

1. Co je to "původně neveřejný" pseudonym?

- * Pseudonym, který původně nebyl veřejný, ale v některých případech může být zveřejněn.
- Pseudonym, který musí být po druhém použití zveřejněn.
- Pseudonym původně neurčený pro veřejnost, který ale neschválil Úřad pro ochranu osobních údajů.
- Pseudonym, který musí být při druhém použití zveřejněn.

2. K bezpečným metodám autentizace klienta bance v systému internetového bankovníctví patří prokázání se

- * osobním klíčem uloženým bezpečně na čipové kartě, USB flashdisku či SD kartě.
- kódem získaným vložením rodného čísla či uživatelského hesla do autentizační "kalkulačky".
- rodným číslem.
- heslem, které si klient zvolil při zakládání účtu.
- * kódem získaným vložením výzvy (challenge) bankovního systému do autentizační "kalkulačky".

3. Digitální podpis v PGP probíhá tak, že se

- vytvoří haš zprávy, který se podepíše veřejným klíčem příjemce
- zpráva se podepisuje přímo klíčem dle volby uživatele
- vytvoří haš zprávy, který se podepíše veřejným klíčem odesílatele
- * vytvoří haš zprávy, který se podepíše soukromým klíčem odesílatele
- vytvoří haš zprávy, který se podepíše soukromým klíčem příjemce

4. Autentizaci obecně

- * může někdy provádět člověk samostatně (bez pomoci počítače nebo čipové karty)
- * může někdy provádět počítač nebo čipová karta samočinně (bez pomoci člověka)
- musí pokaždé provádět počítač nebo čipová karta ve spolupráci s člověkem (počítač nebo karta sama nestačí)
- musí pokaždé provádět člověk ve spolupráci s počítačem nebo čipovou kartou (člověk sám nestačí)

5. Jaká rizika s sebou nese zasílání platebních karet a PINů poštou?

- Libovolná platební karta může být skrze neporušenou obálku snadno zkopírována.
- * Poštovní obálku lze během doručování ztratit.
- * PIN může být skrze neporušenou obálku nepozorovaně přečten.
- Platební karta je skrze obálku vystavena tzv. napětovým a teplotním útokům.

6. Odmítnutí služby (Denial of Service) je

- útok, kdy zpracování požadavku na webovém serveru nevyhnutelně skončí s HTTP chybou 500.
- * útok, který uvede server do stavu, kdy není schopen reagovat na požadavky.
- stav, kdy server včas zjistí útok a zamítne další komunikaci s útočníkem.
- stav, kdy server zjistí nedostatečnou autorizaci uživatele k operaci.

7. Proxy servery jsou na Internetu

- zbytečné, pouze zpomalují rychlost dat a jsou snadno zneužitelné.
- * často způsobem jak obejít lokální bezpečnostní politiku.
- zdrojem všeho zla, patřily by zakázat.
- zaručeným prostředkem anonymního využívání Internetových zdrojů.
- * důležité, rozumí aplikačním protokolům, umožňují anonymizaci.

8. Které z následujících možností obsahují jen relevantní bezpečnostní funkce systémů pro ochranu inf. soukromí?

- nespojitelnost, nepozorovatelnost, anonymita, pseudonymita, identita.
- identita, nepozorovatelnost, anonymita, pseudonymita.
- nezjistitelnost, nespojitelnost, anonymita, pseudonymita.
- * nespojitelnost, nepozorovatelnost, anonymita, pseudonymita.

9. Jaké jsou základní vlastnosti kvantitativní analýzy rizik?

- Výstup je nesrozumitelný.
- * Výstup je v nějaké konkrétní hodnotě, např. v určité částce.
- * Výstup je lehce srozumitelný.
- Postup je plně automatizovatelný.
- Výstup není v nějaké konkrétní hodnotě, např. v určité částce.
- * Postup není automatizovatelný.

10. Jaké jsou základní vlastnosti kvalitativní analýzy rizik?

- * Výstup je nesrozumitelný
- Výstup je v nějaké konkrétní hodnotě, např. v určité částce
- * Postup je do značné míry automatizovatelný
- Výstup je lehce srozumitelný
- * Výstup není v nějaké konkrétní hodnotě, např. v určité částce
- Postup není automatizovatelný

11. Čipová kreditní karta bez mag. proužku

- obvykle neobsahuje procesor, přestože se jí tradičně říká "čipová".
- * skýtá obvykle vyšší bezpečnost než karta s mag. proužkem (bez čipu).
- * obvykle obsahuje malý procesor.
- skýtá obvykle nižší bezpečnost než karta s mag. proužkem (bez čipu).

12. Při podpisu s obnovou dat platí:

- Podepisovaná data lze z podpisu obnovit při znalosti soukromého klíče.
- Podepisovaná data nejsou součástí podpisu, je nutné je obnovit nezávislým komunikačním kanálem.
- * Podepisovaná data mohou být obnovena kýmkoli, kdo vlastní příslušný veřejný klíč.
- * Podpis obsahuje i podepisovaná data.

13. Která z následujících tvrzení platí:

- integrita zaručuje důvěrnost.
- důvěrnost zaručuje integritu.
- * neplatí ani jedno tvrzení.
- silná integrita zaručuje důvěrnost.
- prokazatelná zodpovědnost vyžaduje důvěrnost.

14. Poskytuje TOR testování integrity přenášených dat?

- Ne, proč bychom něco takového potřebovali, stačí zaručená anonymita.
- * Ano, je to obrana proti tagging útokům.
- * Ano, je to vylepšení oproti původnímu návrhu Onion Routing systémů.
- Ano, je to obrana proti mig-in-the-middle útokům.

15. Co patří mezi cíle bezpečnostní politiky?

- Identifikovat ochraňované prostředky firmy.
- Přenést odpovědnost na třetí strany.
- Eliminovat všechny útočníky.
- * Minimalizace (kontrola) rizik.
- * Stanovení strategie pro použití bezpečnostních funkcí.

16. Protože standard GSM obsahoval bezpečnostní chyby,

- * byl navržen protokol 3GSM.
- začalo se v některých zemích používat GSM šifrování SMS zpráv (hlasová data se už tak těžko zpracovávají).
- začalo se v některých zemích používat GSM šifrování hlasových přenosů a SMS zpráv.
- byl navržen protokol 4GSM, ve kterém se šifruje novou symetrickou šifrou SHA-3.

17. V případě, že nespokojení uživatelé jsou "menší zlo" než neoprávnění uživatelé, nastavíme

- biometrický systém tak, že bude mít FAR (False Acceptance Rate) a FRR (False Rejection Rate):
- nízkou hodnotu FRR a nízkou hodnotu FAR.
- vysokou hodnotu FRR a vysokou hodnotu FAR.
- * vysokou hodnotu FRR a nízkou hodnotu FAR.
- vysokou hodnotu FAR a nízkou hodnotu FRR.

