

FAKULTA INFORMATIKY
MASARYKOVA UNIVERZITA



PV157
Autentizace a řízení přístupu

Otázky

14. dubna 2019

Multiple choice

1. Generátory passcode slouží pro

- (a) Urychlení generování sekvenčních čísel
- (b) Bezpečné uložení dlouhodobých klíčů
- (c) Realizaci challenge-response (výzva-odpověď) protokolu
- (d) Personalizaci elektronických pasů

Správně: b, c

2. Český elektronický pas druhé generace s autentizací čipu:

- (a) Lze naklonovat snadno, pokud známe data z MRZ
- (b) Nelze snadno naklonovat (vyžaduje získání soukromého klíče pasu, který nelze z pasu vyčíst) a proto klonování českého pasu zatím nebylo veřejně předvedeno.
- (c) Lze naklonovat jen pokud spolupracuje skutečný držitel pasu a zná svůj PIN

Správně: b

3. Jaký typ paměti je typicky používán u současných čipových karet?

- (a) DRAM
- (b) SRAM
- (c) GRAM
- (d) EEPROM

Správně: b, d

4. Které z následujících dělení modelů řízení přístupu není používáno:

- (a) řízené pravidly / náhodné
- (b) seznam přístupových oprávnění (capabilities) / seznam přístupových práv (ACL)
- (c) synchronní / asynchronní
- (d) symetrické / asymetrické
- (e) volitelné / povinné
- (f) centralizované / decentralizované

Správně: a, c, d

5. Komerční biometrická řešení oproti forenzním nabízí

- (a) plně automatizované systémy.
- (b) možnost opakovaného vytvoření nedostatečně kvalitních registračních vzorků.
- (c) vyšší přesnost.
- (d) uchování zpracovaných charakteristik včetně biometrických vzorků.

Správně: a, b

6. Slabá bezkoliznost u hašovacích funkcí znamená

- (a) Pro dané x nejsme schopni v rozumném čase najít $y \neq x$ tak, že $h(x)=h(y)$
- (b) Pro dané x nejsme schopni v rozumném čase najít $y \neq x$ tak, že $h(x)=y$
- (c) Pro dané x nejsme schopni v rozumném čase najít $y \neq x$ tak, že $x=h(y)$
- (d) V rozumném čase nejsme schopni nalézt x, y ($x \neq y$) tak, že $h(x)=h(y)$

Správně: a

7. Z jakých šifrovacích algoritmů se obvykle tvoří hašovací funkce?

- (a) Asymetrická šifra
- (b) Hašovací funkci nelze vytvořit z žádného šifrovacího algoritmu
- (c) Proudová symetrická šifra
- (d) Blokova symetrická šifra

Správně: d

8. Biometriky jsou

- (a) automatizované metody identifikace nebo ověření identity.
- (b) založeny na opakovatelně měřitelných fyziologických nebo behaviorálních vlastnostech člověka.
- (c) založeny na neopakovatelně měřitelných fyziologických nebo behaviorálních vlastnostech člověka.
- (d) i metody identifikace pomocí čipové karty obsahující vzorky člověka.

Správně: a, b

9. V tiketu používaném v systému Kerberos se objevuje:

- (a) Identifikátor alespoň jedné ze stran
- (b) Soukromý klíč
- (c) Náhodná výzva
- (d) Časové razítko

Správně: a, d

10. Řízení přístupu, při němž vlastník rozhoduje o přístupech ke svým souborům, se nazývá:

- (a) Princip maximálních privilegií.
- (b) Flexibilní řízení přístupu.
- (c) Volitelné řízení přístupu.
- (d) Povinné řízení přístupu.

Správně: c

11. Útok na čipové karty pomocí časové analýzy využívá:

- (a) Délka operace v závislosti na vykonané větvi kódu.
- (b) Délka operace v závislosti na zpracovávaných datech.
- (c) Závislost průběhu odběru proudu na prováděné instrukci.
- (d) Závislost průběhu odběru proudu na zpracovávaných datech.

Správně: a, b

12. Mezi vlastnosti (axiomy) modelu Bell-LaPadula patří

- (a) procesy nesmějí zapisovat data do nižší úrovně
- (b) procesy nesmějí číst data na vyšší úrovni
- (c) procesy nesmějí číst data z nižší úrovně

Správně: a, b

13. Německý elektronický pas druhé generace s autentizací čipu:

- (a) Lze naklonovat snadno, pokud známe data z MRZ
- (b) Nelze snadno naklonovat (vyžaduje získání soukromého klíče pasu, který nelze z pasu vyčíst).
- (c) Lze naklonovat jen pokud spolupracuje skutečný držitel pasu a zná svůj PIN

Správně: b

14. Soubor /etc/shadow obsahuje

- (a) Informaci o délce hesla
- (b) Datum a čas posledního úspěšného přihlášení do systému
- (c) Počet neúspěšných pokusů o zadání hesla
- (d) Haše hesel uživatelů
- (e) Informaci o tom, že haše hesel jsou v souboru /etc/passwd

Správně: d

15. Snímače otisků prstů jsou

- (a) inkoustové (tryskové)
- (b) kapacitní
- (c) polyadické
- (d) optické

Správně: b, d

16. Která z uvedených tvrzení jsou pravdivá:

- (a) Autentizace pomocí IP adresy může být použita pouze v kombinaci s MAC adresou.
- (b) Autentizace pomocí IP adresy je výrazně bezpečnější než autentizace pomocí MAC adresy.
- (c) Autentizace pomocí IP adresy je výrazně méně bezpečná než autentizace pomocí MAC adresy.
- (d) Autentizace pomocí IP adresy není spolehlivá, protože IP může být změněna.

Správně: d

17. Protokol Kerberos zajišťuje

- (a) Autentizaci
- (b) Aprobaci
- (c) Autokracii
- (d) Akumulaci

Správně: a

18. Pro statickou autentizaci dat (SDA) platí, že:

- (a) Potvrzuje pravost pouze statických dat uložených v čipové kartě.
- (b) Je prováděna pouze platebním terminálem (čip pouze zasílá data)
- (c) Řeší problém padělání/duplikace karet
- (d) Potvrzuje pravost statických dat uložených v čipové kartě, ale i dynamických dat zaslaných terminálem
- (e) Je prováděna pouze čipovou kartou (terminál pouze zasílá data)
- (f) Potvrzuje pravost statických dat uložených v čipové kartě, ale i dynamických dat zaslaných čipem

Správně: a, b

19. V současných SIM (Subscriber Identity Module) kartách pro GSM síť je uložen:

- (a) Statická aplikační data a veřejný certifikát operátora
- (b) Asymetrický klíč
- (c) Symetrický klíč
- (d) Statická aplikační data podepsána soukromým klíčem karty

Správně: c

20. Jaká technologie přihlašování do systému e-bankovníctví (a autorizace transakcí) je nejbezpečnější (z nabízených možností)?

- (a) Použití autentizačního kalkulátoru s PINem
- (b) Použití hesla zadaného částečně na klávesnici a částečně na virtuální klávesnici
- (c) Použití šifrované autentizační SMS (tj. s využitím SIM Toolkitu)
- (d) Použití klientského certifikátu, který je uložen na čipové kartě s přístupem chráněným PINem

Správně: a

21. Která z následujících tvrzení jsou platná pro protokol SSL/TLS?

- (a) Implicitně je autentizace serveru i klienta vypnuta.
- (b) SSL/TLS protokol neprovádí elektronické podepisování dat.
- (c) Implicitně je autentizace serveru a klienta povinná.
- (d) Implicitně je autentizace serveru povinná, autentizace klienta je volitelná.

Správně: b, d

22. Která z uvedených tvrzení o uživatelském PINu jsou pravdivá (při standardním nastavení karty)?

- (a) Při změně nezablokovaného PINu je třeba zadat starý i nový uživatelský PIN.
- (b) Při změně nezablokovaného PINu stačí zadat nový uživatelský PIN.
- (c) Při změně zablokovaného PINu je třeba zadat starý i nový uživatelský PIN.
- (d) Při změně zablokovaného PINu je třeba zadat odblokovací PIN a nový uživatelský PIN.

Správně: a, d

23. Praktické problémy biometrik jsou

- (a) uživatelé s poškozenými či chybějícími orgány.
- (b) legislativa a správa charakteristik.
- (c) nízké FRR (nespokojení uživatelé z důvodu častého odmítnutí).
- (d) nízké FAR (aplikace s nízkou úrovní bezpečnosti).

Správně: a, b

24. Autentizace dat znamená

- (a) Totéž co integrity
- (b) Potvrzení, že data nebyla neautorizovaně změněna od doby vytvoření
- (c) Potvrzení, že data pochází od určitého subjektu
- (d) Data nemohl odeslat nikdo jiný než jejich původce

Správně: b, c

25. Jaké kryptografické techniky lze využít pro implementaci autentizace čipu (jako součást EAC) u elektronických pasů?

- (a) SHA-1 a 3DES
- (b) Diffie-Hellman
- (c) SHA-1 a DSA
- (d) Fiat-Shamir
- (e) PGP
- (f) SHA-2 a AES

Správně: b

26. Detekcí narušení se u čipových karet myslí:

- (a) Po narušení jsou stopy narušení obtížně odstranitelné.
- (b) Odolnost proti pokusům o zjištění robustnosti vůči fyzickým útokům.
- (c) Vlastnost části systému umožňující detekovat fyzický útok.
- (d) Při zjištění narušení je automaticky provedena chráněnou částí obranná akce.

Správně: c

27. Odpovědí na narušení se u čipových karet myslí:

- (a) Automatická akce provedená chráněnou částí při detekci pokusu o narušení.
- (b) Po úspěšném provedení narušení jsou stopy narušení odstraněny.
- (c) Vlastnost části systému umožňující detekovat fyzický útok.
- (d) Akce provedená bezpečnostním administrátorem po zjištění pokusu o narušení.

