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.

--

K bezpečným metodám autentizace klienta bance v systému internetového bankovnictví

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".

--

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

--

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)

--

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. napěťovým a teplotním útokům.

--

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.

--

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.

--

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.

--

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.

--

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

--

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).

--

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.

--

Která z následujících tvrzení platí:

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

--

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.

--

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.

--

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.

--

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.

--

Zákon o ochraně osobních údajů:

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

--

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.

--

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.

--

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.

--

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 odpovědi není správná.

--

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.

--

Digitální podpis zajišťuje

- Komprimaci podepisovaných dat.
- Platnost podepisovaných dat.
- Důvěrnost podepisovaných dat.
- Autentizaci podepisovaných dat.

--

Digitální podpis zajišťuje

- Integritu podepisovaných dat.
- Obnovu privátního klíče při jeho ztrátě.
- Důvěrnost podepisovaných dat.
- Autorizaci podepisovaných dat.

--

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.

--

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

--

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)

--

Citlivé osobní údaje dle české legislativy vypovídají o:

- zdravotním stavu.
- postoji k trestné činnosti rodinných příslušníků.
- majetkových poměrech státních úředníků.
- sexuální orientaci.

--

Základní metody autentizace uživatelů jsou založeny na něčem, co

- vím.
- smím.
- mám.

--

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.

--

V případě nepozorovatelnosti (unobservability) je ochraňovanou hodnotou?

- Informace o překročení přiděleného procesorového času pro použití nabízených zdrojů a služeb.
- Informace o přihlášených uživatelích.
- Informace o použití zdrojů a služeb.
- Informace o aplikovaných bezpečnostních opatřeních systému (např. nastavení pravidel firewallu).

--

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.

--

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.

--

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 informaci 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.

--

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 měly mít přístup k datům a službám co nejméně komplikovaný.
- Autorizovaní uživatelé by měly mít přístup k datům a službám co nejméně komplikovaný.

--

Systémy měnící tok a výskyt dat na komunikačním kanálu se nazývají

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

--

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.

--

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.

--

Základní metody autentizace uživatelů jsou založeny na něčem, co

- nelze jednoduše zničit.
- znám.
- jsem.

--

Co je to perturbační technika používaná ve statistických databázích?

- Žádná taková technika neexistuje.

- Pro vyhodnocení dotazu nesmí být použito více záznamu 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.

--

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.

--

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

--

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.

--

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

--

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

--

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

--

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

--

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.

--

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 neutorizovanými osobami

--

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

--

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

--

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.

--

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

--

Pseudonymita (podle A.Pfitzmanna - mixy) znamená:

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

--

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

--

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

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

--

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

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

--

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.

--

Pro anonymitní komunikační sítě 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

--

Projekt AN.ON poskytuje stejné služby jako

- Mixmaster
- Onion routing.
- Mixminion.
- TOR

--

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)

--

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

--

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.

--

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.

--

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

- hrozba
- zranitelnost
- útok
- riziko

--

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.

--

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.

--

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.

--

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.

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

--

Povinnosti spravce osobnich udaju:

- vkladat falesne zaznamy, aby v pripade kradeze dat nebylo mozne snadno posoudit jejich validitu
- neposkytovat data tretim stranam pred sepsanim Smlouvy o poskytnuti osobnich datech
- stanovit prostredky a zpusob zpracovavani osobnich udaju
- archivovat data kodovane, nenili urceno jinak

--

Která technika není platná pro anonymitní komunikační sítě:

- přeuspořádávání 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

--

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

--

Mezi obvykla bezpecnostni politiky patri:Interaplikační bezpečnostni politika

- Interaplikační bezpečnostni politika
- Integrovana bezpecnostni politika
- Horizontalní bezpecnostni politika
- Celkova bezpecnostni politika
- Systemova bezpecnostni politika

--

Problém živosti pro vstupní zařízení spočívá v tom, že:

- Žádná z těchto odpovědi 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.

