

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

- * nespojitelnost, nepozorovatelnost, anonymita, pseudonymita

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

2. Anonymita (podle Společných kritérií) zajišťuje možnost použití zdrojů nebo služeb systému tak, že:

- * identita uživatele zůstane skryta specifickým uživatelům, pro specifické operace

- identita uživatele zůstane skryta, ale v případě potřeby ji lze zpětně zjistit
- specifikované entity jsou schopny určit skutečné uživatelské jméno spojené se specifikovanými subjekty, operacemi, objekty

3. Nespojitelnost (podle Společných kritérií) zajišťuje možnost opakovaného použití zdrojů:

- bez prozrazení identity uživatele, ale v případě potřeby lze identitu zpětně zjistit
- bez prozrazení identity uživatele
- tak, že identita uživatele zůstane skryta specifickým uživatelům, pro specifické operace

- * tak, že ostatní si tato použití nebudou schopni spojit

- tak, že pouze administrátoři uvidí, že ve skutečnosti toto použití inicioval tentýž uživatel

4. Je e-mailová adresa tvaru jmeno.prijmeni@nejakafirma.cz osobním údajem nebo nikoliv?

- * Ne

- Záleží na postoji majitele této adresy

- * Ano

5. Může zaměstnavatel podrobně sledovat a číst veškerou e-mailovou komunikaci zaměstnance, který písemně potvrdil, že svoji e-mailovou adresu nebude používat k soukromým účelům?

- Ano, ale pouze pokud má důvodné podezření, že dochází k porušení písemné dohody
- Ano, ale pouze s vědomím Policie ČR
- Ano

- * Ne

6. Nepozorovatelnost (podle A.Pfitzmanna - mixy) znamená:

- * Stav (daných) předmětů zájmu, kdy nejsou odlišitelné od jiných předmětů zájmu

- Že pravděpodobnost spojení prvků v systému je stejná před a po (prů)běhu nějaké posloupnosti událostí v systému.
- Stav, kdy ostatní uživatelé nemohou pozorovat využívání zdrojů systému

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

- Bytí anonymním pouze vůči uživatelům systému, nikoli vůči administrátorům

- * Používání pseudonymu jako identifikátoru (ID)

- Bytí anonymním s možností zpětného zjištění skutečné identity

8. Digitální pseudonym je řetězec bitů, který:

- by měl být nerozlišitelný od náhodného šumu
- si jeho držitel musí bezpodmínečně zapamatovat
- je konstruován přesně v souladu s pravidly stanovenými Úřadem pro ochranu osobních údajů

- * je unikátní jako ID (s velmi velkou pravděpodobností)

- * je použitelný pro autentizaci jeho vlastníka a předmětů zájmu (např. odeslaných zpráv)

9. Maximální počet identit jedné osoby může být

- 1
- * **kolik chce (když se bude dostatečně snažit)**
- 2 pro vdané ženy
- 4 pro jedince s dvěma svatbami a jedním rozvodem

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

- * **K návrhu a správě atributů identity**
- K dlouhodobé archivaci odcizených identifikačních průkazů
- Systém pro správu veřejných klíčů s identifikátory

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

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

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

- * **sexuální orientaci**
- postoji k trestné činnosti jiných
- majetkových poměrech státních úředníků

13. Co řeší Zákon o ochraně osobních údajů?

- upravuje právo na ochranu osobních údajů u jedinců se záznamem v trestním rejstříku po dobu výkonu trestu
- * **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**

14. Zákon o ochraně osobních údajů:

- se vztahuje na zabezpečení zpracovávaných osobních údajů v případě automatizovaných prostředků
- se nevztahuje na data poskytovaná dobrovolně státním institucím
- * **se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány, nebo pokud nejsou pro podnikání**

15. IEEE - principy SW inženýra stanoví např.

- povinnost žít čestně, zdravě a podle pravidel IEEE tak, aby na něj mohla být společnost hrdá
- zastávat pouze takové pozice, na které má náležitou schopnost
- * **zajistit čestnost a nezávislost ve svých odborných odhadech**
- povinnost používat pouze software, za který nebylo prokazatelným způsobem zapláceno
- * **vykonávat svou činnost v souladu s veřejným zájmem**

16. Co je to statistická databáze?

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

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

- Na seznamu přístupů do další návštěvy lékaře nebyl nikdo z administrativního personálu.