Správně: a

28. Běžné komerční biometrické zařízení

- (a) je vybaveno detekcí průniku nebo má zvýšenou odolnost proti průniku.
- (b) typicky dobře šifruje přenášená data pomocí kvalitních algoritmů.
- (c) se neautentizuje vůči dalším komunikujícím.

Správně: c

29. Které z uvedených režimů nepodporuje IPsec:

- (a) Transportní režim.
- (b) Dynamický virtuální režim.
- (c) Tunelovací režim.
- (d) Překládový režim.

Správně: b, d

30. Který z výroků o autentizaci na základě dynamiky psaní na klávesnici je pravdivý?

- (a) Měří se čas stlačení klávesy a čas mezi stisky kláves.
- (b) Uživatele je možno autentizovat kontinuálně.
- (c) K autentizaci stačí běžná klávesnice.
- (d) Algoritmy pracují na principu srovnávání vzorů (pattern matching) nebo neuronových sítí (neural networks).

Správně: a, b, c, d

31. Na jakém problému je založena bezpečnost RSA

- (a) Obchodní cestující
- (b) Eliptické křivky
- (c) Faktorizace čísel
- (d) Diskrétní logaritmus

Správně: c

32. Jednosměrnost u kryptografických hašovacích funkcí znamená

- (a) V rozumném čase nejsme schopni najít x , y tak, aby $h(x)=h(y)$
- (b) Pro dané y nelze v rozumném čase najít x tak, aby $h(x)=y$
- (c) Pro dané $h(y)$ nelze v rozumném čase najít x tak, aby $h(x)=h(y)$
- (d) Pro dané y lze v rozumném čase najít x tak, aby $h(x)=y$

Správně: b

33. Které z uvedených kategorií čipových karet podle technologie komunikace rozlišujeme?

- (a) Hybridní karty.
- (b) Bezkontaktní karty.
- (c) Kontaktní karty.
- (d) Polymorfní karty.

Správně: b, c

34. Na jakém druhu kryptografie je založena základní verze Kerbera?

- (a) Hybridní
- (b) Symetrická
- (c) Asymetrická

Správně: b

35. Biometrické charakteristiky se dělí na

- (a) geotypické
- (b) genotypické
- (c) biomatické
- (d) fenotypické

Správně: b, d

36. Aktualizace klíče se vzájemnou autentizací protokolem AKEP2 (Authenticated Key Exchange Protocol 2) je založena na:

- (a) Generátorech passcode
- (b) Algoritmu MAC (Message Authentication Code)
- (c) Digitálních podpisech
- (d) Bez klíčových kryptografických hašovacích funkcí

Správně: b

37. Jaká primární autentizační metoda slouží k automatizované verifikaci identity předkladatele pasu?

- (a) Znalost tajemství (v tomto případě PINu) zakódovaného v MRZ
- (b) Znalost tajemství ověřená pomocí protokolu výzva-odpověď
- (c) V čipu zakódovaný 128bitový identifikátor (platný typicky 10 let)
- (d) Biometriky (obličej, otisk prstu, duhovka)

Správně: d

38. Které protokoly umožňují vytvoření sdíleného tajemství?

- (a) Protokoly pro ustavení klíče
- (b) Protokoly implementované v Kerberu
- (c) Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- (d) Silné autentizační protokoly

Správně: a, b

39. Pro ověření japonského elektronického pasu na českých hranicích je třeba:

- (a) CSCA certifikát ČR, který je třeba předem získat diplomatickými prostředky
- (b) CSCA certifikát Japonska, který si držitel pasu může přinést na CD nebo USB flash disku
- (c) CSCA certifikát Japonska, který je třeba předem získat diplomatickými prostředky
- (d) DS certifikát, který je možné vyčíst z pasu
- (e) CSCA certifikát Japonska, který je možné vyčíst z pasu
- (f) DS certifikát, který si držitel pasu musí přinést na CD nebo USB flash disku

Správně: c, d

40. Co je to narozeninový paradox?

- (a) Lze jej ilustrovat faktem, že v sále s 23 lidmi je pravděpodobnost stejného data narození dvou lidí větší než 50 %
- (b) Situace, kdy se začátkem roků rodí víc mužů než žen
- (c) Pravděpodobnost nalezení stejného data narození k pevně zvolenému datu je při 23 lidech větší než 50 %
- (d) Statisticky podložená vysoká úspěšnost nalezení kolize

Správně: a, d

41. Které z uvedených kategorií čipových karet podle technologie uchování a práce s daty rozlišujeme?

- (a) Paměťové karty se speciální logikou.
- (b) Karty s magnetickým proužkem.
- (c) Paměťové karty.
- (d) Procesorové karty.

Správně: a, c, d

42. Oční duhovka je snímána pomocí

- (a) ultrafialového paprsku.
- (b) černobílé kamery.
- (c) kvalitní barevné kamery.
- (d) laserového paprsku s třídou bezpečnosti 1.

Správně: b

43. Mezi chyby biometrických systémů patří

- (a) ARR (Acceptance Rejection Rate)
- (b) EDR (Error Disqualification Rate)
- (c) FAR (False Acceptance Rate)
- (d) FRR (False Rejection Rate)

Správně: c, d

44. Jaké jsou možnosti prevence padělání tokenů?

- (a) Modifikace dostupného vybavení (modifikace vybraných barev u kopírky, vkládání identifikátoru).
- (b) Utajení všech informací nutných ke konstrukci tokenu.
- (c) Utajení některých informací nutných ke konstrukci tokenu.
- (d) Čestné prohlášení všech uživatelů systému.
- (e) Kontrola a licence souvisejících živností.
- (f) Omezení dostupnosti potřebného vybavení.

Správně: a, c, e, f

45. Digitální podpis ověříme pomocí

- (a) Veřejného klíče podepisující osoby
- (b) Soukromého klíče podepisující osoby
- (c) Privátního klíče podepisující osoby
- (d) Certifikátu veřejného klíče podepisující osoby
- (e) Klíče sdíleného s podepisující osobou

Správně: a, d

46. Které časově proměnné parametry se používají v kryptografických protokolech?

- (a) Monoliticky rostoucí sekvence
- (b) Náhodná komplexní čísla
- (c) Náhodné sekvence
- (d) Náhodná časová razítka
- (e) Náhodná čísla
- (f) Časová razítka

Správně: e, f

47. K čemu slouží soubor .rhosts?

- (a) K nastavení adres počítačů s povoleným přihlášením bez další autentizace.
- (b) Uchování informací o adresách autentizovaných počítačů připojených k serveru.
- (c) K uchování uživatelů s právem číst (read).
- (d) K uchování RSA klíče(ů) serveru.

Správně: a

48. Digitální podpis může vytvořit

- (a) Pouze osoba vlastníci sdílený klíč
- (b) Pouze osoba vlastníci soukromý klíč
- (c) Pouze osoba vlastníci veřejný klíč
- (d) Pouze osoba vlastníci certifikovaný klíč

Správně: b

49. Které biometrické charakteristiky bývají nazývány také dynamickými?

- (a) fyziologické
- (b) genotypické
- (c) behaviorální
- (d) fenotypické

Správně: c

50. Které z uvedených útoků na čipové karty nepatří mezi fyzické útoky?

- (a) Preparace čipu
- (b) Odběrová analýza
- (c) Ozařování čipu
- (d) Časová analýza

Správně: b, d

51. Jaký je u ssh rozdíl mezi Server key a Host key?

- (a) Server key je krátkodobý klíč použitý pro odvození Host key.
- (b) Host key je dlouhodobý klíč.
- (c) Server key je krátkodobý klíč použitý pro vlastní autentizaci serveru.
- (d) Host key je krátkodobý klíč použitý pro vlastní autentizaci serveru.

Správně: b, c

52. Co nepatří mezi mechanismy zabraňující jednodušším útokům na e-bankovníctví s autentizací pouze na základě hesla?

- (a) Anonymizovaný login
- (b) testy délky a kvality hesla
- (c) Virtuální klávesnice pro zadávání hesla
- (d) SSH certifikáty
- (e) Personalizovaný login
- (f) SSL certifikáty

Správně: a, d

53. Jaké typy záznamů lze používat na čipové kartě?

- (a) Nestrukturovaná data.
- (b) Exponenciální záznam s pevnou délkou.
- (c) Lineární záznamy s pevnou nebo variabilní délkou.
- (d) Cyklické záznamy.

Správně: a, c, d

54. Biometrické technologie mohou být založeny na některém z těchto typů charakteristik:

- (a) fyziologický
- (b) morální
- (c) environmentální
- (d) behaviorální
- (e) chemoterapický

Správně: a, d

55. Co je to zaručený elektronický podpis

- (a) Jednoznačně ověřitelný podpis
- (b) Podpis, který má záruky srovnatelné jako elektronický podpis
- (c) Elektronický podpis, za který se dokážeme nějak důvěryhodně zaručit
- (d) Podpis vytvořený pomocí kryptografických prostředků

Správně: a, d

56. Která tvrzení platí pro elektronickou značku

- (a) Elektronické značky jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu
- (b) Technologicky jde o totéž co zaručený elektronický podpis
- (c) Ověření elektronické značky je obtížnější než ověření elektronického podpisu
- (d) Elektronická značka je ke zprávě připojena tak, že je možné detekovat následné změny ve zprávě

Správně: a, b, d

57. Co je to Chaffing and winnowing

- (a) Pro každý bit zprávy vytvoříme dvě zprávy (správný, chybný MAC), příjemce si ponechá zprávu se správným MAC
- (b) Zprávu rozdělíme na jednotlivé bity a ty šifrujeme z využitím MAC každý zvlášť
- (c) Každý bit zprávy zkopírujeme několikrát za sebe, aby se předešlo chybám v důsledku chybovosti MAC komunikačního kanálu
- (d) "Oddělení zrna od plev"

Správně: a, d

58. Jaké jsou obecné nevýhody tokenů?

- (a) Cena tokenů je příliš vysoká pro komerční využití.
- (b) Bez tokenu není autorizovaný uživatel rozpoznán.
- (c) Ztráta tokenu vede většinou ke kompromitaci celého systému.
- (d) Ke kontrole je obvykle třeba speciální čtečka nebo vycvičená osoba.