18. Zákon o ochraně osobních údajů:

- * nevztahuje se na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.
- * vztahuje se na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.
- * nevztahuje se na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány, nebo pokud nejsou pro podnikání.
- vztahuje se na zabezpečení zpracovávaných osobních údajů v případě automatizovaných prostředků dodávaných ze zemí mimo EU.
- nevztahuje se na data poskytovaná dobrovolně státním institucím.

19. Pod pojmem symetrická kryptografie rozumíme:

- * Kryptografie s využitím stejného klíče pro šifrování i dešifrování.
- Kryptografie s takovým algoritmem, jehož všechny operace splňují matematickou vlastnost symetrie nad danou grupou.
- Kryptografie s takovým algoritmem, který umožňuje komukoli symetricky ověřit pravost podpisu.
- Kryptografie s využitím klíče, který je na binární úrovni symetrický.

20. Systém detekce průniku (IDS)

- je možné použít buď v síti nebo na počítači
- * je možné použít v síti i na počítači
- poskytuje lepší ochranu než firewall
- má smysl používat pouze jako síťový prvek, kdy detekuje a informuje o probíhajícím útoku.

21. Chybovost biometrických systémů vyjádřená pomocí FAR

(False Acceptance Rate) je:

Podíl počtu neúspěšně provedených pokusů o podvod ku počtu úspěšně provedených pokusů o přihlášení do systému.

Podíl počtu úspěšně provedených pokusů o podvod ku počtu všech pokusů o podvod.

* Podíl počtu úspěšně provedených pokusů o podvod ku počtu všech pokusů o přihlášení do systému.

Podíl počtu neúspěšně provedených pokusů o podvod ku počtu všech pokusů o podvod.

22. Chybovost biometrických systémů vyjádřená pomocí FTE (Fail to Enroll) je:

Podíl počtu uživatelů, které systém zaregistroval na více než jeden pokus, ku počtu všech uživatelů systému.

Podíl počtu uživatelů, které systém neverifikoval, ku počtu všech pokusů uživatelů o přihlášení do systému.

Podíl počtu uživatelů, které systém zaregistroval, ku počtu uživatelů systému, které systém nezaregistroval.

* Žádná z těchto odpovědí není správná.

23. Chybovost biometrických systémů vyjádřená pomocí FRR (False Rejection Rate) je:

Podíl počtu akceptovaných pokusů o legitimních legitimních uživatelů ku počtu odmítnutých pokusů o přihlášení legitimních uživatelů.

Podíl počtu všech pokusů o přihlášení legitimních i nelegitimních uživatelů ku počtu všech pokusů o přihlášení legitimních uživatelů.

Podíl počtu akceptovaných pokusů o přihlášení legitimních uživatelů ku počtu všech pokusů o verifikaci legitimních uživatelů.

* Podíl počtu odmítnutých pokusů o přihlášení legitimních uživatelů ku počtu všech pokusů o přihlášení.

24. Digitální podpis zajišťuje

Komprimaci podepisovaných dat.

Platnost podepisovaných dat.

Důvěrnost podepisovaných dat.

* Autentizaci podepisovaných dat.

25. Digitální podpis zajišťuje

* Integritu podepisovaných dat.

Obnovu privátního klíče při jeho ztrátě.

Důvěrnost podepisovaných dat.

Autorizaci podepisovaných dat.

26. Pokud má hašovací funkce vlastnost silné bezkoliznosti, znamená to, že:

Nelze nalézt dva navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné.

Je výpočetně neproveditelné nalézt k danému vstupu jiný vstup tak, aby byly výsledné haše pro oba vstupy stejné.

* Je výpočetně neproveditelné nalézt dva libovolné navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné.

Nelze nalézt dva navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné na alespoň 1/2 pozic.

27. Pokud má hašovací funkce vlastnost slabé bezkoliznosti, znamená to, že:

Nelze nalézt dva navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné na alespoň 1/2 pozic.

* Je výpočetně neproveditelné nalézt k danému vstupu jiný vstup tak, aby byly výsledné haše pro oba vstupy stejné.

Nelze nalézt dva navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné.

Je výpočetně neproveditelné nalézt dva libovolné navzájem různé vstupy takové, aby byly výsledné haše pro oba vstupy stejné.

28. Které z následujících pojmů se vztahují ke Společným kritériím (CC).

Subjekt hodnocení (Subject of Evaluation, SOE)

* Profil bezpečnosti (Protection Profile, PP)

Specifikace síťové bezpečnosti (Network Security Target, NST)

* Předmět hodnocení (Target of Evaluation, TOE)

* Specifikace bezpečnosti (Security Target, ST)

Profil prokazatelné bezpečnosti (Provable Protection Profile, PPP)

29. Citlivé osobní údaje dle české legislativy vypovídají o:

* zdravotním stavu.

postoji k trestné činnosti rodinných příslušníků.

majetkových poměrech státních úředníků.

* sexuální orientaci.

30. Základní metody autentizace uživatelů jsou založeny na něčem, co

* vím.

smím.

* mám.

31. Z jakého důvodu se doporučuje podepisovat vlastní veřejný klíč privátním klíčem:

pro zvýšení entropie veřejného klíče.

* pro zajištění jeho integrity.

nedoporučuje se.

pro zvýšení jeho důvěryhodnosti o vyšší počet podpisů.

pro zarovnání délky veřejného klíče na hodnotu dělitelnou délkou veřejného modula.

32. V případě nepozorovatelnosti (unobservability) je ochraňovanou hodnotou?

Informace o překročení přiděleného procesorového času pro použití nabízených zdrojů a služeb.

Informace o přihlášených uživateli.

* Informace o použití zdrojů a služeb.

Informace o aplikovaných bezpečnostních opatřeních systému (např. nastavení pravidel firewallu).

33. Proti obecným OR (Onion Routing) sítím přináší TOR navíc

poskytuje téměř real-time anonymní spojení pro různé služby.

podporu šifrování dat proudovou šifrou se symetrickým klíčem.

* adresářové servery s informacemi o jednotlivých routerech.

* podporu skrytých služeb a míst setkání.

34. Která z uvedených tvrzení jsou pravdivá?

- Symetrická kryptografie se využívá pouze pro šifrování, zatímco asymetrická pouze k podepisování.
- Pokud chceme využít asymetrickou kryptografii k šifrování, musí zůstat oba klíče utajeny.
- Teoreticky lze použít asymetrickou kryptografii i k šifrování, ale v praxi se toho nevyužívá.
- * Symetrická kryptografie využívá jeden klíč sdílený mezi dvěma a více uživateli.