- Na seznamu přístupů k záznamu byl pouze pacient, další lékaře přidává primář oddělení.
- * **Na seznamu přístupů k záznamu byl pouze ošetřující lékař a pacient.**

18. 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.

19. Co znamená pojem důvěrnost dat?

- Data jsou v nezměněné podobě tak, jak byla vytvořena.
- * **Utajení obsažené informace.**
- Zajištění integrity dat.

20. Mezi bezp. funkce systémů pro ochranu inf. soukromí nepatří:

- * **integrita**
- nepozorovatelnost
- pseudonymita
- nespojitelnost
- * **identita**
- * **neslučitelnost**

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

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

22. Anonymita (podle Společných kritérií) zajišťuje možnost použití zdrojů nebo služeb systému tak, že:

- * **identita uživatele zůstane skryta**
- * **identita uživatele zůstane skryta specifickým uživatelům, pro specifické operace**
- identita uživatele zůstane skryta, ale v případě potřeby ji lze zpětně zjistit
- specifikované entity jsou schopny určit skutečné uživatelské jméno spojené se specifikovanými subjekty, operacemi, objekty

23. Pseudonymita (podle Společných kritérií) zajišťuje možnost použití zdrojů nebo služeb systému tak, že:

- * **identita uživatele zůstane skryta, ale specifikované entity za specifikovaných podmínek mohou tento stav zvrátit**
- identita uživatele zůstane trvale skryta
- identita uživatele zůstane skryta specifickým uživatelům, pro specifické operace
- identita uživatele zůstane skryta, ale specifikované entity za nespecifikovaných podmínek mohou tento stav zvrátit
- identita uživatele zůstane skryta ostatním uživatelům, ale ne administrátorům
- identita uživatele zůstane skryta, ale to platí pouze pro původně neveřejné pseudonymy

24. Nepozorovatelnost (podle Společných kritérií) zajišťuje možnost použití zdrojů nebo služeb systému tak, že:

- ostatní uživatelé systému nemohou pozorovat používání daného zdroje nebo služeb, ale v případě potřeby lze toto chování zpětně spojit s konkrétním uživatelem
- specifikované entity jsou schopny pozorovat specifikované operace prováděné specifikovanými entitami na nespecifikovaných objektech

- * ostatní uživatelé (ani administrátoři) systému nemohou pozorovat používání daného zdroje nebo služeb

- ostatní uživatelé, s výjimkou administrátorů, nemohou pozorovat používání daného zdroje nebo služeb

- * specifikované entity nejsou schopny pozorovat specifikované operace prováděné specifikovanými entitami na specifikovaných objektech

- uživatelé nejsou zodpovědní za své chování v systému

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

- Subjektivní (ze strany hodnotitele) hodnocení bezpečnosti systému

- Popis, jakým způsobem je v hodnoceném systému dosaženo daných vlastností

- Sada doporučení, jak hodnocený systém zabezpečit

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

26. Anonymita subjektu (podle A.Pfitzmanna - mixy) znamená stav:

- bytí neidentifikovatelným v rámci dané množiny subjektů, tzv. anonymitní množině, ale s výjimkou administrátorů - ti jsou schopni identitu kdykoliv zjistit

- bytí neidentifikovatelným v rámci libovolné podmnožiny z množiny všech subjektů

- * bytí neidentifikovatelným v rámci dané množiny subjektů, tzv. anonymitní množině

- * ve kterém má daný subjekt minimální prokazatelnou zodpovědnost (accountability)

- bytí neidentifikovatelným v rámci dané množiny subjektů, tzv. anonymitní množině s tím, že v případě potřeby je identitu subjektu možno zpětně dohledat

27. Pro větší anonymitní množinu je:

- * podle některých názorů anonymita stejná jako při menší anonymitní množině

- podle některých názorů anonymita menší než při menší anonymitní množině

- * podle některých názorů anonymita větší než při menší anonymitní množině

28. Nespojitelnost (podle A.Pfitzmanna - mixy) znamená:

- * Že pravděpodobnost spojení prvků v systému je stejná před a po (prů)běhu nějaké posloupnosti událostí v systému.