Správně: b, d

59. V dobrých autentizačních protokolech se typicky

- (a) Heslo posílá v hašované podobě
- (b) Heslo neposílá vůbec
- (c) Heslo posílá v otevřené podobě

Správně: a, b

60. Proces použití biometrik pro autentizaci zahrnuje

- (a) registraci
- (b) verifikaci
- (c) degustaci
- (d) demonstraci

Správně: a, b

61. Decentralizovaná správa řízení přístupu k objektu znamená

- (a) klíč (totožný) od budovy má víc lidí
- (b) přístupová práva nastavují příslušní vlastníci jednotlivých objektů
- (c) obtížnou komunikaci mezi držiteli jednotlivých částí přístupového hesla či jiného tokenu
- (d) pro přístup k objektu je třeba shromáždit hesla či jiné tokeny rozdistribuované mezi více lidí
- (e) řízení přístupu provádí více autorizačních systémů zároveň

Správně: b

62. Co je to semi-invazivní časová analýza?

- (a) Druh semi-invazivního útoku zneužívající u mnohých čipových karet možnost ovlivnění vstupního hodinového cyklu.
- (b) Speciální semi-invazivní útok na autentizační kalkulátor s hodinami.
- (c) Žádná z výše uvedených odpovědí.
- (d) Metrika sloužící k určení a vyhodnocení efektivnosti semi-invazivních útoků.

Správně: c

63. Útok na čipové karty pomocí indukce chyb je založen na:

- (a) Využití chybného běhu algoritmu po prudkém ovlivnění vnějších podmínek k získání tajných dat.
- (b) Využití indukce chyb po prudkém ovlivnění vnějších podmínek k testování změny chování algoritmu.
- (c) Jako první krok útoku je provedeno fyzického poškození.
- (d) Využití opravných kódů pro automatické odstranění chyby po prudkém ovlivnění vnějších podmínek.

Správně: a, b

64. Jaké jsou hlavní výhody biometrik

- (a) rychlé a (relativně) přesné výsledky.
- (b) nemůžeme je ztratit, zapomenout nebo předat jiné osobě.
- (c) jsou tajné.
- (d) jednoduchá správa vzorků.

Správně: a, b

65. Jaký mechanismus je použit pro zajištění bezpečnosti v autentizační hlavičce IPsec?

- (a) Message Authentication Code se sekvenčním číslem.
- (b) Diffie-Hellman autentizace bez klíčů.
- (c) Message Authentication Code s náhodným číslem.
- (d) Digitální podpis využívající RSA nebo DSA.

Správně: a

66. Co patří mezi bezpečnostní problémy používání bankovních karet s čipem?

- (a) Možnost odpozorování PINu na frekventovaných místech.
- (b) Špatná průkaznost nelegitimní autorizace platby pomocí PINu.
- (c) Velká obtížnost kopírování karty.
- (d) Výpočetní výkon nepostačuje pro kryptografické zabezpečení transakcí.

Správně: a

67. Na co není výhodné použít biometriky

- (a) na autentizaci dat.
- (b) na ochranu přístupu k tajnému klíči.
- (c) na doplňkovou formu autentizace.

Správně: a

68. Na jaké vrstvě funguje protokol SSL/TLS?

- (a) mez aplikační a datovou vrstvou
- (b) na linkové vrstvě
- (c) na síťové vrstvě
- (d) na datové vrstvě

Správně: a

69. Jaké vlastnosti má základní řízení přístupu (BAC) u elektronických pasů?

- (a) Tajný klíč lze získat z dat v MRZ
- (b) Umožňuje ustavení sdíleného symetrického klíče
- (c) Tajný klíč lze získat pouze z dat uložených v čipu
- (d) Umožňuje explicitní autorizace pro přístup k citlivým datům

Správně: a, b

70. Úspěšné odposlechnutí citlivých dat ze sběrnice platebního terminálu může vést:

- (a) K přečtení citlivých informací banky (sdílené tajné klíče uložené v terminálu)
- (b) K modifikaci nepodepsaného seznamu podporovaných verifikačních metod (CVM)
- (c) K získání přesné kopie dat na magnetickém proužku
- (d) K získání PINu
- (e) K narušení anonymity jednotlivých komunikujících stran
- (f) K modifikaci podepsaného seznamu podporovaných verifikačních metod (CVM)

Správně: b, c, d

71. Autentizace v soudobých systémech e-bankovníctví je výhradně

- (a) Třífaktorová
- (b) Žádná z dalších odpovědí není správně
- (c) Dvoufaktorová
- (d) Jednofaktorová

Správně: b

72. Forenzní řešení biometrik popisují tyto výroky

- (a) výsledek identifikace je získán obvykle za 1s či rychleji.
- (b) miniaturizace zařízení je jedním z hlavních cílů.
- (c) pro používání je nutná odborná znalost systému.
- (d) cena je vysoká, ale s tím se počítá.

Správně: c, d

73. Soubor /etc/passwd může obsahovat

- (a) Datum a čas posledního úspěšného přihlášení do systému
- (b) Počet zbývajících neúspěšných pokusů o zadání hesla
- (c) Haše hesel uživatelů
- (d) Informaci o délce hesla
- (e) Informaci o tom, že haše hesel jsou v souboru /etc/shadow

Správně: c, e

74. Pro autentizaci obrazovou informací platí

- (a) Uživatel musí správně vybarvit předložený obrázek
- (b) Uživatel musí do systému nahrát správný obrázek
- (c) Uživatel musí systému slovně popsat obrázek sloužící k autentizaci
- (d) Uživatel musí vybrat správný obrázek nebo jeho část

Správně: d

75. Na čem podle specifikace EMV závisí dohoda autentizační metody uživatele?

- (a) Rozhodnutí přísluší plně platebnímu terminálu
- (b) Na prioritně uspořádaném seznamu podporovaných verifikačních metod (CVM)
- (c) Na tom, zdali má být prováděna transakce on-line či offline
- (d) Na konkrétní implementaci statické, dynamické či kombinované autentizace dat

Správně: b

76. Pro bezpečné používání digitálního podpisu

- (a) Je nutné zajistit integritu privátního klíče
- (b) Je nutné zajistit integritu veřejného klíče
- (c) Je nutné udržet privátní klíč v tajnosti
- (d) Je nutné udržet veřejný klíč v tajnosti

Správně: b, c

77. V současných českých elektronických pasech musí být uloženy soubory obsahující:

- (a) Kvalifikovaný certifikát držitele pasu (vydaný akreditovanou CA)
- (b) Haš soukromého klíče čipu, zajišťující integritu daného klíče
- (c) Digitálně podepsané haše všech tzv. DG souborů
- (d) Barevnou fotografii držitele pasu (formát JPEG/JPG2000) a otisky prstů (komprese WSQ)

Správně: c, d

78. Co je vyžadováno pro autentizaci transakce při offline verifikaci se šifrováním PINu?

- (a) Originální PIN nutný pro verifikaci, který musí být bezpečně uložen v čipu
- (b) Fyzicky i prostředím dobře zabezpečený PINpad
- (c) Úspěšné proběhnutí automatické správy rizik
- (d) Nový RSA pár klíčů pro šifrování PINů

Správně: a, b, d

79. Jaké jsou obecné výhody tokenů?

- (a) Rychlé zjištění ztráty.
- (b) Mohou zpracovávat a přenášet další informace.
- (c) Nikdy je nelze zneužít po náhodném nálezku.
- (d) Většinou nejsou jednoduše kopírovatelné.

Správně: a, b, d

80. Která z následujících tvrzení jsou platná pro protokol SSL/TLS?

- (a) Autentizace komunikujících stran je založena na symetrické kryptografii.
- (b) Po průběhu Handshake protokolu je komunikace šifrována symetrickým klíčem.
- (c) SSL/TLS protokol zajišťuje integritu a autenticitu dat.
- (d) Po úvodní Handshake protokolu je komunikace šifrována veřejným klíčem příjemce.

Správně: b, c

81. Jaké jsou typické velikosti pamětí u současných čipových karet?

- (a) < 100KB RAM, < 100KB ROM, > 1MB EEPROM
- (b) > 256KB RAM, 100KB ROM, < 100KB EEPROM
- (c) 128KB RAM, 512KB ROM, 512KB EEPROM
- (d) < 10KB RAM, 100KB ROM, < 100KB EEPROM

Správně: d

82. Z jakého důvodu se používá Server key namísto Host key pro vlastní autentizaci u SSH?

- (a) Zrychlení procesu autentizace klienta vůči serveru.
- (b) Pro zajištění kompatibility s protokolem telnet.
- (c) Ochrana dlouhodobého klíče Host key před kompromitováním.
- (d) Zrychlení procesu autentizace serveru vůči klientovi.

Správně: c

83. Které z protokolů se v současnosti v běžných aplikacích využívají více?

- (a) Challenge-response protokoly (protokoly výzva-odpověď)
- (b) Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)

Správně: a

84. Biometrická data při opakovaném měření kvalitním zařízením

- (a) jsou vždy shodná na 99 % a víc.
- (b) nejsou nikdy shodná na 100 %.
- (c) nejsou nikdy shodná na 100 % až na otisky prstů.
- (d) jsou typicky shodná na 100 %.