35. Co je to odvození (inference)?

- * Odvozením získáváme nepřímý přístup k informacím bez přímého přístupu k datům, která tyto informace reprezentují.
- Odvození nových informací se stejnou citlivostí zpracováním a analýzou skupiny informací určité citlivosti.
- Opak agregace.
- * Odvození informací o vyšší citlivosti zpracováním a analýzou skupiny informací o nižší citlivosti.
- Odvození nových informací s nižší citlivostí zpracováním a analýzou skupiny informací o vyšší citlivosti.

36. Pod pojmem dostupnost dat rozumíme

- Data by měla být dostupná i neautorizované osobě v případě kritické události.
- Průběh autentizace osoby pro práci s daty a službami by měl být dostupný i lidem se sníženou pracovní schopností.
- Uživatelé by měli mít přístup k datům a službám co nejméně komplikovaný.
- * Autorizovaní uživatelé by měli mít přístup k datům a službám co nejméně komplikovaný.

37. Systémy měnící tok a výskyt dat na komunikačním kanálu se nazývají

- * mixy.
- * anonymitní.
- mutexy.
- minixy.
- minmaxy.

38. Bezpečnostní politika zahrnuje

- Specifikaci technologických opatření kterými budou prosazovány bezpečnostní požadavky společnosti
- Seznam konkrétních osob, které mají povoleno přistupovat k citlivým datům společnosti.
- * Požadavky, pravidla a postupy určující způsob ochrany a zacházení s hodnotami společnosti.

39. Protokoly SSL/TLS

- není snadné integrovat do již existujících aplikací.
- * se chovají k protokolům aplikační vrstvy OSI modelu transparentně.
- není vhodné používat ve starších operačních systémech pro 32bitové procesory.
- nepředstavují zvýšené nároky na výpočetní výkon komunikujících stran.
- * vyžadují zajištění vhodného systému správy (kryptografických) klíčů.

40. Základní metody autentizace uživatelů jsou založeny na něčem, co

- nelze jednoduše zničit.
- * znám.
- * jsem.

41. Co je to perturbační technika používaná ve statistických databázích?

Žádná taková technika neexistuje.

Pro vyhodnocení dotazu nesmí být použito více záznamů než je stanovená maximální (perturbační) mez.

Pro vyhodnocení dotazu může být použito pouze menší množství záznamů než je stanovená maximální (perturbační) mez.

* Technika stavějící např. na zaokrouhlování mezivýsledků dotazů.

* Technika umožňující zjistit konzistentní, ale ne spolehlivé odpovědi na sérii podobných dotazů.

* Přidávání pseudonáhodného "šumu" k množině záznamů, na jejichž základě se vyhodnotí dotaz.

42. Která z těchto tvrzení jsou správná?

Se zvýšením FAR se zvyšuje FRR.

* Se snížením FAR se zvyšuje FRR.

* Se zvýšením FAR (False Acceptance Rate) se snižuje FRR (False Reject Rate).

Se snížením FAR se snižuje FRR.

43. Co je výsledkem hodnocení systému podle Společných kritérií (CC)?

Popis, jakým způsobem je v hodnoceném systému dosaženo daných vlastností

Subjektivní (ze strany hodnotitele) hodnocení bezpečnosti systému

Sada doporučení, jak hodnocený systém zabezpečit

* Diskrétní hodnocení (ano/ne) daných požadavků na hodnocený systém

44. Pod pojmem hybridní kryptosystémy rozumíme například

Data jsou před podpisem zašifrována algoritmem asymetrické kryptografie.

* Data jsou šifrována náhodným symetrickým klíčem, ten je šifrován veřejným klíčem příjemce.

Data jsou před šifrováním algoritmem symetrické kryptografie hašována, šifrována je pouze výsledná haš.

45. Mezi bezpečnostní požadavky podle standardu pro hodnocení kryptografických modulů

FIPS 140-1/2 patří:

* Fyzická bezpečnost

* Rozhraní modulu

* Bezpečnost O/S

Testování GUI modulu

* Služby a autentizace

Odolnost vůči lidskému faktoru

46. Bezpečnost je založena především na

* prevenci, detekci a reakci na možné problémy

správném nastavení bezpečnosti sítě i koncových stanic

aktualizovaném antiviru a správně nastaveném firewallu, příp. i využití PGP

dohodě s uživateli

47. Mezi bezpečnostní požadavky podle standardu pro hodnocení kryptografických modulů FIPS 140-1/2 patří:

Elektromagnetická rezonance

* Správa klíčů

* Služby a autentizace

* Rozhraní modulu

Flexibilita modulu

* Metody pro zmírnění jiných útoků

48. Cibulové schéma používané např. v Onion Routing

- * využívá symetrické i asymetrické kryptografie
- používá pouze asymetrickou kryptografii
- používá pouze symetrickou kryptografii, protože je rychlejší
- kryptografie se nepoužívá vůbec, není potřeba

49. Která z těchto tvrzení, pokud mluvíme o biometrických systémech, jsou správná?

- * Proces identifikace je náročnější než proces verifikace.
- Na začátku procesu verifikace není identita známa.
- * Na začátku procesu verifikace je identita známa.
- Proces verifikace je náročnější než proces identifikace.

50. Co je cílem zajištění důvěrnosti dat?

- Utajit existenci sémantiky dat před nedůvěryhodnými osobami
- Zamezit změně sémantického obsahu dat neautorizovanými osobami
- * Zabránit zjištění sémantického obsahu dat neautorizovanými osobami

51. Autentizace je

- překlep - správně je "autorizace"
- volitelná (ale obvykle přítomná) fáze procesu prokazování identity
- * všechny ostatní možnosti jsou nepravdivé
- proces nezbytný pro ustavení šifrované komunikace u bezdrátového spojení

52. Systém detekce průniku (IDS)

- je možné použít buď v síti nebo na počítači
- má smysl používat pouze jako síťový prvek, kdy detekuje a informuje o probíhajícím útoku
- * je možné použít v síti i na počítači
- poskytuje lepší ochranu než firewall

53. Které tvrzení je správné:

- Při TLS/SSL "Handshake" se povinně kontrolují certifikáty obou stran.
- "Record" protokol dovoluje předávat/ukládat nezabezpečená data pro potřeby vlády USA, podle §708, odstavce 17 zákona o vnitřní bezpečnosti.
- * TLS/SSL "Handshake" protokol slouží k ustavení zabezpečeného spojení,
- "Record" protokol představuje základní vrstvu.
- Při TLS/SSL "Handshake" se provádí autentizace uživatele heslem.
- Použití TLS/SSL "Handshake" protokolu je volitelné v závislosti na požadavcích klienta a serveru.

