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

1º Exame
30 de junho de 2021

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

1. Para efeitos de autenticação de servidores Web na Internet é fundamental a existência de certificados de chave pública e de cadeias de certificação aceites de forma generalizada. Explique porquê.

2. Considere o padrão PKCS #11. Explique o que é (ou para que serve)?

3. Considere a arquitetura PAM (*Pluggable Authentication Modules*) e a autenticação multimétodo (*multi-factor).* Explique de que forma é que a primeira facilita a concretização da segunda.

4. Considere os ataques em modo desligado (*off-line*) com dicionários a protocolos de autenticação. Explique em que consistem.

5. Explique como funciona o protocolo de autenticação do GSM.

6. A autenticação no SSH é mútua, mas não similar em cada sentido, nem integrada no mesmo protocolo. Explique porquê.

7. Considere a arquitetura de autenticação 802.1X. Explique como é que na mesma podem ser concretizados sistemas de autenticação federada (considere o caso da eduroam)?

8. O modelo de controlo de acesso baseado em papeis (*Role-Based Access Control*, RBAC) é normalmente preferível para sistemas de informação em vez dos sistemas baseados em ACL típicos dos sistemas de ficheiros. Explique em que consiste o modelo RBAC.

9. Considere os modelos de controlo de fluxos de informação. Explique como é que os mesmos atuam tendo em conta certificações de segurança (*security clearance*s) e classificações de segurança (*security classifications*).

10. A gestão de identidades agregada, baseada num IdP (*Identity Provider*) para vários serviços (*Service Providers*) é normalmente usada para concretizar o conceito de *Single Sign-On* (SSO). Explique como é normalmente concretizado, na prática, para aplicações Web.

11. Considere uma interação via SAML (*Security Assertion Markup Language*) entre um IdP (*Identity Provider*) e um SP (*Service Provider*). Qual é o serviço que o SP requer do IdP via SAML?

12. Considere o conceito de autenticação biométrica. Indique, justificando:
    a. Duas vantagens.
    b. Duas desvantagens.

13. Considere o protocolo de autenticação S/Key. Explique de que maneira explora uma *hashing chain* para gerar uma sequência de senhas descartáveis (*One-Time Passwords*, OTPs)?

14. O Kerberos usa os conceitos de bilhete (*ticket*) e de chaves de sessão. Explique de que forma esses conceitos são usados para concretizar um ambiente com *Single Sign-On* (SSO)?

15. Como é que no Kerberos um serviço obtém de forma fidedigna a identidade da origem de uma mensagem, a partir de um bilhete (*ticket*) e de um autenticador (*authenticator*) da mesma?

16. 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.

17. O OAuth 2.0 é uma norma que permite conceder direitos de acesso a recursos. Indique quem são as entidades consideradas na mesma e qual o seu papel.

18. O anonimato é uma condição que depende não do próprio (o que quer manter o anonimato) mas do atacante (o que quer quebrar o anonimato). Explique o que é um conjunto de anonimização.

19. Os sistemas de gestão de identidade baseados em IdP (*Identity Providers*) agregam diversos atributos de identidade para vários serviços (*Service Providers*). Explique qual é o seu modelo normal de operação?

20. O IKE2 é um protocolo que permite negociar *Security Associations* IKE e IPSec. Explique para que serve cada um destes tipos de *Security Associations*?