--

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

- důvěrnosti
- integrity
- dostupnosti
- prokazatelné zodpovědnosti

--

Obvykle nejmene bezpecnym bodem behem prubehu autentizace v internetovem bankovnictvi je:

- autentizace banky
- autentizace pocitace klienta
- autentizace klienta

--

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

--

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

- Zákazníci sami se chovají nezodpovědně.

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

--

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.

--

Která z těchto tvrzení jsou správná?

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

--

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.

--

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.

--

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.

--

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.

--

Projekt AN.ON poskytuje stejné služby jako

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

--

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.

--

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.

--

Bezpečnostní politika je

- Dokument schválený vrcholovým managementem a specifikující využití IT pro zajištění cílů organizace.
- Soubor opatření a mechanizmů 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.

--

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.

--

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).

--

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.

--

Tvrzení "Využití služby pro neautorizovaný přístup" by mohlo označovat

- riziko.
- zranitelnost.
- hrozbu.
- útok.
- bezpečnostní politiku.

--

Podezřelé chování v síti zjistíte

- antivirovým programem.
- honeypotem.
- antispyware programem.
- IDS.
- firewallem.

--

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

--

Proč platební karty s čipem mají magnetický proužek?

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

--

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.

--

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.

--

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.

--

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

- Čipová karta s magnetickým proužkem
- Platební terminál

- Bankomat
- Čipová karta

--

Které dvě z těchto biometrických technik jsou nejpřesnější?

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

--

Protokoly SSL/TLS umožňují

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

--

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

- Pseudonym osoby >pseudonym rolevztahu>pseudonym vztahu >pseudonym role >pseudonym transakce.
- Pseudonym osoby >pseudonym role a pseudonym vztahu >pseudonym rolevztahu>pseudonym transakce.
- Pseudonym transakce >pseudonym rolevztahu>pseudonym role a pseudonym vztahu > pseudonym osoby.
- Pseudonym osoby >pseudonym transakce >pseudonym role a pseudonym vztahu > pseudonym rolevztahu.
- Pseudonym osoby >pseudonym rolevztahu>pseudonym role >pseudonymvztahu >pseudonym t transakce.

--

Která z těchto tvrzení jsou správná?

- Biometriky po analýze s využitím kryptografie o subjektu zprávy vypovídají.
- Jeden vzorek lze využít jen v jednom systému.
- Žádná z těchto odpovědi není správná.
- Biometrická data jsou tajná.

--

Co znamená pojem důvěrnost dat?

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

--

Místa setkání a skryté služby TORu je/jsou:

- místa, kde uživatelé získavají 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.

--

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

--

Je lepší používat TOR nebo Mixminion?

- Jednoznačně TOR.
- Ani jedno, ani druhé.
- Záleží na tom, co chceme dělat.
- Jednoznačně Mixminion.

--

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).

--

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.

--

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.

--

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.

--

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.

--

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 poupravených záznamů, které jsou náhodně vybrány ze všech existujících záznamů v databázi.
- Výsledek dotazu je zcela náhodný a nepředvídatelný.

--

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 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.

--

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.

--

Typické operace na firewallu jsou

- hašovat
- xorovnat
- zakázat
- povolit
- prelozit

--

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.

--

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.

--

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.

--

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 záznamu než je stanovená maximální mez.

--

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.

--

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

--

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.

--

Co je to "Security through obscurity"?

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

--

Co je nejčastější příčinou bezpečnostních incidentů?

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

--

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.

--

Onion Routing systémem označujeme

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

--

Zabezpečení provozu na úrovni IP dosáhnu pokud zvolím:

- IPsec
- Stunnel
- PGP
- IPv6
- IPv4s

--

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 mechanizmem ochrany čipu je magnetický proužek.
- Bez techniky velmi náročného rozebrání čipu a jeho analýzy není možné vytvořit kopii.

