Identificação, Autenticação e Autorização
2º Semestre, 2021/22

1º Teste
19 de maio de 2022

- Todas as perguntas têm a mesma cotação.
- A duração total do teste é de 2 horas.

1. O modelo de controlo de acesso baseado em papéis (*Role-Based Access Control*, RBAC) é normalmente preferível para sistemas de informação em vez dos sistemas baseados em ACL (*Access Control List*) típicos dos sistemas de ficheiros. Explique porquê.

2. As políticas de controlo de acesso baseadas em papéis (*Role-Based Access Control*, RBAC) podem ser aperfeiçoadas através da inclusão de mecanismos suplementares. É o caso do modelo NIST, onde o Flat RBAC permite o mecanismo *user-role review*, e do Symmetric RBAC, que permite o mecanismo *permission-role review*. Explique:
   a. Em que consiste o *user-role review*?
   b. Em que consiste o *permission-role review*?

3. O sistema operativo Windows tem mecanismos de controlo de integridade para processos e diretorias que são parecidos com o modelo de integridade de Biba. Explique:
   a. Como funciona o modelo de integridade de Biba?
   b. Como funcionam os mecanismos de controlo de integridade do Windows?

4. As *capabilities* do Linux permitem associar privilégios a aplicações concretas. Explique:
   a. Como é que são associadas às aplicações?
   b. Quais as vantagens que têm relativamente ao uso do mecanismo Set-UID?

5. Considere o conceito de *Control Groups* (cgroups) do Linux. Explique de que forma os mesmos podem ser usados para controlar o uso de recursos por processos.

6. O OAuth 2.0 é uma norma que permite conceder direitos de acesso a recursos. Indique:
   a. Quem são as entidades consideradas na mesma.
   b. Como se autenticam entre si (considere o fluxo base, *authorization code flow*).

7. O Oauth 2.0 permite o acesso a recursos protegidos com base em *access tokens*. Explique:
   a. Que entidade fornece estes *access tokens*?
   b. Que entidade autoriza o fornecimento destes *access tokens*?

8. A gestão de identidades agregada, baseada num IdP (*Identity Provider*) para vários serviços (*Service Providers*) permite evitar uma gestão de identidades baseada em silos. Explique:
   a. Quais são as desvantagens da gestão de identidades baseada em silos?
   b. Qual é uma potencial desvantangem para a privacidade de uma pessoa que advém do uso de um IdP para vários serviços?

9. A proteção do anonimato dada por uma política de k-anonimato pode não ser suficiente, podendo ter de ser complementada com uma política de ℓ-diversidade. Explique em que consiste cada uma.

10. Como é que normalmente os sistemas operativos guardam de forma protegida as credenciais de acesso (senhas) que os seus utentes usam para iniciar uma sessão?