- * Nespojitelnost dvou a více prvků (např. subjektů, zpráv, událostí) tak, že v takovém systému nejsou prvky ani více, ani méně ve vzájemném vztahu s ohledem na předchozí znalost systému.

- Nespojitelnost tří a více prvků (např. subjektů, zpráv, událostí) tak, že budou anonymní pouze vůči uživatelům systému, nikoli vůči administrátorům.

29. Co je to veřejný pseudonym?

- * Je veřejně znám od počátku, např. v seznamu osob

- Pseudonym používaný uvnitř veřejně nedostupného systému

- Pseudonym použitelný pouze na veřejnosti

- * Např. telefonní číslo ve Zlatých stránkách

- Je znám veřejnosti za poplatek

30. Co je to "původně neveřejný" pseudonym?

- Pseudonym původně neurčený pro veřejnost, který ale neschválil Úřad pro ochranu osobních údajů

- Pseudonym, který musí být po druhém použití zveřejněn

- Pseudonym, který musí být při druhém použití zveřejněn

- * Pseudonym, který původně nebyl veřejný, ale v některých případech může být zveřejněn

31. Co je to "původně nespojený" pseudonym?

- Je znám pouze vlastníku a jeho nejbližšímu okolí

- Pseudonym, který není spojen s žádným loginem
- Pseudonym původně určený pro veřejnost, který ale neschválil Úřad pro ochranu osobních údajů
- * **Není od počátku znám nikomu kromě jeho vlastníka**
- * **Např. ID v chatu**

32. Co je to identita (podle A. Pfizmana - mixy)

- * **Libovolná podmnožina atributů určitého jedince, která tohoto jedince jednoznačně určuje v jakékoliv množině jedinců**
- Pevně stanovená podmnožina atributů určité skupiny jedinců, která tuto skupinu jednoznačně určuje v jakékoliv množině jedinců
- Taková podmnožina atributů určitého jedince, která jeho identitní skupinu jednoznačně určuje v jakékoliv množině jedinců
- Libovolná podmnožina atributů určitého jedince, která jeho identitní skupinu jednoznačně určuje v jakékoliv množině jedinců

33. Co představuje pseudonym osoby?

- Identifikace dané osoby
- Pseudonym původně určený pro veřejnost, který ale neschválil Úřad pro ochranu osobních údajů
- * **Reprezentace dané osoby**
- * **Např. číslo mobilního telefonu dané osoby**

34. Co platí pro pseudonym role?

- * **Jedna osoba může pro různé role využívat různé pseudonymy**
- * **Např. login pro přístup do internetového bankovníctví**
- Více osob musí pro tutéž roli využívat tentýž pseudonym
- Více osob může pro více rolí využívat různé pseudonymy

35. Co je to pseudonym vztahu?

- * **Například použití různých přezdivek (nickname) pro komunikaci s každým partnerem**
- Pro každého partnera je použito jeho jméno podle platného občanského průkazu
- * **Pro každého partnera je použito jiné jméno**
- Pro každého partnera je použito stejné jméno

36. Co je to pseudonym transakce?

- * **Pseudonym, který neumožňuje zjistit, že dvě různé transakce byly ve skutečnosti provedeny jedním subjektem**
- Např. login pro přístup do internetového bankovníctví
- Pseudonym, který se použije k ověření pravosti transakce
- * **Pseudonym, který je unikátní pro každou transakci**