54. Podle čeho je určen počet kol/rund u algoritmu Rijndael.

- Délka bloku
- Délka klíče a bloku
- Inicializační vektor
- Inicializační vektor a délka bloku
- Délka zprávy
- * Délka klíče

55. Pseudonymita (podle A.Pfitzmanna - mixy) znamená:

- * Používání pseudonymu jako identifikátoru (ID)
- Bytí anonymním s možností zpětného zjištění skutečné identity
- Bytí anonymním pouze vůči uživatelům systému, nikoli vůči administrátorům

56. Pod pojmem slabá integrita dat rozumíme

- Data nesmí bez svolení autorizované osoby změnit svůj stav vůbec
- * Data nesmí bez svolení autorizované osoby nepozorovaně změnit svůj stav
- Data nesmí být bez svolení autorizované osoby zpracovávána na sémantické úrovni

57. Co jsou (z pohledu uživatele) dvě nejméně bezpečné součásti dnešních platebních systémů?

- * Čipová karta s magnetickým proužkem
- Bankomat
- * Platební terminál
- Čipová karta

58. Jaký je v dnešních platebních systémech pro zákazníka největší bezpečnostní problém?

- Banky už v 90. letech zavrhlý používání bezpečného protokolu SET (Secure Electronic Transaction).
- Napěťové útoky jsou snadnou a efektivní cestou jak obejít bezpečnostní mechanismy čipu na platební kartě.
- * Současný systém funguje tak, že zákazníkovi nezaručuje vazbu mezi zobrazenou a potvrzovanou transakcí.
- Zákazníci sami se chovají nezodpovědně.

59. Co je to kritický dotaz ve statistické databázi?

- * Dotaz, který databáze nesmí vyhodnotit, neboť by tím došlo ke zjištění informací o jednotlivci nebo malé skupině osob.
- Dotaz, jehož vyhodnocení trvá dlouhou dobu a vyžaduje veškerou výpočetní sílu databáze, která se v tím může stát nedostupnou pro ostatní dotazy.
- * Sekvence složená z legitimních dotazů na statistickou databázi s cílem získat informace o jednotlivci nebo malé skupině osob.
- Dotaz, který může být položen pouze v okamžiku, kdy v databázi neprobíhají žádné aktualizace dat.

60. Pro anonymitní komunikační síť platí:

- dosažená anonymita je aplikačně nezávislá
- obsah posílaných zpráv není mezi uzly šifrován
- * mohou být náchylné vůči analýze provozu
- * vstupy nelze jednoduše spojit s výstupy

61. Projekt AN.ON poskytuje stejné služby jako

- Mixmaster.
- * Onion routing.
- Mixminion.
- * TOR.

62. Které z následujících metod lze využít k analýze rizik?

- Metoda AES (Advanced Evaluation Standard)
- * Metoda ALE (Annual Loss Expentancy)
- Metoda ARO (Annualized Rate of Occurence)
- * Metoda BPA (Business Process Analysis)
- Metoda RSA (Risk System Analysis)

63. Certifikát veřejného klíče (nař. X.509) vydaný důvěryhodnou certifikační autoritou umožňuje

- * Získat veřejný klíč konkrétního uživatele
- Zabránit ztrátě privátního klíče
- * Ověřit identitu předkladatele veřejného klíče
- Získat přístup k šifrovaným datům konkrétního uživatele v kritické situaci oprávněnou organizací

64. Který z následujících protokolů brání tomu, aby se ten komu jednou prokážete znalost tajné informace nemohl později vydávat za vás:

- * protokol, založený na důkazu nulového rozšíření znalosti (zero-knowledge).
- protokol, který používá šifrování pro zabezpečení přenosu autentizačních dat.
- protokol typu výzva-odpověď (challenge-response), který využije asymetrickou kryptografii jen pro podpis, nikoliv ale pro šifrování.

65. Jak ověříme pravost certifikátu vydaného důvěryhodnou certifikační autoritou?

- Využijeme meta-certifikátu certifikační autority.
- Ověříme zda se shoduje název certifikační autority s názvem uvedeným na daném certifikátu.
- * Ověříme zda je certifikát podepsán danou certifikační autoritou.
- Ověříme, zda je haš certifikátu shodná s haší uvedenou v certifikátu.

66. Pokud existuje v systému zranitelnost a existuje útočník, který ji může využít, výsledný stav je nazýván:

- * hrozba
- zranitelnost
- útok
- riziko

67. Pojmem tranzitivita důvěry označujeme:

- * důvěru cizího uživatele X v náš veřejný klíč, pokud mu důvěřuje uživatel Y, kterému kterým důvěřuje uživatel X.
- důvěru uživatele X v náš veřejný klíč, pokud my důvěřujeme jeho veřejnému klíči.
- takový termín neexistuje.
- * důvěru ve veřejný klíč uživatele X, kterému důvěřuje uživatel Y, kterému důvěřujeme my.
- důvěru v propagaci našeho veřejného klíče od uživatele X na uživatele Y.

68. Proč platební karty s čipem mají magnetický proužek?

- * Kvůli zpětně kompatibilitě.
- Čip provádí kryptografické operace nad daty uloženými na magnetickém proužku.
- Žádná z těchto odpovědí není správná.

69. Kdy je dosažen EER (Equal Error Rate) v biometrických systémech?

Nastavení prahové hodnoty, pro kterou je FAR/FRR rovno 0.8.

Nastavení prahové hodnoty, pro kterou je FRR/FAR rovno 0.8.

* Nastavení prahové hodnoty, pro kterou FRR a FAR jsou stejné.

Nastavení prahové hodnoty, pro kterou je FRR roven 1.

70. Povinnosti správce osobních údajů:

archivovat data kódovaně, není-li řečeno jinak

* uchovávat data pouze po dobu nezbytnou k jejich zpracování

* shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu.

ukládat falešné záznamy, aby v případě krádeže dat nebylo možné snadno posoudit jejich validitu

* uchovávat data pouze po dobu nezbytnou k jejich zpracování

71. Povinnosti správce osobních údajů:

ukládat falešné záznamy, aby v případě krádeže dat nebylo možné snadno posoudit jejich validitu

neposkytovat data třetím stranám před sepsáním Smlouvy o poskytnutí osobních dat

* stanovit prostředky a způsob zpracování osobních údajů

archivovat data kódované, není-li určeno jinak

72. Která technika není platná pro anonymizaci komunikační sítě:

přeuspořádání zpráv v rámci uzlu

* šifrování zpráv mezi uzly algoritmem RSA s délkou klíče závislou na počtu uzlů

pozastavování přijatých zpráv

v čase nedeterministické odesílání přijatých zpráv

* využívání minixů pro přeposílání zpráv

73. K čemu se používají systémy řízení identity (IMS)?

Systém pro správu veřejných klíčů s identifikátory

* K návrhu a správě atributů identity

K dlouhodobé archivaci odcizených identifikačních průkazů

74. Mezi obvyklé bezpečnostní politiky patří:

Interaplikační bezpečnostní politika

Integrovaná bezpečnostní politika

Horizontální bezpečnostní politika

* Celková bezpečnostní politika

* Systemová bezpečnostní politika

75. Problém živosti pro vstupní zařízení

spočívá v tom, že:

Žádná z těchto odpovědí není správná.

