U biometrickych systemov na zaciatku procesu verifikacie je identita znama a proces identifikacie je narocnejsi ako proces verifikacie.

Kerckhoffsuv princip plati aj v sucastnosti a hovori o tom ze pouzity algoritmus je verejne znamy, utajovany je iba kluc.

Projekt AN.ON poskytuje rovnake sluzby ako Onion routing a TOR.

Statisticka databaza obsahuje informacie o jednotlivcoch, ale povoluje iba staticke dotazy, co znamena ze nedovoli ziskat informacie o jednotlivcoch.

Analiza a hodnotenie hrozieb zahrnuje rozvahu, co vsetko by malo byt chranene a vyhodnotenie ake hrozby hrozia ochranovanym hodnotam.

Bezpecnostna politika je subor pravidiel, ktory specifikuje ucinny sposob uplatnovania opatreni potrebnych k dosiahnutiu pozadovanych minimalnych uroven rizik. Zahrnuje poziadavky pravidla a postupy urcujuce sposob ochrany a zachadzania s hodnotami spolocnosti.

Odomykanie zamku na dverach klucom spada pod autentizacne procedury.

Analyza rizik metodou CRAMM sa prevadza strukturovanym pristupom identifikacie a ocenenia hodnot, odhadom hrozieb a zranitelnosti hodnot, vyberom vhodnych protiopatreni.

Pre emailove spravy posielane pomocou Mixminionu plati, ze su anonymne, je mozne na ne v urcitom casovom ramci odpovedat a uzivatel specifikuje cestu po sieti.

Vyuzitie sluzby pre neautorizovany pristup oznacuje HROZBU.

Podozrive chovanie v sieti zistime pomocou honeypotu, IDS a firewallu.

Pre FAR(false acceptance rate) a FRR(false reject rate) plati, ze so zvysenim FAR sa znizuje FRR, so znizenim FAR sa zvysuje FRR.

Magneticky pruzok na platobnych kartach s cipom je koli spatnej kompatibilite.

Agregacia dat je zoskupovanie dat do rozsiahlych databaz.

Pod pojmom asymetricka kryptografia rozumieme, kryptografiu, ktora vyuziva dvojicu sukromneho a verejneho kluca.

Zneuzitie mobilneho telefonu operatorom je mozne tak ze odoslane sms z mobilu na mobil mozu byt jednoducho ukladane a poloha telefonu moze byt sledovana.

Protokoly SSL a TLS umoznuju kontrolovat integritu prenasanych dat a autentizaciu komunikujucich stran (klient server).

Pre hierarchiu podla druhu pseudonymu v smere zvysujucej sa anonymity a nespojitelnosti plati : Pseudonym osoby -> pseudonym role a pseudonym vztahu -> pseudonym role-vztahu -> pseudonym transakcie.

Pre obecne principy bezpecnosti IT plati, ze sa usilujeme o jednoduchost, externe zdroje povazujeme za nebezpecne a fyzicky alebo logicky oddelujeme kriticke zdroje.

Zakladne metody autentizacie uzivatelov su zalozene na niecom co viem a

mam.

Analyza rizik metodou ALE je pocitana sposobom : ALE = SLExARO

Chybovost biometrickych systemov je vyjadrena pomocou FRR, co je podil poctu odmietnutych pokusov o prihlasenie legitimnych uzivatelov k poctu vsetkych pokusov o prihlasenie.

TOR poskytuje testovanie prenasanych dat, je to vylepsenie oproti povodnemu navrhu Onion Routing systemov a je to obrana proti tagging utokom.

Pokial ma hashovacia funkcia vlastnost silnej bezkoliznosti, znamena to, ze je vypocetne nemozne najst dve navzajom rozne vstupy, aby boli vysledne hashe rovnake.

V pripade nepozornosti je ochranovanou hodnotou informacia o pouziti zdroja alebo sluzby.

Na sluzbu TOR existuje utok, ktory dokaze znizit anonymitu pouzivatela.