37. Citlivé osobní údaje dle české legislativy vypovídají o:

- postoj k trestné činnosti rodinných příslušníků
- * **sexuální orientaci**
- majetkových poměrech státních úředníků
- * **zdravotním stavu**

38. Pro osobní údaje dle české legislativy platí:

- dozor nad osobními údaji provádí Policie ČR
- * **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

39. Povinnosti správce osobních údajů:

- archivovat data kódovaně, není-li řečeno jinak
- * **stanovit prostředky a způsob zpracování osobních údajů**
- vkládat falešné záznamy, aby v případě krádeže dat nebylo možné snadno posoudit jejich validitu
- neposkytovat data třetím stranám před sepsáním Smlouvy o poskytnutí osobních dat

40. 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
- * **upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů**

41. Pro osobní údaje dle české legislativy neplatí:

- * **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
- * **o osobní údaj se jedná i v policii neschválených sběrech dat, které provádí fyzická osoba výlučně pro osobní potřebu**
- * **zpracovávání osobních údajů je zakázáno, vyjma případů pro osobní potřebu**

42. Co je to agregace dat?

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

43. V souvislosti se sdružováním dat do rozsáhlých databází ukládá zákon 101/2000 sb. o ochraně osobních údajů

- * **Povinnost informovat osobu, jejíž data budou uložena a zpracovávána v databázi, že se tímto způsobem bude s poskytnutými daty nakládat.**
- Povinnost informovat zkoumanou osobu (subjekt) o tom, že se podařilo zjistit o něm citlivé informace a zda může potvrdit jejich pravdivost.
- * **Povinnost nesdružovat data, která byla původně získána k rozdílným účelům, do jednoho celku.**

44. Jaké jsou faktory přímo ovlivňující pravděpodobnost neoprávněného (vy)užití informací?

- * **Výše trestu těm, kdo s daty neoprávněně manipuluje.**
- * **Výše trestu těm, kdo data neohlídali a spolupodíleli se na jejich úniku.**
- Kódování dat.
- * **Úroveň bezpečnostních mechanismů.**
- Výše trestu těm, kdo data hlídali a zajistili restriktivní manipulaci.

45. Jaká protiopatření zabraňující neoprávněnému přístupu k informacím se používají ve statistických databázích?

- Anonymita, pseudonymita, nespojitelnost, nesledovatelnost.
- * **Náhodný výběr, minimální rozsah dotazu, perturbační techniky.**

- Náhodný výběr, maximální rozsah dotazu, turbační techniky.

46. Jak pracuje technika náhodného výběru ve statistických databázích?

- Výsledek dotazu je zaokrouhlen na hodnotu náhodně vybraného záznamu.
- Výsledek dotazu je zcela náhodný a nepředvídatelný.
- Výsledek dotazu je vyhodnocen na základě mírně poupravených záznamů, které jsou náhodně vybrány ze všech existujících záznamů v databázi.
- * Výsledek dotazu je vyhodnocen na základě náhodně vybraných záznamů ze všech existujících záznamů v databázi.
- Žádná taková technika neexistuje.

47. Jak pracuje technika minimálního rozsahu dotazu ve statistických databázích?

- Pro vyhodnocení dotazu může být použito méně záznamů než je stanovená minimální mez, ale pouze za zvláštních bezpečnostních opatření (např. podpis dohody o mlčenlivosti).
- Žádná taková technika se ve statistických databázích nepoužívá.
- Žádná taková technika neexistuje.
- * Pro vyhodnocení dotazu nesmí být použito méně záznamů než je stanovená minimální mez.