Vstupní zařízení není schopno určit, zda vzorek je právě od osoby, která stojí u vstupního zařízení.

* Vstupní zařízení není schopno určit, zda vzorek je od živé osoby.

Osoba, která se přihlašuje u vstupního zařízení není schopná určit kam její vzorek bude přeposláno.

76. Pokud neautorizovaná osoba zjistí sémantický obsahu chráněných dat, jedná se o narušení

- * důvěrnosti
- integrity
- dostupnosti
- prokazatelné zodpovědnosti

77. Obvykle nejmeně bezpečným bodem během průběhu autentizace v internetovém bankovníctví je:

- * autentizace banky
- autentizace počítače klienta
- autentizace klienta

78. Cílem projektu Eternity server je

- navrhnout službu, která je odolná vůči útoku typu Denial of Service
- * poskytnout trvalé úložiště dat
- poskytnout trvalé úložiště dat s operacemi uložit, nalézt a smazat
- * vytvořit datové úložiště, které je odolné vůči výpadkům

79. Jaký je v dnešních platebních systémech pro zákazníka největší bezpečnostní problém?

- Zákazníci sami se chovají nezodpovědně.
- Banky už v 90. letech zavrhlý používání bezpečného protokolu SET (Secure Electronic Transaction).
- Napěťové útoky jsou snadnou a efektivní cestou jak obejít bezpečnostní mechanismy čipu na platební kartě.
- * Současný systém funguje tak, že zákazníkovi nezaručuje vazbu mezi zobrazovanou a potvrzovanou transakcí.

80. PGP umožňuje nastavit úroveň důvěry pro konkrétní veřejný klíč. Toto nastavení se používá pro:

- filtrování zpráv, které mohou být poslány danému uživateli.
- * indikaci důvěry v původ dat podepsaných vlastníkem odpovídajícího privátního klíče.
- indikaci důvěry v původ dat podepsaných daným veřejným klíčem.
- kontrolu skupiny lidí, které může být distribuován náš veřejný klíč.
- indikaci důvěry v klíč na základě jeho bitové velikosti.

81. Která z těchto tvrzení jsou správná?

- * Kopírování měřených biologických charakteristik člověka není sice triviální, ale ani nemožné.
- Biometrická data jsou tajná.
- Biometricky po analýze s využitím kryptografie o subjektu zprávy vypovídají.
- * Biometricky v ideálním případě určují identitu člověka přesně a lze tak spojovat jednotlivě jeho činy.

82. Existuje nějaký útok na službu TOR, který sníží anonymitu uživatelů?

- * Ano, existuje útok, který může snížit anonymitu uživatelů.
- Ano, existuje útok, který stoprocentně "odanonymizuje" všechny uživatele.
- Ne, TOR je navržen tak, aby odolal všem známým i neznámým typům útoků.
- Ne, žádný takový útok zatím není znám.

83. Která z těchto tvrzení, pokud mluvíme o biometrických systémech, jsou správná?

- Proces verifikace je náročnější než proces identifikace.
- Na začátku procesu verifikace není identita známa.
- * Na začátku procesu verifikace je identita známa.
- * Proces identifikace je náročnější než proces verifikace.

84. Kerckhoffsův princip v současnosti neplatí:

- Anžto dokážeme hrubou silou prolomit klíče o délce větší než 80 bitů.
- Jelikož současné délky klíčů neumožňují efektivní útoky hrubou silou.
- Protože dokážeme účinně utajovat šifrovací algoritmy.
- * Nesmysl, Kerckhoffsův princip platí i v současnosti.

85. Kerckhoffsův princip říká, že:

- * Použitý algoritmus je veřejně znám, utajován je pouze klíč.
- Klíč není třeba utajovat, pokud je použitý algoritmus veřejně znám.
- Použitý algoritmus je přístupný pouze autorizovaným osobám, klíč je utajován.
- Klíč není třeba utajovat, pokud použitý algoritmus je také tajný.

86. Projekt AN.ON poskytuje stejné služby jako

- * Onion routing.
- Mixmaster.
- Mixminion.
- * TOR.

87. Co je to statistická databáze?

- Databáze, která umožňuje získávat statistické informace o jednotlivcích.
- * Databáze, která obsahuje informace o jednotlivcích, ale povoluje pouze statistické dotazy, tj. nedovolí získat informace o jednotlivcích.
- Databáze, která je dohledována Českým statistickým úřadem.

88. Analýza a hodnocení hrozeb zahrnuje:

- * Rozvahu, co všechno by mělo být chráněno.
- Pravidla a postupy, určující způsob ochrany a zacházení s ochraňovanými hodnotami.
- Techniky pro implementaci bezpečnostních funkcí chránících ochraňované hodnoty.
- * Vyhodnocení, jaké hrozby hrozí ochraňovaným hodnotám.

89. Bezpečnostní politika je

- Dokument schválený vrcholovým managementem a specifikující využití IT pro zajištění cílů organizace.
- Soubor opatření a mechanismů potřebných k dosažení požadované minimální úrovně prevence a detekce zranitelností.
- Dokument schválený členem představenstva a stanovující přesná pravidla pro zajištění technických i lidských zdrojů pro využití IT pro zajištění cílů organizace.
- * Soubor pravidel specifikující účinný způsob uplatňování opatření potřebných k dosažení požadované minimální úrovně rizik.

90. Klasické odemykání zámku na dveřích klíčem

* spadá pod autentizační procedury.

nespadá pod autentizaci (klíč není ani něco, co znám, vím, ani něco, co "jsem").

spadá pod autentizační procedury, ale jen když klíč do zámku pasuje.

91. Jakým způsobem je prováděna analýza rizik metodou CRAMM?

Infrastrukturní přístup: identifikace a ocenění hodnot zohledňující zejména investice a rizika infrastruktury

Nestrukturovaný přístup: vytvoření tabulky rizik a zranitelností na základě spirálového modelu.

Nestrukturovaný přístup: inkrementální odhad hrozeb a zranitelností hodnot na základě rozšířeného spirálového modelu.

* Strukturovaný přístup: i. identifikace a ocenění hodnot; ii. odhad hrozeb a zranitelností hodnot; iii. výběr vhodných protiopatření.

Strukturovaný přístup: i. odhad hrozeb a zranitelností hodnot; ii.

naprogramování vhodných protiopatření.

Adhoc přístup: odhad hrozeb a zranitelností hodnot na základě běžného seznamu aktiv (metoda lze paralelizovat).

92. Pro emailové zprávy posílané pomocí systému Mixminion platí

* jsou anonymní.