Pertubacna technika pouzivana v statistickych databazach zaokruhluje medzivysledky dotazov, umoznuje zistit konzistentne ale nie spolahlive odpovede na serie dotazov a pridava pseudonahodny sum k mozine zaznamov z ktorych sa vyhodnocuje dotaz.

Anonymita zaistuje moznost pouzitia zdrojov alebo sluzieb tak, ze identita uzivatela zostane skryta a zostane skryta aj specifickym uzivatelom pre specificke operacie.

Autentizacia protokolom s nulovym rozsirenim znalosti zabranuje overovatelovi aby sa mohol neskor neopravnene vydavat za prokazujici stranu a aby sa nedozvedel tajomstvo ktore vlastni prokazujuca strana.

System detekcie prieniku IDS je mozne pouzit v sieti aj na pocitaci.

PGP umoznuje nastavit uroven dovery pre konkretny verejny kluc a toto nastavenie sa pouziva na indikaciu dovery v povode dat podpisanych vlastnikom odpovedajuceho privatneho kluca.

Pokial neautorizovana osoba zisti semanticky obsah chranenych dat, ide o dovernost.

Digitalny podpis zaistuje integritu podpisovanych dat.

Pre osobne udaje podla ceskej legislativy plati ze sa jedna o akykolvek udaj tykajuci sa urceneho alebo urcitelneho subjektu udajov, ak ide na zaklade jedneho alebo viacerych osobnych udajov priamo alebo nepriamo zistit identitu subjektu povazuje sa subjekt za urceny alebo urcitelny, o osobny udaj sa nejedna pokial je treba k zisteniu identity subjektu udajov neprimerane mnozstvo casu, materialnych prostriedkov.

Zakladne vlastnosti kvantitativnej analyzi rizik su ze postup neni automatizovatelny, vystup je v konkretnej hodnote a je lahko zrozumitelny.

Miesta stretnutia a skryte sluzby TORu su sluzby, ktore umoznuju anonymnu prevadzku napr. Weboveho priestoru a sluzby umoznujuce serveru kontrolovat anonymne dorucene poziadavky.

Riesenia pre odosielanie anonymnych emailov su zalozene na remaileroch u ktorych rozlisujeme niekolko typov, broadcastovych sietiach, mixoch.

V pripade ze nespokojny uzivatelia su mensie zlo ako neopravneny uzivatelia, tak nastavime biometricky system tak ze bude mat vysoku hodnotu FRR a nizku hodnotu FAR.

Dovernost dat znamena utajenie obsiahnutych informacii.

PGP umoznuje digitalne podpisat data a overit podpis, sifrovat a desifrovat data.

Anonymita zaistuje moznost pouzitia zdrojov systemu tak ze, identita uzivatela zostane skryta a zostane skryta aj specifickym uzivatelom pre specificke operacie.

Pretoze standart GSM obsahoval bezpecnostne chyby bol navrhnuty 3GSM.

Povodne neverejny pseudonym je pseudonym ktory povodne nebol verejny ale v niektorych pripadoch moze byt zverejneny.

K bezpecnostnym metodam autentizacie klienta banky v internetovom bankovnictve patri preukazanie sa osobnym kluc ulozenym na cipovej karte, usb, alebo sd karte, kodom ziskanym vlozenim vyzvy bankovneho systemu do autentizacnej kalkulacky.

Odmietnutie sluzby je utok ktory uvedie server do stavu, kedy neni schopny reagovat na poziadavky.

Proxy servery su na internete casto sposobom ako obis lokalnu bezpecnostnu politiku, su dolezite, rozumeju aplikacnym protokolom, umoznuju anonymizaciu.

Relevantne bezpecnostne funkcie systemu su nespojitelnost, nepozorovatelnost, anonymita a pseudonymita.

Cipova kreditna karta bez mag. pasika ma vyssiu bezpecnost ako s mag. pruzkom, obvykle obsahuje maly procesor.