48. Mezi bezp. funkce systémů pro ochranu inf. soukromí patří:

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

49. Pseudonymita (podle Společných kritérií) zajišťuje možnost použití zdrojů nebo služeb systému tak, že:

- identita uživatele zůstane skryta, ale specifikované entity za nespecifikovaných podmínek mohou tento stav zvrátit
- identita uživatele zůstane skryta ostatním uživatelům, ale ne administrátorům
- * identita uživatele zůstane skryta, ale v případě potřeby ji lze zpětně zjistit
- identita uživatele zůstane skryta, ale to platí pouze pro původně neveřejné pseudonymy
- * identita uživatele zůstane skryta, ale specifikované entity za specifikovaných podmínek mohou tento stav zvrátit
- identita uživatele zůstane trvale skryta

50. Co je to pseudonym role-vztahu?

- Pseudonym, který lze pro danou roli a vztah použít pouze jednou a při další takové komunikaci musí být vygenerován nový
- * Pseudonym, který je unikátní pro roli a vztah (partnera)
- * Takový pseudonym, že komunikační partner se nedozví, že dva pseudonymy použité v různých rolích patří ve skutečnosti pouze jednomu uživateli
- Pseudonym, jehož použití je omezeno pouze pro unikátní roli a vztah (partnera)

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

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

- Pseudonym osoby -> pseudonym role-vztahu -> pseudonym role -> pseudonym vztahu -> pseudonym transakce

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

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

52. Pro osobní údaje dle české legislativy platí:

- * jedná se o jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů.

- zpracovávání osobních údajů je zakázáno, vyjma případů pro osobní potřebu

- * jde-li na základě jednoho či více osobních údajů přímo či nepřímo zjistit identitu subjektu, považuje se subjekt údajů za určený nebo určitelný

- * o osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času nebo materiálních prostředků

- dozor nad osobními údaji provádí Policie ČR

53. Povinnosti správce osobních údajů:

- neposkytovat data třetím stranám před sepsáním Smlouvy o autorizovaném poskytnutí osobních dat

- archivovat data kódovaně, není-li řečeno jinak

- * stanovit prostředky a způsob zpracování osobních údajů

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

- ověřovat neautorizované výskyty osob

- * zpracovávat pouze pravdivé a přesné osobní údaje

54. Povinnosti správce osobních údajů:

- * uchovávat data pouze po dobu nezbytnou k jejich zpracování

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

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

- archivovat data kódovaně, není-li řečeno jinak

- * uchovávat data pouze po dobu nezbytnou k jejich zpracování

55. Zákon o ochraně osobních údajů:

- * 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

- nevztahuje se na data poskytovaná dobrovolně státním institucím

- vztahuje se na zabezpečení zpracovávaných osobních údajů v případě automatizovaných prostředků dodávaných ze zemí mimo EU

- * nevztahuje se na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní spotřebu

56. Pravidla přístupu do počítačové sítě (FI) MU

- v případě nutnosti je povoleno rekonfigurovat PC, které je pod správou CVT FI

- uživatel smí kopírovat programové vybavení jen pro potřeby svého ročníku

- * je zakázáno odposlouchávat provoz a vytvářet kopie poštovních zpráv

- v počítačových učebnách a na počítačích FI je možné hrát pouze legálně zakoupené hry

- * je povoleno používat pouze legální software

- * je zakázáno pracovat pod cizí identitou

57. Pravidla přístupu do počítačové sítě (FI) MU

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

58 Co je to odvození (inference)?

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

59. Jaké ochranné mechanismy se používají k zabránění neoprávněného použití informací v databázích?-

- Kódování dat.
- Kryptování dat.
- *** Zákaz agregace u velkých databází.**
- *** Statistické databáze.**
- Povinná autentifikace.

60. Co je to kritický dotaz ve statistické databázi?

- Dotaz, jehož vyhodnocení trvá dlouhou dobu a vyžaduje veškerou výpočetní sílu databáze, která se v tím může stát nedostupnou pro ostatní dotazy.
- *** Dotaz, který databáze nesmí vyhodnotit, neboť by tím došlo ke zjištění informací o jednotlivci nebo malé skupině osob.**
- *** 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.