* je možné na ně v určitém časovém rámci odpovědět.

* uživatel specifikuje cestu po síti.

odpovědi jsou v systému doručovány odlišně od normálních emailů.

hlavičky mailů nejsou modifikovány.

jsou pseudonymní.

93. Tvrzení "Využití služby pro neautorizovaný přístup" by mohlo označovat

riziko.

zranitelnost.

* hrozbu.

útok.

bezpečnostní politiku.

94. Podezřelé chování v síti zjistíte

antivirovým programem.

* honeypotem.

antispysware programem.

* IDS.

* firewallem.

95. Jaký je rozdíl mezi termíny security a safety?

Je to to samé, čeština používá jen jeden termín - bezpečnost

Safety - stav ochrany IS proti ztrátám; security - nedojde k ohrožení lidského života

- Security - stav ochrany IS proti ztrátám; safety - nedojde k ohrožení lidského života
-

96. Proč platební karty s čipem mají magnetický proužek?

Čip provádí kryptografické operace nad daty uloženými na magnetickém proužku.

* Kvůli zpětné kompatibilitě.

Žádná z těchto odpovědí není správná.

97. Co je to agregace dat?

- * Seskupování (osobních) dat do rozsáhlých databází.
Odvozování nových (typicky citlivějších) informací, na základě zpracování informací s nižší úrovní citlivosti.
"Pročišťování" velkých databází.
Zálohování dat jako obrana proti živelným pohromám.

98. Pod pojmem asymetrická kryptografie rozumíme

- Kryptografie s algoritmem, který je opakem symetrické kryptografie a nepoužívá žádný klíč.
- Kryptografie s využitím klíče, který je výstupem kvalitní hašovací funkce.
- * Kryptografie s využitím dvojice soukromého a veřejného klíče.
Nic z ostatních uvedených možností.

99. Ke zneužitím mobilního telefonu operátorem patří:

- * SMS posílané z mobilu na mobil mohou být jednoduše ukládány.
- * poloha mobilního telefonu může být sledována.
žádná z těchto odpovědí není správná, protože celá komunikace je bezpečně šifrována.

100. Co jsou (z pohledu uživatele) dvě nejméně bezpečné součásti dnešních platebních systémů?

- * Čipová karta s magnetickým proužkem
- * Platební terminál
Bankomat
Čipová karta

101. Které dvě z těchto biometrických technik jsou nejpřesnější?

- dynamika podpisu
- * vzor oční duhovky
- hlas
- * vzor oční sítnice

102. Protokoly SSL/TLS umožňují

- * kontrolu integrity přenášených dat.
komunikovat anonymně.
zajistit nepopíratelnost.
- * autentizaci komunikujících stran (klient i server).
autentizaci jen a pouze jedné strany.

103. Zvolte správnou hierarchii podle druhu pseudonymu (ve směru zvyšující se anonymity a nespojitelnosti).

- Pseudonym osoby >pseudonym role>pseudonym vztahu >pseudonym role >pseudonym transakce.
- *Pseudonym osoby >pseudonym role a pseudonym vztahu >pseudonym role>pseudonym transakce.
Pseudonym transakce >pseudonym role>pseudonym role a pseudonym vztahu >pseudonym osoby.
Pseudonym osoby >pseudonym transakce >pseudonym role a pseudonym vztahu >pseudonym role>pseudonym transakce.
Pseudonym osoby >pseudonym role>pseudonym role >pseudonym vztahu >pseudonym transakce.

104. Která z těchto tvrzení jsou správná?

Biometricky po analýze s využitím kryptografie o subjektu zprávy vypovídají.

Jeden vzorek lze využít jen v jednom systému.

* Žádná z těchto odpovědí není správná.

Biometrická data jsou tajná.

105. Co znamená pojem důvěrnost dat?

* Utajení obsažené informace.

Zajištění integrity dat.

Data jsou v nezměněné podobě tak, jak byla vytvořena.

106. Místa setkání a skryté služby TORu je/jsou:

místa, kde uživatelé získávají anonymitu tak, že to ostatní nevidí.

* služba, která umožňuje anonymní provoz např. webového serveru.

místa, kde se setkávají pouze anonymní uživatelé.

* je služba umožňující serveru kontrolovat anonymní příchozí požadavky.

107. Pretty Good Privacy (PGP) umožňuje

* šifrovat a dešifrovat data

* digitálně podepsat data a ověřit podpis

anonymně přistupovat k webu

odeslat, přijmout a odpovědět na anonymní e-mail

chránit počítač před zneužitím

108. Je lepší používat TOR nebo Mixminion?

Jednoznačně TOR.

Ani jedno, ani druhé.

* Záleží na tom, co chceme dělat.

Jednoznačně Mixminion.

109. Remailer je

* služba pro anonymní posílání a příjem e-mailů.

je část poštovního serveru, která se stará o opakování neúspěšných pokusů.

veřejný poštovní server (považovaný za chybně nakonfigurovaný).

110. Autentizace protokolem s nulovým rozšířením znalostí (zero-knowledge)

* zabrání ověřovateli, aby se mohl později neoprávněně vydávat za prokazující se stranu.

zabrání prokazující se straně, aby se dozvěděla, jak zní tajemství, které vlastní ověřovatel.

* zabrání ověřovateli, aby se dozvěděl tajemství, které vlastní prokazující se strana.

sdělí ověřovateli pouze počet nul v tajném klíči prokazující se strany.

zabrání ověřovateli, aby se zároveň autentizoval prokazující se straně.

111. Jaké byly důvody (a motivace) pro zavedení kritérií bezpečnosti?

Standardizace kryptografických primitiv.

Jednalo se o chytrý marketingový tah výrobců špatně zabezpečených operačních systémů.

* Usnadnění specifikace požadavků na návrh a vývoj.

Snazší a rychlejší vývoj implicitně bezpečných systémů.

* Potřeba minimalizace nákladů na individuální ohodnocení.

112. Pro konzervativní kontrolu certifikátu veřejného klíče platí:

Nic z ostatních uvedených možností.

Klíč považujeme za platný, dokud nejsme přesvědčeni o opaku.

Klíč považujeme za zneplatněný, pokud standard X.509 nestanoví jinak.

* Klíč považujeme za neplatný, dokud nejsme přesvědčeni o opaku.

113. Pro liberální kontrolu certifikátu veřejného klíče platí:

* Klíč považujeme za platný, dokud nejsme přesvědčeni o opaku.

Klíč považujeme za neplatný, dokud nejsme přesvědčeni o opaku.

Klíč považujeme za zneplatněný, pokud standard X.509 nestanoví jinak.

Nic z ostatních uvedených možností.

114. Jak pracuje technika náhodného výběru ve statistických databázích?

* Výsledek dotazu je vyhodnocen na základě náhodně vybraných záznamů ze všech existujících záznamů v databázi.