--

Které z následujích 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.

--

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.

--

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).

--

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.

--

Pro komunikaci mezi jednotlivými Onion Routery (OR) platí

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

--

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.

--

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.

--

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.

--

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

--

Tvrzení "Systém je chráněn sdíleným heslem" by mohlo označovat

- bezpečnostní politiku
- útok
- hrozbu
- riziko
- zranitelnost

--

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

--

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

- žádná z těchto odpovědi není správná
- heslo dlouhé alespoň 8 znaků a vytvořené náhodně ze sady min. 95 znaků
- autentizační kalkulačka

- certifikovaný USB disk

--

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

--

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.

--

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

--

Které dvě z těchto biometrických technik jsou nejpohodlnější pro uživatele?

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

--

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

--

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).

--

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 spojovat jednotlivě jeho činy.
- Jeden vzorek lze využít jen v jednom systému.

--

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

--

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

--

Nepozorovatelnost (podle A.Pfitzmanna – mixy) znamená

- že pravděpodobnost spojení prvků v systému je stejná před a po (prů)běhu nějaké posloupnosti událostí v systému
- Stav (daných) předmětů zájmu, kdy nejsou odlišitelné od jiných předmětů zájmu
- Stav, kdy ostatní uživatelé nemohou pozorovat využívání zdrojů systému.

--

Která z uvedených tvrzení jsou pravdivá? (založeno na zákonu o elektrickém podpisu 227/2000 Sb.)

- Elektronický podpis vytváří člověk, zatímco elektronickou značku vytváří počítač
- Elektronický podpis a elektronická značka se liší v úrovni ochrany soukromého klíče.
- Elektronický podpis a elektronická značka jsou technologicky totožné.
- Elektronický podpis je vytvářen soukromým klíčem, zatímco elektronická značka je vytvářena klíčem veřejným.
- Mezi elektronickým podpisem a elektronickou čtečkou není žádný rozdíl.

--

Co to je pozitivni kompromitace statisticke databaze?

- Nesmysl
- Opak castecne kompromitace
- Kompromitace se zametenim stop
- Opak negativni kompromitace
- Vysledkem zpresneneho dotazu je nenulovy pocet odpovedi

--

Jak pracuje technika minimalniho rozsahu dotazu ve statistickych databazich?

- zadna takova technika neexistuje.
- Pro vyhodnoceni dotazu muze byt pouzito mene zaznamu nez je stanovena
- minimalni mez, ale pouze za zvlastnich bezpecnostnich opatreni (napr. podpis dohody o mlcenlivosti).
- zadna takova technika se ve statistickych databazich nepouziva.
- Pro vyhodnoceni dotazu nesmi byt pouzito mene zaznamu nez je

stanovena minimalni mez.

--

Mezi obvykle bezpecnostni politiky patri:

- Systemova bezpecnostni politika
- Celkova bezpecnostni politika
- Interaplikacni bezpecnostni politika
- Integrovana bezpecnostni politika
- Horizontalni bezpecnostni politika

--

Duveryhodnost dat?

- Utajeni obsazene informace.
- Data jsou v nezmenene podobe tak, jak byla vytvorena.
- Technicky se realizuje napr. pomoci digitalniho podpisu.
- Data ziskana od duveryhodneho zdroje.

--

Nespojitelnost (podle Spolecnych kriterii) zajistuje moznost opakovaneho pouziti zdroju:

- tak, ze identita uzivatele zustane skryta specifickym uzivatelum, pro specificke operace bez prozrazeni identity uzivatele, ale v pripade potreby lze identitu zpetne zjistit
- tak, ze pouze administratori uvidi, ze ve skutecnosti toto pouziti inicioval tentyz uzivatel
- tak, ze ostatni si tato pouziti nebudou schopni spojit bez prozrazeni identity uzivatele

--

Jake jsou faktory primo ovlivnujici pravdepodobnost neopravneneho (vy)uziti informaci?