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

- Pro vyhodnocení dotazu nesmí být použito více záznamů než je stanovená maximální (perturbační) mez.
- *** Technika stavějící např. na zaokrouhlování mezivýsledků dotazů.**
- Pro vyhodnocení dotazu může být použito pouze menší množství záznamů než je stanovená maximální (perturbační) mez.
- *** Technika umožňující zjistit konzistentní, ale ne spolehlivé odpovědi na sérii podobných dotazů.**
- Žádná taková technika neexistuje.
- *** Přidávání pseudonáhodného "šumu" k množině záznamů, na jejichž základě se vyhodnotí dotaz.**

62. Důvěryhodnost dat?

- Data získaná od důvěryhodného zdroje.
- *** Data jsou v nezměněné podobě tak, jak byla vytvořena.**
- *** Technicky se realizuje např. pomocí digitálního podpisu.**

- Utajení obsažené informace.

63. Pro zajištění prokazatelné zodpovědnosti (accountability)?

- Je 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 umožňujících propojení činnosti s konkrétní osobou tak, že daná osoba se nemůže zříci zodpovědnosti za svoji činnost.
- Je prováděna archivace dat pro udržení schopnosti správy účtu.

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

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

65. Pod pojmem slabá integrita dat rozumíme

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

66. Pod pojmem silná integrita dat rozumíme

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

67. 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

68. 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

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

- * hrozba
- útok
- riziko
- zranitelnost

70. Pod pojmem důvěrnost dat rozumíme

- Snaha zamezit změně sémantického obsahu dat neautorizovanými osobami
- * Snaha zabránit zjištění sémantického obsahu dat neautorizovanými osobami
- Snaha utajit existenci sémantiky dat před nedůvěryhodnými osobami

71. Pod pojmem dostupnost dat rozumíme

- Průběh autentizace osoby pro práci s daty a službami by měl být dostupný i lidem se sníženou pracovní schopností
- Osoby by měly mít přístup ke svým datům a službám co nejsnadněji
- Data by měla být dostupná i neautorizované osobě v případě kritické události

-* Autorizované osoby by měly mít přístup ke svým datům a službám co nejsnadněji

72. Pod pojmem prokazatelná zodpovědnost rozumíme

- Uživatelé se musí před použitím systému autentizovat vůči jeho majiteli
- Uživatelé systému jsou zodpovědní za činy, které lze jednoznačně prokázat
- U každé činnosti lze jednoznačně prokázat, kdo je za ni zodpovědný.

-* Za veškeré činy v systému jsou uživatelé zodpovědní vůči majiteli dat

73. Kerckhoffsův princip říká, že:

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

-* Použitý algoritmus je veřejně znám, utajován je pouze klíč

74. Zaručený elektronický podpis je

- Podpis, který je proveden nad zaručeně koretními daty
- Nic takového dle českého zákona neexistuje
- Podpis, který je připojen ke zprávě tak, aby ho bylo možné zaručeně ověřit

-* Podpis, který je jednoznačně spojen s podepisující osobou

75. Digitální podpis zajišťuje

- Obnovu privátního klíče při jeho ztrátě
- Autorizaci podepisovaných dat

-* Integritu podepisovaných dat

- Důvěrnost podepisovaných dat

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

- Zabránit ztrátě privátního klíče

-* Získat veřejný klíč konkrétního uživatele

- Získat přístup k šifrovaným datům konkrétního uživatele v kritické situaci oprávněnou organizací

-* Ověřit identitu předkladatele veřejného klíče

77. Jaké druhy kryptografie dle typu použitých klíčů rozlišujeme

- Symetrická, asymetrická, s náhodnými klíči
- Pouze asymetrickou, symetrická je speciálním případem asymetrické
- Symetrická, asymetrická, antisymetrická

-* Symetrická, asymetrická, bez klíčů

78. Od kryptografické hašovací funkce požadujeme

-* Rychlost výpočtu, jednosměrnost, bezkoliznost

- Bezkoliznost, antisymetričnost, jednosměrnost, rychlost výpočtu
- Jednosměrnost, koliznost, rychlost výpočtu
- Obousměrnost, bezkoliznost, rychlost výpočtu