Pri podpise s obnovou dat plati ze podpisane data mozu byt obnovene kymkolvek, kto vlastni prislusny verejny kluc a podpis obsahuje aj podpisovane data.

Medzi ciele bezpecnostnej politiky patri minimalizacia rizik a stanovenie strategie pre pouzitie bezpecnostnych funkcii.

Zakon o ochrane osobnych udajov sa nevztahuje na spracovavanie osobnych udajov, ktore prevadza fyzicka osoba vylucne pre osobnu spotrebu, vztahuje sa na kazde spracovavanie osobnych udajov ci uz automatizovane alebo inak, nevztahuje sa na nahodne zhromazdovanie osobnych udajov, pokym tieto udaje nie su dalej spracovavane, alebo pokial nie su pre podnikanie.

Cibulova schema pouzivana v Onion Routingu vyuziva symetricku a asymetricku kryptografiu.

Pod pojmom symetricka kryptografia rozumieme kryptografiu s vyuzitim

rovnakeho kluca pre sifrovanie a desifrovanie.

Digitalny podpis zaistuje autentizaciu podpisovanych dat.

Citlive osobne udaje podla ceskej legislativy vypovedaju o zdravotnom stave a sexualnej orientacii.

Zakladne metody autentizacie uzivatelov su zalozene na niesom co viem a mam.

Podpisovat vlastni verejny kluc privatnym klucom sa doporucuje pre zaistenie jeho integrity.

V pripade nepozorovatelnosti je ochranovanou hodnotou informacia o pouziti zdrojov a sluzieb.

Proti obecnym Onion Routing sietiam prinasa TOR naviac adresarove server s informaciami o jednotlivych routroch a podporu strytych sluzieb a miest stretnutia.

Odvodenie, pomocou neho ziskavame nepriami pristup k informacia bez priameho pristupu k datam, ktore tieto informacie reprezentuju, pristup k informaciam s vyssou citlivostou spracovanim a analyzou skupiny informacii nizsej citlivosti.

K analyze rizik je mozne pouzit BPA(Business Process Analysis) a ALE(annual Loss Expentancy)

Pod pojmom dostupnost dat rozumieme ze autorizovani uzivatelia by mali mat pristup k datam a sluzbam co najmenej komplikovany.

Pod pojmom tranzitivita dovery oznacujeme doveru vo verejny kluc uzivatela X, ktoremu doveruje uzivatel Y, ktoremu doverujeme my.

Systemy meniacie tok a vyskyt dat na komunikacnom kanaly sa nazyvaju anonymitne alebo mixy.

Pod pojmom hybridne kryptosystemy rozumieme napriklad data ktore su sifrovane nahodnym symetrickym klucom a ten je sifrovany verejnym klucom prijemcu.

Protokoly SSL a TLS sa chovaju k protokolom aplikacnej vrstvy OSI modelu transparentne a vyzaduju zaistenie vhodneho systemu spravy klucov.

Zakladne metody autentizacie uzivatelov su zalozene na niecom so som a viem.

Problem zivosti pre vstupne zariadenia spociva v tom ze vtupne zariadanie nie je schopne urcit ci je vzorka od zivej osoby.

Vysledkom hodnotenia systemu podla spolocenskych kriterii (CC) je diskretne hodnotenie ano alebo nie danych poziadaviek na hodnoteny system.

Medzi bezpecnostne poziadavky podla standartu a pre hodnotenie kryptografickych modulov FIPS 140-1/2 patri fyzicka bezpecnost, rozhranie

modulu, bezpecnost o/s, sluzby a autentizacie.

Cibulova schema pouzivana napr. v Onion Routingu pouziva symetricku aj asymetricku kryptografiu.

Cielom zaistenia dovernosti dat je zabranit zisteniu semantickeho obsahu dat neautorizovanymi osobami.

System detekcie prieniku (IDS) je mozne pouzit v sieti aj na pocitaci.