- uroven bezpecnostnich mechanizmu.
- Vyse trestu tem, kdo s daty neopravnene manipuluje.
- Vyse trestu tem, kdo data hlidali a zajistili restriktivni manipulaci.

- Vyse trestu tem, kdo data neohlidali a spolupodileli se na jejich uniku.
- Kódovani dat.

--

Typicke operace na firewallu jsou

- hasovat
- prelozit
- zmenit
- zakazat

--

Je vubec mozne, aby melo vnejsi prostredi (teplota atp.) nejaky vliv na bezpecnost cipovych karet?

- ne, neni to mozne
- ano, je to mozne

--

Pod pojmem prokazatelna zodpovednost rozumime

- Za veskere sve ciny v systemu jsou uzivatele zodpovedni vuci majiteli dat
- Uzivatele se musi pred pouzitim systemu autentizovat vuci jeho majiteli
- U kazde cinnosti lze jednoznacne prokazat, kdo je za ni zodpovedny.
- Uzivatele systemu jsou zodpovedni za ciny, ktere lze jednoznacne prokazat

--

Nespojitelnost nezohlednuje identitu uzivatele ale

- Rozsah sluzeb a zdroju, ktere jsou v systemu aktualne vyuzivane
- Jeho pseudonymitu a nesledovatelnost
- Rozsah sluzeb a zdroju, ktere byly pouzity jednim uzivatelem
- Rozsah sluzeb a zdroju, ktere byly pouzity ruznymi uživateli

--

Komu v platebnich systemech poskytuji soucasne tokeny nejnizsi ochranu?

- Bankam
- Provozovatelum site bankomatu (v pripade, ze provozovatelem neni primo banka)
- Obchodnikum
- Zakaznikum

--

Co je to verejny pseudonym?

- Napr. telefonni cislo ve Zlatych strankach

- Pseudonym pouzivany uvnitr verejne nedostupneho systemu
- Je znam verejnosti za poplatek
- Pseudonym pouzitelny pouze na verejnosti
- Je verejne znam od pocatku, napr. v seznamu osob

--

Anonymita (podle Spolecnych kriterii) zajistuje moznost pouziti zdroju nebo sluzeb systemu tak, ze:

- specifikovane entity jsou schopny urcit skutecne uzivatelske jmeno spojene se specifikovanymi subjekty, operacemi, objekty
- identita uzivatele zustane skryta specifickym uzivatelum, pro specificke operace
- identita uzivatele zustane skryta, ale v pripade potreby ji lze zpetne zjistit

--

Firewall je

- umela prekazka pred potencialne nebezpecnym okolim
- software pro detekci a blokaci podezrelych aktivit v systemu
- spolehlivou ochranou pred zneuzitim pocitacu ve vnitrni siti

--

Nepozorovatelnost (podle Spolecnych kriterii) zajistuje moznost pouziti zdroju nebo sluzeb systemu tak, ze:

- ostatni uzivatele systemu nemohou pozorovat pouzivani daneho zdroje nebo sluzeb, ale v pripade potreby lze toto chovani zpetne spojit s konkretnim uzivatelem
- uzivatele nejsou zodpovedni za sve chovani v systemu
- ostatni uzivatele, s vyjimkou administratoru, nemohou pozorovat pouzivani daneho zdroje nebo sluzeb
- specifikovane entity nejsou schopny pozorovat specifikovane operace provadene specifikovanymi entitami na specifikovanych objektech
- ostatni uzivatele (ani administratori) systemu nemohou pozorovat pouzivani daneho zdroje nebo sluzeb
- specifikovane entity jsou schopny pozorovat specifikovane operace provadene specifikovanymi entitami na nespecifikovanych objektech

--

IEEE - principy SW inzenyra stanovi napr.