79. Která z uvedených tvrzení jsou nepravdivá?

- Algoritmy používané pro asymetrickou kryptografii jsou typicky pomalejší než algoritmy pro symetrickou kryptografii

-* Symetrická kryptografie využívá dva klíče, veřejný a privátní

-* U asymetrické kryptografie je privátní klíč sdílen mezi dvěma a více uživateli

- Symetrická kryptografie využívá obvykle klíče s kratší délkou

80. Pod pojmem depozitování klíčů rozumíme

-* Uložení kopie klíče na chráněné místo tak, aby mohlo dojít k jeho obnově při ztrátě

- Uchování klíčů v takové podobě, aby je bylo možné hromadně zálohovat

- Uchovávání více klíčů pohromadě tak, aby nedošlo k jejich vyjádření neautorizovaným osobám

-* Uchování kopie klíče přístupné v případě krizové situace odpovědnou organizací

81. Certifikační autorita

- Monitoruje chování uživatele po vydání certifikátu

-* Ověřuje identitu uživatele před vydáním certifikátu

- Umožňuje přístup k privátnímu klíči uživatele pro vládní organizace

-* Umožňuje zneplatnit vydaný certifikát

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

- protokol, který používá šifrování pro zabezpečení přenosu autentizačních dat

- protokol typu výzva-odpověď (challenge-response), který využije asymetrickou kryptografii jen pro podpis, nikoliv pro šifrování

-* protokol, založený na důkazu nulového rozšíření znalostí (zero-knowledge)

83. Co znamená útok analýzou provozu (v případě anonymních komunikačních sítí)?

- útočník modifikuje provoz v síti za účelem získání citlivých informací

- útočník modifikuje provoz v síti s cílem ovlivnit účastníky komunikace

-* útočník pasivně poslouchá provoz v síti a pomocí statistických metod se snaží odhalit účastníky komunikace

- útočník aktivně směřuje provoz v síti a pomocí statistických metod se snaží odhalit účastníky komunikace

84. V jaké z uvedených možností dochází nejčastěji k selhání bezpečnosti:

-* Úmyslné a neúmyslné chyby obsluhy počítačů

- Chyby při návrhu matematického algoritmu

- Chyby při implementaci matematického algoritmu

- Chyby při implementaci celého systému

85. Má smysl utajovat i samotnou existenci dat?

- ne, stačí šifrovat

- má, ale pouze v případě, že taková data chceme druhé straně předat anonymním způsobem

-* existují případy, kdy i informace o existenci dat může představovat bezpečnostní riziko

86. Pokud neautorizovaná osoba zjistí sémantický obsah chráněných dat, jedná se o narušení:

- integrity

- prokazatelné zodpovědnosti

- dostupnosti

-* důvěrnosti

87. Proč dochází ke zpoždění komunikace při použití systémů pro poskytování anonymity:

- je to pouze falešný pocit sucha a bezpečí

- * protože zpráva typicky není doručena "nejlepší" cestou a je směrována "neefektivně"

- aby měl správce systému dost času na přečtení obsahu zpráv

- * je to cena, kterou platíme za anonymitu

88. Poštovní PO Boxy svým charakterem odpovídají bezpečnostní funkci:

- * **Pseudonymita**

- Nesledovatelnost
- Nespojitelnost
- Nedoručitelnost
- Anonymita

89. V obecném pojetí se soukromá informace chápe jako:

- Informace, která je volně k dispozici

- Informace, kterou chceme sdílet s jinými a nezáleží nám na dalším šíření takto poskytnuté informace

- * **Informace u které (pokud už ji někomu poskytneme) chceme kontrolovat její pohyb**