Správně: b

85. IP spoofing označuje:

- (a) Podvržení IP adresy příjemce.
- (b) Zachycení IP adresy odesílatele i příjemce.
- (c) Zachycení IP odesílatele.
- (d) Podvržení IP adresy odesílatele.

Správně: d

86. Která z uvedených tvrzení o autentizačních kalkulátorech jsou pravdivá?

- (a) Přístup k využití kalkulátoru může být chráněn PINem.
- (b) Pracují na principu protokolu výzva/odpověď s využitím tajné informace.
- (c) Kalkulátor nelze zneužít i při znalosti PINu.
- (d) Výzva je zadávána manuálně nebo automaticky načtena z vhodného média.

Správně: a, b, d

87. Odolností vůči narušení se u čipových karet myslí:

- (a) Automatická akce provedená chráněnou částí při zjištění pokusu o narušení.
- (b) Vlastnost části systému umožňující detekovat fyzický útok.
- (c) Vlastnost části systému chráněné proti neautorizované modifikaci podstatně lépe než zbylá část systému.
- (d) Ochrana proti útoku rušením radiového signálu (RFID).

Správně: c

88. Proč je u tokenů založených na hodinách potřeba řešit otázku posuvu hodin?

- (a) Pravým důvodem je přechod na letní/zimní čas a přestupné roky.
- (b) Žádná z výše uvedených odpovědí.
- (c) Nutnost synchronizace drobných odchylek mezi serverem a tokenem.

Správně: c

89. Matice přístupových práv

- (a) je reprezentace standardních přístupových práv v unixových OS (RWX-RWX-RWX)
- (b) zaznamenává pro každý objekt a každý subjekt údaje o čase, trvání, ... přístupu daného subjektu k danému objektu
- (c) má alespoň dva rozměry - subjekt a objekt
- (d) může mít i tři rozměry - subjekt, objekt a uživatel
- (e) definuje přinejmenším to, jaká přístupová práva mají jednotlivé subjekty k jednotlivým objektům

Správně: c, e

90. Které z uvedených útoků na čipové karty nepatří mezi logické útoky?

- (a) Časová analýza
- (b) Útok přes aplikační rozhraní
- (c) Ozařování čipu
- (d) Preparace čipu

Správně: c, d

91. Autentizace pomocí verifikace hlasu probíhá typicky

- (a) pomocí běžného mikrofону.
- (b) pomocí soustavy mikrofónů rozmístěných ve vzdálenosti cca 0,5 m ve 4 směrech.
- (c) v samostatné odhlučněné komoře, pro odstranění okolního šumu.
- (d) využitím telefonu.

Správně: a, d

92. Které z uvedených typů autentizačních kalkulátorů se používají v IT bezpečnosti?

- (a) Kalkulátor s hodinami.
- (b) Kalkulátor s tajnou informací.
- (c) Kalkulátor bez vstupní klávesnice.
- (d) Kalkulátor s vestavěným budíkem (z angl. embedded alarm).

Správně: a, b, c

93. Pro ss-vlastnost modelu Bell-LaPadula platí:

- (a) je považována za nebezpečnou a není doporučováno ji používat
- (b) účelem je ochránit důvěrnost citlivých dat
- (c) procesy nesmějí zapisovat data do nižší úrovně
- (d) zachovává integritu dat
- (e) procesy nesmějí číst data na vyšší úrovni

Správně: b, c, e

94. Které z výroků o autentizaci na základě rozpoznání obličeje nejsou pravdivé?

- (a) Autentizaci komplikuje osvětlení a pozadí.
- (b) Přesnost se v posledních 5 letech příliš nezlepšila.
- (c) Jedná se o velice výpočetně náročnou metodu autentizace.
- (d) Autentizaci komplikuje změna účesu, náušnice a brýle.

Správně: b

95. "Solení"hesel

- (a) Pomůže vyřešit situaci, kdy mají uživatelé stejná hesla
- (b) Zajistí delší efektivní heslo
- (c) Je dodatečná technika při ukládání hesel pro určitou formu identifikace
- (d) Je dnes již jen velmi zřídka používaná technika

Správně: a, b

96. Útok na čipové karty pomocí odběrové analýzy využívá:

- (a) Závislost průběhu odběru proudu na ukládaných datech do paměti EEPROM.
- (b) Data získaná odběrem vzorku paměti EEPROM.
- (c) Závislost průběhu odběru proudu na zpracovávaných datech.
- (d) Závislost průběhu odběru proudu na prováděné instrukci.

Správně: a, c, d

97. Co je to CVV2?

- (a) Druhý kontrolní součet uložený na magnetickém proužku (slouží k detekci dvoubitových a opravě jednobitových chyb)
- (b) Hodnota vytištěná na zadní straně karty (sloužící jako dodatečný zabezpečovací mechanismus pro platby kartou přes Internet)

Správně: b

98. Pokud ukládáme hesla šifrovaně

- (a) Musíme věřit administrátorovi
- (b) Musíme znát (jako uživatelé) šifrovací klíč
- (c) Nesmí být použit šifrovací algoritmus DSA
- (d) Šifrovací klíč musí být přístupný autentizační službě

Správně: a, d

99. Jak eliminujeme útoky hrubou silou na PINy?:

- (a) Pravidelnou změnou hodnoty PINu
- (b) Omezením počtu pokusů o zadání PINu
- (c) školením uživatelů

Správně: b

100. Pro pojem výpočetní bezpečnost platí následující tvrzení.

- (a) Výsledek náročného výstupu je podepsaný, z důvodu zaručení integrity
- (b) Časová náročnost prolomení určitého algoritmu mnohonásobně převyšuje dostupný výpočetní výkon
- (c) Algoritmus jako takový nemusí být považován za neprolomitelný, dosud pouze nebyl nalezen efektivní způsob řešení/výpočtu
- (d) Ani jedno z uvedených tvrzení neplatí

Správně: b, c

101. K čemu slouží autentizační agent u ssh?

- (a) K autentizaci dat přenášených mezi serverem a uživatelem.
- (b) Opakované požadavky vyžadující heslo řeší agent po prvním zadání automaticky.
- (c) Automaticky autentizuje server vůči uživateli bez nutnosti zadávat opakovaně heslo.
- (d) Autentizační agent se u ssh nepoužívá, neboť je použita asymetrická kryptografie.

Správně: b

102. Mezi metody volitelného řízení přístupu patří:

- (a) Hašování dat.
- (b) Přihlašování doplňkovou biometrikou.
- (c) Seznamy přístupových práv.
- (d) Bell-LaPadula.

Správně: c

103. K čemu slouží MAC (Message authentication code)

- (a) K zajištění důvěrnosti
- (b) K zajištění integrity
- (c) K ověření zprávy síťové karty
- (d) K detekci chyb při přenosu dat
- (e) K transformaci hašovací funkce

Správně: a, b, d

104. Při kombinaci šifrování veřejným klíčem a podpisu dokumentu se doporučuje operace provést v následujícím pořadí:

- (a) Podpis, šifrování, podpis
- (b) Šifrování, podpis, šifrování
- (c) Šifrování, podpis
- (d) Na pořadí operací nezáleží
- (e) Podpis, šifrování

Správně: e

105. Základní bezpečnostní problémy RFID jsou:

- (a) Interference
- (b) Idempotence
- (c) Neapolatelnost
- (d) Autentizace
- (e) Soukromí
- (f) Nepopiratelnost

Správně: a, d, e

106. U dynamiky podpisu je důležitý

- (a) aretačně-dynamický tablet.
- (b) čas potřebný pro provedení podpisu.
- (c) pořadí jednotlivých tahů pera.
- (d) výsledný podpis.

Správně: b, c

107. Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí) umožňují, poctivým stranám vždy dosáhnout úspěšného výsledku. Tato vlastnost se nazývá:

- (a) Částečné uspokojení (partial satisfaction)
- (b) Úplnost (completeness)
- (c) Korektnost (soundness)
- (d) Úplné uspokojení (complete satisfaction)

Správně: b

108. Základní fakta o biometrických systémech jsou:

- (a) kopírování biometrik nemusí být triviální, ale není obtížné.
- (b) biometrická data mohou být velmi citlivé informace.
- (c) biometrická data jsou tajná.

Správně: a, b

109. Které z uvedených možností nezajišťuje protokol IPsec?

- (a) Ochranu proti analýze šifrovaného provozu na síťové vrstvě.
- (b) Integrita a autentizace původu dat.
- (c) Nepopiratelnost přijetí dat.
- (d) Důvěrnost dat, ochrana proti přehrání.

Správně: a, c

110. U autentizace pomocí hesel

- (a) Musíme řešit aspekt zapamatovatelnosti vs. bezpečnosti
- (b) Musíme řešit aspekt bezpečnosti bez ohledu na zapamatovatelnost
- (c) Musí uživatel prokázat, že si dokáže zapamatovat alespoň 10 náhodně zvolených symbolů

Správně: a

111. Jaké bezpečnostní problémy lze identifikovat v soudobém bankovníctví?

- (a) Použití pouze asymetrické kryptografie v kombinaci s hašovacími funkcemi (pouze pro podpisy)
- (b) Dodatečné autorizační SMS zprávy jen u některých operací e-bankovníctví
- (c) Nedostatečné zabezpečení platebních terminálů
- (d) Použití autentizačních kalkulátorů
- (e) Social engineering např. při telefonním hovoru
- (f) Zasílání embosované karty poštou a nedostatečně zabezpečené doručování PINu a hesla

Správně: b, c, e, f

112. Pravděpodobnost, že se nepoctivý útočník může úspěšně vydávat za jinou stranu je u zero-knowledge protokolů (protokoly s nulovým rozšířením znalostí) mizivá. Tato vlastnost se nazývá:

- (a) Částečné uspokojení (partial satisfaction)
- (b) Korektnost (soundness)
- (c) Úplné uspokojení (complete satisfaction)
- (d) Úplnost (completeness)

Správně: b

113. Které biometrické charakteristiky bývají nazývány také statickými?

- (a) fenotypické
- (b) behaviorální
- (c) fyziologické
- (d) genotypické

Správně: c

114. Která z uvedených tvrzení o tokenech založených na hodinách jsou pravdivá:

- (a) Token s hodinami nelze použít bez přítomnosti klávesnice.
- (b) Autentizační hodnota je vygenerována na základě aktuálního času a tajné informace.
- (c) Přístup k využití tokenu s hodinami musí být vždy chráněn PINem.
- (d) Je potřeba řešit otázku synchronizace hodin mezi serverem a tokenem.