TLS a SSL „Handshake“ protokol sluzi k ustanoveniu zabezpeceneho spojenia, „Record“ protokol predstavuje zakladnu vrstvu.

Pocet kol u algoritmu Rijndael je urceny dlzkou kluca.

Pseudonymita znamena pouzivanie pseudonymu ako identifikatoru.

Pod pojmom slaba integrita dat rozumieme ze data nesmu bez povolenia autorizovanej osoby nepozorovane zmenit svoj stav.

Najmenej bezpecne sucasti platobnych systemov su platobne terminaly a cipova karta s magnetickym pruzkom.

Najvacsi bezpecnostny problem v dnesnych platobnych systemoch pre zakaznika je ze zakaznikovi nezarucuje vazbu medzi zobrazenou a potvrdenou transakciou.

Kriticky dotaz v statickej databaze je dotaz, ktorym by doslo k zisteniu informacii o jednotlivcovi alebo malej skupine osob, alebo sekvencia zlozena z legitivnych dotazov s cielom ziskat informacie o jednotlivcoch alebo malej skupine osob.

Pre anonymne komunikacne siete plati ze mozu byt nachylne k analyze prevadzky a vstupy nejde jednoducho spojit s vystupmi.

Digitalny podpis zaistuje integritu podpisovanych dat.

Cielom zaistenia dovernosti dat je zabranit zisteniu semantickeho obsahu dat neautorizovanym osobam.

Bezpecnostna politika je subor pravidiel specifikujuci ucinny sposob uplatnenia opatreni potrebnych k dosiahnutiu potrebnych minimalnych urovni rizik.

PGP umoznuje nastavit uroven dovery pre konkretny verejny kluc a toto nastavenie sa pouziva pre indikaciu dovery v povode dat podpisanych vlastnikom odpovedajucemu privatnemu klucu.

Pre emailove spravy posielane pomocou systemu Mixminion plati ze uzivatel specifikuje cestu po sieti, je mozne na ne v urcitom casovom ramci odpovedat a su anonymne.

Medzi bezpecnostne poziadavky podla standartu pre hodnotenie kryptografickych modulov FIPS 140-1/2 patri rozhranie modulu, metody pre zmiernenie inych utokov, sprava klucov, sluzby a autentizacie.

Pseudonym vztahu je ked je pre kazdeho partnera pouzite ine meno a pouzite rozne prezyvky pre komunikaciu s kazdym partnerom.

Ci je lepsie pouzivat TOR alebo Mixminion zalezi od toho co chceme robit.

Security through obscurity je viera ze iba dobre utajeny algoritmus je bezpecny.

Profil bezpecnosti je implementacne nezavisla skupina bezpecnostnych poziadaviek urcitej skupiny predmetu hodnotenia.

V pocitacovej sieti je zakazane odpocuvat siet a vytvarat kopie postovych sprav, treba si zvolit dobre hesla a nezistovat hesla inych.

Vyraz script kiddies oznacuje utocnika, ktory nema dostatok znalosti o systeme a vyuziva bezne dostupne predpripravene nastroje na zname zranitelnosti, casto sposobom pokus omyl.

Technika maximalneho rozsahu dotazu v statistickych databazach neexistuje.

Pre liveralnu kontrolu certifikatu verejneho kluca plati ze kluc povazujeme za platny pokial nie sme presveceny o opaku.

Pre zaistenie dozatelnej zodpovednosti je na zaciatku prace v systeme obvykle robena autentizacia alebo identifikacia a je robena archivacia dat umoznujuca prepojenie cinnosti s konkretnou osobou tak, ze dana osoba sa nemoze zriect zodpovednosti za svoju cinnost.

Bezpecnostna politika je subor pravidiel specifikujuci uplatnenie opatreni potrebnych k dosiahnutiu minimalnych urovni rizik.

Cielom zaistenia dovernosti dat je zabranit zisteniu semantickemu obsahu dat neautorizovanymi osobami.