- * **Informace, kterou nechceme sdílet s jinými**

90. Nespojitelnost nezohledňuje identitu uživatele, ale:

- Rozsah služeb a zdrojů, které byly použity různými uživateli

- Rozsah služeb a zdrojů, které jsou v systému aktuálně využívány

- Jeho pseudonymitu a nesledovatelnost

- * **Rozsah služeb a zdrojů, které byly použity jedním uživatelem**

91. V případě nepozorovatelnosti (unobservability) je ochraňovanou hodnotou:

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

- * **Informace o použití zdrojů a služeb**

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

- informace o přihlášených uživateli

92. Co je to "Security through obscurity"?

- * **Víra, že pouze dobře utajený algoritmus je bezpečný**

- Souhrnný název pro bezpečnostní mechanismy vybudované na teorii složitosti

93. V případě, že neoprávnění uživatelé jsou "menší zlo" než nespokojení uživatelé, nastavíme biometrický systém tak, že bude mít FAR (False Acceptance Rate) a FRR (False Rejection Rate):

- * **vyšší hodnotu FAR a nižší hodnotu FRR**

- vyšší hodnotu FRR a nižší hodnotu FAR

- vyšší hodnotu FRR a vyšší hodnotu FAR

- nižší hodnotu FRR a nižší hodnotu FAR

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

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

- * **zabráni 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

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

95. Která z těchto tvrzení jsou správná?

- Biometrická data jsou tajná.

- * Některé biometriky hodně o subjektu vypovídají.

- * Biometriky v ideálním případě určují identitu člověka přesně a lze tak spojit jednotlivě

jeho činy.

- Jeden vzorek lze využít jen v jednom systému.

96. Podle českého zákona o e-podpisu (227/2000) je zaručený elektronický podpis:

- * Elektronický podpis, který je jednoznačně spojen s podepisující osobou

- Elektronický podpis, který je proveden nad zaručeně korektními daty

- Nic takového dle českého zákona neexistuje

- Elektronický podpis, který je připojen ke zprávě tak, aby ho bylo možné zaručeně ověřit

97. Mezi základní pravidla bezpečnostního modelu Bell-LaPadula patří:

- Procesy nesmějí číst data na nižší úrovni.

- Procesy nesmějí číst/zapisovat data z/do nižší úrovně.

- * Procesy nesmějí číst data na vyšší úrovni.

- * Procesy nesmějí zapisovat data do nižší úrovně.

- Procesy nesmějí zapisovat data do vyšší úrovně

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

- smím

- * mám

- * vím

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

- * vzor oční duhovky

- vzor oční sítnice

- EKG

- * srovnání tváře

100. Čipová kreditní karta bez mag. Proužku

- skýtá obvykle nižší bezpečnost než karta s mag. proužkem (bez čipu)

- * obvykle obsahuje malý procesor

- obvykle neobsahuje procesor, přestože se jí tradičně říká "čipová"

- * skýtá obvykle vyšší bezpečnost než karta s mag. proužkem (bez čipu)

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

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

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

102. Výraz script kiddies označuje:

- 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.**
- Útočníka, který je schopen kreativně odhalovat nové zranitelnosti i bez znalostí o systému

103. Proč platební karty s čipem mají magnetický proužek?

-* Kvůli zpětné kompatibilitě.

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

104. Nespojitelnost (podle A.Pfitzmanna - mixy) znamená:

-* Nespojitelnost dvou a více prvků (např. subjektů, zpráv, událostí) tak, že v takovém systému nejsou prvky ani více, ani méně ve vzájemném vztahu s ohledem na předchozí znalost systému.

- Nespojitelnost tří a více prvků (např. subjektů, zpráv, událostí) tak, že budou anonymní pouze vůči uživatelům systému, nikoli vůči administrátorům.

-* Že pravděpodobnost spojení prvků v systému je stejná před a po (prů)běhu nějaké posloupnosti událostí v systému.

105. Chybovost biometrických systémů vyjádřená pomocí FAR (False Acceptance Rate) je:

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

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

106. Komu v platebních systémech poskytují současné tokeny nejnižší ochranu?

- Provozovatelům sítě bankomatů (v případě, že provozovatelem není přímo banka)
- Obchodníkům
- Bankám

-* Zákazníkům

107. K potenciálním 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