Žádná taková technika neexistuje.

Výsledek dotazu je zaokrouhlen na hodnotu náhodně vybraného záznamu.

Výsledek dotazu je vyhodnocen na základě mírně upravených záznamů, které jsou náhodně vybrány ze všech existujících záznamů v databázi.

Výsledek dotazu je zcela náhodný a nepředvídatelný.

115. Pro zajištění prokazatelné zodpovědnosti (accountability)?

Ja na začátku práce v systému obvykle prováděno dešifrování dat pro práci s účtem.

* Je na začátku práce v systému obvykle prováděna autentizace nebo identifikace.

Je prováděna archivace dat pro udržení schopnosti správy účtu.

* Je prováděna archivace dat umožňujících propojení činnosti s konkrétní osobou tak, že daná osoba se nemůže zříci zodpovědnosti za svoji činnost.

116. Šifrování v PGP probíhá tak, že se data šifrují

asymetricky, klíče se zašifrují soukromým klíčem příjemce a přiloží k datům.

asymetricky, klíče se zašifrují veřejným klíčem příjemce a přiloží k datům.

symetricky, symetrický klíč se zašifruje soukromým klíčem příjemce a přiloží k datům.

* symetricky, symetrický klíč se zašifruje veřejným klíčem příjemce a přiloží k datům.

117. Typické operace na firewallu jsou

hašovat

xorovat

* zakázat

* povolit

Plus preložit!!!

118. Které dvě z těchto biometrických technik bývají obvykle nejlevnější s ohledem na celkové náklady na nasazení u koncových uživatelů, resp. jejich pracovních stanic?

* otisk prstu.

vzor oční sítnice.

* dynamika psaní na klávesnici.

DNA.

119. Co řeší Zákon o ochraně osobních údajů?

- * vztahuje se na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby, není-li stanoveno jinak. upravuje právo na ochranu osobních údajů u jedinců se záznamem v trestním rejstříku po dobu výkonu trestu.

120. Magnetický proužek standardní platební karty obsahuje:

- * údaje o majiteli.
údaje o posledních 3-5 transakcích s kartou.
- * údaje o kartě.
údaje o částce, kterou držitel této karty naposledy vybral nebo platil.

121. Jak pracuje technika maximálního rozsahu dotazu ve statistických databázích?

- Pro vyhodnocení dotazu může být použito pouze menší množství záznamů než je stanovená maximální mez.
- * Žádná taková technika neexistuje.
Pro vyhodnocení dotazu nesmí být použito více záznamů než je stanovená maximální mez.

122. Výraz script kiddies označuje:

- Útočníka, který je schopen kreativně odhalovat nové zranitelnosti i bez znalostí o systému.
- Hackera, který píše skripty a odhaluje nové zranitelnosti systému. Má částečné informace o systému.
- * Útočníka, který nemá dostatek znalostí o systému a využívá běžně dostupné předpřipravené nástroje na známé zranitelnosti, často způsobem pokus-omyl.

123. Pravidla přístupu do počítačové sítě (FI) MU

- v případě nutnosti je povoleno rekonfigurovat PC, které je pod správou CVT FI.
- * je zakázáno odposlouchávat provoz a vytvářet kopie poštovních zpráv.
je povoleno provozovat vlastní herní server jen po 22:00.
- * je třeba volit si dobrá hesla, nezjišťovat hesla jiných.
v počítačových učebnách a na počítačích FI je možné hrát pouze legálně zakoupené hry.
uživatel smí poskytovat jen takové programové vybavení a datové soubory, k nimž vlastní platnou licenci

124. Co je to profil bezpečnosti (Protection Profile, PP)?

- Cílová kombinace komponent jasně profilujících konkrétní hodnocený systém.
- * Implementačně nezávislá skupina bezpečnostních požadavků určité skupiny předmětu hodnocení.
Implementačně nezávislá skupina bezpečnostních požadavků schválená příslušnou národní autoritou (v ČR NBÚ).
Předmět hodnocení, který již musí být definován formálním profilačním jazykem.
Cílová kombinace komponent spojených s konkrétním produktem nebo systémem.
Produkt nebo systém (či jeho část), který je předmětem hodnocení.

125. Co je to "Security through obscurity"?

- * Víra, že pouze dobře utajený algoritmus je bezpečný.
Souhrnný název pro bezpečnostní mechanismy vybudované na teorii složitosti.

126. Co je nejčastější příčinou bezpečnostních incidentů?

- * Chyby (neúmyslné).
Vliv přírody, zdrojů.
Záměrný útok (sabotáž) zaměstnanců (i bývalých).
Vnější útočníci.
Škodlivý software.

127. Které z tvrzení o anonymitní množině neplatí

- * velikost anonymitní množiny je smysluplný ukazatel.
- * nezáleží na chování uživatelů v dané skupině.
záleží i na kontextových informacích v systému.
pro určení velikosti anonymitní množiny se užívá entropie.

128. Onion Routing systémem označujeme

- * systém poskytující své služby pro různé protokoly.
rezistentní systém pro anonymitní komunikační síť.
- * systém pro anonymní komunikaci při použití veřejné sítě.
systém fungující po vrstvách (např. TCP/IP).

129. Zabezpečení provozu na úrovni IP dosáhnou pokud zvolím:

- * IPsec
Stunnel
PGP
- * IPv6
IPv4s

130. Které z těchto tvrzení je správné, pokud mluvíme o kartách s čipem?

- * Čip je schopen provádět výpočet a autentizovat se pomocí důkazu nulového rozšíření znalosti.
Lze snadno vytvořit kopii čipu, ale ne současně čipu a magnetického proužku.
Dodatečným mechanismem ochrany čipu je magnetický proužek.
- * Bez techniky velmi náročného rozebrání čipu a jeho analýzy není možné vytvořit kopii.

131. Které z následujících bodů lze zařadit mezi obecné principy pro bezpečnost IT?

- Nepoužívejte klíče s délkou < 128 bitů.
- * Usilujte o jednoduchost.
- * Externí zdroje pokládejte za nebezpečné.
- * Fyzicky nebo logicky oddělte kritické zdroje.
Nikdy nezveřejňujte kritické bezpečnostní algoritmy.

132. Pod pojmem riziko rozumíme:

- existenci zranitelnosti v systému a přítomnost útočníka, který ji může využít.
- * pravděpodobnost uplatnění hrozby.
pravděpodobnost odhalení zranitelnosti.
rozsah dopadu uplatnění hrozby.

133. Řešení pro odesílání anonymních e-mailů jsou založena na:

- anonymity před příjemcem lze dosáhnout velmi těžko.
- anycastových sítích, remailerech a mixech.
- * remailerech, u kterých rozlišujeme několik typů (tříd).
- * broadcastových sítích, remailerech a mixech.
- využití účtu na freemailu (Seznam).