Sifrovanie v PGP prebieha tak ze sa data sifruju symetricky, symetricky kluc sa zasifruje verejnym klucom prijemcu a prilozi sa k datam.

Typicke operacie firewallu su zakazat a povolit.

Pod pojmom hybridne kryptosytemy rozumieme napriklad data ktore su zasifrovane nahodnym symetrickym klucom a ten je sifrovany verejnym klucom prijemcu.

Najlacnejsimi biometrickymi technikami su otlacky prstov a dynamika pisania na klavesnici.

Zakladne vlastnosti kvalitativnych analyz rizik je ze vystup je nezrozumitelny, neni v niakej konkretnej hodnote a postup je ciastocne automatizovatelny.

Zakon o ochrane osobnych udajov sa vztahuje na osobne udaje ktore spracovavaju statne organy, organy uzemnej samospravy, ine organy verejnej moci, ako aj fyzicke a pravnicke osoby, ak neni definovane inak.

Dovody pre zavedenie kriterii bezpecnosti su ulahsenie specifikacie

poziadavok na navrh a vyvoj a potreba minimalizacie nakladov na individualne ohodnotenie.

Medzi bez. funkcie systemu pre ochranu inf. sukromia nepatri integrina, neslucitelnost a identita.

Digitalny podpis zaistuje integritu podpisanych dat.

Proxy servery su na internete dolezite, rozumeju aplikacnym protokolom, umoznuju anonymizaciu a casto sposobom ako obist lokanu bezpecnostnu politiku.

Protokoly SSL a TLS umoznuju autentizaciu komunikujucich stran, kontrolu integrity prenasanych dat.

Pod pojmom dostupnost dat rozumieme ze autorizovani uzivatelia by mali mat pristup k datam a sluzbam co najmenej komplikovane.

Pravost certifikatu vydaneho doveryhodnou certifikacnou autoritou overime tak ze overime ci je podpisany danou certifikacnou autoritou.

Pre anonymne komunikacne siete plati ze mozu byt nachylne na analyzu prevadzky a vstupy nejde jednoducho spojit s vystupmi.

Zakladne metody autentizacie uzivatelov su zalozene na nieco co som a viem.

Pojmom tranzitivita dovery oznacujeme doveru vo verejny kluc uzivatela X, ktoremu doveruje uzivatel Y a tomu doverujeme my, doveru cudzieho uzivatela X v nas verejny kluc , pokial mu doveruje uzivatel Y, ktoremu doveruje uzivatel X.

Dovernost dat znamena utajenie obsiahnutej informacie.

Odvodenie informacii vyssej citlivosti spracovanim a analyzou skupiny informacii nizsej citlivosti a odvodenim ziskavame nepriamy pristup k informaciam bez priameho pristupu k datam, ktore tieto informacie reprezentuju.

Remailer je sluzba pre anonymne posielanie a prijem mailov.

Autentizacia protokolom s nulovym rozsirenim znalosti zabrani overovatelovi aby sa mohol neskor neopravnene vydavat za preukazujucu sa stranu a zabrani overovateli, aby sa dozvedel tajomstvo ktore vlastni preukazujuca sa strana.

Dovody pre zavedenie kriterii bezpecnosti boli ulahsenie specifikacie poziadavok na navrh a vyvoj a potreba minimalizacie nakladov na individualne ohodnotenie.

Zakladne vlastnosti kvalitativnych analyz rizik, postup je ciastocne automatizovatelny, vystup je nezrozumitelny a vystup neni v nejakej konkretnej hodnote.

Pre konzervativnu kontrolu certifikatu verejneho kluca plati ze kluc povazujeme za neplatny pokial nie sme presveceni o opaku.

Technika nahodneho vyberu v statickych databazach pracuje tak ze vysledok dotazu je vyhodnoteny na zaklade nahodne vybranych zaznamov zo vsetkych existujucich zaznamov v databazi.