Identificação, Autenticação e Autorização
2º Semestre, 2020/21

2º Exame
14 de julho de 2021

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

1. Considere o sistema de controlo de integridade obrigatório do Windows. Explique como funciona.

2. Um *Access Token* do Oauth 2.0 pode ser considerado como uma capacidade? Justifique.

3. O modelo de controlo de acesso baseado em papeis (*Role-Based Access Control*, RBAC) pode ter uma variante que permite restrições (*constraints*), tal como a separação de deveres (*separation of duties*). Explique que vantagens podem advir da exploração desta variante.

4. Os modelos de controlo de fluxos de informação podem usar compartimentos, ou categorias, para classificar sujeitos e objetos para além da sua certificação de segurança (*security clearance*) e classificação de segurança (*security classification*), respetivamente. Explique que vantagens advém dessa classificação adicional.

5. O padrão PKCS #11 define uma interface para *cryptotokens* (equipamentos criptográficos). Explique que utilidade podem ter estes equipamentos, e esta interface, para operações de autenticação.

6. Considere a arquitetura PAM (*Pluggable Authentication Modules*). Explique de que forma é que a mesma dá total liberdade ao administrador de uma máquina para definir os métodos de autenticação de uma aplicação em particular (que use o PAM, naturalmente).

7. Explique em que consistem os ataques com dicionários a protocolos de autenticação.

8. O protocolo de autenticação do GSM é imune a ataques de dicionário. Explique porquê.

9. Explique como é realizada a autenticação dos servidores no SSH.

10. Considere a arquitetura de autenticação 802.1X. Explique qual a relevância para a mesma da existência (e uso) do protocolo EAP (*Extensible Autentication Protocol*)?

11. Explique em que consiste o conceito de *Single Sign-On* (SSO).

12. Considere uma interação via SAML (*Security Assertion Markup Language*) entre um IdP (*Identity Provider*) e um SP (*Service Provider*). Explique como é que o SP se assegura que a informação que recebe vem efetivamente do IdP.

13. Considere o conceito de autenticação biométrica. Na mesma é preciso calibrar o equipamento que faz a leitura das características biométricas de modo a ajustar duas taxas: a de falsos negativos (*False Rejection Rate*, FRR) e a de falsos positivos (*False Acceptance Rate*, FAR). Explique por que razão esta calibração pode ser complexa em cenários reais.