- vykonavat svou cinnost v souladu s verejnym zajmem
- zastavat pouze takove pozice, na ktere ma narok a schopnosti
- povinnost zit cestne, zdrave a podle pravidel IEEE tak, aby na nej mohla byt spolecnost hrda
- zajistit cestnost a nezavislost ve svych odbornych odhadech
- povinnost pouzivat pouze software, za ktery nebylo prokazatelnym zpusobem zaplaceno

--

Pro zajisteni prokazatelne zodpovednosti (accountability)?

- Je provadena archivace dat pro udrzeni schopnosti spravy uctu.
- Je na zacatku prace v systemu obvykle provadena autentizace nebo identifikace.
- Je provadena archivace dat umoznujicich propojeni cinnosti s konkretni osobou tak, ze dana osoba se nemuze zrici zodpovednosti za svoji cinnost.
- Ja na zacatku prace v systemu obvykle provadeno desifrovani dat pro praci s uctem.

--

Mezi zakladni pravidla bezpecnostniho modelu Bell-LaPadula patri:

- Procesy nesmeji cist/zapisovat data z/do nizsi urovne.
- Procesy nesmeji zapisovat data do nizsi urovne.
- Procesy nesmeji cist data na nizsi urovni.
- Procesy nesmeji zapisovat data do vyssi urovne.
- Procesy nesmeji cist data na vyssi urovni.

--

Pro emailove zpravy posilane pomoci systemu Mixminion plati

- jsou anonymni
- hlavicky mailu nejsou modifikovany
- uzivatel specifikuje cestu po siti
- odpovedi jsou v systemu dorucovany odlisne od normalnich emailu
- je mozne na ne v urcitem casovem ramci odpovedet
- jsou pseudonymni

--

Ktera technika neni platna pro anonymitni komunikacni site:

- vyuzivani minixu pro preposilani zprav
- sifrovani zprav mezi uzly algoritmem RSA s delkou klice zavislou na poctu uzlu
- pozastavovani prijatych zprav
- v case nedeterministicke odesilani prijatych zprav
- preusporadavani zprav v ramci uzlu

--

Pod pojmem dostupnost dat rozumime

- Prubeh autentizace osoby pro praci s daty a sluzbami by mel byt dostupny i lidem se snizenou pracovni schopnosti
- Uzivatele by mely mit pristup k datum a sluzbam co nejmene komplikovany
- Data by mela byt dostupna i neautorizovane osobe v pripade kriticke udalosti

- Autorizovani uzivatele by mely mit pristup k datum a sluzbam co nejmene komplikovany

--

Maximalni pocet identit jedne osoby muze byt

- 2 pro vdane zeny
- kolik chce (kdyz se bude dostatecne snazit)
- 4 pro jedince s dvema svatbami a jednim rozvodem
- 1

--

V souvislosti se sdruzovanim dat do rozsahlych databazi uklada zakon 101/2000 sb. o ochrane osobnich udaju

- Povinnost nesdruzovat data, ktera byla puvodne ziskana k rozdilnym ucelum, do jednoho celku.
- Povinnost informovat zkoumanou osobu (subjekt) o tom, ze se podarilo zjistit o nem citlive informace a zda muze potvrdit jejich pravdivost.
- Povinnost informovat osobu, jejiz data budou ulozena a zpracovavana v databazi, ze se timto zpusobem bude s poskytnutymi daty nakladat.

--

Podle ceskeho zakona o e-podpisu (227/2000) je zaruceny elektronicky podpis:

- Elektronicky podpis, ktery je jednoznacne spojen s podepisujici osobou
- Elektronicky podpis, ktery je proveden nad zarucene korektnimi daty
- Nic takoveho dle ceskeho zakona neexistuje
- Elektronicky podpis, ktery je pripojen ke zprave tak, aby ho bylo mozne zarucene overit

--

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

- 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, 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 skryta ostatním uživatelům, ale ne administrátorům

--