquias do TPM possui uma árvore de chaves, as quais começam em chaves primárias. Explique o processo de criação destas chaves.

18. Um TPM tem a capacidade de exportar dados gerados dentro de si de tal forma que, mais tarde, consegue verificar que foram por si gerados aquando de uma futura importação. Explique como.

19. O TPM permite assinar (com uma chave privada conhecida apenas por si) dados calculados internamente por si ou dados fornecidos a partir do exterior. Como é que o TPM consegue evitar que os dados fornecidos a partir do exterior simulem dados calculados internamente?

20. Os smartcards possuem uma interface de comunicação mestre-escravo, baseada em mensagens designadas por APDU (*Application Protocol Data Unit*). Estes APDU permite manipular entidades do smartcard, como é o caso do seu sistema de ficheiros. Porém, tem de haver uma sincronização no acesso concorrente de várias aplicações a um dado *smartcard*. Explique:
    a. Por que razão tal é necessário?
    b. Como é que tal é feito?