134. Při podpisu bez obnovy dat platí:

- Po provedení podpisu jsou původní data smazána a nelze je obnovit.
- * Podpis neobsahuje podepisovaná data.
Před provedením podpisu je nutné obnovit podepisovaná data, po provedení podpisu to již bez znalosti soukromého klíče není možné.
- * Nepodepisují se přímo původní data, ale jejich haš – otisk.

135. Pro komunikaci mezi jednotlivými Onion Routery (OR) platí

- * seznam přeposlaných paketů se ukládá.
topologie uzlů připomíná hvězdicu s pevně daným středem.
komunikace se šifruje pomocí asymetrické kryptografie.
- * každý OR odstraní vrstvu paketu dešifrováním.
- * komunikace se šifruje pomocí šifry se symetrickým klíčem.

136. Jaký způsob předání veřejného klíče je považován za důvěryhodný:

- * ověření otisku klíče telefonem.
- * osobní předání na USB disku.
zaslání emailem s paralelním umístěním na webovou stránku.
vystavení na klíčový server.
- * zaslání důvěryhodným zprostředkovatelem.

137. Britská medicínská asociace nařizuje při zakládání nového záznamu pacienta, aby:

- Na seznamu přístupů k záznamu byl pouze pacient, další lékaře přidává primář oddělení.
- * Na seznamu přístupů k záznamu byl pouze ošetřující lékař a pacient.
Na seznamu přístupů do další návštěvy lékaře nebyl nikdo z administrativního personálu.

138. Britská medicínská asociace nařizuje při práci se záznamy pacientů:

- * Implementaci opatření zamezujících agregaci dat.
- * Zaznamenávání veškerých modifikací provedených se záznamy pro potřeby auditu.
- * Nutnost informovat pacienta (na jeho žádost) o aktuálním stavu seznamu přístupů k jeho záznamu.
Nutnost informovat rodinné příslušníky pacienta (na jejich žádost) o aktuálním stavu seznamu přístupů k jeho záznamu.

139. PIN je u kreditních karet vyžadován, aby

- * karta po okopírování šla obtížněji zneužít
celý systém plateb kartami vypadal bezpečněji (ve skutečnosti však bezpečnost vůbec nezvedá - je zde jen pro psychologický efekt)
- * člověk, který kartu zcizí, ji nemohl snadno použít k platbám
karta šla hůře okopírovat
zajistil absolutní ochranu peněz před jakýmkoli útokem na bezpečnost karty

140. Tvrzení "Systém je chráněn sdíleným heslem" by mohlo označovat

- bezpečnostní politiku
- útok
- hrozbu
- riziko
- * zranitelnost

141. Citlivé osobní údaje dle české legislativy vypovídají mj. o:

- * národnostním, rasovém nebo etnickém původu
- postoji k trestné činnosti rodinných příslušníků
- * politických postojích
- postoji k trestné činnosti jiných

142. Bezpečnost použití těchto zařízení pro autentizaci je porovnatelná s bezpečností použití čipových karet pro stejný účel:

- žádná z těchto odpovědí není správná
- heslo dlouhé alespoň 8 znaků a vytvořené náhodně ze sady min. 95 znaků
- * autentizační kalkulačka
- certifikovaný USB disk

143. Mezi vlastnosti Onion Routingu (OR) rozhodně patří

- * zpoždění komunikace by měla být co nejmenší
- využívá se zejména v privátních sítích
- závislost na specializovaném hardwaru
- neumožňuje komunikaci klient-server
- * aplikace mohou s OR fungovat bez nutnosti jejich modifikace

144. Mezi vlastnosti Onion Routingu (OR) rozhodně nepatří

- * využívá se zejména v privátních sítích.
- mezi jednotlivými OR se předávají šifrovaná data.
- umožňuje spojení klient-server.
- * výběr následujícího komunikačního uzlu je nezávislý na uživateli.
- komunikační cesta je definována při sestavení komunikačního kanálu.

145. Pro osobní údaje dle české legislativy platí:

- * jde-li na základě jednoho či více osobních údajů přímo či nepřímo zjistit identitu subjektu, považuje se subjekt údajů za určený nebo určitelný .
- * jedná se o jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů.
- zpracovávání osobních údajů je zakázáno, vyjma případů pro osobní potřebu .
- dozor nad osobními údaji provádí Policie ČR .
- * o osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času nebo materiálních prostředků.

146. Které dvě z těchto biometrických technik jsou nejpohodlnější pro uživatele?

- EKG
- * srovnání tváře
- * vzor oční duhovky
- vzor oční sítnice

147. Jakým způsobem je počítána analýza rizik metodou ALE (Annual Loss Expentancy)

ALE=SLOxARE, kde SLO=Single Loss of Opportunity a ARE=Annualized Rate of Executions
ALE=SLO/ARE, kde SLO=Single Loss of Opportunity a ARE=Annualized Rate of Executions
ALE=SLO+ARE, kde SLO=Single Loss of Opportunity a ARE=Annualized Rate of Executions
ALE=SLE/ARO, kde SLE=Single Loss Expentancy a ARO=Annualized Rate of Occurence
* ALE=SLExARO, kde SLE=Single Loss Expentancy a ARO=Annualized Rate of Occurence
ALE=SLE+ARO, kde SLE=Single Loss Expentancy a ARO=Annualized Rate of Occurence

148 - lol. Bylo by možné spolehlivě autentizovat studenta MU na základě trojice celých čísel výška[cm] : váha[kg] : věk[roky]?

Ano, jde o údaje cizím lidem neznámé.
* Ne, MU studentů příliš mnoho, aby toto bylo spolehlivé.
Ano, jde o fyzickou vlastnost (biometrika).

149. Která z těchto tvrzení jsou správná?

Biometrická data jsou tajná.
* Některé biometricky hodně o subjektu vypovídají.
správně*Biometricky v ideálním případě určují identitu člověka přesně a lze tak spojovat jednotlivě jeho činy.
Jeden vzorek lze využít jen v jednom systému.

150. Digitální pseudonym je řetězec bitů, který:

* je unikátní jako ID (s velmi velkou pravděpodobností)
je konstruován přesně v souladu s pravidly stanovenými Úřadem pro ochranu osobních údajů
* je použitelný pro autentizaci jeho vlastníka a předmětů zájmu (např. odeslaných zpráv)
by měl být nerozlišitelný od náhodného šumu
si jeho držitel musí bezpodmínečně zapamatovat

151. Provoz v anonymitní síti

je pro zachování určité míry anonymity nepodstatný
* je pro zachování určité míry anonymity důležitý
neobsahuje falešné zprávy
je často zaměňován za falešné zprávy
* je často obohacován o falešné zprávy