Správně: b, d

115. Mezi obecné výhody tokenů nepatří:

- (a) Obtížná kopírovatelnost.
- (b) Snadné zjištění ztráty.
- (c) Snadná detekce a odpověď na narušení.
- (d) Možnost zpracovávání informací.

Správně: c

116. Pro vztah řízení přístupu a autentizace platí:

- (a) jedná se o dva naprosto nesouvisející pojmy
- (b) jde o ekvivalentní termíny
- (c) řízení přístupu je obvyklou podmínkou pro autentizaci
- (d) autentizace je obvyklou podmínkou pro řízení přístupu

Správně: d

117. Které z níže uvedených typů protokolů existují?

- (a) Autentizační protokoly bez ustavení klíče
- (b) Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí) pro ustavení klíče.
- (c) Autentizované protokoly pro ustavení klíče
- (d) Protokoly pro ustavení klíče
- (e) Neautentizované protokoly pro ustavení klíče

Správně: a, c, d, e

118. Čím je dáno, že komunikace s RFID tagem musí probíhat pouze na přímou viditelnost?

- (a) Použitými kryptografickými mechanismy
- (b) Použitou vlnovou délkou
- (c) Použitým frekvenčním pásmem
- (d) Množstvím přenášených dat

Správně: b, c

119. Které z příkladů autentizace počítačů jsou možné:

- (a) Privátním klíčem asymetrické kryptografie.
- (b) Kombinace IP, MAC, GUID (global unique identifier).
- (c) Kombinace IP adresy a tajného klíče symetrické kryptografie.
- (d) Tajným klíčem symetrické kryptografie.

Správně: a, d

120. Která z následujících tvrzení jsou platná pro protokol SSL/TLS?

- (a) SSL/TLS protokol nezajišťuje důvěrnost dat.
- (b) Implicitně je autentizace serveru a klienta je povinná.
- (c) Autentizace komunikujících stran je založena na asymetrické kryptografii.
- (d) SSL/TLS protokol umožňuje vzájemnou autentizaci serveru a klienta.

Správně: c, d

121. Mezi nejslibnější technologie v oblasti identifikace v počítačových systémech pomocí biometrik nepatří

- (a) otisk prstu.
- (b) tvar ruky.
- (c) ověření mluvího.
- (d) snímání oční duhovky.
- (e) DNA.

Správně: b, e

122. Která z tvrzení jsou platná pro termín "separace oprávnění" při řízení přístupu

- (a) týká se rozlišení procesů autentizace a autorizace
- (b) žádní dva uživatelé systému nesmějí mít nikdy stejná oprávnění
- (c) označuje stav, kdy je k provedení operace nutný souhlas více osob
- (d) tento termín neexistuje
- (e) vyjadřuje skutečnost, že se jednotlivé úrovně oprávnění nesmí překrývat

Správně: c

123. Která z následujících tvrzení platí pro princip nejmenších privilegií:

- (a) žádný uživatel nemá přístup k objektům, které nepotřebuje
- (b) k objektu nemají přístup uživatelé, kteří jej nezbytně nepotřebují
- (c) uživatelé systému mají na počátku nejvyšší možná oprávnění
- (d) označuje stav, kdy je k provedení operace nutný souhlas více osob
- (e) přístup k souboru má pouze uživatel s menšími privilegii než administrátor

Správně: a, b

124. Pokud při kontrole japonského pasu na českých hranicích není k dispozici CSCA certifikát Japonska:

- (a) nic se neděje protože není vůbec potřeba
- (b) lze alternativně použít CSCA certifikát České republiky
- (c) lze ověřit platnost dat v pasu, jen pokud haše DG souborů odpovídají obsahu DG souborů
- (d) nelze ověřit platnost dat v čipu pasu

Správně: d

125. Markanta v oblasti biometrik znamená:

- (a) Významný bod v otisku prstu.
- (b) Výrazné poškození dané biometricky u konkrétního uživatele.
- (c) Zpracovaný obraz oční duhovky se zvýrazněnými přechody.
- (d) Biometrická technologie s významně vysokou hodnotou EER.

Správně: a

126. Zajistit autentizaci digitálních dat a zpráv lze ???

- (a) Pomocí klasického (ručního) podpisu
- (b) Pomocí zaručeného elektronického podpisu
- (c) Pomocí MAC
- (d) Pomocí klíčované hašovací funkce
- (e) Pomocí parciálně zaručeného elektronického podpisu

Správně: b, c, d

127. Které z uvedených typů karet se používají v IT bezpečnosti?

- (a) Kontaktní karty s čipem.
- (b) Karty s bezkontaktním magnetickým proužkem.
- (c) Bezkontaktní karty s čipem.
- (d) SIM karty v mobilních telefonech.

Správně: a, c, d

128. Proti jakým útokům brání protokol ssh?

- (a) Odposlech hesla a pozdější přehrání (na uživatelské PC)
- (b) Analýza šifrovaného provozu na síťové vrstvě
- (c) Odposlech hesla a pozdější přehrání (na síťové vrstvě)
- (d) DNS/IP/Routing spoofing

Správně: c, d

129. Která z tvrzení o mechanismu SUID platí:

- (a) přiděluje se konkrétním uživatelům při vytváření účtů
- (b) umožňuje kontrolovatelné spouštění zavíraných programů bez ID
- (c) může přidělovat administrátorská práva konkrétním procesům
- (d) propůjčuje skupinu vlastníka souboru tomu, kdo jej spouští
- (e) propůjčuje identitu vlastníka souboru tomu, kdo jej spouští

Správně: c, e

130. Zjistitelnost narušení se u čipových karet myslí:

- (a) Po narušení jsou stopy narušení obtížně odstranitelné.
- (b) Při zjištění narušení je automaticky provedena chráněnou částí obranná akce.
- (c) Odolnost proti pokusům o zjištění robustnosti vůči fyzickým útokům.
- (d) Vlastnost části systému umožňující reagovat na fyzický útok.

Správně: a

131. Které z uvedených režimů podporuje IPsec:

- (a) Překladový režim.
- (b) Transportní režim.
- (c) Tunelovací režim.
- (d) Dynamický virtuální režim.

Správně: b, c

132. Jaké jsou nevýhody autentizace hašovaným heslem?

- (a) Příliš snadná transformace na zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- (b) Útok přehráním
- (c) Možnost impersonace
- (d) Náchylnost ke slovníkovému útoku

Správně: b, c

133. PIN je

- (a) Osobně sdílená informace
- (b) Kombinace čísel a písmen (A-F) pro potřeby autentizace
- (c) Veřejně známá informace
- (d) Kombinace čísel pro potřeby autentizace

Správně: d

134. K čemu slouží CRC (Cyclic redundancy check)

- (a) K ověření autenticity dat
- (b) Ke kompresi dat
- (c) K zašifrování dat
- (d) K detekci chyb při přenosu dat

Správně: d

135. Co zajišťujeme použitím náhodných čísel?

- (a) Odolnost proti uvážnutí a stárnutí
- (b) Aktuálnost
- (c) Nezvratnost
- (d) Stálost a stabilitu
- (e) Čerstvost
- (f) Jedinečnost

Správně: b, e, f

136. Čeho lze dosáhnout zopakováním zero-knowledge protokolu (protokol s nulovým rozšíření znalostí)?

- (a) Zvýšení bezpečnosti - zvýší se záruka, že nedojde k rozšíření žádných znalostí
- (b) Zvýšení bezpečnosti - sníží se pravděpodobnost, že nepoctivý útočník se může úspěšně vydávat za jinou stranu
- (c) Ničeho - ke spolehlivé autentizaci stačí 1 kolo protokolu
- (d) Ničeho - nezvýší se záruka, že nedojde k rozšíření žádných znalostí

Správně: b

137. Co je klonování elektronického pasu:

- (a) Jedná se o neautorisované čtení pasu bez znalosti dat z MRZ
- (b) Jedná se o neautorizovanou změnu dat v čipu, která je detekovatelná díky ověření digitálního podpisu.
- (c) Jedná se o opakované využití náhodného identifikátoru čipu využívaného pro nízkoúrovňovou komunikaci pomocí ISO 14443
- (d) Jedná se o kopii souborů z jednoho pasu do jiného

Správně: d

138. Která z následujících tvrzení snímání geometrie ruky jsou pravdivá?

- (a) Snímače snímají 2D snímky ruky shora, zespodu a ze stran (dohromady 4 snímky, u špičkových zařízení i 5-6).
- (b) Snímače snímají 2D snímky ruky mikrokamerami ve fixačních kolících.
- (c) Snímače snímají zjednodušený 3D náhled ruky.
- (d) Tvar ruky je jedinečný (ve skupinách o tisících uživatelů).
- (e) Tvar ruky není jedinečný (ve skupinách o tisících uživatelů).

Správně: c, e

139. Který z následujících protokolů je součástí SSL/TLS protokolu?

- (a) Kerberos protokol.
- (b) Record Layer protokol.
- (c) IPSec protokol.
- (d) Handshake protokol.

Správně: b, d

140. O RBAC (Role Based Access Control) je možné říci, že:

- (a) jednotlivým uživatelům jsou přiřazovány odpovídající role
- (b) jedná se o nadstavbu BAC použitého u elektronických pasů
- (c) jde o zastaralý koncept ochrany soukromí
- (d) místo rolí se v moderních operačních systémech používá stránkování
- (e) nejde ani o volitelné, ani povinné řízení přístupu
- (f) existuje standardizovaná metodika řazení uživatelů do jednotlivých rolí

Správně: a, e

141. Integrita dat znamená

- (a) Data v původní podobě lze obnovit i přesto, že byla modifikována
- (b) Data nebyla neautorizovaně změněna pouze v průběhu přenosu nezabezpečeným kanálem
- (c) Data nebyla neautorizovaně změněna
- (d) Data nebyla autorizovaně předána

Správně: c

142. Digitálně podepisujeme

- (a) Pouze haš podepisovaného dokumentu
- (b) V případě malých dokumentů celou zprávu, v případě velkých dokumentů jejich haš
- (c) Vždy přímo celý dokument

Správně: a

143. Při používání digitálního podpisu používáme

- (a) Digitální klíč
- (b) Privátní a veřejný klíč
- (c) Sdílené symetrické klíče mezi všemi komunikujícími partnery
- (d) Digitální pečetě

Správně: b

144. Jaký je vztah mezi chybovou analýzou a útoky na a přes API?

- (a) Chybová analýza s útoky na a přes API nijak nesouvisí.
- (b) API mnohdy obsahuje četné chyby hodné důkladné analýzy.
- (c) Chybová analýza je nezbytná součástí každého útoku na a přes API.
- (d) Každý útok na a přes API je nezbytnou součástí chybové analýzy.

Správně: a

145. Český elektronický pas s aktivní autentizací:

- (a) Lze naklonovat snadno, pokud známe data z MRZ
- (b) Nelze snadno naklonovat (vyžaduje získání soukromého klíče pasu, který nelze z pasu vyčíst) a proto klonování českého pasu zatím nebylo veřejně předvedeno.
- (c) Lze naklonovat jen pokud spolupracuje skutečný držitel pasu a zná svůj PIN

Správně: b

146. Jak zajistíme integritu veřejného klíče

- (a) Utajením soukromé části veřejného klíče
- (b) Pomocí klíčované hašovací funkce
- (c) Částečným utajením veřejného klíče
- (d) Pomocí párového privátního klíče
- (e) Pomocí certifikátu veřejného klíče

Správně: e

147. Úspěšnost útoku hrubou silou se dá odhadnout podle vzorce

- (a) $(\text{velikost abecedy} * \text{délka hesla}) / (\text{počet odhadů za jednotku času})^{\text{čas platnosti}}$
- (b) $(\text{čas platnosti} * \text{počet odhadů za jednotku času}) / (\text{velikost abecedy})^{\text{délka hesla}}$
- (c) $(\text{délka hesla} * \text{počet odhadů za jednotku času}) / (\text{velikost abecedy})^{\text{čas platnosti}}$
- (d) $(\text{počet odhadů za jednotku času} * \text{délka hesla}) / (\text{čas platnosti})^{\text{velikost abecedy}}$

Správně: b

148. Proč musíme povolit určitou variabilitu mezi registračním vzorkem a později získanými biometrickými daty?

- (a) Z důvodu možné transplantace orgánu, aby i po ní bylo snímání možné.
- (b) Protože buňky mají přirozenou tendenci obnovovat se a tudíž mohou vznikat malé odlišnosti.
- (c) Protože biometrická data nejsou nikdy 100 % shodná.
- (d) Pokud je registrační vzorek nasnímám opravdu kvalitně, tak variabilita nemusí být povolena.

Správně: c

149. K čemu se používá CAPTCHA

- (a) K odlišení uživatelů od robotů
- (b) K odlišení chytrých robotů od robotů první generace
- (c) K testu uživatelů, zda chtějí luštit text v obrázku a opisovat jej
- (d) Je to dynamicky se měnící designový prvek www stránek

Správně: a

150. Německý elektronický pas první generace bez aktivní autentizace:

- (a) Nelze snadno naklonovat (vyžaduje získání soukromého klíče pasu, který nelze z pasu vyčíst).
- (b) Lze naklonovat jen pokud spolupracuje skutečný držitel pasu a zná svůj PIN
- (c) Lze naklonovat snadno, pokud známe data z MRZ

Správně: c

151. Které z uvedených možností jsou proveditelnými útoky při provedení autentizace prostřednictvím .rhosts

- (a) Vrácení podvržené IP adresy po dotazu na DNS server.
- (b) Útok hrubou silou.
- (c) Uvedení nepředpokládaného loginu uživatele.
- (d) IP spoofing.

Správně: a, c, d

152. Pro dynamickou autentizaci dat (DDA) platí, že:

- (a) Řeší problém padělání/duplikace karet
- (b) Potvrzuje pravost pouze statických dat uložených v čipové kartě.
- (c) Je prováděna platebním terminálem i čipem
- (d) Potvrzuje pravost statických dat uložených v čipové kartě, ale i dynamických dat zaslaných čipem
- (e) Je prováděna pouze čipovou kartou (terminál pouze zasílá data)
- (f) Potvrzuje pravost statických dat uložených v čipové kartě, ale i dynamických dat zaslaných terminálem

Správně: a, c, f

153. Zaručený elektronický podpis

- (a) Autorizuje podepisující osobu ve vztahu k datové zprávě
- (b) Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě
- (c) Je spojen s dostatečnou finanční zárukou
- (d) Umožňuje detekci změn ve zprávě, ke které je připojen
- (e) Je jednoznačně spojen s podepisující osobou
- (f) Je jednoznačně ověřitelný

Správně: b, d, e, f

154. Které z následujících nejsou hašovací funkce

- (a) RSA
- (b) MD5
- (c) SHA-1
- (d) AES
- (e) MD4
- (f) RC4

Správně: a, d, f

155. Které protokoly zaručují určitou míru jistoty o identitě jiné strany?

- (a) Protokoly pro ustavení klíče
- (b) Autentizační protokoly
- (c) Zero-knowledge protokoly (protokoly s nulovým rozšířením znalostí)
- (d) Protokoly implementované v Kerberu

Správně: b, c, d

156. Volitelné řízení přístupu

- (a) v určitých případech nezabrání neoprávněnému zveřejnění důvěrných dat
- (b) zavádí striktní hierarchii členění důvěryhodnosti dat
- (c) zavádí striktní hierarchii členění bezpečnosti dat

Správně: a

157. Které časově konstantní parametry se používají v kryptografických protokolech?

- (a) Žádné z uvedených
- (b) V omezeném čase monoliticky rostoucí sekvence (zabraňují tzv. borcení časové osy)
- (c) XOR hodnotou "-1" pro modifikaci náhodné výzvy (tzv. keksík)
- (d) Komplexní čísla s fixní imaginární i reálnou složkou
- (e) Sekvenční číslo (jeho hodnota závisí na implementaci)
- (f) Náhodná časová razítka (platná po určitou dobu - typicky několik desítek hodin)

Správně: a

158. Co patří mezi bezpečnostní problémy používání bankovních karet pouze s magnetickým proužkem?

- (a) Autentizační podpis je součástí karty.
- (b) Malá odolnost proti chybové analýze.
- (c) Relativně jednoduše se kopírují.
- (d) Přítomný hologram se obtížně automatizovaně kontroluje.

Správně: c, d

159. Mezi nevýhody ACL (seznam přístupových práv) patří:

- (a) je pomocí nich obtížné zjistit všechny subjekty, ke kterým má daný objekt přístup
- (b) je pomocí nich obtížné zjistit všechny objekty, ke kterým má daný uživatel přístup
- (c) je pomocí nich obtížné zjistit všechny subjekty, které mají k danému uživateli přístup
- (d) malá režie a tvrdá vyjadřovací schopnost

Správně: b

160. Které z uvedených možností autentizace klienta vůči serveru podporuje protokol ssh?

- (a) RSA autentizaci klienta.
- (b) Využitím protokolu pro nulové rozšíření znalosti.
- (c) Stroje uvedené v souborech .rhosts nebo hosts.equiv.
- (d) Heslem uživatele bez autentizace serveru.

Správně: a, c

161. Která z uvedených tvrzení pro Encapsulated Security Payload (ESP) nejsou pravdivá?

- (a) ESP nemá zajištěnu integritu a autenticitu dat, zajišťuje pouze důvěrnost dat.
- (b) ESP zajišťuje integritu, autenticitu a důvěrnost dat.
- (c) ESP zajišťuje obranu proti analýze šifrovaného provozu na úrovni síťové vrstvy.
- (d) ESP zajišťuje integritu, autenticitu a důvěrnost dat, nezajišťuje však obranu proti útoku přehráním.

Správně: a, c, d

162. Co znamená pojem elektronický podpis ve smyslu zákona o elektronickém podpisu?

- (a) Takový pojem zákon neobsahuje
- (b) To stejné, co digitální podpis
- (c) Ručně psaný podpis
- (d) Libovolná identifikující informace připojená ke zprávě

Správně: d

163. Jaká jsou platná tvrzení pro aktivní autentizaci elektronických pasů?

- (a) Pro autentizaci je použit zero-knowledge protokol (Fiat-Shamir), který zároveň ověří, zda má pas k dispozici soukromý klíč
- (b) Soukromý klíč je uložen v čipu, bez možnosti jeho přímého získání
- (c) Veřejný klíč je uložen ve čtečce el. pasů a je digitálně podepsán
- (d) Protokol výzva-odpověď lze použít pouze pokud čip neumožňuje efektivní implementaci zero-knowledge protokolu

Správně: b

164. Jaká je nevýhoda digitálního podepisování prováděného až po zašifrování dat

- (a) Žádná, naopak výhodou je možnost snadné verifikace podpisu ještě před dešifrováním
- (b) Výrazné urychlení kryptoanalýzy
- (c) Možnost snadného odstranění digitálního podpisu
- (d) Žádná, naopak, výhodou je možnost několikanásobného podepsání zašifrovaných dat

Správně: c

165. Silná bezkoliznost u hašovacích funkcí znamená

- (a) V rozumném čase nejsme schopni nalézt x, y ($x=y$) tak, že $h(x) \neq h(y)$
- (b) V rozumném čase nejsme schopni nalézt x, y ($x=y$) tak, že $h(x) = h(y)$
- (c) V rozumném čase nejsme schopni nalézt x, y ($x \neq y$) tak, že $h(x) = h(y)$
- (d) V rozumném čase nejsme schopni nalézt x, y ($x \neq y$) tak, že $h(x) \neq h(y)$

Správně: c

166. Jaká technologie PINmailerů je bezpečnější při útocích prosvícením?

- (a) Laserový tisk
- (b) Průklepový tisk

Správně: b

167. K prvkům hardwarové podpory řízení přístupu patří např.

- (a) tzv. zero address: pokud se proces pokusí přistupovat k nulové adrese, což bývá známkou chyby, je násilně zastaven
- (b) tzv. poštovní adresování: paměť je rozdělena na oblasti, aby OS mohl chránit paměť kontrolou znalosti tajného PSČ (tzv. ZIP code)
- (c) zákaz přístupu všem procesům kromě OS do adres paměti nižších než jistá hranice (tzv. fence address)
- (d) randomizace adres haldy (heap), na kterých se alokují dynamické proměnné běžících programů
- (e) existence několika úrovní oprávnění (tzv. rings) definujících přístupnost různých registrů a strojových instrukcí programovému kódu

Správně: c, e

168. Které z uvedených odpovědí jsou pravdivé?

- (a) Cena výroby jednoho kusu tokenu klesá při výrobě mnohakusové série.
- (b) Cena padělání typicky nezávisí na počtu padělaných kusů.
- (c) Cena padělání jednoho kusu klesá při uplatnitelnosti mnohakusové série padělku.
- (d) Relativní cena padělání se zvyšuje s každým dalším padělkem.

Správně: a

169. Jaké jsou používané algoritmy při digitálním podepisování

- (a) CBC
- (b) AES
- (c) DSA
- (d) RSA
- (e) El-Gamal

Správně: c, d, e

170. Při hašování hesel pro autentizaci uživatelů pomocí hesel:

- (a) Ukládáme pouze haš hesla a rekonstrukce otevřené podoby není možná
- (b) Ukládáme pouze haš hesla s možností rekonstrukce hesla v otevřené podobě
- (c) Při ukládání můžeme využít techniky "solení"

Správně: a, c

171. Mezi skryté kanály (covert channels) patří:

- (a) čítač vadných sektorů (Bad Blocks Counter, BBC)
- (b) zaplnění disku
- (c) kanál částečně autorizovaného přenosu dat sběrnice MAC
- (d) aktuální zátěž procesoru
- (e) aktuální uzel v síti (Current Network Node, CNN)

Správně: b, d

172. Chybovost biometrických systémů závisí na:

- (a) Schopnosti a motivaci uživatelů.
- (b) Nastavení systému.
- (c) Typu snímače.
- (d) Okolním prostředím.

Správně: a, b, c, d

173. Útok na hesla může být

- (a) Slovníkový
- (b) Pomocí sociálního inženýrství
- (c) Matrixovou metodou
- (d) Hrubou silou
- (e) Na základě určitých znalostí o uživateli

Správně: a, b, d, e

174. Protokoly výzva-odpověď mohou být založeny na:

- (a) klíčované hašovací funkci
- (b) symetrickém šifrování
- (c) digitálním podpisu
- (d) MAC kódu, resp. funkci

Správně: a, b, c, d

175. Základní techniky zajištění soukromí u RFID tagů jsou:

- (a) Selektivní blokování tagů
- (b) Deaktivace či rušení RFID tagu
- (c) Kryptografické metody pro zajištění soukromí pomocí soukromých klíčů asymetrické kryptografie (s potenciální možností využití hybridního šifrování)
- (d) Využití protokolů zajišťujících anonymitu jednotlivých stran
- (e) Důsledné utajení existence RFID tagu
- (f) Změna jedinečného identifikátoru

Správně: a, b, f

176. Vhodná tajná informace pro autentizaci je

- (a) Rodné příjmení matky
- (b) Tel. číslo, pokud není uvedeno ve Zlatých stránkách
- (c) Heslo
- (d) PIN
- (e) Fráze (passphrase)

Správně: c, d, e

177. Mezi reálně používané biometrické technologie patří

- (a) dynamika pohybu hlavy
- (b) otisk prstu
- (c) srovnání obličeje
- (d) geometrie (tvaru) nohy
- (e) vzor oční panenky

Správně: b, c

178. Mezi problémy při správě víceúrovňových systémů (MLS) typicky patří:

- (a) nestabilita aplikací využívajících MLS
- (b) nevhodné chování procesů
- (c) náročná administrace
- (d) neexistující nástroje pro administraci
- (e) propojování jednotlivých MLS systémů
- (f) obtížná/nejednoznačná klasifikace dat

Správně: c, e, f

179. Co nezajišťuje protokol ssh?

- (a) Autentizaci uživatele.
- (b) Ochranu proti analýze provozu.
- (c) Ochranu proti distribuovanému odmítnutí služby.
- (d) Autentizaci serveru.

Správně: b, c

180. Přístupová hesla můžeme rozlišit na

- (a) Jednorázová
- (b) Veřejná
- (c) Původně neveřejná
- (d) Skupinová
- (e) Unikátní pro danou osobu
- (f) Jednocestná

Správně: a, d, e

181. Dynamická autentizace dat (DDA) se liší oproti statické autentizaci dat (SDA) tím, že:

- (a) vyžaduje čip s dostatečnou paměťovou kapacitou, ale nevyžaduje koprocessor
- (b) vyžaduje nový unikátní pár RSA klíčů
- (c) vyžaduje nový unikátní pár AES klíčů
- (d) vyžaduje, aby byl veřejný klíč podepsán a uložen společně se statickými aplikačními daty
- (e) vyžaduje bezpečně uložený certifikát umožňující kartě ověřit pravost platebního terminálu
- (f) vyžaduje čip s kryptografickým koprocessorem

Správně: b, d, f

182. Současné čipové karty:

- (a) Umožňují pouze provádění kryptografických operací asymetrické kryptografie.
- (b) Neumožňují provádění kryptografických operací.
- (c) Umožňují provádění kryptografických operací symetrické a asymetrické kryptografie s využitím koprocessoru.
- (d) Umožňují pouze provádění kryptografických operací symetrické kryptografie.

Správně: c

183. Fyzickou bezpečností se u čipových karet myslí:

- (a) Ochrana proti hloubkové odběrové analýze na úrovni procesoru.
- (b) Ochrana proti fyzickému zkoušení PINu hrubou silou.
- (c) Fyzická překážka kolem čipu karty ztěžující neautorizovaný přístup.
- (d) Odolnost proti útokům vyžadujícím fyzický přístup ke kartě.

Správně: d

184. Mezi základní nedostatky při snímání obličeje nepatří

- (a) nasazené kontaktní čočky.
- (b) pestré a barevné pozadí.
- (c) nasazená čepice.
- (d) zavřené oči.

Správně: a

185. Jaké vlastnosti má Shamirův protokol bez klíčů (Shamir's no-key protocol)

- (a) Nevyžaduje žádné ustavení sdílených klíčů
- (b) Vyžaduje komutativní šifrovací algoritmus
- (c) Funguje obzvláště dobře (a prokazatelně bezpečně) jen při použití One-Time Pad
- (d) Prokazuje, že $P \neq NP$
- (e) Umožňuje vzájemnou autentizaci

Správně: a, b

186. Co je to heslo založené na frázi?

- (a) Heslo, které obsahuje pouze malá písmena
- (b) Heslo založené na veřejně známé frázi, aby si jej všichni snadno zapamatovali
- (c) Heslo, které lze jednoduše přechýšit
- (d) Pomůcka pro zapamatování složitějšího hesla

Správně: d

187. Jaké vlastnosti mají magneto-optické čipové karty?

- (a) Umožňují snímání čárových kódů zobrazovaných na monitoru při vstupu do internetového bankovníctví a jejich okamžité zpracování v čipu.
- (b) Žádná z výše uvedených odpovědí.
- (c) Poskytují magneto-optické rozhraní pro vysokorychlostní a prokazatelně bezpečný přenos dat.
- (d) Neumožňují provádění kryptografických operací i přesto, že obsahují sofistikovanější magneto-optický proužek. Každá z dvou komunikujících stran má svůj symetrický klíč.

Správně: b

188. Kolik zpráv se vymění ve Shamirově protokolu bez klíčů, aby obě strany sdílely stejný klíč?

- (a) 2
- (b) 4
- (c) 3
- (d) žádná z těchto odpovědi není správná

Správně: c

189. Útok na čipové karty přes aplikační rozhraní (API) je založen na:

- (a) Využití chyby v návrhu rozhraní.
- (b) Nezamýšleném dopadu zpracování útočníkem zaslaných specifických vstupních dat.
- (c) Nedostupnosti aplikačního rozhraní vnitřnímu prostředí karty.
- (d) Využití indukce chyb do zpracování dat zaslaných přes aplikační rozhraní.

Správně: a, b

190. Které politiky řízení přístupu existují a používají se:

- (a) asystematické řízení přístupu
- (b) volitelné řízení přístupu
- (c) povinné řízení přístupu
- (d) biometrické řízení provozu
- (e) skryté řízení přístupu

Správně: b, c

191. Ukládání hesel lze realizovat

- (a) Hašovaně
- (b) Impulzně
- (c) V otevřené podobě
- (d) Šifrovaně
- (e) Hlasovaně

Správně: a, c, d

192. Jaká je správná sekvence operací při ověřování PINu odolná proti přerušení napájení?

- (a) Zvýšení čítače, test čítače pokusů větší než 0, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.
- (b) Test čítače pokusů větší než 0, snížení čítače, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.
- (c) Test čítače pokusů větší než 0, zvýšení čítače, ověření korektnosti PINu, zvýšení čítače při dobrém PINu.
- (d) Test čítače pokusů větší než 0, ověření korektnosti PINu, snížení čítače při špatném PINu.

Správně: b

193. Co je to hašovací funkce?

- (a) Funkce, která mapuje libovolně velký vstup na výstup s délkou 128, 192, 256 nebo 512 bitů
- (b) Funkce, která mapuje libovolně velký vstup na výstup fixní délky a není prostá
- (c) Funkce, která mapuje libovolně velký vstup na výstup fixní délky a je prostá
- (d) Funkce, která mapuje vstup fixní délky na výstup variabilní délky (podle entropie vstupu)
- (e) Šifrovací funkce se schopností deprese vstupních dat

Správně: b

194. Chybové hlášení o změně integritního součtu veřejného klíče serveru u SSH může být způsobeno ???

- (a) Změnou dlouhodobého klíče serveru jeho administrátorem
- (b) Chybějícím záznamem veřejného klíče v souboru známých serverů
- (c) Podvržením serveru útočnickovým strojem
- (d) Změnou souboru s veřejným klíčem serveru na uživatelově PC ???

Správně: a, c

195. Které z uvedených možností zajišťuje protokol IPsec?

- (a) Nepopíratelnost přijetí dat.
- (b) Důvěrnost dat, ochrana proti útoku přehráním.
- (c) Autentizace a integrita původu dat.
- (d) Podporu správy klíčů.

Správně: b, c, d

196. Testování živosti obvykle nemá následující dopady

- (a) nepříjemné pocity brnění v oblasti testovaného vzorku.
- (b) zvýšený počet nesprávných odmítnutí.
- (c) zvýšení ceny zařízení.
- (d) vyšší náklady na vývoj a výrobu.

Správně: a

197. Při autentizaci tajnou informací je nutné dodržet

- (a) Tajnou informaci musí vědět jen oprávněný uživatel
- (b) Tajnou informaci musíme sdělit administrátorovi pro případně admin. zásahy v našem systému
- (c) Z tajné informace se musí nejprve vytvořit inicializační vektor
- (d) Prostor, ze kterého vybíráme hodnotu tajné informace musí být rozsáhlý

Správně: a, d

198. Která z uvedených tvrzení o řízení přístupu k datům na čipových kartách jsou pravdivá?

- (a) Data jsou uchována na magnetickém proužku a před použitím v čipu kontrolována.
- (b) Každý soubor má přiřazenu hlavičku s přístupovými právy.
- (c) Data na kartě nemohou být po zápisu nikdy čtena ani měněna.
- (d) Založeno především na řízení přístupu k souborům.

Správně: b, d

199. Co je to odpověď na narušení?

- (a) Žádná z výše uvedených odpovědí.
- (b) Služba internetového bankovníctví umožňující automaticky detekovat a upozornit na aktivní nebezpečný software v počítači.
- (c) Reakce nechráněné části systému na potencionální útok.
- (d) Reakce chráněné části systému na probíhající pokus o útok.

Správně: d

200. Z hlediska lidské paměti je vhodné volit

- (a) Složitá, ale snadno zapamatovatelná hesla
- (b) Jednoduchá a jednoduše zapamatovatelná hesla
- (c) Obtížně zapamatovatelná hesla a každý měsíc nutit uživatele ke změně
- (d) Hesla založená na frázích

Správně: a, b, d

201. Pro urychlení počítačových systémů využívajících digitální podpis

- (a) u čipových karet bývají použity kryptografické koprocesory
- (b) používají obě strany identický privátní klíč
- (c) se často používá podchlazování ochranných komponent čipových karet
- (d) obvykle využíváme hašovací funkce pro reprezentaci podepisovaných dat
- (e) lze využít prokazatelnou odpovědnost metodou Monte Carlo

Správně: a, d

202. Pro autentizaci v sítích GSM se používá:

- (a) asymetrická kryptografie s protokolem RAND
- (b) dvoufaktorová autentizace – SIM a (nepovinný) PIN
- (c) jedno nebo dvoufaktorová autentizace podle nastavení PINu
- (d) Shamirův bezklíčový protokol
- (e) zero-knowledge protokol Fiat-Feige se čtyřmi faktory

Správně: b, c

203. Úspěšnost hádání hesel hrubou silou:

- (a) klesá s velikostí použité abecedy
- (b) záleží na zapamatovatelnosti a struktuře hesla
- (c) roste s dobou platnosti hesla
- (d) ovlivnil výzkum Zvirana & Hagy (1993)
- (e) klesá s délkou hesla
- (f) klesá s rostoucí rychlostí útočnickova počítače

Správně: a, c, e

204. Offline verifikace karet ní transakce:

- (a) je zakalkulovaná v systému řízení rizik a provádí se pro snížení transakčních nákladů
- (b) se dnes již v bankomatech neprovádí
- (c) se za určitých podmínek provádí v PINpadu
- (d) vyžaduje přiblížení pasu s čipem podporujícím DDA k PINpadu
- (e) se používá jen v zemích Eurozóny (země platící eurem)
- (f) je povolena jen při biometrické autentizaci uživatele

Správně: a, b, c

205. Terminologický nesmysl je:

- (a) zajištění integrity dat pomocí hašovací funkce
- (b) kryptografické hašovací funkce mají být rychlé a jednosměrné
- (c) vodotisk hesla /etc/shadow
- (d) zaručený elektronický podpis založený na kvalifikovaném certifikátu
- (e) kryptace sdíleného souboru s ufpornem
- (f) kryptoanalýza zakryptovaného souboru

Správně: c, e, f

206. Pro bezpečnostní úrovně modelu Bell-LaPadula $L1=(TS, obrana, ekonomika)$ a $L2=(S, obrana)$ platí:

- (a) $L1$ a $L2$ jsou neporovnatelné
- (b) $L1$ dominuje $L2$
- (c) $L2$ dominuje $L1$
- (d) $L1$ a $L2$ jsou neporovnatelné, pokud neplatí exkluzivita *-vlastnosti

Správně: b

207. Token s generátorem jednorázových hesel lze považovat za mechanismus dvoufaktorové autentizace:

- (a) jen pokud se jím vygenerované heslo dá použít právě ve dvou autentizačních systémech
- (b) jen pokud se heslo generuje na základě dvou faktorizačních problémů
- (c) pokud se uživatel musí autentizovat vůči tokenu před jeho použitím svým heslem
- (d) pokud se uživatel musí autentizovat vůči tokenu před jeho použitím svým PINem

Správně: c, d

208. Hybridní čipová karta

- (a) pracuje se dvěma různými čipy
- (b) je nyní výhradní technologií pro bankovní karetní operace
- (c) poskytuje možnost komunikace přes kontaktní i bezkontaktní rozhraní
- (d) je založena na využití kombinace asymetrické a symetrické kryptografie

Správně: a, c

209. Dodatečná autorizace citlivých/významných operací se provádí obvykle:

- (a) autorizací této operace klíčem z kořenového certifikátu
- (b) reputačním systémem bankovního dozorce
- (c) odděleným (separátním) kanálem
- (d) s použitím dalšího autorizačního kroku
- (e) SSL certifikátem s tzv. extended validation (EV)

Správně: c, d

210. Která z následujících tvrzení o čipových kartách jsou pravdivá?

- (a) Bezkontaktní čipová karta potřebuje anténu pro komunikaci i získávání energie.
- (b) Komunikaci mezi čtečkou a bezkontaktní čipovou kartou lze odposlechnout.
- (c) Kontaktní čipová karta má vlastní zdroj energie a komunikuje se čtečkou přímo.
- (d) U bezkontaktní čipové karty je zajištěno autorizované smazání dat při výpadku napájecího napětí.

Správně: a, b

211. PIN je

- (a) s obvodním bankéřem sdílená informace
- (b) nejčastěji volen v hodnotách 1234, 0000, 0007 nebo 1111
- (c) doplňkovým bezpečnostním mechanismem pro operace s bankomatem
- (d) nastaven bankou jako haš hesla internetového bankovníctví

Správně: b, c

212. Mezi techniky pro zajištění soukromí v autentizačních systémech patří:

- (a) maskování prvních 5 bajtů strojově čitelné zóny elektronických pasů
- (b) pravidelná změna identifikátoru čipu
- (c) uložení podepsaných hašů do EF.SO_D elektronických pasů
- (d) pasivní rušení (Faradayova klec) čipu

Správně: b, d

Full text

1. Napište 2 výhody a 2 nevýhody autentizace biometrikou oproti jiné metodě.
2. Popište, jak probíhá man in the middle útok na Diffie-Hellman protokol.
3. Co jsou a jak fungují tokeny založené na hodinách? Jaké jsou jejich bezpečnostní nedostatky?
4. model Bell-LaPadula (nepamatuji si přesně)

1. Statická autentizácia dát u EMV.
2. Výkonová analýza u čipových kariet.
3. Časové razítka.
4. Výhody a nevýhody autentizácie heslom.

1. Popište, jak probíhá man in the middle útok na Diffie-Hellman protokol.
2. Popište stručně jak se provádí odběrová analýza u čipové karty.
3. Napište 2 výhody a 2 nevýhody autentizace biometrikou oproti jiné metodě.
4. Jak probíhá Shamirův protokol (přesné znění si nepamatuji).